UNIVERSITY OF THE AEGEAN

Department Of Product And Systems Design Engineering

Methodologies and Technologies for Designing Secure Electronic Voting Information Systems

A dissertation presented

By

Dimitrios Zissis

Submitted to the Department of Product and Systems Design Engineering

for the partial fulfilment of the requirements for the degree of

Doctor of Philosophy

in the subject of

Information and Communication Systems Security

2007-2011

University of the Aegean

Department of Product and Systems Design Engineering

Methodologies and Technologies for Designing

Secure Electronic Voting Information Systems

A dissertation presented by

Dimitrios Zissis

submitted to the Department of Product and Systems Design Engineering
for the partial fulfilment of the requirements for the degree of

Doctor of Philosophy

in the subject of
Information and Communication Systems Security

Supervised by
Dr. Dimitrios Lekkas
Assistant Professor
University of the Aegean

Advisory Committee
Dr. Dimitrios Lekkas
Dr. Thomas Spyrou
Dr. Filippos Azariadis

This work is dedicated to my parents
for supporting and encouraging me
throughout these years

Foreword and Acknowledgements

This dissertation is the result of work conducted at the Department of Product and Systems Design Engineering in Hermoupolis, Syros. None of this work would have been possible without the initial intervention of Ms A. Brisnovali, who introduced me to the department and research team in Syros, while encouraging me to explore the realms of academic research and teaching. I would like to take this opportunity to thank her.

At this point of this journey I was introduced to Dr. Dimitrios Lekkas, who warmly welcomed me into his research group and found research funding for a large amount of this work. Dr. Lekkas has been my mentor throughout this journey, without whom none of this work would have been possible. His invaluable help, endless encouragement and advice made this work possible, while helping me get through the difficulties encountered along the way. Dr. Lekkas' expertise in the field, combined with his teaching ability, led me to grasping complex issues in an unalarming fashion. Our numerous casual conversations, evidently led to a number of published papers. I would also like to thank Dr. Lekkas for introducing me to academic teaching by providing me a teaching assistantship in his courses throughout these years.

Dr. Thomas Spyrou and Dr. Filippos Azariadis have provided their guidance and support from the very beginning of this journey. Dr. Spyrou warmly welcomed and helped me get started at the department and provided precious advice along the way. Professor Darzentas made this dissertation possible, by creating a multidisciplinary research environment in Syros and by providing his endless support to the Department of Product and Systems Design Engineering and its members. I would like to thank all the above for their endless support and encouragement.

Along the way I have met and worked with a number of fellows at the university grounds whom I would like to thank for making my time there easier, Argyris Arnellos, Elias Xidias, Panagiotis Koutsampasis, Konstantinos Tserpes and all the others that were there. It has been an honour for me to meet and work with all of the above. I would also like to thank my close friends, outside of university grounds, for their support throughout these years. My apologies and thanks to anyone else I have neglected to mention.

Finally, I would like to thank my parents, to whom I dedicate this work, for believing in me, encouraging me, guiding me and supporting me throughout all of these years.

Dimitris Zissis, Syros, April 2011

Abstract & Keywords

This dissertation explores methodologies and technologies for designing secure electronic voting systems. The field of electronic democracy and especially electronic voting is mostly undiscovered territory and its dimensions are still being explored, as debates on the matter continue to be conflictual. Concerns are often voiced on security issues, but also on the sociological and political implications that may arise from the introduction of this technology. Initially this dissertation attempts to exorcise complexity and reevaluate under a perspicacious vision, the conflictual issues, while providing an analysis of current state of electronic voting.

This thesis approaches the issue from an inter-disciplinary scope, while mainly focusing on a security perspective, as deploying a system in a secure manner requires meeting technical and procedural levels of assurance in respect to social and regulatory frameworks. This dissertation is intentionally meant to sit on the fence, between Information and Communication Security and the emerging field of application of computer science, electronic governance. From an e-governance perspective, this study attempts to explore secure technologies, which through their implementation enhance citizen participation, openness, and interoperability in governance. From an Information and Communication Security perspective, a structured analysis is adopted to identify vulnerabilities, involved in the digitalization of government transactions and the electoral process, while also exploring the notion of trust and transparency within this context. As ICT security is identified as the greatest barrier to the deployment of electronic voting solutions, this dissertation identifies a number of information security risks, vulnerabilities and threats, which lead to the documentation of a set of requirements, which should be met when designing a secure e-voting system. From these requirements, a design framework stems, with guidelines and recommendations of considerations that can assist in reducing these vulnerabilities. The research methodology adopted towards achieving this goal, is based on software engineering and information systems design approaches. The basic steps for designing the system architecture include the collection of requirements and the analysis of abstract functional specifications.

Keywords: electronic voting, Information and Communication security, Information Systems design, e-participation, e-democracy

TABLE OF CONTENTS

Index of Tables

Illustration Index

Chapter 1

Introduction

1 INTRODUCTION

Abstract. In this first chapter, the research problem is formulated through the definition of its boundaries or delimitations. Through the definition of the research problem the dissertation research area is outlined. Light is shed on specific research questions this repost is structured around answering. The research approach adopted by this dissertation is briefly described and justified. This chapter also includes the motivation for this research and the overall contribution to the body of knowledge in the field.

1.1 Electronic voting

At the dawn of the third millennium, countries and states globally, are exploring new frontiers by attempting to connect with their citizens through novel technologies. In relation to technological progress, exploring methods of increasing involvement in democracy and sovereign institutions has taken center stage, as electronic participation channels present a bidirectional communication gateway between the "people" and their elected representation. Recognizing the benefits offered by electronic solutions, political parties are recruiting web 2.0 information systems, including social communication networks (such as Facebook and Twitter) to mobilize their core supporter groups and attract a younger audience, hoping to alleviate the low voter turnout problems, by demonstrating a versatile and more progressive profile. In these years, numerous information policies and instruments have made electronic governments a global reality. Since their initial introduction, electronic government services have been continuously maturing and evolving in availability and sophistication.

Progressively, Information and Communication Technologies (ICT) are being introduced into various aspects of the electoral process. It is now a common fact, that back-end computers are already an integral part of almost all elections held internationally. Even in countries not officially exploring electronic voting implementations, back end computer systems are most possibly introduced at some stage of the electoral process, either for ballot counting or for voter list generation. Voter registration databases are now automated, ballots are cast into computer based equipment in an ever increasing number, and end of day results are often calculated and transmitted electronically between municipal headquarters and to the media. These back-end "uncertified" computers may hold more dangers than an efficiently

designed and protected electronic voting system. History shows that electronic voting cannot be stopped in our technically oriented society, where an increasing number of processes are mapped into the electronic world and voters become more and more mobile (Melanie Volkamer, 2009). It is becoming apparent that the basic question no longer focuses on whether ICT should be accepted in the electoral process, but rather on what kind of technology should be implemented and to what extent.

1.2 Description of the problem

As electronic voting systems are gaining momentum, exploring the related security issues is critical. Voting is the most vital citizen participation process in democracy, as it can inherently facilitate the expression of general will. Losing faith in the process of empowering our government, relates to losing faith in our government itself. The issue of security in the context of the electoral process, is referred to as one of the most important constrains in the implementation of electronic voting and e-voting is addressed as one of the most complex safety critical Information Systems (IS) to design. “Election security has to be viewed as a component of national security, since the very legitimacy of democratic government depends on elections that are fair, open, trustworthy, and seen to be so.” (Jefferson, Rubin, Simons, & Wagner, 2004). The failure of e-voting technology would have profound consequences for the reliability of and public confidence in our electoral system (Moynihan, 2004).

In recent years, official pilots and trials have been held internationally, by a plethora of countries, aiming to evaluate the benefits and drawbacks of electronic voting, but evidence does not seem to be conclusive; mostly due to the diversity of the systems implemented, which are meant to support a multifarious range of contexts and requirements. Although the benefits of introducing electronic voting systems are often stated, concerns which are most often voiced are not just based on the security risks, but also sociological and political implications, that may be raised from the introduction of this technology. Digitalizing communications between governments and the “people” is a process necessary to be viewed within a wider framework.

Unmistakably, an examination of e-democracy, and evidently e-voting, cannot be performed *in vitro*; in isolation from other scientific and academic fields, as a purely technological approach would lead to sterile “engineering” results, while a number of affecting fields operate in concert, to structure what is perceived as the field of electronic voting. Electronic voting is a social and political project much more than a technical project.

It is seen as bringing social improvement, by widening the circle of citizens involved in politics and political decision-making (Republique Et Canton De Geneve).

Electronic voting security also includes a wide spectrum of fields, procedures, issues and actors which are relative to the technological approach taken. It effectively relates to the procedures and standards that are put into place to overcome technological security shortcomings (Mohen, 2001) (Williams, 2004) (Xenakis, 2004). Crucial to the success of such systems, are the decisions made on system characteristics and elements. Beforehand selections, must guide the design process though to the implementation of the identified technologies. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability).

1.3 Motivation and why it is important?

An article published in "IT Now"(the British Computer Society's IT magazine) grabbed my attention, in this, a young board member of PGP, Gary Sharp wrote,

"*This General Election will be little different from the years gone by. Politicians from the right, left, middle and centre will stand up on a new Ikea soapbox and try and convince us that he or she will transform our lives for the next five years. In turn we will pick up a pencil, for possibly the first time since leaving school, and walk into a voting booth that wouldn't look out of place in an episode of Dad's Army and help that champion of integrity, honesty and vision head towards Westminster. But why in the 21st century Britain are we still stuck with a voting system that our parents, grandparents and great grand parents were faced with at General Elections in the 1940s, 50's and 60's? Why am I not voting via my laptop, my mobile, my TV, at the supermarket check-out or when I bought my train-ticket?***"** (IT Now, 2010).

Visiting an electoral poll, waiting in line, and scribbling down crosses and numbers, does seem apparently out dated for a society with the ability to transport "bits" of information across borders in microseconds, do commerce cross currency at any time, in any country and perform banking transactions from one's mobile phone. Additionally, the voting procedure seems alarmingly error-prone. Requiring various citizens to hand count a number of scribbled papers, does not generally inspire confidence; is that not what computers are good at? Is that not why thousand of years ago the abacus was invented? Two clicks away from casting a vote,

does seem much more appealing.

Similar publications,such as this, have been catching my attention for a while, as general interest in the field grows. Silently, while election turnout has been steadily decreasing, computers and ICT's have been appearing in different stages of the electoral process. These “black-box” computers and systems have been introduced for tasks ranging from voter registration to result transmission, but they do not seem to be sufficiently protected. Laptops containing electoral databases have been forgotten on the back seat of taxis, only to be lost forever and networks used for final result transmission have failed potently... At around the same time, after the Florida voting fiasco in the US, similar problems were making the news, with headlines such as; “Cybercriminals are stealing your votes”, “Hackers in your local vote recording machine”, “e-Voting machines store your bank account number!” and such...

From a computer and information security perspective, I was accustomed to the idea that there was no such thing as a perfectly safe computer or network. Our inter-networked lives are constantly threatened from a number of vulnerabilities and weaknesses, existent deep within these technological solutions; but cryptography, digital signatures and other security countermeasures seemed to be (almost) successfully tackling these threats online,so why wouldn’t they work in an electronic voting environment?

Traditional voting processes do not seem that secure either though. In 2011 the concept of hiding a piece of paper in an envelope to maintain its secrecy is becoming fuzzy; as anonymity can easily be broken with cheap fingerprint technology (not to speak about DNA traces). We have all heard stories like the one below,

“old-timers used to tell stories of how Martin (Lomasney, a Boston politician] would greet them at the polls on the day of elections. “*here 's your ballot” he'd say, “I've already marked it for you. When you get in there, pick up the ballot they give you and give them back this one” When you came out you'd give Martin the clean ballot, and he'd mark it off and give it to the next guy in the line.*” (Volkamer, 2009)

So why couldn’t technology successfully replace a process that can not be deemed risk free? The traditional voting method still remains widely trusted; as it allows for public oversight of the ballot after vote casting, while maintaining voters privacy. The ballot is deposited by the user into a sealed sea-through box, which is safeguarded under public view, until the final stage of the elections. The voter ballot remains in public view until the final part of the electoral process. Thus the voter hands over control of his ballot to the implicated

public and authorities. How can this trust be generated in a digital environment?

Overall, a number of reasons led me to conducting research in this field,

- Election procedures seem to be incredibly out-dated, involving processes of scribbling down numbers and checking that final sums add up. These processes are error-prone , time and cost consuming.
- It is often understated that a large proportion of the electorate body cannot easily participate in current elections. We seem to turn a blind eye on inequalities that exist in the voting apparatus at present. Individuals with disabilities are frequently unable to perform their electoral duties unaided and in most cases require help during vote casting. Entering the voting kiosk with a member of the committee, denies them the right to privacy, making this group a target to a number of threats,coercion etc. According to a survey by the Eurostat Office of the European Commission from 1992 about 12% of the European population suffer from a handicap, which adds to a total of more than 37 million persons.
- A large portion of the electorate does not participate in elections, especially younger voters. Turnout levels in elections are rapidly decreasing, reforming the vote casting process could inherently re-engage a large portion of the population.
- Progressively to en-strengthen and speed up these error prone processes, computers are being introduced at various stages of the electoral vote casting or vote tabulation. These computers and information systems are not effectively treated as safety critical. Electronic government and voting IS's, deal with an immense amount of critically sensitive information, requiring that the confidentiality, integrity and availability of this data, be preserved at all costs.
- As an increasing number of countries and states have been approaching this issue (including the United States, France, United Kingdom, Estonia, Switzerland, Canada India, Brazil, the Netherlands and others), the basic question in electoral administration seems to no longer focus on whether ICT should be accepted in the electoral process, but rather on what kind of technology should be implemented and to what extent.

1.4 The difficulty of implementing electronic voting

It is now common ground to perform commercial exchanges with individuals who have no prior knowledge of one another, over an untrusted network, the Internet. These exchanges

are performed from the ease of ones home or office, from the street, through ones mobile phone or even during a long flight. Banking transactions are performed in the same fashion, across borders and currencies. These are a few examples of safety critical information systems that are often brought up when discussing the difficulty of implementing secure electronic voting.

Electronic voting requires a level of security higher than e-commerce; “e-commerce grade security is not good enough for public elections” (Adida, 2006). The issue of security in the context of the electoral process is referred to as one of the most important constraints in the implementation of electronic voting, and electronic voting implementation has been addressed as one of the most complex IS to design. “Security is as important as reliability in guaranteeing the integrity of the voting process and public confidence in the system. Losing confidence in elections means losing confidence in our system of government” (Jefferson, Rubin, Simons, & Wagner, 2004).

Trust in an e-commerce environment is based on the belief that in the event that the system should fail, there are policies and guarantees in place, to protect the customer. Evidently a customer puts his trust in the Bank, and not in the banks IS, having the knowledge that in the worst case scenario he will be able to verify the mishappenings with an alternative method (visiting the local bank) and policies are at hand to protect him. In a commercial setting, people can detect most errors and fraud by cross-checking bills, statements, and receipts; and when a problem is detected, it is possible to recover ones losses (at least partially) through refunds, insurance, tax deductions, or legal action.

In essence, electronic voting is much more complex due to one key aspect, verifiability. Verifiability refers to having the capability to confirm or substantiate a claim by experimentation or observation. In contrast to banking or other IS's used for commerce, voting systems must not provide receipts of transactions that would allow clients (voters) to validate and identify mishappenings, because that would violate the principle of voter anonymity and enable coercion. Online banking is made feasible only because at any given time and in any given transaction, all implicated parties and exchanges are recorded. Transactions can then be checked for accuracy at a later date. E-voting does not allow this kind of auditability, because one party of the transaction must always remain anonymous (Mcgaley, 2008). Essentially, the difficulty of electronic voting is that it requires public verification of a process that must remain secret at all costs. Traditional voting processes, achieve this requirement by depositing cast ballots in a sea-through box for public oversight. In electronic elections, a contradiction

exists between critical system functional requirements, verifiability, auditability and anonymity. In this contradiction, electronic voting complexity has its deepest roots.

Additionally electronic voting systems used for binding public elections, represent high value targets. Stakes are exponentially high as a lot is in play. Attacks on an electronic voting system can be categorized according to motive; such as publicity attacks, profit attacks, terrorist attacks and attacks which are motivated by a willingness to create an instability in current state of government and much more. Due to the high risk security profile of electronic voting, it is required that every component or entity in the electoral procedure exhibits the principles of security (confidentiality, integrity, availability) and controls must be applied to defend these. Electronic voting demands the implementation of protection mechanisms that attempt to counter all identified threats and exhibit the ability to prevent unrecorded ones.

1.5 Research Area

This dissertation explores methodologies and technologies for designing secure electronic voting systems. Electronic voting IS's belong to the wider field of applications of computer science, exploring ICT to increase participation in governance and democracy, often referred to as e-government. This dissertation is intended to exist at the meeting point of field's between electronic governance and Information and Communication Security. This research attempts to approach the issue from an inter-disciplinary scope, while focusing on security issues, because deploying a system in a secure manner requires meeting technical and procedural levels of assurance in respect to social and regulatory frameworks. From an Information and Communication Security perspective, a structured analysis is adopted to identify vulnerabilities, involved in the digitalization of government transactions and the electoral process, exploring the notion of trust and transparency within this context. A number of information security risks, vulnerabilities and threats are documented, leading to the identification of a set of requirements which should be met when designing an e-voting system. These requirements lead to the development of a design framework with with guidelines and recommendations of considerations that can assist in reducing these vulnerabilities. The research methodology adopted towards achieving this goal, is based on software engineering and information systems design approaches.

This dissertation attempts to give answers to these research questions:

- How can we define electronic government and electronic participation?

- What is electronic voting and what are its boundaries?
- What should an e-voting system do?
- What problems does electronic voting face?
- What requirements is an electronic voting system required to meet?
- Is electronic voting worth the overall risk?
- Is it possible to design a secure electronic voting system?
- What countermeasures need to be deployed to design a secure electronic voting system?

Specifically this dissertation,

- Explores the notion of electronic government and electronic participation
- Investigates the notion of electronic voting
- Examines the notion of trust in electronic voting within this context
- Investigates the notion of security in electronic government
- Explores the notion of security in electronic voting
- Documents a full set of multidisciplinary requirements for e-voting
- From these requirements stem the e-voting design principles
- Proposes a design framework with recommendations of considerations that can assist in reducing these vulnerabilities

1.6 Research Approach and Methodology

This dissertation explores the notion of electronic voting and determines the technologies necessary for a secure implementation. This dissertation adds to the existing body of knowledge on e-voting, while attempting to exorcise complexity and reevaluate under a perspicacious vision the conflictual issues. The benefits and detriments actualised from the technology's introduction are investigated in a multi-disciplinary manner. The research methodology that is adopted towards achieving this goal is based on software engineering and information systems design approaches (Illustration 1). The basic steps for designing the

system architecture include the collection of requirements and the analysis of abstract functional specifications. Focusing on the crucial aspect of security, an Information Systems Security methodology is adopted, which can be decomposed into three main aspects, hardware, software and communications, with the purpose of identifying specific threats on assets and applying information security mechanisms of protection and prevention, at the three levels or layers. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability) (NIST, SP800-60). The documentation of a complete set of requirements leads to the identification of specific design principles and recommendations of considerations that can assist in reducing these threats and vulnerabilities. These requirements thus become building blocks for the development of a design framework. The approach presented in this dissertation can set guidelines on how to approach the design of security critical information systems.

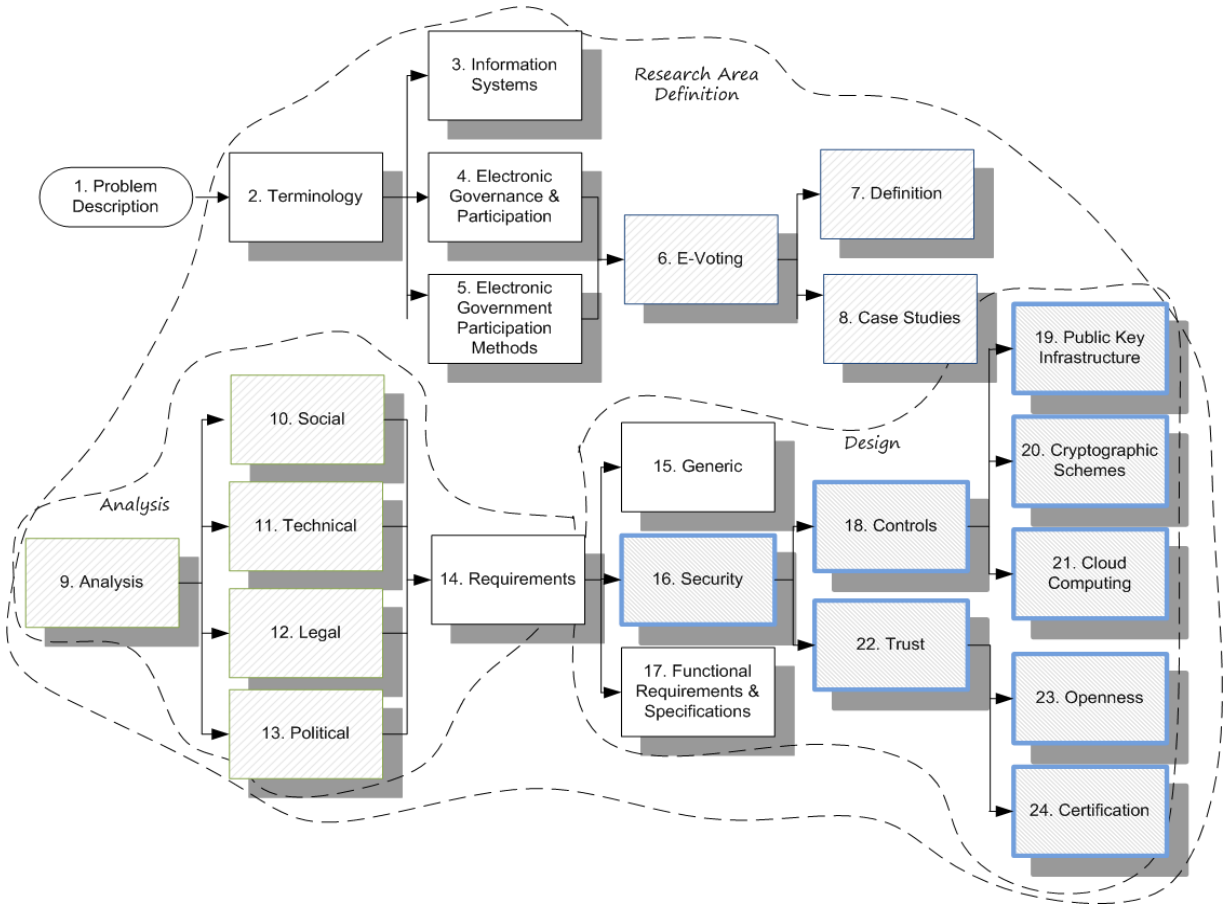

Illustration 1: Research Approach. In this thesis e-voting is investigated in a multidisciplinary manner, leading to the identification of social, legal, political and technical requirements. Following this, a software engineering and information systems design approach is adopted, with emphasis on information system security.

1.7 Thesis Outline and Summary of contribution

This section aims to provide an outline of this thesis. A short description for every chapter is provided (Illustration 2). Each chapter in this dissertation stands on the findings of the previous chapter building towards the proposed design of an electronic voting system.

In this first chapter, the research problem is formulated through the definition of its boundaries or delimitations. Through the definition of the research problem the dissertation research area is outlined. Light is shed on specific research questions, this repost is structured around answering. The research approach adopted by this dissertation is briefly described and justified. This chapter also includes the motivation for this research and the overall contribution to the body of knowledge in the field.

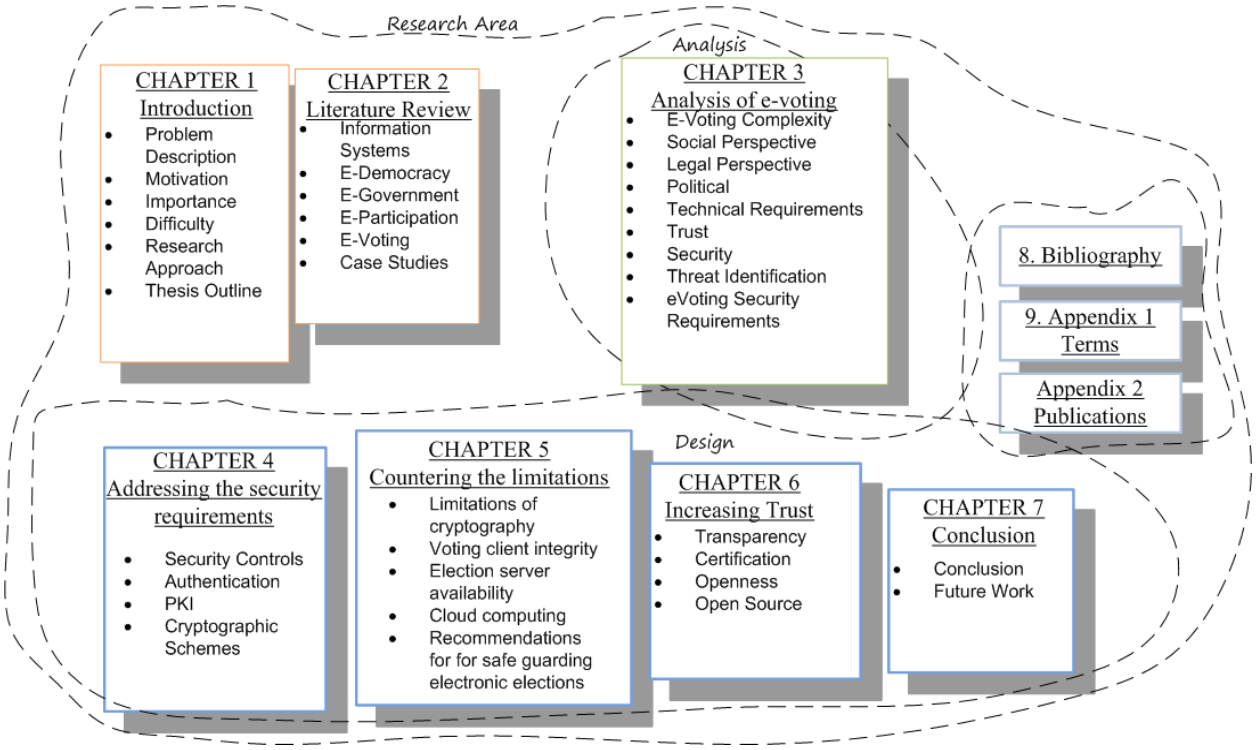

Illustration 2: Dissertation Structure

The consecutive chapter (Chapter 2) outlines the broad field of study and then leads into the focus of the research problem. In this context, the concepts of governance in relation to Information and Communication Technologies are discussed. A number of electronic methods are reviewed which enable effective participation in electronic governments. Successively electronic voting is presented and a number of case studies are evaluated.

The third chapter, explores the complexity of electronic voting and attempts to shed light on the perplexities of its implementation. As a number of affecting fields operate in concert, to structure what is perceived as the dimensions of electronic voting, a multidisciplinary

approach is employed to identify and define the true dimensions and implications involved in the adoption and development of an optimal information system. In this section, electronic voting is viewed through the perspective of four separate dimensions, sociological, legal, political and finally technical. Each of these approaches leads to the identification of a set of requirements from which stem the design guidelines and principles for an electronic voting system.

The fourth chapter explores proposals for meeting the predefined requirements, specifically from an information and communication security perspective. Essentially securing an Information System (IS), involves identifying unique threats and challenges which need to be addressed by implementing the appropriate countermeasures. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process, to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability). A number of safeguards, including Public Key Infrastructure and election cryptographic schemes are documented and evaluated as solutions to electronic voting security. At the core of most security approaches is authentication and identification. Towards securely authenticating interacting parties in electronic governance and electronic voting, the restrictions of current e-id approaches are explored, and leveraging the electronic passport PKI solution to meet the demands of an interoperable cross border e-id solution is examined. Additionally a number of cryptographic schemes that attempt to provide verifiability in elections with respect to voter privacy are explored.

The following section(Chapter 5) explores the limitations of the proposed solutions and includes recommendations of controls that can assist in reducing a number of previously identified threats and vulnerabilities. Within this scope, cloud computing is explored, as currently a multitude of applications and services are being transported to this deployment model, ranging from electronic government services, to word processing applications. We are currently witnessing events in which the clouds capabilities are being leveraged to perform malicious acts, such as using cloud instances as bots to perform DDOS or crack passwords. Diametrically opposed to this, cloud implementations are being implemented to achieve advanced security features, mostly due to the universality of the architecture, the resiliency and elasticity of services. In this section we explore cloud computing applicability to electronic government and electronic voting, evaluate the technology's benefits and

detriments, while identifying the unique security issues introduced by this innovative architecture.

Following this, chapter 6 explores methods of increasing trust in electronic voting system through increasing transparency by disclosing software source code, related documents and adopting open source design approaches. Within this context and while exploring methods of increasing transparency in electronic voting, public certification processes are studied.

In the conclusive chapter the findings of this dissertation are summarized and proposals for the implementation of electronic voting solutions are documented. This dissertation includes three appendix chapters containing a list of terminology and abbreviations used throughout the body of this text, but also a summary in Greek and English.

Chapters	Short Summary
Chapter 1 **Introduction**	• Problem Description, • Motivation, • Research Area, • Approach, • Contribution
Chapter 2 **Literature Review**	• Electronic Governance, • Electronic Participation, • Electronic Voting, • Case studies
Chapter 3 **E-voting Analysis**	• Electronic Voting Analysis, • Social Perspective, • Legal Perspective, • Political Perspective, • Technical Perspective, • Security, • Identification of Requirements
Chapter 4 **Addressing the security requirements**	• Strong Authentication • Public Key Infrastructure • Leveraging e-Passport Infrastructure • Cryptographic Schemes
Chapter 5 **Countering the limitations**	Cloud Computing, ◦ Cloud computing Architecture ◦ Cloud Computing Security ◦ A cloud Solution to e-voting • Recommendations of controls for • addressing security requirements
Chapter 6 **Increasing Trust**	• Increasing trust, • transparency, • certification, • openness, • open-source
Chapter 7 **Conclusions**	• Conclusions • Further Research
Bibliography	• Reference Section
Appendix 1	• Terminology
Appendix 2	• Supportive Publications
Appendix 3	• Summary in Greek

Table 1: Summary of Dissertation Chapters

This dissertation contributes to the body of knowledge in the identified research field in the areas described below,

- ✔ Provides an outline definition of electronic government, electronic participation and electronic voting and within this context evaluates electronic methods of effectively increasing participation in electronic democracy (J01[1]; C03)
- ✔ Provides an interdisciplinary approach to electronic voting, that sheds light on

1 Supportive Publications can be found in Appendix B

many of the complexities and perplexities exhibited during the design of electronic voting system. Within this context a holistic view of design requirements is provided, which take into consideration the many dimension of electronic voting (J02; B03).

- ✔ From an Information and Communication Security perspective, a structured analysis is adopted to identify vulnerabilities involved in the digitalization of government transactions and the electoral process, while exploring the notion of trust and transparency within this context. The documentation of a complete set of requirements leads to the identification of specific design principles and recommendations of considerations that can assist in reducing these threats and vulnerabilities. Thus fulfilling these requirements leads to the development of a design framework for secure electronic voting. (J02; J03; C01; C02; C04; C05; C06)
- ✔ explores the notion behind the hype of cloud computing and evaluates its relevance to electronic government and electronic voting information systems. This dissertation explores increasing participation and sophistication of electronic government services, through implementing a cloud computing solution. In turn, adopting a cloud computing approach for electronic government and electronic voting solutions is investigated, reviewing the architecture within the previously described context. This dissertation proposes a high level electronic governance and electronic voting solution, supported by cloud computing architecture and cryptographic technologies. An assessment of cloud computing from a security perspective is presented. (J02; J03)
- ✔ Towards securely authenticating interacting parties in electronic governance and electronic voting, the restrictions of current e-id approaches are explored, and leveraging the electronic passport PKI solution to meet the demands of an interoperable cross border e-id solution is proposed. (C06; J04)
- ✔ The essence of trust is explored in the context of electronic government and electronic voting. Increasing trust in electronic voting system is proposed through increasing transparency by disclosing software source code, related documents and adopting open source design approaches (C04).

Chapter 2

Literature Review

2 LITERATURE REVIEW

Chapter Abstract: This chapter outlines the broad field of study and then leads into the focus of the research problem. This section discusses the concepts of governance in relation to Information and Communication Technologies. A number of electronic methods are reviewed which enable effective participation in electronic governments. Successively electronic voting is presented and a number of case studies are evaluated.

2.1 Information Systems

The transformation of information into knowledge, has been the goal of various civilisations since the beginning of time, as knowledge has been perceived to equate to power (*scientia potentia est*); but unfortunately the possession of vast amounts of information does not equally equate to sweeping knowledge acquisition. Information, needs to be organized, processed and available in the right format to become useful. For this, throughout time, people have invented methods and tools to organise and manage information on their behalf.

An **Information System** is a collection of people, procedures, and equipment designed, constructed, operated, and maintained to collect, record, process, store, retrieve, and display information (Ralston, Reilly, & Hemmendinger, 2003). Nowadays, Information Systems make use of Information Technology (these are sometimes referred to as *computer-based information systems* (CBIS) to distinguish them from earlier i.e. manual systems). **Information technology** (IT) is defined as "a microelectronics-based combination of computing and telecommunications used for the acquisition, processing, storage and dissemination of vocal, pictorial, textual and numerical information" (Strehlow, Wright, & Materials, 1993).

Communication and computer technologies have drastically altered traditional ways of interaction and communication with information; but also between the entities themselves. In the 1960s, a mere few could have predicted the impact that an undersized academic network of four mainframe computers, residing at different universities and research centers, initially used to exchange research documents, would have on the future of communications. This was the predecessor to today's Internet, a global system of interconnected computer networks, which currently has approximately 1.571 billion users worldwide (approximately 2 out of 7 of

the global population is an Internet user).

At present the Internet is reshaping most traditional ways of communication, but also ways of doing business and commerce. Instant messaging, social networking, on-line shopping and banking are methods of communication of the twenty-first century. Information And Communication Technology (ICT) is no longer perceived as a supplementary tool but as a crucial asset. Technology is no longer the inhibitor. The global economy is now being shaped through the demand of technological innovations and information system needs, which in turn pressurizes the knowledge curve to meet with the continuous shift in necessities. High speed Internet connections (a/k/a broadband connections) are now being perceived as a basic commodity in the global village's market, and are treated as key economic indicators.

At the dawn of the third millennium, countries and states globally, are exploring new frontiers by attempting to connect with their citizens more efficiently and effectively through ICT. Using ICT, governments are targeting overcoming economic, social, and environmental challenges, while creating a more open, flexible, and collaborative government. Recognizing the benefits offered by electronic solutions, political parties are recruiting web 2.0 information systems, including Facebook, Twitter and YouTube, to mobilize their core supporter groups and attract a younger audience, hoping to alleviate the low voter turnout problems and demonstrate a versatile progressive profile.

2.2 Electronic democracies and governments

Digitalizing communications between governments and the "people" is a process necessary to be viewed within the wider framework of electronic democracy. Since the publication of "the nerves of government" (Deutsch, 1963), Information and Communication Technologies (ICT) have been considered vital for political systems. ICT's were recognized to have tremendous administrative "potential" (Yildiz, 2007), ICTs could help create a networked structure for interconnectivity (McClure & Bertot, 2000), service delivery (Bekkers & Zouridis, 1999), efficiency and effectiveness (Heeks, 2001a), interactivity (DiCaterino & Pardo, 1996), decentralization, transparency (La Porte, DeJong, & Demchak, 1999), and accountability (Ghere & Young, 1998; Heeks, 2001b)

E-government is defined as "utilizing the Internet and the World-Wide-Web for delivering government information and services to citizens" (UN & ASPA, 2001). It may also include using other ICT's in addition to the Internet and the Web, such as "database, networking, discussion support, multimedia, automation, tracking and tracing, and personal identification

technologies" (Jaeger P.T., 2003). ICT is believed to be reshaping democratic processes. Electronic Democracy is identified as the electronic representation of democratic processes (Von Lucke, 2004), which in turn are divided into the sub processes (Parycek, 2003):

- Information acquisition,
- Formation of an opinion and expressing the decision itself.

In these years, numerous information policies and instruments have made electronic governments a global reality. Recently Wolfgang Schäuble, German Ministor of Interior, stated that "every policy initiative becomes sooner or later an ICT project" {Document not in library: (Schäuble, 2007)}. Since their initial introduction, electronic government services have been continuously maturing, evolving in availability and sophistication. E-governments have been progressing from an "initial online presence, through a limited number of individual governmental pages," towards a "totally integrated presence, which has the ability to cross departments and layers of government".

In Europe availability of government services online has risen to 82% in 2010, a strong increase from 69% in 2009, while in terms of sophistication, Europe stands at 90%, an increase of 7% since 2009 (this assesses the degree of interaction between service provider and user, from simple information provision to personalised proactive case handling). There is a continuous annual progress in availability but also of the sophistication of the services provided (Capgemini, 2009 ; Capgemini, 2010).

The EU Ministerial Declaration of 2009 (Ministerial Declaration on eGovernment, 2009), in accordance with relevant initiatives globally (US Federal Cloud Computing Initiative, July 30, 2009) (E-Government Act of 2002, December 17, 2002,) (Memorandum for chief information officers, 2007), determines the next generation electronic government goals and objectives. This strategic plan is a multi-step process aiming at overcoming economic, social and environmental challenges; leading to a more open, flexible and collaborative electronic government (Illustration 3).

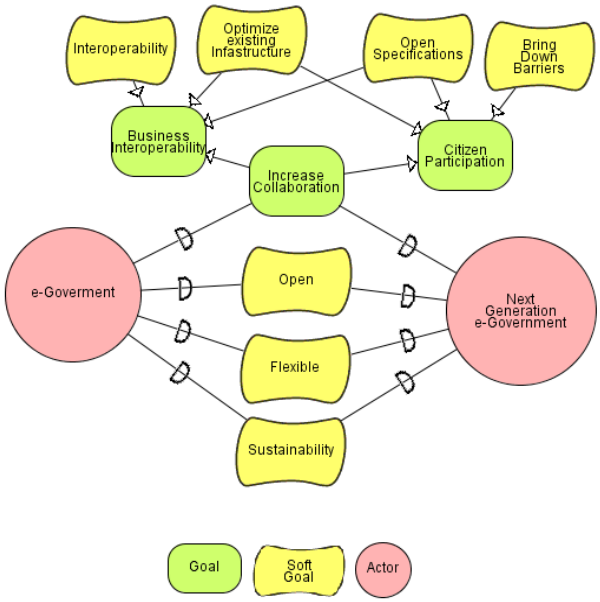

Illustration 3 represents the goals and objectives (soft goals) identified in the EU'09 initiative.

Improving collaboration between citizens and government agencies is critical to the success of these initiatives, as it will lead to increasing the efficiency and effectiveness of its services. Fulfilling these goals will provide economies of scale and knowledge for governments and society. Developing more inclusive services that will help bring down barriers experienced by digitally or socially excluded groups is identified as a necessity. These initiatives aim to provide better public services, delivered with fewer resources, by optimizing the use of available resources and instruments, while improving organizational processes and promoting a sustainable low-carbon economy.

The eGovernment Action Plan aims to increase the take-up of online public services to 50% of EU citizens by 2015 and to make available online a number of cross border services (MEMO/10/681, 2010). The eGovernment Action Plan foresees actions to strengthen personal mobility in the Single Market thanks to digital services. One objective is to provide citizens with electronic access to their personal data, in strict compliance with data protection requirements, and to enable them to follow on-line, each step of the administrative procedure as well as to complete an administrative task online ***anywhere*** in the EU. In a true digital Single Market, people should be able to apply on-line to study, reside or retire anywhere in the EU. The Action Plan will encourage the exchange of best practices between Member States (MEMO/10/681, 2010).

It is becoming apparent that present and future implementations of electronic government services should not be treated in an asynchronous and asymmetrical manner by respective

states and countries, but make use of a common interoperable platform leveraging existing infrastructures, while achieving economies of scale and knowledge.

Towards this goal, the Lisbon Treaty, which entered into force on 1 December 2009, introduces a whole new dimension of participatory democracy, alongside that of representative democracy on which the European Union is founded (SEC(2010) 370, 2010). "*It reinforces the citizenship of the Union and recognizes every citizen's right to participate in the democratic life of the Union. The Lisbon Treaty, introduces a new form of public participation in European Union policy shaping, the European citizens' initiative, which enables one million citizens who are nationals of a significant number of Member States to call directly on the European Commission to bring forward an initiative of interest to them in an area of EU competence."(SEC(2010) 370, 2010).*

This new provision is a significant development in the democratic life of the European Union, as it introduces a number of critically important issues. Most importantly it initiates the exploration of electronic participation channels with the capacity to hold the expression of citizen's opinion in a pan European context. It provides an opportunity to bring the Union closer to its citizens and to foster greater cross-border debate about EU policy issues, by bringing citizens from a range of countries together in supporting one specific issue.

The guiding principles for the implementation of the citizen initiative, in the Lisbon Treaty are as follows; (SEC(2010) 370, 2010),

- The conditions should ensure that citizen initiatives are representative of a Union interest, whilst ensuring that the instruments remain easy to use.
- The procedures should be simple and user-friendly, whilst preventing fraud or abuse of the system and they should not impose unnecessary administrative burdens on Member States.

Given the importance of these new provisions of the Treaty for citizens, civil society and stakeholders across the EU, and considering the complexity of some of the issues to be addressed, the Commission launched a broad public consultation with the adoption of a "GreenPaper" on 11 November 2009. Respondents broadly supported the idea of having a common set of procedural requirements for the collection and verification of statements of support, so as to ensure a *uniform* process across the EU, and to avoid organizers having to comply with different rules in each Member State (SEC(2010) 370, 2010). The possibility of online "signing" was called for almost unanimously, being in line with the development of an

e-society, since it would greatly facilitate the collection of signatures (COM(2010) 119, 2010). However, in order to ensure that statements of support collected online are as genuine as those collected in paper format, and that the Member States can *check them in similar fashion*, the proposal requires that online collection systems should have adequate security features in place, and that the Member States should certify the conformity of such systems with those security requirements, without prejudice to the responsibility of the organizers for the protection of personal data (COM(2010) 119, 2010).

These initiatives and policies can be translated into an innovative Information System (IS) design framework, with a completely new set of goals for electronic governments. It is thus vital, that all present and future plans and implementations for electronic democracy build upon the principles identified in numerous policies and initiatives, as these can be understood as design guidelines for the next generation of e-government information systems. These include:

- Targeting enhancing participation in electronic democracy (Lisbon Treaty 2010).
- Providing better services delivered over fewer resources, by optimizing the use of available resources and instruments (Ministerial Declaration of e-Government, 2009).
- Targeting overcoming existing economic, social and environmental challenges (Ministerial Declaration of e-Government, 2009).
- Promoting cross border interoperability of services (e-Government Action Plan, 2010).
- Promoting cross border collaboration and scalability (e-Government Action Plan, 2010).
- Encouraging the exchange of best practices between Member States(e-Government Action Plan, 2010).
- Are designed as part of a horizontal security service, so as to ensure uniform conditions of access to e-government services across member states (Com(2010) 119, 2010).

2.3 Electronic participation

E-Participation can principally be understood as technology-mediated interaction between the civil society sphere and the formal political sphere, and between the civil society sphere

and the administration sphere (Clive Sanford, 2007). The task of e-Participation is to empower people with ICTs to be able to act in bottom-up decision processes, to make informed decisions, and to develop social and political responsibility. Therefore, e-Participation is a means to empower the political, socio-technological, and cultural capabilities of individuals, giving the possibility that individuals can involve themselves and organize themselves in the information society. (Christian Fuchs, 2006).

Areas of participation have been categorized according to the context of participation (C. Fraser):

Information Provision: ICT to structure, represent and manage information in participation contexts.

Community building-Collaborative Environments: ICT to support individuals come together to form communities, to progress shared agendas and to shape and empower such communities.

Consultation: ICT in official initiatives by public or private agencies to allow stakeholders to contribute their opinion, either privately or publicly, on specific issues.

Campaigning: ICT in protest, lobbying, petitioning, and other forms of collective action (except of election campaigns, see electioneering as participation area).

Electioneering: ICT to support politicians, political parties and lobbyists in the context of election campaigns.

Deliberation: ICT to support virtual, small and large-group discussions, allowing reflection and consideration of issues.

Discourse: ICT to support analysis and representation of discourse.

Mediation: ICT to resolve disputes or conflicts in an online context.

Spatial planning: ICT in urban planning and environmental assessment.

Polling: ICT to measure public opinion and sentiment.

Voting: ICT in the context of public voting in elections, referenda or local plebiscites.

A number of electronic tools are targeted at increasing participation; these are also

referred to as e-methods (Macintosh, 2004) (Zissis, Lekkas, & Papadopoulou, 2009). These web based tools cover various areas of participation. Each one of the e-methods presented below is accompanied by a SWOT analysis. SWOT analysis (Strengths, Weaknesses, Opportunities and Threats analysis) is a descriptive method for identifying and listing positive or negative factors about an issue, in a more representational and concentrated way. Eventually all the data from the SWOT matrices are combined in one criteria form in order to make a comparison between e-participations' tools.

The first step for the SWOT analysis was to establish a series of criteria. These criteria were carefully selected as to maintain a balance in sought after technical requirements and social requirements. Fraser et al. (2006) have identified a number of preconditions for the successful deployment of e-Participation tools. One of the identified preconditions is related to security and privacy in e-Participation contexts. E-Participation services need to be easy to use, simple and without time-consuming procedures to ensure the participation of users. However, there is also a need to implement security and privacy measures in e-Participation services to ensure that the users will trust a system. If users' expectations of security and privacy are not met, or if the measures are excessive, then participation will be ineffective, either due to a lack of trust in the system, or due to system usability problems. It is, therefore, important that a proper balance between security, usability and transparency of e-Participation services be achieved.

A number of technical and social requirements can be identified:

- Deployment Complexity: How difficult is the deployment of an e-participation tool?
- Information Richness: What amount of information is the specific e-method able to contain?
- Security: Can the user's navigation be secured?
- Interactivity: To what degree are the communication channels unidirectional or bidirectional?
- Scalability: How effectively can the application scale to meet a broader public or extend its current capabilities?
- Accessibility: Is it possible for this method to meet the accessibility guidelines stated by the W3C Recommendation 5-May-1999?
- Privacy: Can the user's privacy be preserved?

- User Hardware Requirements: What kind of hardware is the user required to posses to execute the application (ex. High speed Broadband connection)?
- User Technical Knowledge Required: Is the user required to be familiar with certain technologies in order to use the e-method?

2.3.1 Webcasts

A webcast is the Internet audio and/or video stream produced from a live event, or an online simulcast of a broadcast signal (Elaine G. Toms, 2005). A web-casting system can be classified as a form of multimedia system, and a webcast, thus, is a multi-media object with multiple components. In addition to video, the webcast usually includes the slides from a presentation, and may include other artefacts. Webcasts are usually transmitted and seen by the participants at the same time (real-time) and their duration may be over one hour, although they can be archived to allow people to view them at a later time, creating an issue of data storage. This system offers its participants a way to see and hear a transmission but in general it's not very interactive.

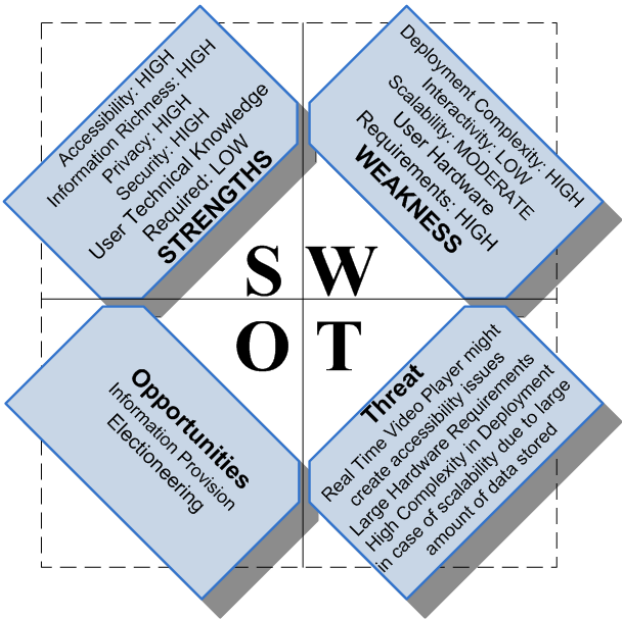

Illustration 4: SWOT analysis for webcasts

2.3.2 Frequently Asked Questions

This method presents information through questions (Q) and answers (A) that can be

searched using keywords or by inputting a question or statement in 'natural language'. However the information cannot be considered to be sufficient to cover and communicate a whole topic as the system question-answer provides participants a very fragmental opinion.

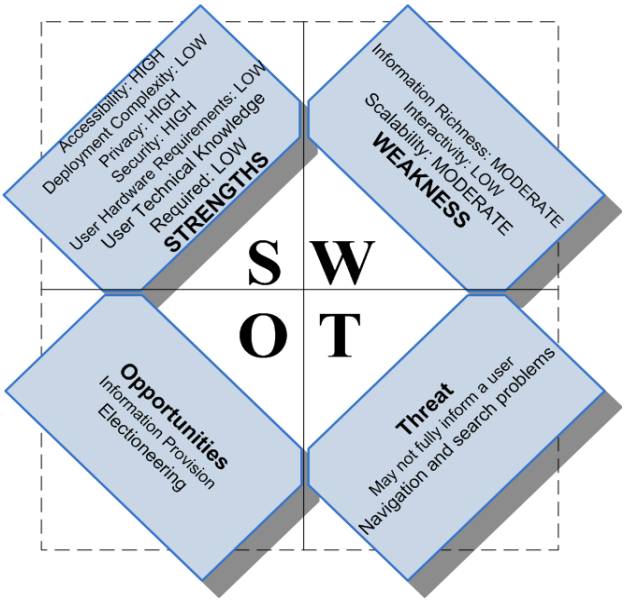

Illustration 5: SWOT analysis for Frequently Asked Questions

2.3.3 Blogs

A web-blog is a web page with minimal to no external editing, providing on-line commentary, periodically updated and presented in reverse chronological order, with hyper-links to other online sources (Drezner, 2004). Software required to run a blog is available free of charge on the internet, is relatively easy to use and requires no specialist knowledge of web languages to operate

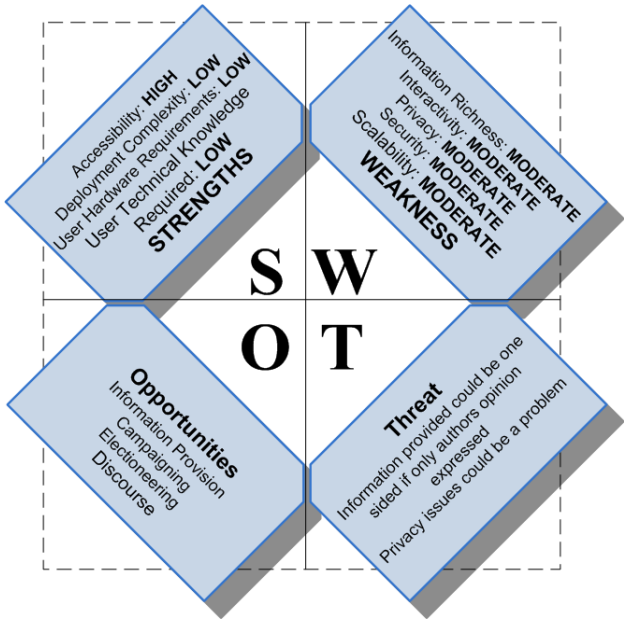

Illustration 6: SWOT analysis for blogs

2.3.4 Quick polls

An opinion poll is a survey of opinion from a particular sample. Opinion polls are usually designed to represent the opinions of a population by asking a small number of people a series of questions and then extrapolating the answers to the larger group, within confidence intervals. The answers given are anonymous, no personal or demographical data required.

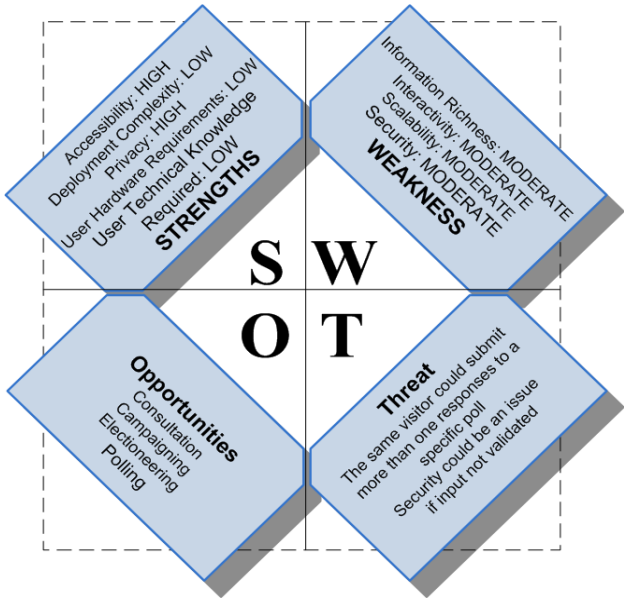

Illustration 7: SWOT analysis for quick polls

2.3.5 Surveys

A survey is a process for gathering information, without detailed verification, on the activity being examined. It is in fact a questionnaire with specific structure of close-ended questions (typically with ordered response categories) and some open-ended questions.

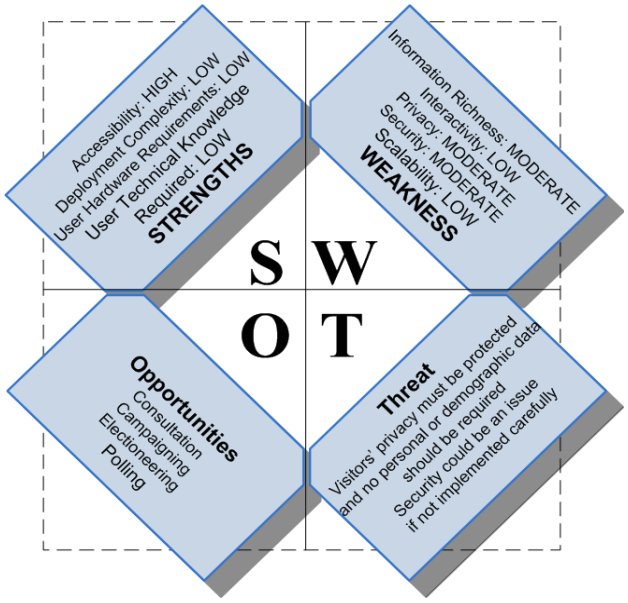

Illustration 8: SWOT analysis for surveys

2.3.6 Chat Rooms

A chat room or chat-room is a term used primarily by mass media to describe any form of synchronous conferencing, occasionally even asynchronous conferencing. The term can thus mean any technology ranging from real-time online chat over instant messaging and online forums, to fully immersive graphical. Chat rooms sometimes have a 'moderator' to facilitate interaction with the panel and to control the discussion.

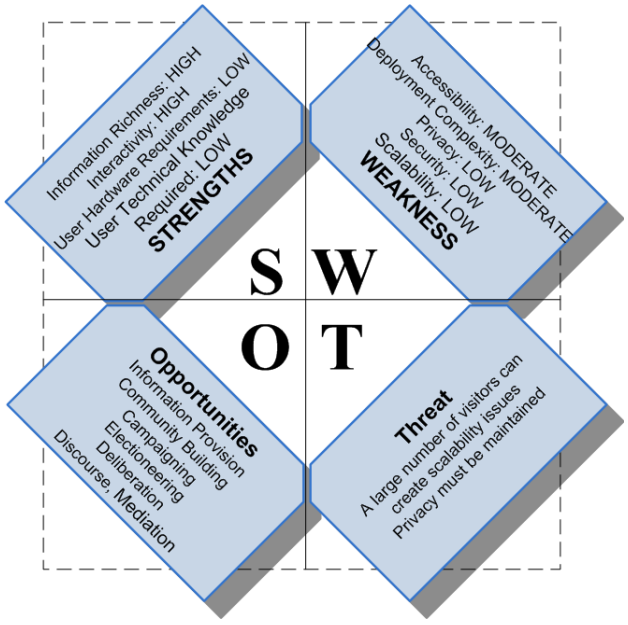

Illustration 9: SWOT analysis for chatrooms

2.3.7 Decision-making games

Decision-making games allow users to view and interact with animations that describe, illustrate or simulate relevant aspects of an issue. There is usually some competitive aspect

such as a quiz. The content, level of difficulty and types of interfaces are dependent on the target audience. Information can be provided through a question and answer type game similar to a FAQ. The user can be presented with a graphical representation of a place or situation and various options that, when selected, change the representation in some way to simulate the effect of real-life decision-making.

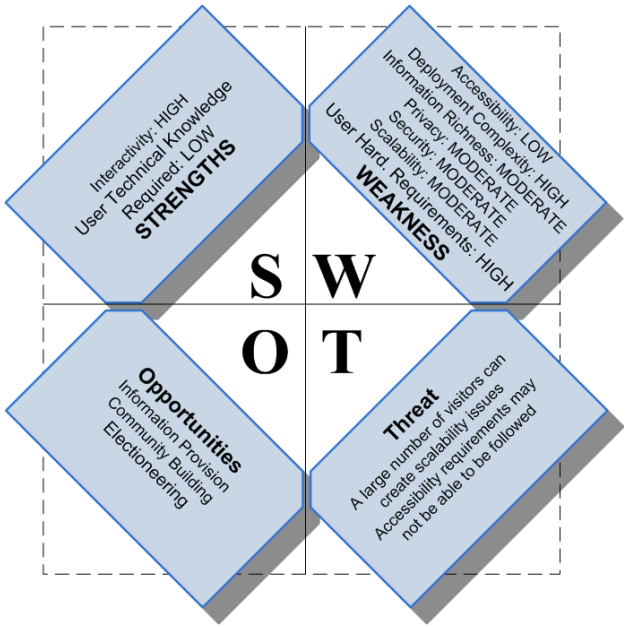

Illustration 10: SWOT analysis for Decision-making games

2.3.8 Discussion forums

An Internet forum is a web application for holding discussions and posting. Internet forums are also commonly referred to as Web forums, message boards, discussion boards, (electronic) discussion groups, discussion forums, bulletin boards, fora (the Latin plural) or simply forums. It typically shows a list of topics people are concerned about. Users can pick a topic and see a 'thread' of messages and replies, then post their own message. Communication channels can either be asynchronous or synchronous.

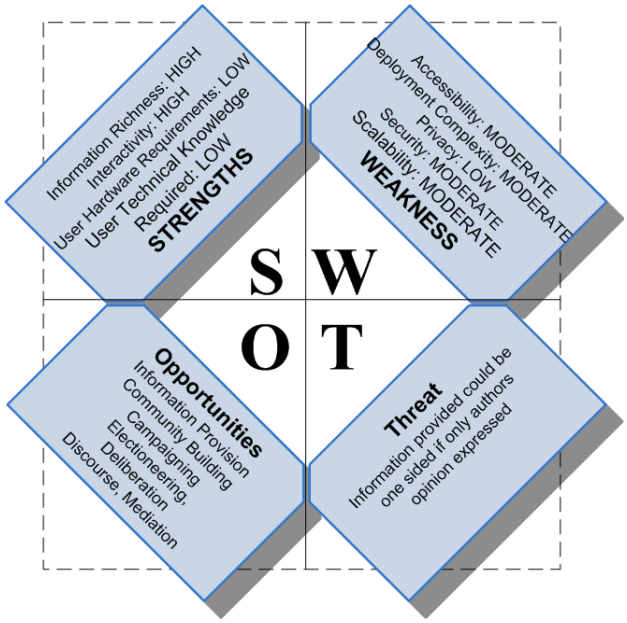

Illustration 11: SWOT analysis for Discussion forums

2.3.9 E-Panels

E-Panels represent a recruited set, as opposed to a self-selected set, of participants who have agreed to discuss a variety of issues, using ICTs at specific intervals, over a period of time. Sometimes we may have no interaction, if online questionnaires are used, but it is also possible to support intensive engagement, by providing participants a number of e-tools in order to contribute online.

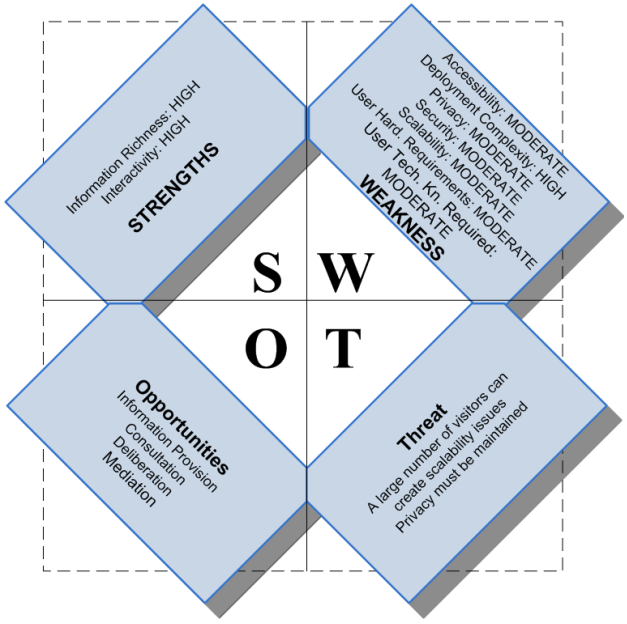

Illustration 12: SWOT analysis for e-panels

2.3.10 E-petitions

An Internet petition is a form of petition posted on a website. Website visitors are questioned if they want to add their email addresses or names in the petition form, and after

enough "signatures" have been collected, the resulting letter may be delivered to the author of the petition, usually via e-mail. An integrated discussion forum can also be incorporated to allow users to voice their support or concerns for the e-petition.

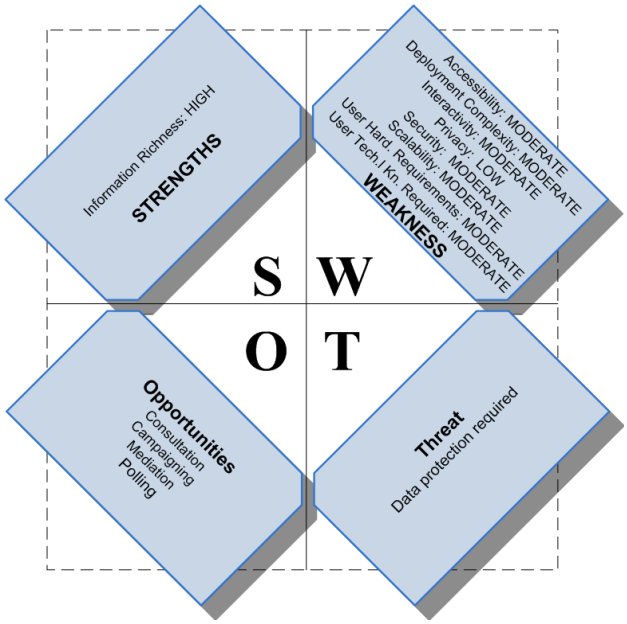

Illustration 13: SWOT analysis for e-petitions

2.3.11 E-deliberative polling

Deliberative polling, combines small-group discussions, involving large numbers of participants with random sampling of public opinion. Its overall purpose is to establish a base of informed public opinions on a specific issue. Citizens are invited to take part at random, so that a large enough participant group will provide a relatively accurate, scientific representation of public opinion.

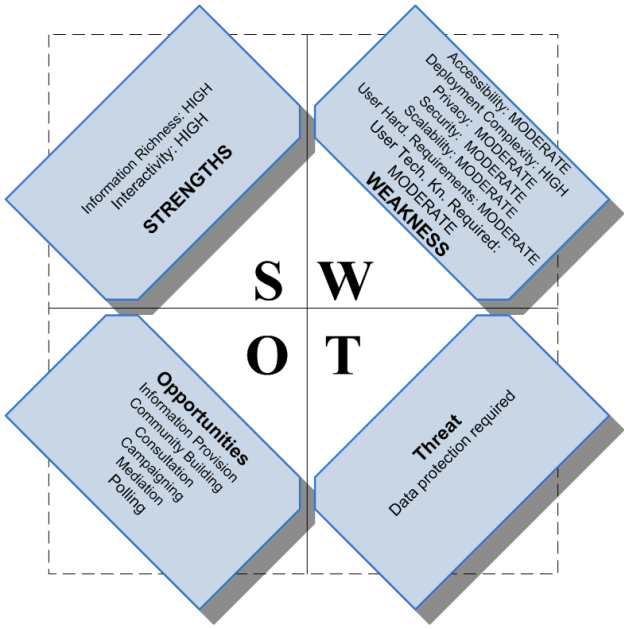

Illustration 14: SWOT analysis for E-deliberative polling

2.3.12 virtual communities

A virtual community, e-community or online community is a group of people that primarily interact via communication media such as, email or Usenet, rather than face to face. If the mechanism is a computer network, it is called an online community.

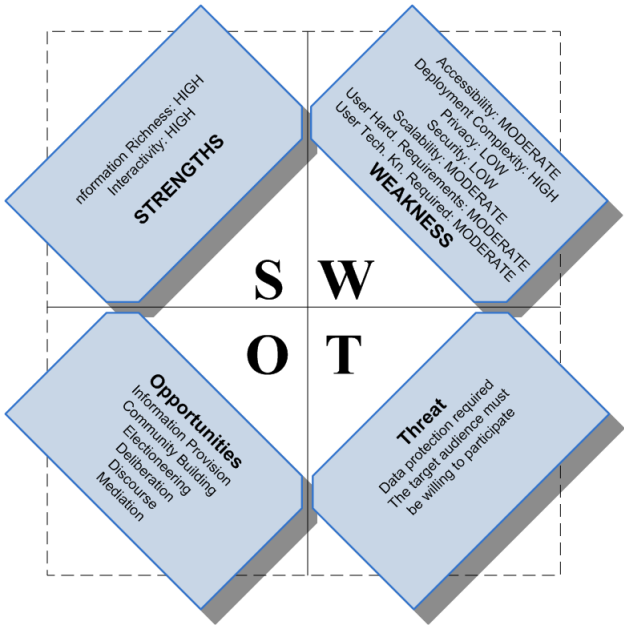

Illustration 15: SWOT analysis for virtual communities

2.3.13 Alert mechanisms – Email alerts and RSS feeds

RSS or Real Simple Syndication is technology designed to allow users to subscribe to a specific content feed and be automatically alerted when new updates are available.

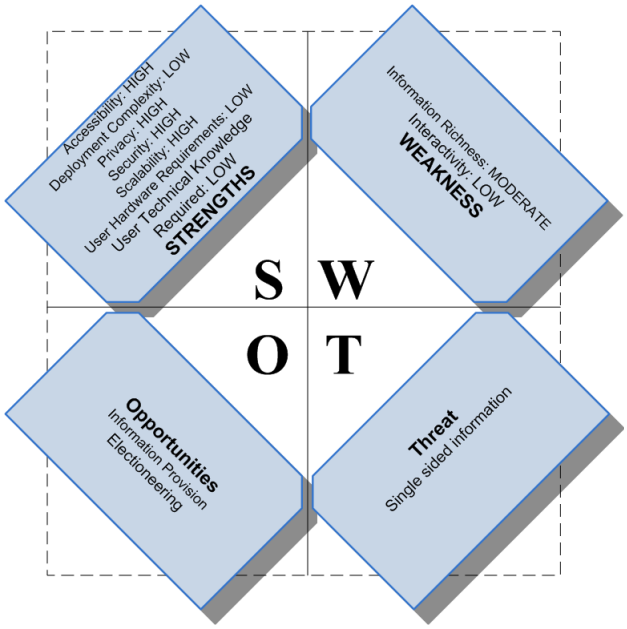

Illustration 16: SWOT analysis for email and RSS alerts

2.3.14 E-methods comparison

The following table is a criteria rating form for the above analysed e-methods. For each criterion established, a weight is given to declare its importance. Then each e-method is rated corresponding to its coverage of the perquisites. The rates that each method gets are multiplied with the weight, in order to get a total score (note that the ratings are according to the swot analysis of each method). *It is essential to note at this point that it doesn't matter which method gets the maximum score. Instead the important thing is the fluctuation that each method's ratings presents, which implies that one method may be more proper for one application than another.*

"**Total Score**" corresponds to the sum of an e-method's rates

[Total Score = Sum of an e-methods Rates]

"**Summary**" corresponds to the weighted sum of the rates multiplied by the corresponding criteria weights.

[Summary = Sum (Rating * Weight for each criteria)]

Decision Matrix		e-Methods												
		1: WebCasts	2: FAQ	3: Blogs	4: Quick Polls	5: Surveys	6: ChatRooms	7: Decision-Making Games	8: Discussion Forums	9: e-Panels	10: e-Petitions	11: e-Deliberative Polling	12: Virtual Communities	13: Alert Mechanisms
Criteria	**Weight**	**Rate**												
Accessibility	3	3	3	3	3	3	2	1	2	2	2	2	2	3
Deployment Complexity	-1	3	1	1	1	1	2	3	2	3	2	3	3	1
Hardware Required from User	-2	3	1	1	1	1	1	3	1	2	2	2	2	1
Information Richness	3	3	2	2	2	2	3	2	3	3	3	3	3	2
Interactivity	2	1	1	2	2	1	3	3	3	3	2	3	3	1
Privacy	3	3	3	2	3	2	1	2	1	2	1	2	1	3
Security	3	3	3	2	2	2	1	2	2	2	2	2	1	3
Scalability	1	2	2	2	2	1	1	2	2	2	2	2	2	3
User Technical Knowledge Required	-2	1	1	1	1	1	1	1	1	2	2	2	2	1
Total Score	**10**	**22**	**17**	**16**	**17**	**14**	**15**	**19**	**17**	**21**	**18**	**21**	**19**	**18**
Summary		**29**	**32**	**28**	**31**	**25**	**22**	**18**	**26**	**24**	**20**	**24**	**18**	**33**

Table 2: Short description of the benefits and drawbacks of each e-method

Rating	Description
0	No Fit
1	Low Fit
2	Moderate Fit
3	High Fit

Table 3: Rates

Weights	Description
1	Low Importance
2	Moderate Importance
3	High Importance

Table 4: Weights for positive factors

Weights	Description
-1	Low Importance
-2	Moderate Importance
-3	High Importance

Table 5: Weights for negative factors

Weights	Criteria	Justification
3 or -3	Accessibility Information Richness Privacy Security	If users' expectations of security and privacy are not met, or if the measures are excessive, then participation will be ineffective, either due to a lack of trust in the system, or due to system usability problems. Security, usability and transparency are equally of high importance in e-Participation services. Accessibility is of high importance as inequalities in accessibility will exclude a number of users from participating. Information Richness (acquisition) is a crucial element of e-Participation, leading to e-Democracy.
2 or -2	Interactivity Hardware Required from User User Technical Knowledge Required	As technology's primary goal is becoming user friendlier such a gap in hardware requirements and technical knowledge requirements, is evidently going to disappear. An efficiently designed e-democracy system will provide the means for bi-directional exchange of information and re engagement of active citizens in the political process (interactivity). So these factors do not affect participation or users in the same way that the above mentioned do.
1 or -1	Scalability Deployment Complexity	As e-methods are targeted at increasing participation in democratic processes, Scalability and Deployment Complexity, do not directly influence end users.

Table 6: Explanation of criteria weighting

Towards an electronic society and an electronic democracy it is important to assess the suitability of each available method. Competent e-participation channels in e-democracy depend on the technologies used. This is the purpose of the comparison of e-methods presented in this section, to point out the characteristics of each method in order to make appropriate use of them. Although a final score has been awarded to each method it cannot be a conclusive result, leading to the use or not of a specific e-method, only a guide to each methods advantages and disadvantages. There is no e-method that can be suitable for all applications, and vice versa, no application can make use of all e-methods. An e-method must be chosen regarding each situation's demands and considering the above mentioned advantages and disadvantages that the particular e-method has.

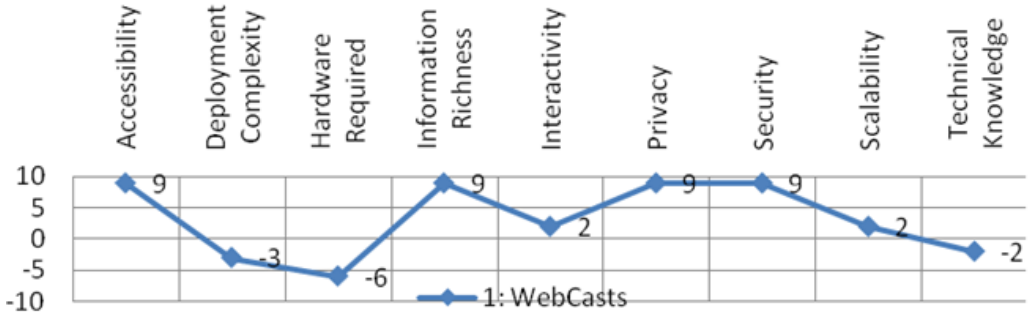

Illustration 17: Webcasts: Ensure information richness but introduce serious drawbacks on user hardware requirements and deployment complexity.

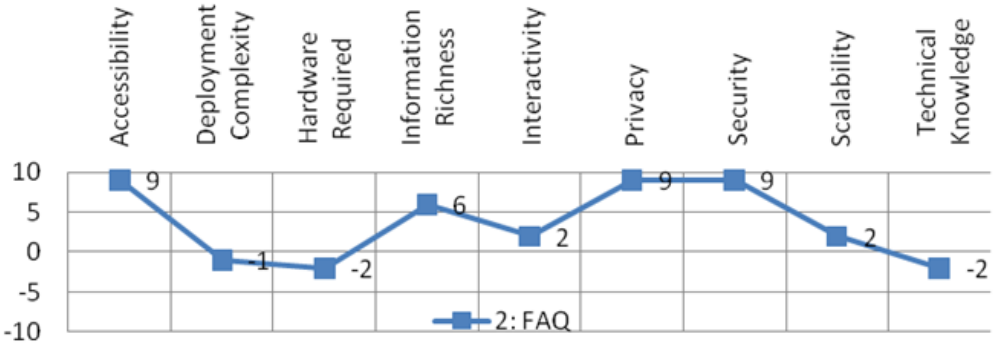

Illustration 18: FAQ: Provide information in a simple and straightforward way while maintaining security and privacy. Information can be single sided as usually only answers provided to set questions

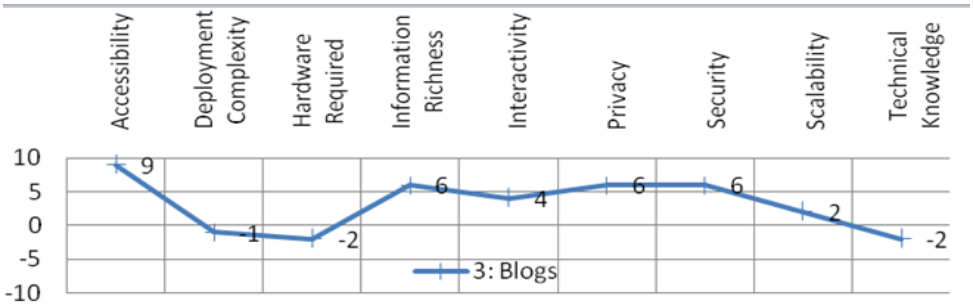

Illustration 19: Blogs: Can provide a means to hold vast amount of information but essentially single sided.

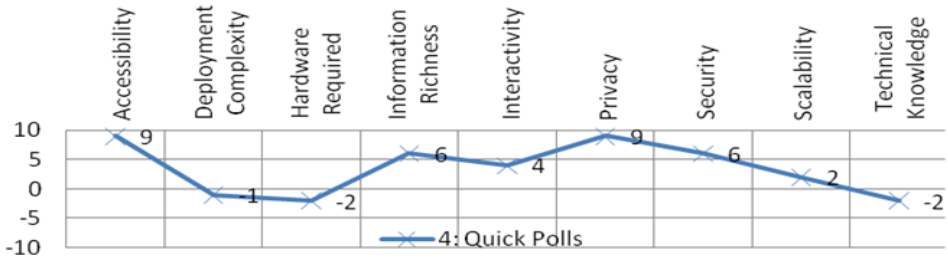

Illustration 20: Offers a simple method for opinion expression while able to maintain users privacy and security.

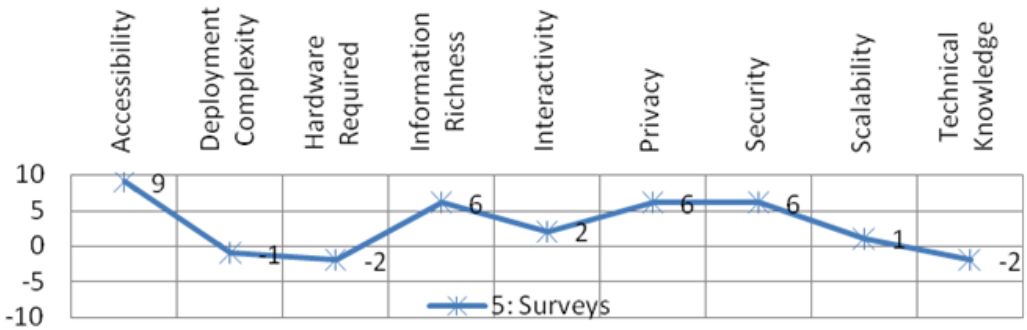

Illustration 21: A moderate tool for opinion expression that could possibly introduce security implications. Information usually unidirectional, as candidates answer pre-set questions.

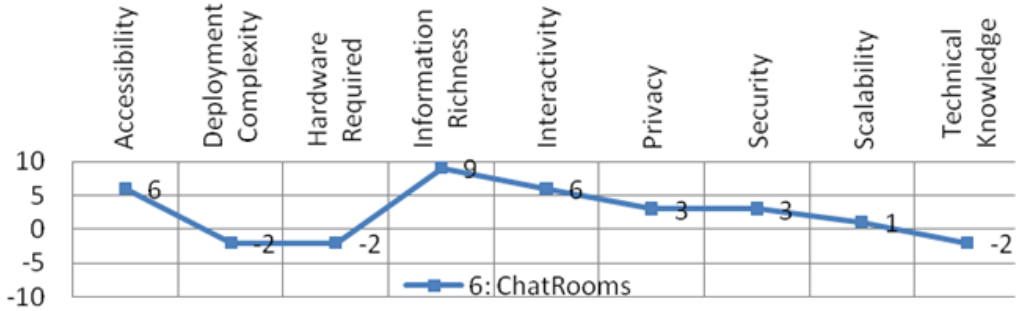

Illustration 22: A truly bidirectional information exchange method but with serious privacy and security weaknesses.

Illustration 23: A highly engaging interactive solution but with serious disadvantages on accessibility, deployment complexity and user hardware requirements

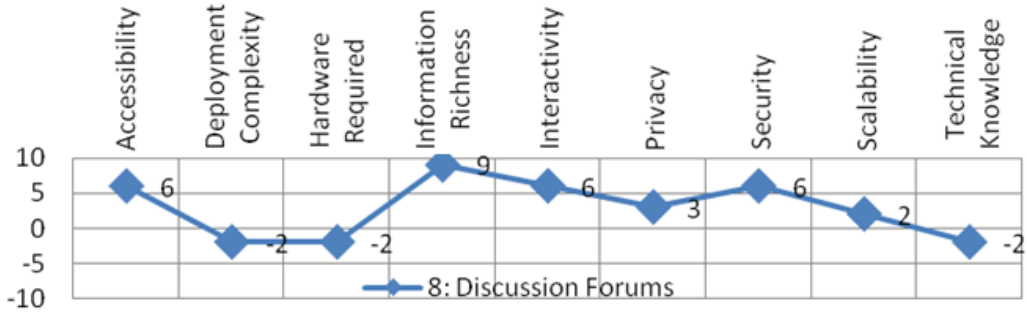

Illustration 24: *An interactive platform capable of meeting biderectional information exchange needs but with privacy weaknesses.*

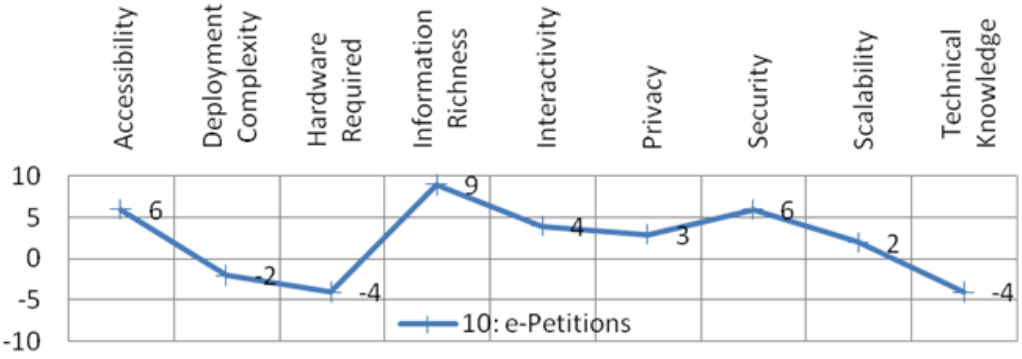

Illustration 26: An opinion expression platform with serious privacy issues.

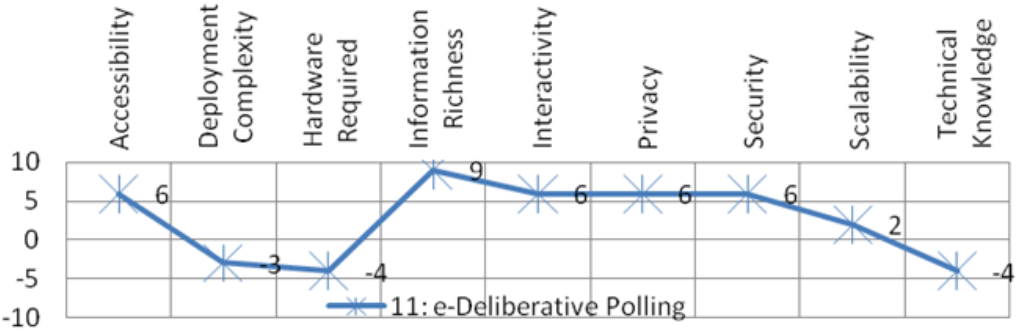

Illustration 27: A complex electronic method to deploy that can provide rich information.

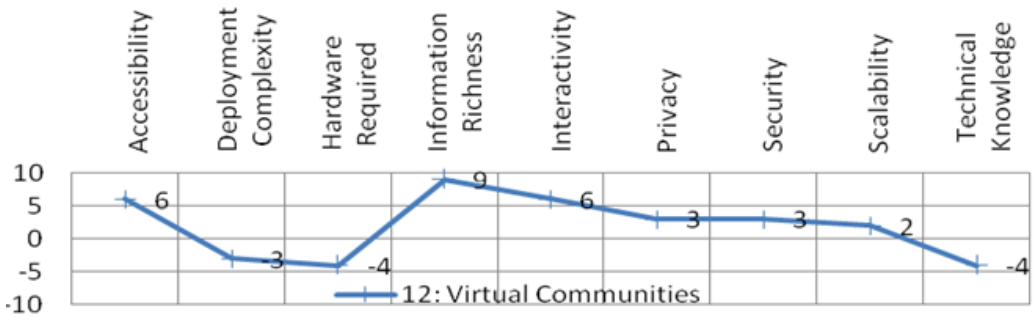

Illustration 28: Highly complex to deploy interactive information exchange and opinion expression platform at the cost of security and privacy.

Illustration 29: A secure and straightforward method of bidirectional information exchange.

Accurate identification of user requirements and needs is the only guarantee of successful system design. The selection of electronic methods to be implemented according to identified requirements, is of grave importance. A information system focusing on meeting the needs of a wide and diversified public, interested in conforming with accessibility guidelines, could make use of webcasts, blogs, faqs, quickpolls, surveys and alerts mechanisms, but should avoid implementing decision making games. On the other hand, design teams interested in designing highly interactive information systems, not steering clear of high deployment complexity and hardware requirements, should consider making use of decision making games, chat rooms, discussion forums, e-panels, e-deliberative forums and online communities. It is decisive that systems with high privacy and security requirements should avoid chat rooms and online communities, except if they are operated under surveillance.

There is no e-method that can be suitable for all applications, and vice versa, no application can make use of all e-methods. An e-method must be chosen regarding each situation's demands and considering the above mentioned advantages and disadvantages that the particular e-method has. Accurate identification of user requirements and needs is the only guarantee of successful system design. Efficiently performing systems have evolved from

careful and detailed planning on the drawing board, to real world operating systems.

Electronic government solutions have met their preliminary goals of information acquisition and facilitating formation of an opinion, a shift of focus is occurring towards the next aim of e-democracy; expression of opinion. What is currently lacking from most electronic government information systems is the capacity to support effective citizen participation in the decision making process, beyond the electronic implementation of traditional bureaucratic services.

2.4 Voting

Voting is the most vital citizen participation process in democracy, as it can inherently facilitate the expression of general will. Voting is the strongest tool for expressing citizen content and exercising oversight over government bodies. Voting should not be understood as a mechanical process, but as having a creative capacity of its own, as it provides for the unification of the people (Rosanvallon, 2006). Although the act of voting is viewed as a personal right, the process engages the development of the nation as a whole. The selection of procedures and tools implemented to support this "unification" are of vital importance, as they must respect the creative capacity of the unifying process, without introducing disparities.

Voters in democracies around the world currently cast their vote in one of a variety of ways. Hence, elections differ quite a bit from nation to nation, not only with respect to the technology chosen to determine the elected candidates (e.g., proportional, majoritarian), but also in respect to the procedures, the way in which votes can be cast, the organizations involved, etc. Focusing in Europe, for instance, voting ranges from cases such as that of Estonia, in which voters can cast their ballot over the Internet, to that of countries, such as Greece and Italy, in which the voting procedures are completely manual. The technologies currently used internationally, span from plain paper ballots to punch cards, optical scan systems and remote vote casting systems. Each of these technologies has its own benefits and detriments. In the following section, we shall provide a short description of available voting technologies to more clearly outline electronic voting and what this includes.

2.4.1 Voting Technologies

This section describes the available technologies implemented in electoral procedures internationally. Throughout this section these citations have been used as reference text (Cranor, 2003; Weldemariam, 2010; Jones, 2003).

Traditional paper ballot: This form of voting was first used in Australia in 1858. The most basic form is using blank piece of paper upon which a voter writes his choice of candidates. The voter then seals his vote inside an envelope, places his ballot into a box, which when elections end, is opened and votes are counted. An election conduced using the Australian secret ballot is only trustworthy, if every ballot is strictly accounted for and no blank ballots escape the control of the election officials. Because we expect each official to have partisan interests, ballots must never be handled by one official without close supervision from someone representing an opposing political party. The greatest weakness in this scheme, lies in the way that votes are counted. As with all other ballot handling, tally teams must include representatives of opposing parties, and if the members use different criteria for accepting a mark on a ballot as a vote, the count may be biased. Accessibility is another disadvantage of these ballots, as the form and presentation of the ballot is restricted. The process of calculating the final tally is time consuming and exceptionally vulnerable to human errors.

Lever Voting Machines: Mechanical voting machines were first introduced in 1892 in New York. This technology was soon after adopted by most urban centers across the US, as they were believed not to be subject to bias in counting, and secondly because they seemed to offer instant election results. With lever machines, votes are counted instantly when the voter exits the polling booth. Lever voting machines essentially suffer from two categories of weaknesses, firstly they maintain no backup record of votes cast; and secondly the machines themselves appear to be too complex. These machines can contain hundreds of moving parts/wheels, that require testing prior to elections, something rarely done.

Punch card voting: This system was first used in Georgia, United States in 1962, using IBM's Portapunch punch mechanism. The ballot is a form of the traditional Australian ballot, designed to be tallied using standard punch card data processing equipment and with a mechanical aid. Used to ensure that votes are cast in a uniform manner. These systems (Votomatic system is most widely used), have several drawbacks, most critical being the way votes are punched. The system punches holes on a ballot to show voter intention. Unfortunately the system does not always guarantee a clean cut (punch) and there is no

intuitive basis on how to judge voter intention when in doubt. Hanging Chad's were made infamous in the highly contentious 2000 United States presidential election, where many Florida votes were cast using the Votomatic punch card ballots. Incompletely-punched holes resulted in partially-punched chad, where one or more corners were still attached, a *hanging chad*, *dimpled chad* or *pregnant chad* - where all corners were still attached, but an indentation appears to have been made. These votes were not counted by the tabulating machines (6,358 out of 433,043).

Optical Mark-Sense Voting: A voting system where voters mark paper ballots by hand or using a ballot marking device, then the ballots are stored in a locked ballot box and run through a scanning device to count them (VoterAction, 2008). This technology was developed in the 1950's to automate the entrance examinations at the ACT college, soon after Westinghouse Learning Systems began exploring its application to elections. To the voter, these implementations seem similar to the Australian ballot, as the ballot appears the same, except for index marks in the margins used by the ballot scanner to locate voting targets. First generation optical scanners used infra-red light to scan voter intentions on the ballot and were unable to reliably count marks made with anything but carbon black inks or graphite. Next generation systems use invisible light and generously accept single lines, check marks, "X" in or near voting targets to show voter intentions. The major problem with this technology is its accuracy. Unfortunately, mark sense ballot tabulators, judge ballots using mechanical criteria that differ significantly from the intuitive criteria people use. Identical ballots can be read differently by different machines, because they use different sensing technology. All optical mark-sense ballot tabulators are computer based, which brings about issues of software security and trustworthiness.

Direct Recording Electronic Voting: These systems were originally introduced in 1986 and emulated the look of the traditional lever voting machines, whilst replacing the levers and mechanical parts with buttons and microelectronics. Direct-recording electronic (DRE) voting machines, record votes by means of displaying a ballot provided with mechanical or electro-optical components, which can be activated by the voter (typically buttons or a touch-screen); that processes data by means of a computer program; and records voting data and ballot images in memory components (VoterAction, 2008). The first design essentially mimics the interface of a lever machine. In a sense that, the entire displayed ballot is visible at once on the screen. As opposed to the lever machine, in which a voter moves levers to make choices, with this kind of design the voter navigates from one screen to the next by pushing a button

available on the screen, this in turn triggers an underlying electronic switch and turns on a small light next to the choice. In the second design, a ballot page is displayed on a screen, and the voter uses mechanical devices such as arrow keys and buttons to make choices on a page and to navigate among pages. The third type is similar to the second type, with the exception of having a touchscreen display, where the voter makes a choice by touching the name of the candidate on the DRE screen and casts the ballot by pressing a separate button. These systems are physically hardened machines, preventing access to the typical PC connectors, e.g., USB ports (Weldemariam, 2010). DREs are particularly interesting because they solve a number of complex operational problems (Adida, 2006):

- ballots can easily be offered in different languages,
- voters with vision impairment can magnify the screen or use a headset that provides auditory feedback,
- ballot management is vastly simplified using memory cards instead of paper

For over a decade these machines were required to contain redundant storage of votes cast, but this appeared to be dysfunctional, as redundant storage was created by the same software that created the original record. As a results, recounts are of limited use. *The DRE voting machines are examples of e-voting systems, but only represent a portion of what is today considered as electronic voting*.

Currently, a universally acceptable definition for e-voting is lacking. The term is being ambiguously used to describe a variety of IS's ,which intend to achieve a wide spectrum of election related tasks; ranging from vote casting over electronic networks to electronic voter registration.

In general, two types of e-voting can be identified (Buchsbaum, 2004):

- **e-voting supervised** by the physical presence of representatives of governmental or independent electoral authorities, like electronic voting machines (DRE) at polling stations or municipal offices, or at diplomatic or consular missions abroad;
- **remote e-voting**[2] within the voter's sole influence, not physically supervised by representatives of governmental authorities, like voting from one's own or another person's computer via the internet (i-voting), by touch-tone telephones, by mobile phones (including SMS), or via Digital TV, or at public open-air kiosks - which

2 Throughout this dissertation, if not otherwise implicitly stated, e-voting is used to refer to remote e-voting within the voters sole influence

themselves are more venues and frames for different machines, such as; PCs or push-button voting machines, with or without smart card readers.

But also electronic voting solutions, differ widely in complexity, due to the context of elections they are required to support. Electronic voting systems have been used to support legally binding federal elections, but also small scale unofficial elections such as student elections. These e-voting systems differ widely to the features they support, but also to the risk profile they exhibit.

Electronic voting is viewed as a critical constituent for improving citizen collaboration, considered as a means to further enhance and strengthen the democratic processes in modern information societies(EU Recommendation Rec, 2004). Electronic voting is believed to have the capacity to engage citizens in a wider spectrum, than what is currently available in a conventional electoral process, as it provides citizens with a means to express their timely opinion on civil affairs such as legislation, representatives and such. E-voting is believed to provide a macro economical cost efficient method for increasing election accuracy and efficiency (Hof, 2004), (Clark, 2005) (Prosser, 2003). Additionally, electronic voting has the capacity to escalate usability and accessibility of the voting process(EU Recommendation Rec(2004)11). These Information Systems, attempt to increase election turnout while benefiting transparency and openness in democracy.

Electronic voting is envisioned as having a number of advantages; these include (Council of Europe-Commitee of Ministers, 2004):

- facilitating the participation in elections and referendums for all those who are entitled to vote, and particularly of citizens residing or staying abroad;
- widening access to the voting process for voters with disabilities, or those having other difficulties in being physically present at a polling station and using the devices available there;
- increasing voter turnout by providing additional voting channels;
- bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;
- reducing, over time, the overall cost to the electoral authorities conducting an election or referendum;

- delivering voting results reliably and more quickly; and
- providing the electorate with a better service, by offering a variety of voting channels;

Remote electronic voting offers the same advantages as "supervised"(or sometimes referred to as poll site) electronic voting ,while adding the following (Brown, 2003):

- Economies of scale with respect to the size of the electoral roll (i.e. an increase in the size of the electoral roll, does not increase the cost of the election linearly).
- Allows geographic independence of the voters and the resulting convenience of use.
- Is believe to have the ability to facilitate increased electoral participation.

Recently the Association of Central and Eastern European Election Officials (ACEEEO) advised election authorities in central and eastern Europe to develop a plan for the modernization of the election process that includes e-voting. "Such plans should be integrated into national strategies on the development of e-government" (ACEEEO, 2005). Numerous governments are currently in the process of evaluating electronic voting solutions, by holding a succession of trials and pilots to determine the benefits and drawbacks offered by their deployment. As the number of countries approaching the issue is increasing (United States, France, United Kingdom, Estonia, Switzerland, Canada India, Brazil, the Netherlands and others), electronic voting has become an all-important subject, as concerns over privacy, confidentiality, efficiency but also sociological, legal and political impacts, have been raised.

2.5 e-voting case studies

It is probably no exaggeration to say that a large number of countries have expressed a clear interest in electronic voting and have their own experience in using it in their electoral practices, through conducting a number of trials and pilots. Supervised e-voting machines are used by voters in all elections in Brazil and India, and also on a large scale in Venezuela and the United States. They have been used on a large scale in the Netherlands but recently have been decommissioned, due to public concern. Remote e-voting systems have gained popularity and have been used for government elections and referendums in the United Kingdom, Estonia and Switzerland, as well as municipal elections in Canada, and party primary elections in the United States and France.

We can see a multitude of different approaches to e-voting, revealing the wide range of political cultures and contexts within which it must find its place (GENERAL, AND, AFFAIRS, & INSTITUTIONS, 2009). The approaches adopted can thus seem contradictory, or indeed diametrically opposed (Monnoyer-Smith, 2008). It is interesting to review a number of countries as case studies

2.5.1 US

The US has been experimenting with different forms of electronic voting for a number of years. Currently numerous voting technologies have been implemented across the country (Illustration 30). In the 2004 presidential election around 40 million votes were cast electronically in polling sites. Voting over the Internet, on the other hand, is met with great skepticism. The SERVE voting system (Secure Electronic Registration and Voting Experiment), an Internet-based voting experiment, primarily directed towards military personnel stationed abroad, was being built for the U.S. Department of Defense's FVAP (Federal Voting Assistance Program). The SERVE system was planned for deployment in the 2004 primary and general elections, and would allow the eligible voters first to register to vote in their home districts, and then to vote, entirely electronically via the Internet, from anywhere in the world. The SERVE system received heavy criticism, due to security issues, and was eventually abandoned.

This year some 32 states and DC allow military and overseas voters to return their ballots by fax, e-mail, or through a Web portal. U.S. citizens who live overseas, whether military or civilian, have a host of new options for requesting, receiving and returning ballots for federal elections. The Military and Overseas Voters Empowerment Act, signed into law in 2009, requires states to provide absentee ballots in at least one electronic format. The Defense Department’s Federal Voting Assistance Program, charged under the MOVE Act with facilitating overseas voting, has established an online Electronic Voting Support Wizard, that develops state-operated websites that allow voters access and mark ballots and then print them for mailing or return them electronically. In October 2010, DC's pilot Internet voting system for overseas and military voters was hacked in a dramatic fashion by University of Michigan researchers, who changed votes on submitted ballots, discovered voters' personal information – and who observed users in Iran and China attempting to break into the system. The District of Columbia's pilot project for Internet voting for overseas and military voters has been scaled back to allow only electronic delivery of blank ballots to voters (though voted ballots may be

e-mailed or faxed).

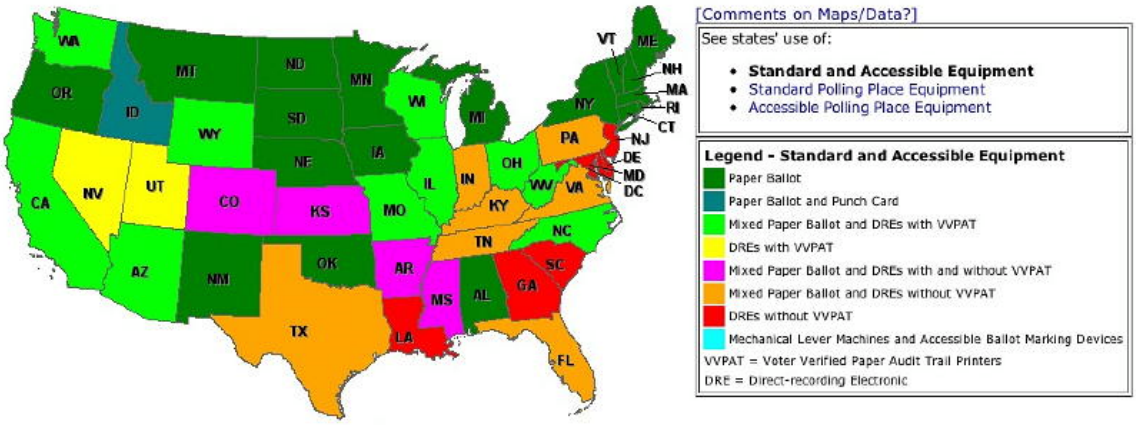

Illustration 30: Electronic Voting in the US

Source: http://www.verifiedvoting.org

Concerns are often raised in the US on the security and operational issues introduced by e-voting. In the initial years of introducing electronic voting machines, there was no certification process certifying that e-voting machines at least adhered to a set of minimum functional requirements. Federal legislation on voting in the US is believed to be inadequate, as it is up to the individual states to introduce e-voting as one or the only option. As an aftermath to the problems that occurred with the punching machines used in the 2000 elections, the Help America Vote Act (HAVA) was passed. This Act caused The U.S. Election Assistance Commission (EAC) to be established as "a national clearinghouse and resource for information and review of procedures with respect to the administration of Federal elections." EAC tasks were to provide technical guidelines for administrating Federal elections, to establish procedures for e-voting systems and to develop a federal program for testing and certifying e-voting systems. In May 2007, California Secretary of State Debra Bowen commissioned a "Top to Bottom review" of all electronic voting systems in the state. She engaged computer security experts, led by the University of California, to perform security evaluations of voting system source code, as well as "red teams" running "worst case" election day scenarios, attempting to identify vulnerabilities to tampering or error. The Top to Bottom review also included a comprehensive review of manufacturer documentation as well as a review of accessibility features and alternative language requirements. The end results of the tests were released on August 3, 2007, the security experts found significant security flaws in all of the manufacturers' voting systems, flaws that could allow a single non-expert to compromise an entire election (Prisajganec, 2010).

2.5.2 European Union

In 2004 the Committee of Ministers of the Council of Europe adopted the Recommendation (2004)11 on legal, operational and technical standards for e-voting. Following this, EU member states agreed to hold biennial meetings in order to keep under review their policies and experiences of e-voting in Europe. The Council of Europe provides guidance to all member countries in the field of electronic voting, while promoting sharing of knowledge and experiences between member states. At the 2008 Biennial Review it was suggested that certain aspects of the initial Recommendation, such as the certification of e-voting systems and the transparency of e-enabled elections, required further consideration. In 2010, the Council of Europe held the third meeting to exchange experiences with remote and non-remote e-voting in its member states(Madrid, November 2008). Besides the exchange of different experiences with remote and/or non-remote e-voting in member states, in the light of the Recommendation Rec(2004)11, guidelines on certification of e-voting systems and on transparency of e-enabled elections were presented and discussed at this meeting.

2.5.3 UK

The United Kingdom conducted numerous experiments during local elections in England and Wales during the period 2002-07. DREs, kiosk voting, Internet voting, text messaging, electronic counting and postal voting were all experimented with. The Electoral Commission evaluated the experiments and advised in their evaluation report on the 2007 experiments, that before more trials and pilots are held in the UK "there must be a comprehensive electoral modernisation framework covering the role of e-voting, including a clear vision, strategy and effective planning. The electoral modernisation framework should be accompanied by an e-voting blueprint, which should describe the envisaged future situation, covering legislative, process and technology aspects ". As these documents are publicly available, it is interesting to review the government response to the Electoral Commission recommendation (UK Govenrment, 2007)

Electoral Commission Recommendation: While from an operational point of view the 2007 e-voting pilots generally worked, the level of risk placed on the availability and integrity of the electoral process was unacceptable. There are clearly wider issues associated with the underlying security and transparency of these e-voting solutions and their impact on the electoral process, together with the cost

effectiveness of the technology, which need to be addressed.

Government's Response: All the pilots supported successful elections. The Government is not aware of any instances of alleged fraud during the elections and does not believe that the pilots increased the risk of electoral fraud. We do not agree that the level of risk placed on accessibility and integrity was unacceptable. We do, however, acknowledge that there were some operational problems around access to e-voting in some situations, but would stress that all pilots had comprehensive contingency plans in place to ensure that electors were not disenfranchised and retained their option of a paper ballot. The pilots are a mechanism for Government to identify and address the wider issues associated with changes to traditional electoral practice and the Government will seek to continue piloting as a sensible and proportionate method of gathering important evidence about how best to improve the electoral system. They also help to produce evidence for how greater value for money could be achieved in future and the scale of implementation required to reduce costs.

To present date, no further e-voting trials have been conducted in the UK, although the governments response claims that, "the Government will continue to consult with stakeholders over the implementation of a published strategy and agrees that issues around transparency, public trust and cost effectiveness should be laid out clearly."

2.5.4 Ireland

Ireland has been planning e-voting since 1999. In that year the basic legislation supporting e-voting was introduced and initial tests started in 2000. E-voting in polling places, using DRE Nedap Machines, was supposed to be available during the elections for the European Parliament and local elections in June 2004.

The Evaluation Commission appointed, opposed the use of e-voting, so all plans were stopped, pending further notice (Norwegian Working Committee, 2006). The Irish government immediately came under increased pressure, public scepticism and social opposition, over the purchase of a controversial electronic voting system, which was highly criticized as failing to meet user requirements, so the Irish government dropped its political support, evidently

leading to project failure, which in turn led to storing the e-voting machines in the closet. On 6 October 2010, Brian Cowen stated that the 7,000 machines would not be used for voting and would be disposed of. As of October 2010, the total cost of the electronic voting project in Ireland has reached €54.6 million, including €3 million spent on voter machine storage in 5 years.

2.5.5 France

France held an e-voting project in the constituency of Brest, during the 2004 local elections, on the 21 and 28 March of that year. (Norwegian Working Committee , 2006). The technical solutions were provided by the same manufacturer that provided the voting machines used in trials in Ireland (Nedap). The voters were given the opportunity to cast their votes in an electronic ballot box, in the polling stations. Another five constituencies took part in an e-voting pilot, but these were not part of the official election. Also, in the European Parliament elections on 13 June, 18 constituencies in France took part in pilot projects on e-voting, although not as an integral part of the official elections. The pilot projects were related to the voters' opportunity to submit their votes electronically.

During the presidential elections of 2007 in France, e-voting systems were used in 82 localities as a pilot test. Some political parties have called the e-voting a "catastrophe", demanding the withdrawal of electronic voting machines for the second round of the presidential election. Concerns in France were mostly targeted at accessibility and usability issues of the e-voting machines. E-voting machines were criticised of humiliating a great number of electors, fuelling social opposition. According to some e-voting satisfaction polls, the fact was explained that at least 5-10% of the electors were not at ease with the electronic voting system. These citizens could be publicly humiliated because of their difficulties in voting, or the number of the citizens not coming to vote could actually grow." (Digital Civil Rights in Europe, 2007). According to a separate study, carried out by Paul Verlaine - Metz University, the voting equipment "creates huge accessibility problems to the sight impaired, being a true discrimination source for them".

2.5.6 Estonia

Estonia has been experimenting with electronic voting since 2001. Their aim was to introduce evoting, remotely from uncontrolled environments, from the very beginning (Drechsler, 2005). Although the first attempt was for evoting to be operational in the elections of 2002, it was not until 2005 that voting over the Internet became an option. Estonia became

the first nation to hold legally binding general elections over the Internet, with their pilot project for the municipal elections in 2005. The electronic voting system withstood the test of reality and was declared a success by Estonian election officials

The e-voting system in Estonia makes use of personal ID-cards, which are issued to all citizens. This is a PKI enabled smart card with all the keys and PIN-codes integrated into it. The card is intended for use in all transactions that require secure user identification and legally binding signatures, including e-voting.

In 2005 elections in Estonia, e-voting remotely over the Internet was an available option only during the advance voting period. Although the advance voting period lasted for nine days (from the 13th to the 4th day before Election Day), VOI was only available for a restricted period of three days (from the 6th to the 4th day before Election Day). Although some politicians express their opposition, the majority of politicians in Estonia are in favor of remote e-voting. Their objections relate to the non-observability of the voting procedure, to the danger of buying and selling votes, and the danger of undue influence.

In the parliamentary elections in 2007, about 30,000 voters used internet voting (This number corresponds to 5 per cent of the participating voters). In the European Parliament elections in 2009 the number of I-voters had almost doubled – more than 58,000 voters used this method (this corresponded to about 15 per cent of all participating voters). Local elections took place on 18 October 2009, and we used I-voting as a voting method for the fourth time (about 104,000 I-voters and about 16 per cent of all participating voters). In the parliamentary elections in 2011, 140,846 I-voters used this voting method. This number corresponds to about 24 per cent of the participating voters (Estonian National Electoral Committee, 2011).

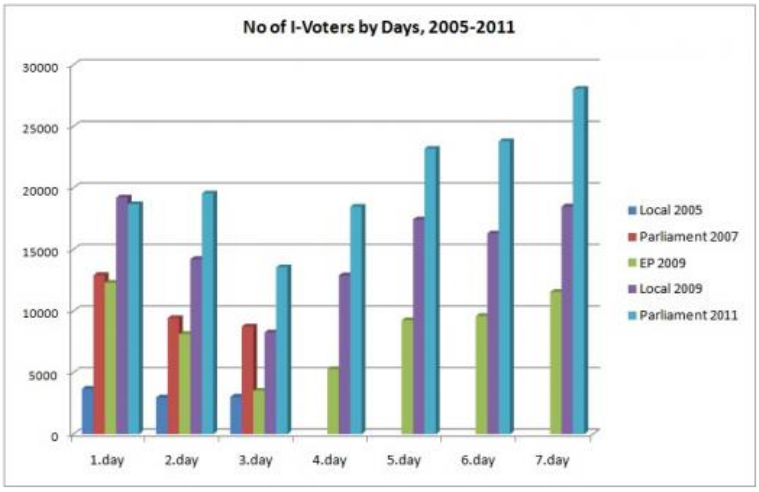

Illustration 31: Number of internet voters in Estonian Internet elections by day, 2005-2011 (Source: Estonian National Electoral Committee, 2011)

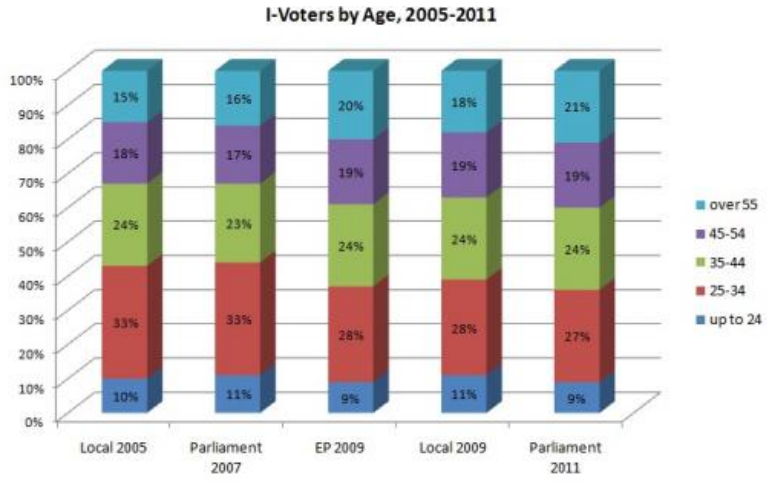

Illustration 32: Internet voters age in Estonian internet elections, period 2005-2011(Source: Estonian National Electoral Committee, 2011)

2.5.7 Spain

Spain performed a number of small scale experiments during 2003 and 2004, but ran a larger pilot project in connection with the referendum on the EU Constitution held in February 2005 (Norwegian Working Committee , 2006). Two million voters from 52 municipalities were given the opportunity to participate in the experiment, which was run from the 1st to 18th of February. The referendum was not legally binding. The voters could cast their votes from any computer with access to the Internet, after identifying themselves by using a smart card

and a PIN code. Ten thousand entitled voters took part in the project.

The current Spanish electoral Act does not allow e-voting and this Act's imminent modification (2011) does not include e voting at all, for both Government and Parliament do not support it. The Council of State (the Spanish government consultative body), issued on February 24th 2009, a report, previously required by the Spanish government, on the proposals for the modification of the General Electoral Regime. This report, as regards to e voting, states that a brief overview of the, not so many, e voting experiences that can be found worldwide, shows that e voting is a mechanism which entails doubts and reservations about the convenience of its implementation, and that the first question to face is if the introduction of e voting procedures is really necessary, when it is clear that the eventual irregularities that may arise in an electoral process can be solved in a satisfactory way by following the regular systems the Spanish law in force regulates. (Spanish Government, 2010)

In the European Parliament Elections 2009, the Ministry of the Interior put to the test the so called Electronically Managed Polling Station (EMPS). The electronically managed polling station is not electronic voting, but a set of information and communication technology equipment provided to make it easier for polling station staff to carry out their duties on the Election Day.

2.5.8 Switzerland

Since 1998, the Swedish government has actively pursued the implementation of electronic voting ("e-voting"), as Switzerland has a large number of elections performed on a yearly basis; Switzerland has between four and six elections/referendums per year. In 2009 - 2010 the number of cantons authorized to conduct e-voting trials, notably increased since 2008, as in addition to the three pilot cantons which own and operate each an e-voting system, nine other cantons are currently conducting e-voting trials. On February the 8th 2009, the Geneva citizens approved with a 70.2% majority the inscription of internet voting in their Constitution. On that February day, Geneva became the second Swiss canton to have a permanent legal basis for iVoting, after Basel Stadt. The Zurich model has additional interesting features which distinguish it from the Geneva model. In addition to Internet based voting, the Zurich system also permits votes to be cast via text messages as well as via interactive television systems (ITV). None of the available data, however, indicate that votes have been submitted via ITV(Gerlach & Gasser, 2009).The Swiss citizens living in the municipalities of Aire-la-Ville, Anières, Avusy, Bernex, Chêne-Bougeries, Chêne-Bourg,

Collonge-Bellerive, Cologny, Grand-Saconnex, Onex, Plan-les-Ouates, Troinex and Vandoeuvres were able to vote online for the federal and cantonal ballot of November the 28th, 2010.

The evidence and analysis suggests that "e-voting might serve as a powerful tool to augment the participation rate, the quality of voting, and aid in the implementation of political rights"(Gerlach & Gasser, 2009). There have not been any reports of manipulations or failures of the e-voting systems during any of the test runs, despite initial scepticism with respect to the maturity of security technologies(Gerlach & Gasser, 2009).

2.5.9 The Netherlands

The Netherlands have been offering e-voting as an option since the late nineties. (Norwegian Working Committee , 2006). When it was first introduced, little attention was paid to the security of the system and to the way electoral results were calculated. Usability, particularly for elderly citizens, was considered more central. During the 2005 election for the European Parliament, voters living abroad had the opportunity to vote over the Internet or over the phone.

The Netherlands have conducted two e-voting experiments for voters living and/or working abroad on election day, in order to facilitate the casting of their vote. The first experiment was held during the European Parliament elections in June 2004, and voters had the option of voting via telephone or Internet (as well as using the usual method of postal voting).

As the result of controversy about the use of electronic voting machines at polling stations, no further action was taken.

The Ministry of the Interior in the Netherlands recently decided not to adopt electronic voting machines. The decision was made after reviewing extensive research, which indicated that none of the available machines offered adequate privacy and security safeguards (Paul, 2009). Developing new equipment that could meet the government's standards was deemed too costly and challenging.

2.5.10 Russia

Russian President Dmitry Medvedev, in his address to the Federal Assembly of the

Russian Federation in November 2009, set the goal of “accelerating the technical modernization of the country's electoral system –of ensuring political competition through technological means”. The Head of State also underscored that "the modernization of the electoral process is part of Russia's national infrastructure"(Russian Federation, 2010).

The computerization of electoral processes in the Russian Federation has its own history of development. The State automated system known as "Vybory" (Elections), was created in 1994; its State-level test run took place in 1999, and in July 2000 it was placed in operation. The system is used for the computerization of information processes, such as the preparation and holding of elections and referendums and ensuring the activities of the election and referendum commissions; it constitutes a database of over 108 million Russian voters and referendum participants residing in the territory of the Russian Federation. Tasks on an ever larger scale are within sight: by the end of 2012, the system is expected to be equipped with computerized workstations, compatible with a ballot processing unit and a unit to enable electronic voting by 15 per cent of polling stations (around 15,000 out of more than 96,000), thus ensuring that 15 per cent of the total number of registered voters will have the opportunity to participate in elections through technical means. In Russia in 2001, scanners were created for processing election ballots, and in 2003, ballot processing units were introduced. In 2005, a test series of electronic voting units was produced in which paperless voting technology was used. No defects in the equipment or technical rejections were recorded.

The draft program for the accelerated technical retooling of the Russian electoral system also makes provision for the possibility of remote electronic voting, so as to ensure additional opportunities for electoral participation without voters having to visit a polling station on election day. “Given the geographical conditions in the Russian Federation, there is an urgent need for remote electronic voting because the number of polling stations set up for Russian citizens living abroad, or in difficult-to-reach or remote locations (in Siberia and the northern territories adjacent to the Arctic Ocean), account for at least one per cent of polling stations; roughly as many polling stations are set up for federal elections on vessels at sea.”(Russian Federation, 2010)

2.5.11 Norway

The Government initiated the E-vote 2011-project in 2008. The stated goal is to perform small scale trials of electronic voting, both in controlled environments and remotely prior to a

limited pilot of remote electronic voting (Internet) for the municipal and county elections in September 2011. Pilots are planned for 10 municipalities and one county.

As the Norwegian electoral system is largely based on voter confidence, transparency is of the outmost importance in the e-voting system. This is why it has been decided that anyone who so wishes, shall have full access to information on the inner workings of the system. The source code and system design documentation will be freely available for anyone to download and examine. The project will also deliver an open source elections administration support system. The September 2011-pilot will allow approximately 160.000 voters in 10 municipalities to vote remotely or in advance polling stations, in the advance voting period (Aug. 10 to Sep. 9). No political decision has been made on how to progress with e-voting beyond the 2011 pilots, as the experiences garnered from the pilots will form a basis for any decision in *Stortinget* (the Parliament) on whether to move forwards, and eventually at what speed.

2.5.12 India

Electronic Voting Machines ("EVM") have been used in Indian General and State election since 1999. In May 2010, 380 million Indians cast their votes on more than 1 million machines. It was the world's largest experiment in electronic voting to date and, while far from perfect, it is widely considered a success. For decades, Indians cast their votes by marking a paper ballot with a rubber stamp. It previously took days to count the votes and months to sort out the allegations of fraud. Fifteen years ago the Indian government commissioned two companies to design a simple electronic voting machine—one that was inexpensive, easy to use (even for the illiterate), and tamper-resistant. A column of buttons runs down one side. Next to each button is the name and symbol of a candidate or party. These are written on slips of paper that can be rearranged. The software is hard-wired into a microprocessor that cannot be reprogrammed. If someone tries to pry open the machine, it automatically shuts down. After much testing, India adopted the machines for nationwide use this year.

Voters use a paper ID card to authenticate themselves and then cast their ballot by pushing one of the buttons. Should trouble arise, an election official can push an override button that shuts down the system. Unlike other machines, the Indian machines are not networked. Each one has to be physically carried to a central counting center, (still they are easier to transport ,as the EVMs compared to ballot boxes are lighter, and come with polypropylene

carrying cases). Unfortunately, they do not provide an audit trail. The Indian machines malfunctioned at 1,800 voting booths (out of 1 million; 0.18%), and voters had the ability to recast their votes. India is currently debating on introducing remote electronic voting as an option.

2.5.13 e-Voting experiences

Electronic voting experiences differ widely on system design, implementations and conclusions. A number of countries have experimented with electronic voting solutions and have concluded to abandon its implementation until further developments in the field are made, while others have succeeded in implementing fully electronic vote casting systems without failures. As we shall see, electronic voting systems are highly complex information systems with many interrelationships and dependencies on the political sphere, the legal constitution in place, the context of the countries electoral system and evidently the decisions made on technical features and principles.

Overall experiences on electronic voting systems have been summarized in Table 7,

Countries	Holding pilots and trials	Legally Binding e-Voting	Legally Binding remote e-Voting	Stopped e-Voting
Argentina	√			
Austria			√	
Australia	√	√	√	
Belgium		√		
Bulgaria	√			
Belarus	√			
Brazil		√		
Canada	√	√	√	
Switzerland			√	
Czech Republic	√			
Chile	√			
Estonia			√	
Finland	√			
France	√	√	√	
Great Britain			√	
Germany				√
Greece	√			
India		√		
Ireland				√
Italy	√			
Japan	√	√	√	
Kazakhstan		√		
Korea	√			
Lithuania	√			
Latvia	√			
Mexico	√			
Malta	√			
Nepal	√			
Netherlands				√
Norway	√			
Peru		√		
Poland	√			
Portugal	√			
Romania	√			
Russia		√		
Spain	√			
SVK	√			
SVN	√			
Sweden			√	
USA		√		
Venezuela		√		

Table 7: Summarized e-Voting experiences internationally

Approaches and conclusions seem to differ widely, while the Netherlands have decided to

revert to traditional voting, abandoning voting machines, France has authorised the latter since 2003 but is refusing to implement e-voting in areas other than professional elections, which is also the case in Portugal. Austria successfully conducted its first remote e-voting legally binding election in 2009, Switzerland has amended its legal regulations to enable remote e-voting, while the United Kingdom, despite its very many "pilot runs" (150 since 2002), has suspended any further experimentation until 2010, officially for "reasons of electoral timetables".

2.6 Why is e-voting so difficult?

Essentially because electronic voting requires a public audit of a process that must remain secret. In elections, there is a conflict between the core requirements of verifiability and secrecy. When we attempt to translate these requirements into design principles for electronic voting systems, the conflict is apparent in contradicting principles. We require a voter to obtain enough information to be able to personally verify that his/her vote was recorded correctly, but not enough information that could lead to voter manipulation (coercion, vote buying, vote selling etc.).

Often electronic voting is falsely compared with other successful safety critical IS such as e-commerce and e-banking applications. In its essence, trust in an e-commerce environment is based on the belief that in the event that the system should fail, there are policies and guarantees in place, to protect the customer. Evidently a customer puts his trust in the Bank and not the banks IS, having the knowledge that in the worst case scenario he will be able to verify the mishappenings in an alternative method(visiting the local bank) and policies are at hand to protect him. In a commercial setting, people can detect most errors and fraud by cross-checking bills, statements, and receipts; and when a problem is detected, it is possible to recover their losses(at least partially) through refunds, insurance, tax deductions, or legal action. This also stands for financial transactions, where a customer can verify transactions through a monthly balance sheet or by contacting their local branch.

This is often referred to as the principle of "checks and balances", this is the same principle that governments are built upon (Cranor, 2003). For an example the American system of government, "the two party system, the three branches of government, the division of congress into the House and the Senate, were devised to guarantee that fair consideration be given to all issues that affect the populace". Computerized voting systems violate this essential principle because they are not, at present, adequately examined, supervised or

controlled. Currently in most e-voting solutions, voters have to have trust in every component of an electronic voting system, that it will not silently malfunction.

In recent years, it has become clear that an e-voting system can only be introduced if voters have trust and confidence in their current electoral system. If such trust exists, voters are then very likely to have confidence in new e-enabled elections. Surveillance is required to enhance trust, as a disconnection occurs between the voting process and the voter.

Digitalizing communications between governments and the "people" is a process necessary to be viewed within a wider framework. It is crucial to view issues involving electronic democracy in clear perspective and bear light on their true nature. Electronic voting is a social and political project, much more than a simple technical project. It is seen as bringing a social improvement in it by widening the circle of citizens involved in politics and political decision-making (Republique Et Canton De Geneve, 2009). As such, concerns are often voiced on security issues, but also sociological and political implications, that may be raised from the introduction of this technology.

2.7 Chapter Summary & Conclusions

This chapter outlines the broad field of study and then leads into the focus of the research problem. In this context, the concepts of governance in relation to Information and Communication Technologies are discussed. A number of electronic methods are reviewed which enable effective participation in electronic governments. For each one of these e-methods a SWOT analysis is provided, listing the Strengths, Weaknesses, Opportunities and Threats, that this particular tool exhibits. A comparison is then made, after the establishment of criteria, regarding many critical aspects such as: security, privacy, accessibility, user's or developer's viewpoints. Deploying electronic methods targeting at increasing participation and effectiveness of electronic government services is a complex situation. The selection of the ideal e-method depends on the accurately identified requirements. There is no e-method that can be suitable for all applications, and vice versa, no application can make use of all e-methods. An e-method must be chosen regarding each situation's demands and considering the above mentioned advantages and disadvantages that the particular e-method has. Accurate identification of user requirements and needs is the only guarantee of successful system design.

Voting is the strongest participatory tool in democracy. Electronic voting is believed to have the capacity to engage citizens in a wider spectrum, than what is currently available in a

conventional electoral process, as it provides citizens with a means to express their timely opinion on civil affairs such as legislation, representatives and such. E-voting is believed to provide a macro economical cost efficient method for increasing election accuracy and efficiency (Hof, 2004), (Clark, 2005) (Prosser, 2003). Additionally, electronic voting has the capacity to escalate usability and accessibility of the voting process(EU Recommendation Rec(2004)11).

As a growing number of countries are approaching the issue, we reviewed a number of case studies but results are inconclusive as electronic voting experiences differ widely on system design, implementations and conclusions. A number of countries have experimented with electronic voting solutions and have concluded to abandon its implementation until further developments in the field are made, while others have succeeded in implementing fully electronic vote casting systems without failures. As we shall see, electronic voting systems are highly complex information systems with many interrelationships and dependencies on the political sphere, the legal constitution in place, the context of the countries electoral system and evidently the decisions made on technical features and principles.

CHAPTER 3

E-VOTING ANALYSIS

3 E-VOTING ANALYSIS

Chapter Abstract: This section explores the complexity of electronic voting and attempts to shed light on the perplexities of its implementation. As a number of affecting fields operate in concert, to structure what is perceived as the dimensions of electronic voting, a multidisciplinary approach is employed to identify and define the true dimensions and implications involved in the adoption and development of an optimal information system. In this section electronic voting is viewed through the perspective of four separate dimensions, sociological, legal, political and finally technical. Each of these approaches leads to the identification of a set of requirements from which the design principles stem, desired for an electronic voting system.

3.1 E-Voting complexity

The field of electronic democracy and especially electronic voting is mostly undiscovered territory and its true dimensions are still mostly unexplored, as debates on the matter are still conflictual. Despite the numerous benefits introduced through the implementation of e-voting, both for the organising state, but also for the voters, the decision to build such a system in order to conduct elections over public networks is neither an easy or straight forward one. The reason being that a long list of multidisciplinary requirements must be fulfilled (Labrinoudakis, Gritzalis, Tsoumas, Karyda, & Ikonomopoulos, 2003). Critiques on electronic voting are often projected as engineering problems, omitting to apprehend the socio-political context, within which, electronic voting solutions exist. E-voting is a problem that requires multidisciplinary input (Mcgaley, 2008). Academic and research literature attempts to approach the issue from a wider viewpoint, avoiding concentrating on a single field of knowledge, but incorporating into the field of electronic democracy, not only the technological or legal questions, which determine the design of an application, but also politics and society's influence. E-Voting, as proposed by Prosser and Krimmer (Prosser & Krimmer, 2004) differentiates four separate dimensions: (i) Politics, (ii) Law, (iii) Technology, and (iv) Society.

In the available literature, requirements are usually identified as falling among the above mentioned fields, which are included in the design process in the form of conditions that the system should meet. An important step in ensuring that any system behaves correctly is laying

down what behaving correctly means for that system (Weldemariam, 2010). In other words, we must accurately identify the system's requirements. (Mcgaley, 2008) "The lack of an adequate requirements definition for e-voting prevents us from determining the quality of a given system, and is therefore a barrier to the use of e-voting for critical elections"(Mcgaley, 2008). In the following section we shall attempt to provide a complete set of requirements from a social, legal and political perspective but also define a list of functional requirements for an electronic voting system.

3.2 Social Perspective and Requirements

As electronic voting targets increasing social collaboration, achieving wide social acceptance is critical. One of the crucial issues discussed at the council of Europe (CoE, 2010), which was conveyed to review developments in the field of e-voting, was the issue of public trust in electronic voting and how to achieve it. "In recent years it has become *clear that an e-voting system can only be introduced if voters have trust and confidence in their current electoral system. If such trust exists, voters are then very likely to have confidence in new e-enabled elections. However, trust should not be taken for granted and states need to do their outmost in order to ensure that it is preserved. All the more so because once trust and public confidence is diminished, it is exceedingly challenging to regain it.*" (GGIS (2010) 5 E)

Trust in general has two main variants; political and social. Trust assessed in political terms is the so-called political trust. Political trust happens when citizens appraise the government and its institutions, policy making in general and/or the individual political leaders as promise-keeping, efficient, fair and honest. Political trust, in other words, is the "judgement of the citizenry that the system and the political incumbents are responsive, and will do what is right even in the absence of constant scrutiny" (Miller and Listhaug 1990, 358). As such, "political trust is a central indicator of public's underlying feeling about its polity" (Newton and Norris 2000, 53). Political trust does not emerge, nor does it operate, in vitro. Social trust, which refers to citizens' confidence in each other as members of a social community, is inseparable from the notion of political trust. Modernization theorists, like Almond and Verba (1963) and Finifter (1970), maintain that increasing social trust is associated with increasing political participation, especially in the form of voting (Blind, 2007).

Electronic voting is an electronic method with the ability of widening participation in the electoral process. E-voting systems have the potential to be more usable than paper, especially

for people with disabilities, such as visual impairment or reduced kinetic ability. Indeed, paper voting systems are not free of usability problems (Mcgaley, 2008). Individuals with disabilities are frequently unable to perform their electoral duties unaided and in most cases require help during vote casting. Entering the voting kiosk with a member of the committee, denies them the right to privacy, making this group a target to a number of threats, coercion etc. Not to exclude a large number of the electorate is unable to attend the polling station to cast a ballot. According to a survey by the Eurostat Office of the European Commission from 1992, about 12% of the European population has a handicap, which adds up to more than 37 million persons and the number is rising(Project, 2010).

E-voting can provide opportunities for improving certain groups' access to the election process. The following groups could benefit (Caarls, 2010) :

- the visually impaired could use headphones connected to DREs and PCs if using Internet voting;
- citizens who are not normally able to go to a polling station to cast their vote can vote via the Internet from their own home;
- the use of electronic media can also facilitate the use of official minority languages, and this could lead to increasing involvement;
- citizens living and working abroad (such as military personnel) could benefit from the introduction of e-voting.

Of course, e-voting should result in inclusion, never exclusion, of certain groups. Electronic voting systems must target at increasing participation in the electoral process by offering an all inclusive platform with the ability to increase participation. To achieve optimum design and guarantee that design choices overcome accessibility and usability inequalities, a methodological user-centered design (UCD) needs to be adopted, incorporating design principles and theories such as Design for all'(DFA) and the Principles of Universal Design(UD). As Ms Gabriele Kucsko-Stadlmayer, the Venice Commission representative, pointed out, "the main disadvantages of remote e-voting, particularly the shortcomings in terms of system security, are much less serious given that e-voting enables population groups previously excluded from the electoral process (eg persons with disabilities, soldiers and other citizens abroad) to exercise their voting rights"(GENERAL, AND, AFFAIRS, & INSTITUTIONS, 2009).

The impact of internet voting on turnout of course is still being debated. The studies, led by the Centre for Research on Direct Democracy (c2d) in the framework of the first online ballots, as well as the phone survey, conducted during the first online federal ballot of September 2004, show that the Internet is not merely a complement to postal voting, but that it reaches a new category of citizens. Voters of less than 55 years of age make wide use of internet voting. Recent Data from the Estonian Elections, reviewing internet voters age groups, over an extended period of elections held from 2005-2011, is indicating that the largest group to make use of the internet voting option is 25-43 years of age (27%), but an additionally large percentage belongs to the age group of over 55 (21%).(Illustration 33).

But electronic voting is not accepted by all. Pressure groups in the Netherlands, the Chaos Computer Club in Germany, the Verified Voting Foundation, and the Black Box Voting organisation in the U.S. as well as the Irish Citizens for Trustworthy E-voting group, highly criticise electronic voting and are very sceptical with respect to the current electronic voting systems (Volkamer, 2009, p. 4). These groups express concerns on the disparities introduced by electronic voting, security issues, inefficiency of systems, cost and others. Claims are often made that electronic voting has not been able to achieve cost reductions; as the cost of system implementation is too large. Krimmer (R. Krimmer, 2010) recently reporting on the use and deployment of an e-voting IS for student elections in Austria, stated that the cost per voter rose to 400 euro each (or 200 per vote as each voter cast two votes), while in other reports of e-voting pilots, cost per voter had risen to 65,000 dollars. Although these numbers are extremely high, they can not be considered as conclusive data; as these are reports from pilot projects. Pilot projects are unable to attract large numbers of voters; thus not being able to achieve economies of scale. The cost per voter decreases with the scale of the election (number of voters) and the number of elections the system is used for.

Electronic voting IS systems, need to provide a voting channel with the ability to overcome any existing inequalities, or at least avoid introducing any additional ones; as an electronic voting election system may itself enforce unequal access to the electoral process, through the unequal ownership of IT and related knowledge. The Digital Divide is a widely used concept that is defined as disparities in computer ownership and Internet access, based on income (Neu, 1998). The divide refers to an imbalance in physical access to hardware and in the necessary knowledge that enables a digital citizen to participate in electronic democracy and in e-voting. The Digital Divide is discussed to hold in the context of socio-economic, racial and geographic differences. The digital divide is often referred to as the primary socio-

political issue (Hoffman L.J., 2000) leading to inequality of citizens votes in the concept of e-voting. It is argued that while Information and Communication Technologies (ICTs), hold the potential to improve the democratic process, expand citizenship and empower the people, they also have the ability to perpetuate or exacerbate existing inequalities and other divides.

Comparison of Internet use by socio-economic groups between 2005 and 2007 shows that there has been a significant reduction in disparities. The share of households with broadband internet access has doubled since 2006, while more than half of individuals in the EU27 use the internet daily (Seibert & Loof, 2010).The most disadvantaged groups are those aged 55-74, the retired and economically inactive, and those with low education. For each of these groups, average Internet use has moved closer to the EU average. Students, the highly educated and young people remain at the top, but Internet use has declined relative to the average, possibly because their usage rates are close to saturation while the average continues to grow.

Through political support, in the form of campaigns, policies and initiatives, differences in computer ownership, but also computer training, social inequalities can be overcome. In this context, initiatives such as e-Inclusion and One Laptop Per Child, but also overall funding of ICT infrastructure development and training, present opportunities to overcome economic distinctions and geographical differences in society, steering towards an all inclusive platform.

It is a matter of democracy, equality, and equity to guarantee that the traditional and the e-voting technologies are at least equivalent, with respect to ease and opportunity of access (L Mitrou, D Gritzalis, & S Katsikas, 2002). Before any medium can be adopted as a mass medium, a critical number of adopters must be reached. Electronic voting will become democratically acceptable only when the majority of eligible voters have easy access to the Internet (Lilian Mitrou, Dimitris Gritzalis, Sokratis Katsikas, & Quirchmayr, 2003). Marcus (Marcus, 1990) states that in general, the critical number of adopters for an innovation is approximately 16% of population. Internet adoption in EU is growing at exponential rates. Recent research results are showing that Internet penetration is growing annually". Currently it is estimated that 57% of European households have Internet access (IP/10/1328, 2010). A Digital Agenda for Europe has been presented by the European Commission which sets an ambitious target of every European-Digital. The European Digital Agenda's target is to bring Internet connections of 30 Mbps or above to all Europeans by 2020 with half European households subscribing to connections of 100 Mbps or higher (IP/10/1328, 2010).

While an average 93% of Europeans can enjoy access to a high speed online connection, the figure is only 70% in rural areas, and in some countries (such as Greece, Poland, Slovakia, Bulgaria and Romania) high speed broadband Internet networks cover just 50% or less of the rural population (IP/09/343, 2010). Across Europe, only 22.5% of people in rural areas use e-government services like lodging tax returns, compared to 32.9% in urban areas. The EU commission is implementing initiatives throughout Europe to boost competition in local access networks, so as to encourage widespread Internet take-up and high-speed Internet access in Europe. The EU is addressing the EU's "Internet broadband gap" between urban and rural areas through rural development policy; about €15 billion is being spent on information and communication technologies priorities under the EU's Cohesion Policy for 2007 -2013 – on e-public services and Internet infrastructure. In many EU member states a number of citizen to government interactions are only now becoming available online, such as in Greece all tax reports need to be submitted electronically.

Additionally, as technology's primary goal is becoming user friendlier and Internet penetration is increasing, such a gap, if existent, is evidently going to disappear. The Internet may hold the capacity to bridge existing disparities, as it can provide a means to overcome economic distinctions and geographic differences by creating an entryway to an extended information network. Macintosh (Macintosh, 2003) identifies as a social requirement" that computerized information campaigns and mass public information systems have to be designed and supported in such a way to help narrow the gap between the 'information rich' and 'information poor' otherwise the spontaneous development of ICT will widen it. It is a fact that in 2010, about four in ten unemployed internet users consulted the internet for learning (Seibert & Loof, 2010).

In view of the digital divide and avoiding introducing any additional disparities, a number of social guidelines can be suggested: (NIST, 2006)(Mcgaley, 2008)(Election Assistance Commission, 2005)

- Prior to the implementation of binding electronic elections a critical mass of electronically enabled citizens must be achieved. E-readiness is the "state of play" of a country's information and communications technology.
- The voting process shall be designed to minimize cognitive difficulties for the voter; the voting system should support a process that does not introduce any bias for or against any of the selections to be made by the voter.

- The voting process shall be designed to minimize interaction difficulties for the voter.
- The voting process shall be designed to minimize perceptual difficulties for the voter.
- The electronic voting option shall remain an optional channel complimentary to traditional poll/ paper based voting, as long as disparities in computer ownership, knowledge etc exist throughout society.

3.3 Legal Perspective and System Requirements

E-voting needs to comply with the existing legal and regulatory framework. Any attempt to introduce e-voting, which enables voters to cast a secure and secret ballot over the Internet or Intranet, must address a series of complex constitutional and legal issues (Lilian Mitrou, Dimitris Gritzalis, Sokratis Katsikas, & Quirchmayr, 2003). In most countries to use remote e-voting channels, laws or even the constitution have to be changed, which require careful planning. Before introducing e-voting, according to national requirements, members should take the necessary steps to create the national legislative background to enable the introduction of e-voting technologies in the voting process (ACEEEO, 2005). Prior to introducing electronic voting, member states should have reviewed and secured all the legal matters in order to avoid conflicts during the process of an e-enabled election. (Directorate General Of Democracy And Political Affairs, 2010).

Often legal issues arise, even in the cases of trials and pilots. In non binding trials, usually it is not required to establish a legal basis, but this is often not the case for binding pilots which require amendments to the legislation. A legal basis could be layed out in three forms (Caarls, 2010) :

- a temporary law permitting e-voting experiments;
- a change in the existing electoral law or in the implementation of existing legislation;
- a temporary law on e-voting followed by changes in the existing electoral law;

In most cases, legislation permitting experiments with e-voting is subject to specific time restrictions or is geared to one or more specific elections (for example, experiments may only

be conducted during local elections). The advantage of a temporary law is that existing electoral legislation does not have to be amended, which would probably take more time and thus slow down the process (Caarls, 2010).

The new culture introduced by ICT cannot and should not ignore the core principles and values of democracy. The introduction of an e-voting system conforms to this demand if it respects fundamental democratic principles and citizen rights, and fullfills the requirements arising from these principles and rights. It is commonly accepted that parliamentary elections have to be free, equal and secret. Furthermore, the principles of universal and direct suffrage belong to European electoral heritage. The principles of freedom and secrecy, as well as the reference to fair elections are enshrined, explicitly or implicitly in a number of international instruments like the Additional protocol to the European Convention of Human Rights or the International Covenant on Civil and Political Rights.(Lilian Mitrou, Dimitris Gritzalis, Sokratis Katsikas, & Quirchmayr, 2003)

It is critical to define how legal aspects constitute requirements on a technical level. The constitutions of many countries require that general elections be universal, free, equal, secret and direct. This set reflects, in turn, to essential voting design principles from a legal perspective(Gritzalis, 2002).

3.3.1 Universality of elections in respect to electronic voting

Gradually throughout history the idea of democracy was equated with the idea of universal suffrage. The first universal elections that took place on April 23,1848, illustrated the belief that the object of voting was more to celebrate social unity, than to exercise a specific act of sovereignty or arbitrate between opposing views. The republic of the universal suffrage implied, above all, the search for a society without divisions during the electoral process. Universal suffrage is a generic principle for democratic elections, requesting that every eligible voter can participate in the election process, and nobody can be excluded or discriminated. Universality of elections can thus be understood in terms of eligibility and of not permitting exclusion or discrimination of voters.

E-voting improves the universality of election procedures by providing an additional option of participation to the electoral process (Gritzalis, 2002).Through improved access options, such as e.g. remote voting procedure which take account of the increased mobility and individualization of voters, the principle of universality is increased (Klaus & Weddeling, 2006). As e-voting improves the generality of election procedures by providing an additional

option for exercising political rights, it prima facie raises no specific problems in relation to the principle of universal suffrage. (Lilian Mitrou, Dimitris Gritzalis, Sokratis Katsikas, & Quirchmayr, 2003). The Federal Constitutional Court of Germany accepted the constitutionality of postal voting, when considering the balance between the improvement and broadening of generality,on one hand, and the risk of loss of freedom and secrecy of election on the other hand. The principle of universal election requires that the voting system must be available for all voters independent of their personal holdings, can be used by all voters without requiring special knowledge, for instance in computer science, does not lose any data (e.g. during ballot transmission), and counts all ballots correctly (Melanie Volkamer & Hutter, 2004).

Eligibility can be ensured through the registration of eligible voters and their identification at the moment of registration. Secure authentication and registration are the means for ensuring that the principles of universal and equal suffrage, summarized as "one voter, one vote", are respected and that elections can not be rigged. (Lilian Mitrou, Dimitris Gritzalis, Sokratis Katsikas, & Quirchmayr, 2003). Providing a secure identification and authentication of the voter is *conditio sine qua non* for e-voting systems to be used in public elections (Lilian Mitrou, Dimitris Gritzalis, Sokratis Katsikas, & Quirchmayr, 2003). Taking into account that there will usually be no country-wide online voter register, a pre-registration for e-voting will be considered as necessary in order to avoid vote fraud. This issue did spur controversy in the UK, when the electoral commission required the introduction of a registration system, the government responded that,

"*The Government understands the Electoral Commission's continued position on introducing a system of individual registration and appreciates the potential benefits such a system might bring. However, this has been debated by Parliament and has been rejected. In respect of the recommendation in relation to e-voting, we do not think that the identifiers commonly proposed for individual registration, namely a signature and date of birth, are the appropriate ones and it is not something that is needed to underpin e-voting.*"

In respect to the universality of elections a number of requirements can be identified which lead to essential design principles (NIST, 2006)

I. Universal suffrage

1. The voter interface of an e-voting system shall be understandable and easily usable.

- *User interface design shall follow best practice to maximise usability*, in particular:
    - Interfaces shall not present cognitive difficulties.
    - Voters shall be consulted during the design and testing of vote casting and registration interfaces.
    - The needs of voters with disabilities shall be taken into account in the design of the interface. Appropriate advocacy groups shall be consulted, and compatibility with relevant products and compliance with relevant standards maximised, to that end.
- Voters shall be educated in the use of the vote-casting interface and regarding any steps required in order to participate.
    - Voters shall be given the opportunity to practice using the interface.
    - Support and guidance shall be available to voters through widely available communication channels.
    - Where there is doubt (such as with remote voting) voters shall be educated as to how they may confirm that they are using an authentic voting channel and that the authentic ballot has been presented.

2. Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting.
3. Providing a secure identification and authentication of the voter is "conditio sine qua non" for e-voting systems to be used in public elections
4. E-voting systems shall be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.
5. Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.
    - A contingency procedure shall be drawn up to prepare for the possibility that one or more voting channels become unavailable, and to provide alternative voting channels where necessary.
    - The e-voting system shall be protected against threats to its availability,

integrity and confidentiality, including: malfunction, breakdown and denial of service attacks.

- The timetable for voting channel availability shall be designed to maximise voter access and shall be made public well in advance of the start of the polling period.

3.3.2 The principle of "free elections" in respect to electronic voting

The principle of free elections requires providing the facility for every voter to cast his/her ballot free of duress and without unlawful and undue influence. The principle of free election requires that vote casting, take place without any violence, coercion, pressure, manipulative interference, or any other influence, exercised either by the state or by one or more individuals. Coercion occurs when the voter is not free to cast a ballot , i.e. when the voter is forced or bought into voting for an option, which he would not have chosen, had he not been under pressure or if he had not been offered a bribe. The distinct problematic nature of electronic voting requires not to provide a voter with a receipt that could lead to coercion, but this is often required to increase trust.

Uncoersibility is defined as the voter not having the power to prove to a third party what his/her vote was (Peralta, 2003). Remote electronic, before election day, is called early voting and it is correlated with absentee voting. Traditionally absentee voters request a ballot by mail, vote from wherever they happen to be, and mail their ballots back to the offices of their home jurisdiction prior to election day. The single largest problem with absentee voting has been the opportunities for vote fraud. A legal solution requires enabling a multiple vote casting, often referred to as "reversible vote" or "vote updating" or "provisional voting". The voter may cancel any previous cast votes by casting a new vote. The voter may vote via the Internet, as many times as he/she wishes, but only the last vote cast will be counted (either electronically or by going to the polling station on the last day). The vote cast at the polling station is the one which will be counted, since this is the only vote which can be guaranteed to have been cast in secret. Vote updating has already been used in some countries, such as in Sweden for traditional paper-based elections, were voters having cast an absentee vote, can cancel this vote by casting a vote on election day in the polling station. If we wish to allow this, while preserving anonymity of the voter, we must seal each ballot in an envelope with the voters identity and a time stamp on the outside. At vote counting, all envelopes deposited

by a given voter must be gathered; and only the envelope with the latest timestamp should be opened while all others remain forever sealed (Jones, 2003). A number of cryptographic protocols have been proposed that attempt to exhibit the properties of coercion-resistance and receipt freeness (these are thoroughly presented in the consecutive chapter). Vote updating in the context of electronic voting has become popular in Estonian elections. The Estonian election system allows multiple online votes to be cast by the same person during the days of advance voting, with each subsequent vote cancelling out the previous one. With vote updating, an intruder can still observe the voter or force him to cast a particular vote but the voter has the possibility to cast another vote and, thus, make another choice cancelling out the previously cast ballots. It becomes unattractive for an attacker to coerce a voter into voting a specific way as the vote can be "reversed" at any future moment in time(usually up until election day). For the same reason, ballot buying becomes unattractive. It has been stated that due to extended vote casting periods, voters are unable to respond to short-term political events. Vote updating permits voters to timely update their vote to respond to short-term political events.

The freedom of decision requires protecting a voter from external influence during vote casting. This could be achieved if a propaganda message is blended on the computer screen while the voter is casting an electronic ballot. The e-voting procedure should make the advertisement of political parties/candidates on the e-voting website technically infeasible (CyberVote Project, 2000).

Additionally the option must be available for a voter to cast a blank or invalid vote. The possibility for casting a consciously invalid (or "white" paper) ballot should be ensured according to the theoretical background of free expression of preferences.

In respect to the freeness of elections a number of requirements can be identified which lead to essential design principles (Council of Europe, 2004; D Gritzalis, 2002; Mcgaley, 2008)

II. Free suffrage

5. The organization of e-voting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.
6. The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection.
7. Voters shall be able to alter their choice at any point in the e-voting process before

casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person. The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting.

- The vote-casting interface shall be free from any information, other than that strictly required for casting the vote. The e-voting system shall prevent the display of other messages that may influence the voters' choice.

8. The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote.
9. The e-voting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed. [3]

3.3.3 The principle of "equality of elections" in respect to electronic voting

In respect to equality of elections it must be guaranteed that all ballots are accounted for equally. Under the principle of equal suffrage, two major requirements are identified:

- equality regarding the participating political parties and candidates
- equality regarding the voting rights of each voter.

Because of the emerging characteristics of the technology, the right to equal accessibility to the voting process should become the right of equal accessibility to election technology. An e-voting system should ensure that the *one voter - one vote* principle is respected, that is only eligible voters can vote, only once, either online or off-line. Another issue is the duration of the e-voting period. The definition of longer voting period to more than one day, may put in question the principle of equality and raise constitutional issues,

3 It has been suggested that this list be with "The e-voting system shall prevent the changing of a vote once that vote has been cast. "Many researchers and academics oppose these statement believing that multicasting or multiple voting can solve coercion problems in electronic voting. An electronic system may enforce the one voter-one vote principle in two ways, either by invalidating the voter's credentials for further voting in the same election event, or by letting the vote receiving server in some way keep track of the identity of the voter and reject multiple ballots from the same voter. The first solution is susceptible to conscious or unconscious errors and mistakes on the client side. Hence, it is better to let the server side handle the duplicate ballots from the same voter. We propose to let the vote-storage server store all the received ballots, rather than rejecting the second and the following ballots. At the end of the voting period, the election system will run through the ballots and only the last ballot received from each voter will be transferred to the electronic ballot box. Thus, the voter may effectively regret and cancel his vote just by casting another one at a later point in time. (Gerhard Skagestein, 2006). Electronic re-vote cannot thus be considered as multiple voting, as the system will take into account only one vote. Allowing to re-vote is considered as a measure against vote-buying and against voting under coercion. (Maaten, 2004)

where it is provided that general election be held simultaneously throughout the state. Where voting by mail has been introduced, this problem has been solved by counting the mailed in ballots simultaneously with the physical ballots. (CyberVote Project, 2000)

In respect to the equality of elections a number of requirements can be identified which lead to essential design principles (Council of Europe, 2004; CyberVote, 2000; D Gritzalis, 2002; Mcgaley & Gibson, 2006)

III. Equal suffrage

10. Only authenticated eligible voters are permitted to cast their vote.

    - An authentication system shall exist to distinguish eligible voters from others, and those who have successfully cast votes from those who have not. Note: this may require special attention where multiple voting channels exist, and where voter registers may not be up-to-date.

11. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result. [4]

12. Only one vote shall count.

3.3.4 The principle of "secrecy of elections" in respect to electronic voting

Secrecy requires that only the voter knows the contents of the ballot cast. Secrecy is the condition of the voter free political decision. In democratic elections the link between the vote and the voter should be irreversible, to ensure that votes are cast freely. Secrecy meaning that no voter should be able to prove that he or she has voted in a particular way.

It is though believed that confirmation of the vote, after the ballot has been transferred and received, enforces confidence in the system and ensures the voters rights (California Internet Voting Task Force, 2000; Lilian Mitrou, Dimitris Gritzalis, Sokratis Katsikas, & Quirchmayr, 2003), but it cannot relate to the content of the vote (CyberVote Project, 2000). Traceability of the vote cast should be excluded, while preserving authenticity and verifiability of the cast ballot. "Audit trails can provide physical, unalterable evidence of how

4 It has been proposed that this list be with "The e-voting system shall prevent any voter from casting a vote by more than one voting channel. Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once."

the voting computers interpreted each vote, but this could potentially lead to "vote selling" or to the need for the voter to show proof to another person of how he/she voted (a number of cryptographic protocols have been proposed that attempt to exhibit the properties of coercion-resistance and receipt freeness that shall be presented in consecutive chapter).

In Estonia, enabling remote electronic voting required revisiting the legal framework of the secrecy of vote. Paragraph 60 of the Estonian constitution explicitly states that elections shall be free and that voting shall be secret. The supporters of the Estonian law which introduced remote electronic voting on a national scale in 2005, used a teleological approach in their argument in order to get rid of the mandatory secrecy of their vote. They argued that constitutional rules should be understood through the problems they are supposed to solve. The principle of secrecy was said to promote the individual vote from any pressure against his or her will. In this teleological reformulation, secret voting has become a means and in no longer an end in itself. So, while all voters still have the right to go to a polling station in which their privacy is guaranteed, the end of secret voting is already in sight. In this view, online voting must be seen as constitutional, since voters who choose this technique have obviously decided that they do not need this kind of shield for their privacy.

In respect to the secrecy of elections a number of requirements can be identified which lead to essential design principles (Buchstein, 2004; Council of Europe, 2004; CyberVote Project, 2000; D Gritzalis, 2002a; Mcgaley & Gibson, 2006) :

IV. Secret suffrage

16. E-voting shall be organised in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.
17. The e-voting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.
18. The e-voting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.
19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.
20. At no stage shall the voter's identity and vote be available together in unencrypted

form to any person (other than the voter) or system , except where required by law and sanctioned by the relevant authority.

3.3.5 The principle of "direct elections" in respect to electronic voting

The principle of direct elections prevents someone from voting on behalf of other eligible voters. Directness requires that there can be no intermediaries in the process of voting decision (D Gritzalis, 2002). On many occasions, individuals with disabilities are denied their right to directness as they are frequently unable to cast their vote unaided. Individuals with disabilities often require that a member of the electoral committee casts their ballot on their behalf, as due to their disability they are unable to cast their vote directly.

This principle may be also adapted to fit an e-voting procedure. The relevant requirement is that each and every online ballot is directly recorded and counted. A problem may arise in case the voting period differs from the voting procedure (on-line or off-line) used to cast the vote. Online voting results may influence the outcome of the entire election process and limit the integrity and legitimacy of the whole process. To avoid this, a system can be developed allowing the recording and maintaining of the cast vote, while prohibiting any counting before the end of the (off-line) voting period.

3.3.6 The principle of "democracy in elections" in respect to electronic voting

Gritzalis D. (D Gritzalis, 2002), proposes adding to the above list the requirement of Democracy. These requirements pertain to the preservation of attributes and properties such as transparency, accountability, security, accuracy and legitimacy of the system.

Transparency

20. Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.
21. Information on the functioning of an e-voting system shall be made publicly available.
22. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results

Verifiability and accountability

24. The components of the e-voting system shall be disclosed, at least to the competent

electoral authorities, as required for verification and certification purposes.

25. Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.

26. There shall be the possibility for a recount. Other features of the e-voting system that may influence the correctness of the results shall be verifiable.

27. The e-voting system shall not prevent the partial or complete re-run of an election or a referendum.

Reliability and security

28. The member state's authorities shall ensure the reliability and security of the e-voting system.

29. All possible steps shall be taken to avoid the possibility of fraud or unauthorised intervention affecting the system during the whole voting process.

30. The e-voting system shall contain measures to preserve the availability of its services during the e-voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks

31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is genuine and operates correctly.

32. Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.

33. While an electronic ballot box is open, any authorised intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report, be monitored by representatives of the competent electoral authority and any election observers.

34. The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.

35. Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.

An additional important issue that needs to be addressed, unique to remote electronic voting, is that of liability. The French Data protection authority, has denied its favourable opinion to the application for trial of e-voting on the grounds that the server being used was situated abroad and was not subject to supervision by national authorities. The Internet, and specifically cloud computing, raises serious jurisdictional issues that must be addressed.

3.4 Political Complexity and Requirements

When considering electronic elections through a political scope, it is important to take into account issues that affect the decision of introducing electronic voting, but also on selection of design features. Crucial to such selections is the context of the political format the IS shall support, with respect to dimensions of scale, election cycles, etc. Switzerland for example has been considering electronic voting for a number of years, (trials have been held as early as 2001), as due to the political context, the country was projected as an ideal candidate. At least four times a year there are popular elections held in Switzerland on national, cantonal and communal levels, for which currently remote electronic voting is seen as a viable option.

Establishing public trust, in the form of political trust (see section 3.2), such as confidence in parliament, is essential prior to the deployment of e-voting. Without such confidence and trust, there is a potential for political and public unrest. Public trust can be fostered through transparency and openness of all aspects of the electoral system and by implementing the various recommendations and guidelines which have been developed by international organisations such as the Council of Europe and OSCE/ODIHR (Caarls, 2010).

Political official attitude towards e-government and overall technological progress is decisive for the success of electronic voting, as such a system cannot be dealt with as a single one-off solution. A country's technological progression and overall macroeconomic investment in ICT infrastructure, has to play a highly crucial role in the political agenda, for the enablement of electronic voting to be accepted. A good communications infrastructure, voters' high e-readiness, the widespread use of the national ID cards, have all been decisive prerequisites in countries that have successfully implemented electronic voting systems, such as Estonia.

In (Robert Krimmer & Schuster, 2008) considering the political factors that can determine the implementation of electronic voting from a political perspective, the issues bellow were identified.

- Stateness, the circumstances or condition of the state at any given time
- State of Rule of law. The rule of law implies that government authority may only exercise rights in accordance with written laws, which were adopted through an established procedure. The principle is intended to be a safeguard against arbitrary rulings in individual cases.
- Stability of democratic institutions
- Election system and election turnout
- Political participation. The general level of participation in a society is the extent to which the people as a whole are active in politics

But also evaluating the information society determinants to electronic voting in "national context" as,

- Status of registers
- Status of e-Government infrastructure
- Digital net infrastructure
- Prices for the entrance to information and communication service and for the use of services
- Diffusion of information and communication services
- Expenditures for information technologies and information and communication referred
- Availability of e-government services
- Transaction penetration
- Degree of the informatization in the public administration and of administrative expirations

It is also necessary to view the effect that the introduction of electronic voting could have on political processes. E-government is not simply about electronic service delivery or

information provision, but active participation and "using ICT to transform the structures, operations and, most importantly, the culture of government" (OECD 2003, p. 17; c.f. Stewart-Weeks 2004). Deliberative democracy is defined as "a form of government in which free and equal citizens justify decisions in a process in which they give one another reasons that are mutually acceptable and generally accessible" (Gutmann and Thompson 2003, p. 7). Its significance to the online environment lies in the possibility to pioneer ICT applications that enable movement beyond managerial models of e-government, towards more participatory modes that "conceive of a more complex, horizontal and multi-directional interactivity" (Chadwick and May 2003, p. 280).

Whether this can be effectively initiated by governments seeking to reform and open up their own decision-making practices, or is best pursued by non-government organisations (NGOs) that utilise the networked environment to better make demands upon governments, remains an open question. (Flew & G. Young, 2005)

3.5 Functional Requirements

An election can be subdivided into three separate stages, Election Initialisation, the Voting Stage and the Ballot Counting stage. In an electronic voting system these can be interpreted to a number of functional requirements in accordance to the pre-identified election stages. Functional requirements are requirements that describe the systems behaviour or function. These are described in the following sections (Ikonomopoulos, Labrinoudakis, Dimitris Gritzalis, Kokolakis, & Vassiliou, 2002).

3.5.1 Election initialisation

Election initialisation: During this phase elections need to be set up and parametrised. Authorities of the polling stations are to check whether the ballot box is empty, verify the validity of the voters' registry list and of the candidates to the posts, and seal the ballot box

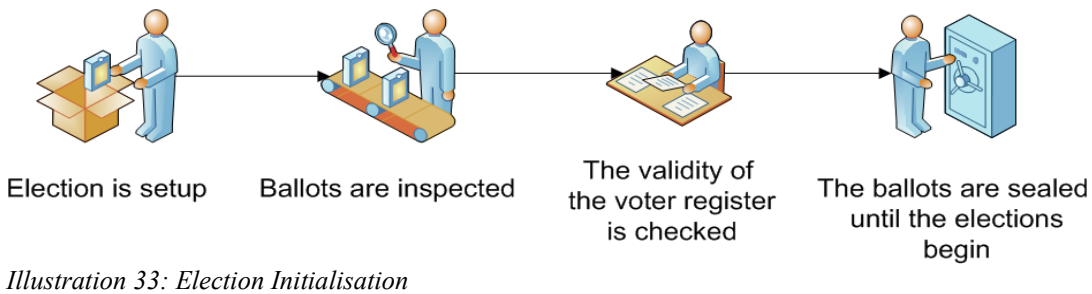

Illustration 33: Election Initialisation

- **Definition of Election Districts**: This process is more or less independent of a specific election. It is performed before the beginning of the election, in order to define the districts and the corresponding number of candidates that will be represented in the government - according to the number of respective electors. According to the distribution of the population the state employees define the election districts for the current election.
- **Candidate registration**: The process permitting an individual to register his/her interest in running as a candidate for an election.
- **Ballot creation**: This process starts after elections districts have been defined. Each party provides a discrete ballot format and a list of representatives per election district. The state creates the ballots and supplies them to all election centres. The steps taken for realizing the use case are:

  a) Each party representative provides the state with the list of candidates per election district and the ballot format for the party.

  b) The state employees create the ballots per eligible district and provide election centres personnel, as well as all authorities responsible for the election process, with them.
- **Ballot Distribution**: The process of distributing ballots to legitimate voters to cast their ballot.
- **Voter Registration**: The process within which a voter registers for an election.
- **Credential Creation**: The process within which authentication credentials are generated for a legitimate voter.
- **Credential Distribution**: The process in which authentication credentials are delivered to voter.
- **Credential management:** The process which allows for the management of credentials, I.e. creation, deletion, revocation etc

3.5.2 The voting Stage

The Voting stage, during which the authorities must check the identity of the voters, their correspondence with the voters' registry lists, and make sure, one is able to cast a vote and that he/she has successfully completed the process.

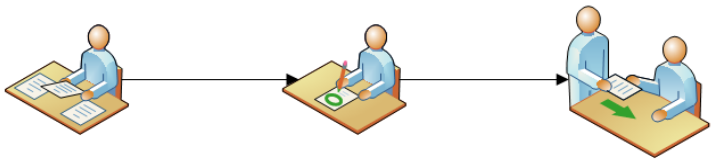

Illustration 34: Voting Stage

- **Vote Casting**: This process is performed after voter authentication has been successfully completed. S/he casts her/his vote, in a way that protects secrecy, and the authorised individual records are updated. The process involves the election centre supervisor and the elector and is performed as follows:

  a) The authorised election centre supervisor provides the elector with all ballots for the corresponding election district. He ensures that the sequence of the ballots is random for each elector in order to avoid favouring a specific party. Party representatives supervise this step to verify both expectations.

  b) The voter recedes in a private area of the centre and chooses one ballot as his vote. The vote is cast in such a way that its contents are concealed.

  c) The election centre personnel update the participation records.

  d) A receipt, confirming that the voter has voted, is provided.

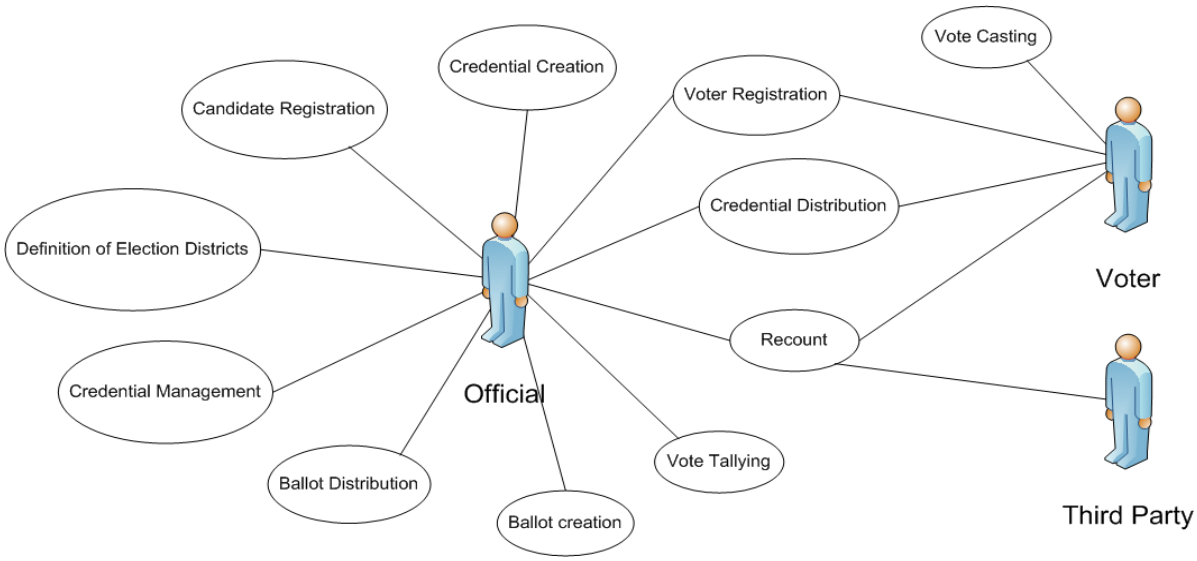

Illustration 35: UML Use Case of functional requirements for electronic voting

3.5.3 Counting of ballots

Counting of ballots, is to be carried out once the vote casting phase is complete. During this phase the authorities of the balloting station must proceed with the opening of the ballot box, the scrutiny of the votes, the systemization of the results, and the issuing of a closing act, which is generally informed to the corresponding computing centre.

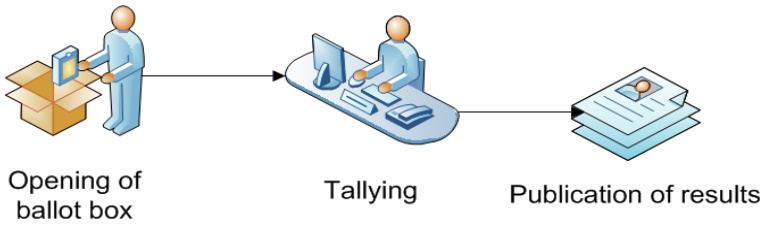

Illustration 36: Counting of Ballots

- **Tallying**: This process is performed to validate votes and determine the number of votes each participating party has received, along with not valid votes. The process takes place after the end of the election, in every election centre, and finishes when all votes have been directly validated and tallied by the election centre personnel:

  a) The supervisor, with the help of the election centre staff and under the supervision of parties' representatives, opens and validates each vote.

  b) Valid votes are counted and added to the results of the election centre.

  c) After all votes have been tallied, their number is compared to the number of electors who have cast a vote at the election centre.

  d) The result is forwarded to the appointed state authority and added to the election poll.

- **Recount**: The electronic voting system must be able to perform a recount if requested

3.6 Generic Requirements

In addition to these functional requirements an electronic voting system needs to exhibit a number of system wide properties, these can be included in the design system phase as generic requirements(Tsekmezoglou & Iliadis, 2005).

- **Scalability** indicating a systems ability to meet rising demands while maintaining performance level.
- **Transparency** an electronic voting system is necessary to be treated as a white box or

open system

- **Flexibility** A system is flexible if it allows a variety of ballot question formats including open-ended questions, is compatible with a variety of standards platforms and technologies, is accessible to people with disabilities.
- **Mobility** a system is mobile if there are no restrictions(other than logistical ones) on the location from which a voter can cast a vote, therefore enabling voters to cast their vote from any geographical location.
- **Reliability**: Reliability is often related to availability, but is a slightly different concept. Reliability can be considered as having two aspects; hardware and software reliability. **Hardware reliability-**Reliability engineering involves all aspects of design, development, and fabrication that minimize the chance of equipment breakdown. The success of complex missions such as space probes depends heavily on reliability engineering, since the failure of a single component, such as an O-ring on a space shuttle, can result and has resulted in total loss of the system. *Software reliability* is defined as the probability that a software fault that causes deviations from the required output by more than a specified tolerance, in a specified environment, does not occur during a specified exposure period
- **Robustness,** the ability of a computer system to cope with errors during execution or the ability of an algorithm to continue to operate despite abnormalities in input, calculations, etc.

3.7 Trusted Information Systems

A critical requisite for electronic voting relates to trust. In a traditional election, a citizen performing his electoral duties does not have any oversight of the actual processes that occurs after leaving the voting booth, but the voter is able to trust the electoral process, as he believes and understands that during this process, all measures are taken to protect the confidentiality, integrity and availability of his vote. Trusting the voting process is particularly difficult, because it requires a public audit of a process, which must ensure a significant amount of secrecy (Adida, 2006). Any attempt to maintain a bidirectional on-line association between voter and votes cast is suspicious, because of the inability to protect such information in this environment. This secrecy cannot be guaranteed by trusting an all-powerful third party: even the auditors cannot be made aware of how individual citizens vote.

E-voting procedures are highly complex, involving algorithms, cryptography and a number of technologies that the average voter does not comprehend and does not trust. One of the central themes that participants of the third meeting to review developments in the field of e-voting at the council of Europe concentrated on was the matter of trust and confidence in e-Voting. Over the years, it has become clear that e-voting systems cannot be introduced unless citizens trust their political and administrative systems (Caarls, 2010). The FFD participants were fairly unanimous on the conditions for implementing e-voting: system robustness and reliability, security, efficiency, transparency and accessibility, verifiability. A combination of all these conditions would create a climate of trust around a system which the citizens regard as complex, impenetrable and highly technical, and over which all the players involved have the feeling of losing all control to private organisations. (GENERAL, AND, AFFAIRS, & INSTITUTIONS, 2009). Therefore, in e-voting much more trust in the technology used and the persons involved (election officials, technology providers, etc.) is required by the voters(D Gritzalis, 2002).

Trust is not a new research topic in computer science, spanning areas as diverse as security and access control in computer networks, reliability in distributed systems, game theory and agent systems, and policies for decision making under uncertainty (Artz & Gil, 2007). Perhaps the most notable example was the development of the Trusted Computer System Evaluation Criteria (TCSEC) (DOD. 5200.28-SD) in the late 70s and early 80s. Here, trust was used in the process of convincing the observers that a system (model, design or implementation) was correct and secure (Nagarajan & Varadharajan, 2011).

The concept of trust, adjusted to the case of two parties involved in a transaction, can be described as follows:

"Trust occurs when parties holding certain favourable perceptions of each other allow this relationship to reach the expected outcomes" (Wheeless and Grotz 1977, 251).

A trusting person, group or institution will be *"freed from worry and the need to monitor the other party's behaviour, partially or entirely"* (Levi and Stoker 2000, 496).

"An entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required" (DOD. 5200.28-SD)

Therefore, an entity can be considered trustworthy, if the parties or people involved in transactions with that entity rely on its credibility. In general, the concept described above can be verbally represented by the term reliability, which refers to the quality of a person or entity

that is worthy of trust. Trust in the information society is built on various different grounds, based on calculus, on knowledge or on social reasons (Lekkas, 2003). The notion of trust in an organisation could be defined as the customer's certainty that the organisation is capable of providing the required services accurately and infallibly. A certainty which also expresses the customer's faith in its moral integrity, in the soundness of its operation, in the effectiveness of its security mechanisms, in its expertise and in its abidance by all regulations and laws, while at the same time, it also contains the acknowledgement of a minimum risk factor, by the relying party. The notion of security refers to a given situation where all possible risks are either eliminated or brought to an absolute minimum (Giddens, 1991).

Exorcising complexity, trust is in effect a matter of e-voting security and transparency. De-constructing the perception of trust, within the context of e-voting IS systems, leads to forming a framework for generating and maintaining the necessary properties which lead to establishing trust. Essentially, software is believed to be "trusted", if the source code has been rigorously developed and analysed, giving us reason to believe that the code does what it is expected to do and nothing more.

A trusted system involves the characteristics (Pfleeger, 2006):

- *Functional correctness*: the program does what it is expected to do and it works correctly
- *Enforcement of integrity*: even if presented erroneous commands or commands from unauthorized users, the program maintains the correctness of the data with which it has contact
- *Limited Privilege*: the program is allowed to access secure data, but the access is minimized and neither the access rights nor the data are passed along to other untrusted programs or back to an untrusted caller.
- *Appropriate confidence level:* The program has been examined and rated to a degree of trust appropriate for the kind of data and environment in which it is to be used.

Building upon this concept, within the boundaries of electronic voting, a trusted IS needs to address the issues of:

- Ensuring that the voter is provided with the means to cast his or her vote.
- Ensuring that the voter is prevented from casting more than one valid vote.

- Ensuring that the cast ballot is confidential in the sense of not being linked to the voter who cast it.
- Ensuring that the vote may not be changed or faked.
- Ensuring that votes are not lost.
- Ensuring that no votes are entered which have not been cast by authorized voters.

These principles are building blocks for the definition of security in electronic voting. From these stem a number of specific requirements that an electronic voting system needs to address/exhibit in order to be secure. The security aspect in the context of the electoral process is referred to as one of the most important constraints in the adoption of electronic voting systems. The Caltech-MIT Voting Technology Project states: "Security is as important as reliability in guaranteeing the integrity of the voting process and public confidence in the system. Losing confidence in elections, means losing confidence in our system of government." (MIT, 2001). As security is identified as the main barrier to the wide deployment of electronic voting IS, the notion of security is investigated within this context.

3.8 Security

Information security essentially means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction {Document not in library: (44 U.S.C. § 3542, n d)}. The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are often interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer{Document not in library: (Wikipedia, 2010)}

Security is correlated to the important aspects of confidentiality, integrity and availability, they thus become building blocks to be used in designing secure systems.

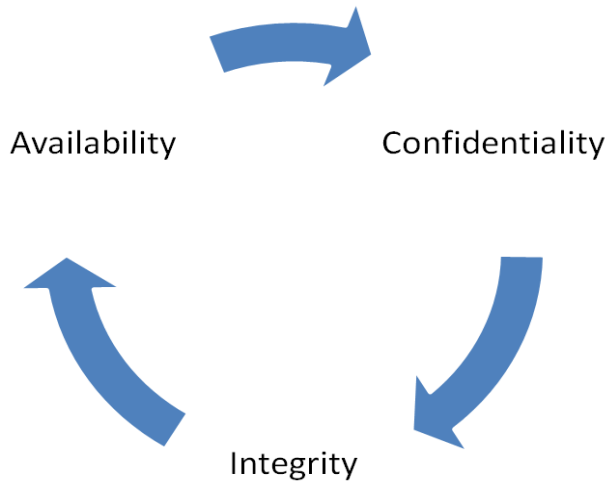

Illustration 37: Building Blocks of IS Security: Confidentiality, Integrity and Availability

These important aspects of security, apply to the three broad categories of assets which are necessary to be secured, data, software and hardware resources(NIST IR 7298).

- **integrity**, which means guarding against improper information modification or destruction, and includes ensuring information **non-repudiation** and **authenticity**;
- **confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- **availability**, which means ensuring timely and reliable access to, and use of information.

A system is insecure if an attacker is able to exploit a vulnerability and compromise assets integrity.

*A **vulnerability** is a weakness in an IS system that can be **exploited** by an attacker interested in **penetrating** a system.*

*A v**ulnerability** can be exploited to threaten an **assets value**.*

*IS security blocks **threats** on a system by **controlling** a vulnerability; this is a defensive measure that reduces or eliminates a given vulnerability.*

Essentially securing an Information System (IS), involves identifying unique threats and challenges which need to be addressed by implementing the appropriate countermeasures. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process, to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent

system requirements (e.g., reliability, maintainability, supportability){Document not in library: (NIST 800-60, 2008)}. This is also referred to as risk management; *"the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization"{Document not in library: (ISACA, 2006)}*.

Security is a multidimensional notion in the context of e-voting. It primarily refers to the respect of secrecy and freedom, but in reality it covers the entire range of functions and election components such as registration, eligibility and authentication. (Lilian Mitrou, Dimitris Gritzalis, Sokratis Katsikas, & Quirchmayr, 2003). Security aims at protecting the integrity, generality, equality , freedom, secrecy and fairness of elections. Crucial to the success of such a system are the decisions made on system characteristics and elements. Beforehand selections, must guide design though the implementation of the identified technologies. Following an Information Systems security approach in the following sections, we shall primarily identify threats on an e-voting systems and then evaluate controls that intended to mitigate or eliminate these risks.

3.9 Identification of threats

Risk occurs when assets are vulnerable to threats. To minimize these threats countermeasures are employed. A security countermeasure refers to a way to detecting, preventing, or minimizing losses associated with a specific IS threat. Threats frequently are categorized according to the type of assets involved.

The definition of a threat contains {Document not in library: (C. Pfleeger & S. Pfleeger, 200}6)

- Threat agents; such as hackers, users, computer processes, development personnel, administrators, and accidents. Further, a threat agent can be described by its expertise, resources, and opportunity.
- Assets, which are violated; such as file content, content of server, or the authenticity of votes cast.
- Averse actions, that is, influencing of one or more properties of an asset
- The attacker's motivation to attack the system; such as transferring unauthorised

money to his account or getting knowledge about the money transfers of popular people.

- The exploited flaw, such as the server configuration or the communication.

Within the context of electronic elections, the following assets have to be protected(Melanie Volkamer, 2009):

- The Authentication data
- The Identification data
- The Ballot
- The Vote
- The Confirmation data
- The Election data
- The Polling phase data
- The Audit records
- The Result
- The infrastructure itself

A system, grabbing the media's attention and of grave importance as an electronic voting system attracts a wide spectrum of threats of vast importance. An attacker must have three things (C. Pfleeger & S. Pfleeger, 2006):

- Motive: the reason to want to perform an attack
- Opportunity: the time and access to complete an attack
- Method: the skills knowledge and tools necessary to complete an attack

Attacks on an electronic voting system can be categorized according to motive; such are publicity attacks, profit attacks, terrorist attacks and attacks which are motivated by creating instability in current government/democracy, Illustration 38

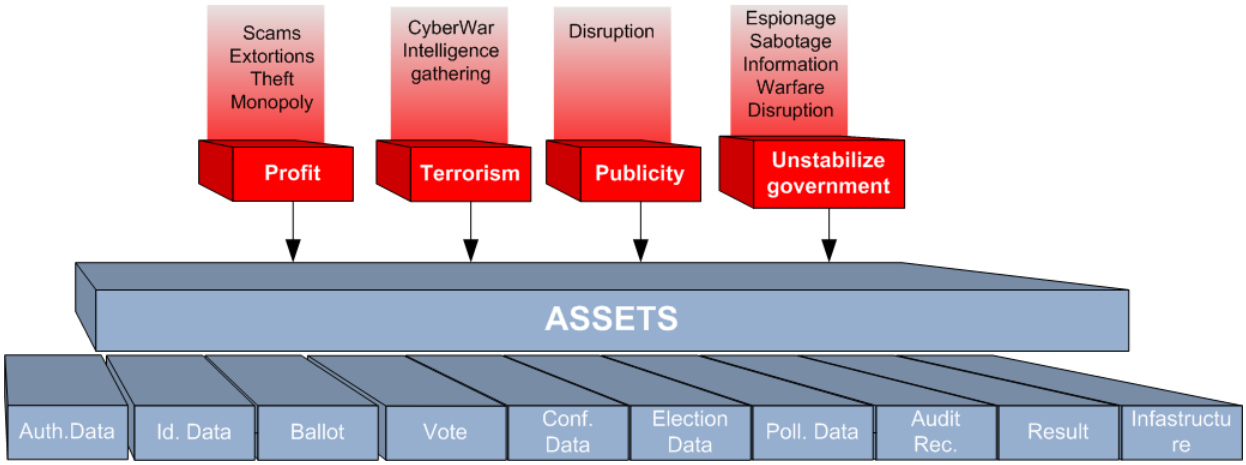

Illustration 38: Categorized Threats to e-voting assets according to motive

Pin pointing expected attacker's profiles, confirms the importance of efficient security characteristics necessary for an information system of such scale. E-Voting needs to be secured from the voters, election officials, programmers, technicians and system administrators (Jones, 2004). The threats posed could be internal e.g. the vendor, election officials. Or they could be external such as individuals, well funded agencies, states, parties, criminals, terrorists, many of whom cannot even be prosecuted (Jefferson, 2004) (Svensson, 2003) (A.Ballas, 2006). The motives of the attackers range from publicity (Mayniham, 2004), to foreign intelligence and terrorist acts (Philips, 2001),to governments manipulating the system for their benefit (Mercuri, 2004),(illustration 39).

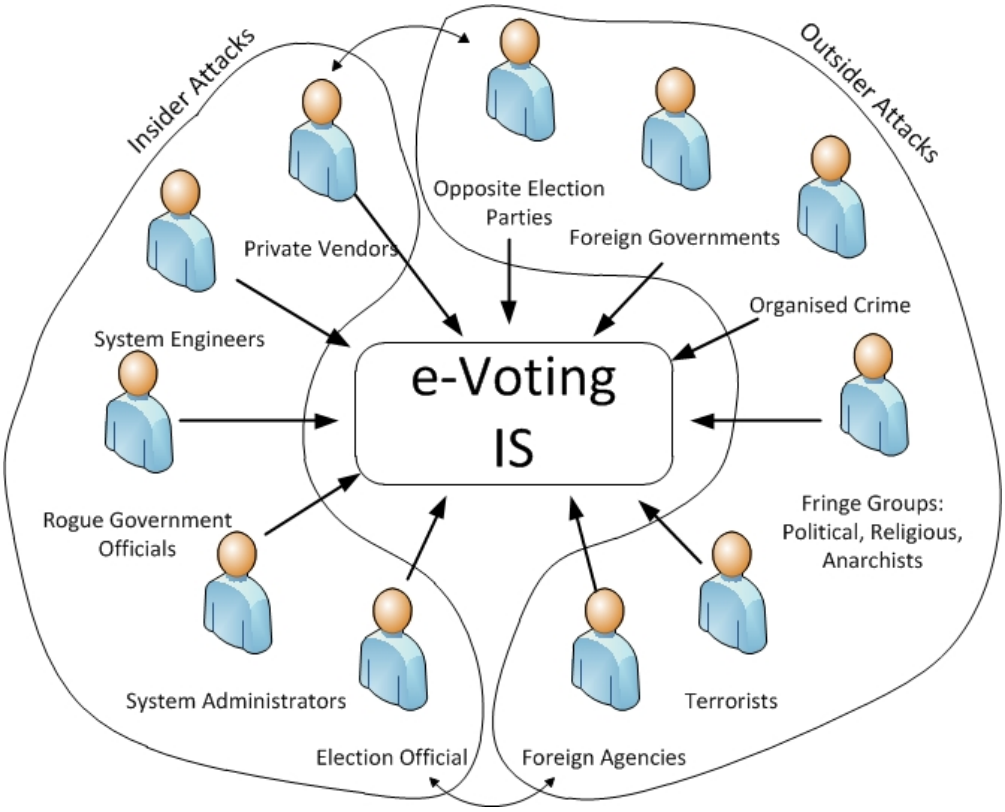

Illustration 39: e-Voting threat agents

An electronic voting system, publicly accessible over the Internet, gives the attacker the opportunity to attack the system at any time. Electronic voting systems are high risk targets attracting a plethora of attacks over a long time period. The E-Government Act 2002, [entitled the Federal Information Security Management Act of 2002 (FISMA)], tasked NIST with responsibilities for standards and guidelines, including the development of guidelines, recommending the types of information and information systems to be included in each category; and minimum information security requirements (i.e., management, operational, and technical controls), for information and information systems, in each such category(FIPS Publication 199) . E-voting can accordingly be classified as a high impact system[5],

Security Categorization={ *(***Confidentiality***, High), (***Integrity***, High), (***Availability***, High)*} information system. In the following section we shall review the methods that can be employed by an attacker to diminish each of these desirable properties.

3.10 e-Voting Security

Information Systems can be decomposed in three main portions, hardware, software and

5The *potential impact* is **HIGH** if—
− The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

communications with the purpose to identify specific threats and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers. There is continuous debate about extending this set to include additional qualities such as accountability, authenticity and legality . As the legal perspective towards electronic voting has been extensively covered in the previous section, this chapter shall view electronic voting security through the principles of confidentiality, integrity, availability, accountability and authenticity. This section adopts an Information Security methodology to electronic voting.

3.10.1 Availability

Availability refers to the property of a system being accessible and usable upon demand by an authorized entity. System availability includes a systems ability to carry on operations even when some authorities misbehave. The system must have the ability to continue operations even in the possibility of a security breach. In the context of electronic voting systems, this property refers to legitimate voters provided with the means to cast their vote. Safeguarding this security requirement, denotes implementing the technological solutions to protect the system against network attacks, which would make the system unavailable to end users. Such attacks include:

- Distributed Denial Of Service(DDOS)
- Connection Flooding
- Traffic Redirection
- Hardware based attack

3.10.2 Confidentiality

Confidentiality refers to only authorized parties or systems having the ability to access protected data. In the context of elections, it refers to data and voter preferences remaining private. An election is private, if neither the election authorities nor anyone else can link any ballot to the voter who cast it, and no voter can prove that he or she voted in a particular way.

It is crucial to protect an electronic election from:

- Eavesdropping
- Wiretapping
- Misdelivery
- Exposure within the network
- Traffic flow analysis

- Vulnerabilities
  - *Hardware*
    - Modification
    - Substitution
    - Interception
  - *Software*
    - Software Deletion
    - Software modification
    - Trapdoors
    - EasterEggs
    - Logic bombs
    - Information leaks
    - Virus
    - Trojan horse

3.10.3 Integrity

Integrity refers to data and system precision, accuracy and consistency. Votes must be recorded correctly and safeguards must ensure that votes cannot be modified, forged or deleted, without detection. In elections, all data involved in entering and tabulating votes must be tamper-proof. Reliability is fundamental as it means that an election system should work robustly, without loss of any votes and therefore be trustworthy and accurate. Integrity refers to the system, data and additionally to personnel. People involved in developing, operating, and administering electronic voting systems must be of unquestioned integrity. Integrity refers to protecting the system against:

- Wiretapping
- Impersonation
- Falsification of messages
- Web defacement Spoofing
- DNS attack
- Malicious code on client
- Vulnerabilities
  - **Hardware**
    - Modification

- Substitution
- Interception

- **Software**
  - Software Deletion
  - Software modification
  - Trapdoors
  - EasterEggs
  - Logic bombs
  - Information leaks
  - Virus
  - Trojan horse

3.10.4 Authenticity

Authenticity refers to ensuring that the involved data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are. In elections it is vital that only registered voters are permitted to cast a vote. The voting counts must be protected from external reading during the voting process. Voter identity and preferences must be secret. Authenticity refers to protecting the system against:

- Impersonation
- Guessing
- Eavesdropping
- Spoofing
- Session hijacking
- Man in the middle *Replay attacks*

3.10.5 Accountability

Accountability refers to information, selectively kept and protected, so that actions affecting security can be traced to the responsible party (audit). Corrupt voters or personnel, may attempt to modify votes/count or the system. Applicable to accountability is system disclosability, which refers to system software, hardware, microcode, and any custom circuitry being open for random inspection at any time (including documentation), despite cries for

secrecy from the system vendors. The property of permitting an external auditing entity to verify that the votes have been counted correctly and a voter to determine if a vote was counted correctly, is crucial.

Accountability refers to protecting the system against

- **Hardware**
  - Modification
  - Substitution
  - Interception
- **Software**
  - Software Deletion
  - Software modification
    - Trapdoors
    - EasterEggs
    - Logic bombs
    - Information leaks
    - Virus
  - Software theft
- All internal operations must be monitored, without violating voter confidentiality. Monitoring must include votes recorded and votes tabulated, and all system programming and administrative operations such as pre- and post-election testing. All attempted and successful changes to configuration status (especially those in violation of the static system integrity requirement) must be noted.
- Monitoring and analysis of audit trails must themselves be nontamperable. All operator authentication operations must be logged.

In detail, availability, confidentiality, integrity, authenticity and accountability refer to safeguarding a system against the threats listed below (Table 8):

	Availability	Confidentiality	Integrity	Authenticity	Accountability
Connection Flooding	x				
DDOS	x				
DNS attack	x		x		
Eavesdropping		x		x	
Exposure within network		x			
Falsification of messages			x		
Hardware interception	x	x	x		x
Hardware modification	x	x	x		x
Hardware substitution	x	x	x		x
Impersonation/ Spoofing			x	x	
Malicious code on client		x	x		
Man in the middle-Replay				xx	
Misdelivery		x			
Software modification					
• EasterEggs		x	x		x
• Information leaks		x	x		x
• Logic bombs		x	x		x
• Trojan horse		x	x		x
• Virus		x	x		x
• Trapdoors		x	x		x
Session Hijacking				x	
Software Deletion		x	x		
Software Theft		x			x
Traffic flow analysis		x			
Traffic Redirection	x			x	
Wiretapping		x	x		

Table 8: List of threats against Availability, Confidentiality, Integrity, Authenticity, Accountability

3.10.6 Security Requirements

The identification of unique threats and challenges leads to the development of a complete set of electronic voting security requirements, which need to be addressed with appropriate countermeasures. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process, to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability).

In the following section security requirements are identified. In this document, requirements have been covered from the sources stated bellow, (Volkhamer, The German Regulations for Electronic Voting Machines,) The recommendations of the Council of Europe, The "Online-Voting Systems for Non-parliamentary Election" catalogue developed by the Physikalisch-Technische Bundesanstalt (PTB – Department of Metrological Information Technology in the National Metrology Institute), (D Gritzalis, 2002b)

3.10.6.1 Security Requirements for the polling phase of elections

1. The remote electronic voting system shall unambiguously identify and authenticate the voter before storing his vote in the e-ballot box.
2. The remote electronic voting system shall store in the e-ballot box only e-votes cast from eligible voters. Any other access to the e-ballot box shall be denied.
3. The remote electronic voting system shall ensure the data protection law with respect to the transmission of any personal data.
4. The remote electronic voting system shall protect the confidentiality of the transmitted authentication information.
5. The remote electronic voting system shall ensure the confidentiality of the transmitted e-votes during the polling phase.
6. The remote electronic voting system shall ensure that protocol messages cannot be deleted undetected.
7. The remote electronic voting system shall verify the freshness, authenticity, integrity, and format correctness of all messages before processing them.
8. The remote electronic voting system shall delete any records related to the voter's voting process from the vote-casting device when finishing the voting process.
9. The remote electronic voting system shall not provide any information in the transmitted protocol messages, which allows to construct the link between a particular voterand his vote.
10. The remote electronic voting system shall ensure that neither the vote itself nor the number of chosen voting options (including an empty ballot), nor a spoilt vote (for

example,by using the length of the protocol messages) can be linked to a particular voter. In addition, it shall be ensured that the sequence of messages does not reveal the link.

11. The remote electronic voting system shall ensure that voters are not able to construct a receipt proving their vote. Neither information sent to, displayed on, sent from, nor intermediate results calculated on his vote-casting device or protocol messages sequences shall serve as proof

3.10.6.2 Security Requirements for the Tallying Phase

1. The voting server shall protect the integrity and authenticity of e-votes after the polling phase.
2. The tallying software shall verify the integrity and authenticity of e-votes.
3. The tallying software shall protect the integrity and authenticity of election data as soon as the tallying is completed.
4. The tallying software shall ensure that its operations and data are unaffected by other applications.

3.10.6.3 Security Requirements for the Voting Server

1. The voting server shall communicate only with the authentic and unaltered client-side voting software.
2. The voting server should be tamper-resistant and tamper-evident.
3. The voting server shall implement an access control policy for the poll worker interface which
    1. restricts all activities to particular user-roles and
    2. requires physical presence.
4. The voting server should not store any information which could link the voter with his vote after the completion of the voting process. Where any information which could link the voter to his vote is stored on the voting server, it shall only be accessible to those with appropriate authority.
5. Plans should clearly define full recovery in case of security breach or

system failure.

3.10.6.4 Security Requirements on the Client-Side

1. The client-side voting software shall ensure that its operations and data are unaffected by other applications running on the vote-casting device.
2. The client-side voting software shall only communicate with the authentic and unaltered voting server.
3. The client-side voting software shall protect the voter from influence during voting

3.10.6.5 Operational Security Requirements for the Remote Electronic Voting System

1. The remote electronic voting system shall ensure that no voter loses his voting right without having cast a vote.
2. The remote electronic voting system shall prevent voter interactions in case of exceptions and malfunctions.
3. The remote electronic voting system shall provide a confirmation to the voter regarding the status of his vote – at least the information that his e-vote has been successfully stored.
4. The remote electronic voting system shall provide feedback to the poll workers in form of error messages in case of exceptions, malfunctions, and breakdowns. Where a voter is in the voting process at that time he shall also get a feedback.
5. The remote electronic voting system shall prevent data loss during normal operations and in case of exceptions, malfunctions, and breakdowns.
6. The remote electronic voting system should be available during the whole polling phase.
7. The remote electronic voting system shall be robust against power outage at the voting server, unexpected user activity, environmental effects (for instance, mechanical, electromagnetic, and climatic) to the voting server, and network problems.
8. The remote electronic voting system shall ensure that in case of exceptions, malfunctions, and breakdowns no voter loses his right to cast a vote nor get the

possibility to cast two votes.

9. The remote electronic voting system shall be capable to determine whether a particular voter cast a vote and his e-vote was successfully stored in case of exceptions, malfunctions, and breakdowns.
10. The remote electronic voting system shall be capable of resuming operations without a disruption of services after a security failure
11. all IT systems shall have a continuity of operations plan prepared in the event of loss or failure

3.10.6.6 Functional Requirements for the Voting Server

1. The access control mechanism shall only allow access to the voting server if at least two different users are logged on.
2. The voting server shall be capable of producing comprehensive audit data.
3. The voting server shall indicate to the poll worker
    1. the number of votes cast so far and
    2. its current state.
4. The voting server shall store in the e-ballot box all e-votes cast by eligible voters during the polling phase
5. The poll worker interface shall warn the poll workers if they try to close the election before the final date.
6. The voting server shall not provide any information about the voting process except the current state and the number of votes cast so far.
7. The voting server should regularly perform automatic self-checks and report the results to the poll workers
8. The voting server shall be capable of performing self-checks.
9. The voting server shall run a self-check before a resuming is possible. In case of irreversible problems the voting server shall prevent a resuming of the polling phase.

The only functionality provided by the poll worker interface is

- identification and authentication,
- starting the polling phase which is only possible once,
- resuming the polling phase after any kind of exceptions, malfunctions, and breakdowns,
- closing the polling phase after which the actions 'starting' and 'resuming' are disabled,
- starting the tallying phase only after having closed the polling phase,
- performing self-checks,
- checking that the voting server has been set up correctly
- checking the current state according to and
- reading the audit trails.

10. The voting server shall not provide any functionality to reach any of the intruder's goals
11. In case of exceptions, malfunctions, and breakdowns, the voting server shall not reveal the link from the last voter to his selections or vote.
12. The acceptance of e-votes into the e-ballot box should remain open for a sufficient phase of time to allow for any delay of data transport.
13. The voting server shall be capable of recording an adequate number of votes.
14. The voting server shall support an adequate number of voting options.

3.10.6.7 Functional Requirements for the Client-Side Voting Software

1. The client-side voting software shall provide the following functionality for the voter:
    - Identification and authentication
    - Make a choice on the ballot

- Change selections before casting a vote
- Initialise vote casting
- Vote casting
- Cancel his voting process at any time
- The voting server shall accurately display the authentic and unaltered ballot.

2. The client-side voting software shall immediately transmit the e-votes to the voting server, whenever a voter has cast his vote.
3. The client-side voting software should provide the functionality for the voter to spoil his vote.
4. The client-side voting software should warn the voter when he tries to spoil his vote in one or more polls.
5. The client-side voting software shall ensure equality and accuracy of presentation of voting options on any vote-casting device.
6. The remote electronic voting system shall avoid the display of other influencing messages.
7. The client-side voting software shall ensure that the voter's selections are accurately represented in the e-vote.
8. The client-side voting software should be compatible with any vote-casting device and with devices used by people with disabilities where appropriate.

3.10.6.8 Functional Requirements for the Tallying Phase

1. The remote electronic voting system shall provide the functionality to upload e-votes into any tallying software.
2. The voting server shall provide the functionality to completely delete all data from previous elections.
3. The tallying software shall accurately calculate results using the appropriate algorithm based on all (authorised) evotes stored in the e-ballot box and only based

on these e-votes.

3.10.6.9 Functional Requirements for the Audit System

1. The audit system shall provide the functionality to record, monitor, and verify audit data.
2. The audit system shall protect the integrity and authenticity of audit records.
3. The audit system shall have access to a reliable time source.
4. The audit system shall record system configuration (including software version numbers) and election configuration (including voting option information) on the voting server at least at the following points
    1. beginning and end of polling phase, as well as
    2. before and after tallying.
5. The audit system shall check the e-ballot box, the ballot content, and the authentication data for evidence of tampering.
6. The audit system and its records should be tamper-resistant and shall be tamper-evident.
7. For every action performed by poll workers the audit system shall record
    - a timestamp,
    - the nature of the action, and
    - the ID of the particular poll worker(where available).
8. The audit system shall record (with timestamps, where appropriate)
    - breakdowns,
    - exceptions,
    - malfunctions, and
    - results of any self-checks.
9. The audit system shall record all security incidents and attempt to store information about these.

10. The audit system shall implement the access control policy defined by the responsible election authority.
11. The audit system should not record any information which might endanger the secrecy of the vote. Where such information is stored it shall only be accessible to those with appropriate authority.
12. The audit system shall ensure the data protection law.

3.11 Chapter Summary & Conclusions

This chapter, explores the complexity of electronic voting and attempts to shed light on the perplexities of its implementation. As a number of affecting fields operate in concert, to structure what is perceived as the dimensions of electronic voting, a multidisciplinary approach is employed to identify and define the true dimensions and implications involved in the adoption and development of an optimal information system. In this section, electronic voting is viewed through the perspective of four separate dimensions, sociological, legal, political and finally technical. Each of these approaches leads to the identification of a set of requirements from which stem the design guidelines and principles for an electronic voting system. It is evident that for electronic voting to be designed and deployed successfully, a long list of multidisciplinary requirements must be fulfilled.

As the security aspect in the context of the electoral process is referred to as one of the most important constraints in the adoption of electronic voting systems, we adopt an Information Systems Security approach to identify the needs of such a complex IS. An Information Systems Security methodology can be decomposed into three main aspects, hardware, software and communications, with the purpose of identifying specific threats on assets and applying information security mechanisms of protection and prevention, at the three levels or layers. The documentation of a complete set of requirements leads to the identification of specific design principles and recommendations of considerations that can assist in reducing these threats and vulnerabilities. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability)(NIST, SP800-60). In the following section we attempt to propose a number of specific design principles and recommendations of considerations that can assist in reducing these threats and vulnerabilities.

Chapter 4

Addressing the Security Requirements

4 ADDRESSING THE SECURITY REQUIREMENTS

Chapter Abstract: This chapter explores security controls that attempt to fulfill the predefined security requirements. A number of safeguards, including Public Key Infrastructure and cryptographic schemes are explored and evaluated as to their effectiveness to countering threats on electronic voting security. At the core of all security approaches lies authentication and identification. Towards securely authenticating interacting parties in electronic governance and electronic voting, the restrictions of current e-id approaches are explored, and leveraging the electronic passport PKI solution to meet the demands of an interoperable cross border e-id solution is examined.

4.1 Security Controls

Harm occurs when a threat is realized against a vulnerability. To protect against harm we seek to (Pfleeger & Pfleeger, 2006):

- prevent it- by blocking the attack or closing the vulnerability
- deter it- by making the attack harder ;but not impossible
- deflect it- by making another target more attractive
- detect it-either as it happens or some time after the fact
- recover from its effects

To achieve this a number of tools(also referred to as controls) are available(Pfleeger & Pfleeger, 2006):,

- **Encryption.** Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted can be transformed back into its original form by an authorized user, who possesses the cryptographic key(decryption). Encryption is a powerful tool for providing privacy, authenticity, integrity and limiting access to data. Encryption clearly addresses the need for confidentiality of data. Additionally, it can be used to ensure integrity; data that cannot be read generally cannot easily be changed in a

meaningful manner. Information and communication security often employs encryption, in the form of protocols, to ensure data security communicated across insecure networks. A protocol is an agreed-on sequence of actions, that leads to a desired result. For example, some operating system protocols ensure availability of resources as different tasks and users request them. Thus, encryption can also be thought of as supporting availability. In network applications, encryption can be applied between hosts(host to host or link encryption), or between applications (end to end).

- **Software Controls.** In addition to encryption, software controls are used to prevent attacks. Programs themselves must be secure enough to prevent outside attack. They must also be developed and maintained so that we can be confident of the programs' dependability.

Program controls include the following:

- internal program controls: parts of the program that enforce security restrictions, such as access limitations in a database management program;
- operating system and network system controls: limitations enforced by the operating system or network to protect each user from all other users;
- independent control programs: application programs, such as password checkers, intrusion detection utilities, or virus scanners, that protect against certain types of vulnerabilities;
- development controls: quality standards under which a program is designed, coded, tested, and maintained to prevent software faults from becoming exploitable vulnerabilities;

Software controls often affect the way the user interacts with an information system. Software controls must be designed in a way that does not diminish system usability. Ease of use and potency are often competing goals in the design of a collection of software controls.

- **Hardware Controls** Numerous hardware devices have been created to assist in

providing computer security. These devices include a variety of means, such as

- hardware or smart card implementations of encryption
- locks or cables limiting access or deterring theft
- devices to verify users' identities
- firewalls
- intrusion detection systems
- circuit boards that control access to storage media

- Policies and Procedures: Sometimes, we can rely on agreed-on procedures or policies among users, rather than enforcing security through hardware or software means. In fact, some of the simplest controls, such as frequent changes of passwords, can be achieved at essentially no cost, but with tremendous effect. Training and administration follow immediately after establishment of policies, to reinforce the importance of security policy and to ensure their proper use.
- Physical Controls: Some of the easiest, most effective, and least expensive controls are physical controls. Physical controls include locks on doors, guards at entry points, backup copies of important software and data, and physical site planning that reduces the risk of natural disasters.

A single security control is mostly inefficient, as no control can be considered a gold standard. A layered solution is able to control a plethora of vulnerabilities. Security mechanisms (defenses) need to be layered, so that compromise of a single security mechanism is insufficient to compromise an entire host or network; this is referred to as Defense in Depth.

Designing a secure information system should commit to a number of widely accepted principles (NIST 800-123) (Curtin & Neumann, 2001)(Saltzer & Schroeder., 1975)(Howard & LeBlanc, 2002)(Viega & McGraw, 2001):

- **Defense-in-Depth**—Employing a single security mechanism is generally insufficient. Security mechanisms (defences) need to be layered so that compromise of a single security mechanism is insufficient to compromise a host or network. No “silver bullet” exists for information system security.

- **Security through obscurity** should be avoided. Systems should be designed so that their security does not rely upon the secrecy of their design or implementation . The reason is simple; if the leak of information about how the system works can compromise its security, then the system is fragile.
- **Simplicity**—Security mechanisms (and information systems in general) should be as simple as possible. Complexity is at the root of many security issues. One factor in evaluating a system's security is its complexity. If the design, implementation, or security mechanisms are highly complex, then the likelihood of security vulnerabilities increases. Subtle problems in complex systems may be difficult to find, especially in copious amounts of code.
- **Fail-Safe**—If a failure occurs, the system should fail in a secure manner, i.e., security controls and settings remain in effect and are enforced. It is usually better to lose functionality rather than security.
- **Complete Mediation**—Rather than providing direct access to information, mediators that enforce access policy should be employed. Common examples of mediators include file system permissions, proxies, firewalls, and mail gateways.
- **Separation of Privilege**—A system should ensure that multiple conditions are met before granting permissions to an object. According to Saltzer and Schroeder "Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key." The relevance of this observation to computer systems was pointed out by R. Needham in 1973. The reason is that, once the mechanism is locked, the two keys can be physically separated and distinct programs, organizations, or individuals made responsible for them. From then on, no single accident, deception, or breach of trust is sufficient to compromise the protected information. This principle is often used in bank safe-deposit boxes(Barnum & Gegick, 2005a).
- **Least Privilege**—This principle dictates that each task, process, or user is granted the minimum rights required to perform a specific task. By applying this principle consistently, if a task, process, or user is compromised, the scope of damage is constrained to the limited resources available to the compromised entity.
- **Reluctance to Trust—**Developers should assume that the environment in which

their system resides is insecure. Trust, whether it is in external systems, code, people, etc., should always be closely held and never loosely given. When building an application, software engineers should anticipate malformed input from unknown users. Even if users are known, they are susceptible to social engineering attacks, making them potential threats to a system.

- **Compartmentalise—** Minimize the amount of damage that can be done to a system by breaking up the system into as few units as possible while still isolating code that has security privilege.
- **Weakest Link—** An information system is only as safe as its weakest link. According to Schneier in "Security Processes: **Secure the Weakest Link.** Spend your security budget securing the biggest problems and the largest vulnerabilities. Too often, computer security measures are like planting an enormous stake in the ground and hoping the enemy runs right into it. Try to build a broad palisade"(Schneier, 2000).
- **Least Common Mechanism—** Avoid having multiple subjects sharing mechanisms to grant access to a resource (Barnum & Gegick, 2005b). For example, serving an application on the Internet allows both attackers and users to gain access to the application. Sensitive information can potentially be shared between the subjects via the mechanism. A different mechanism (or instantiation of a mechanism) for each subject or class of subjects, can provide flexibility of access control among various users and prevent potential security violations, that would otherwise occur if only one mechanism was implemented.
- **Compromise Recording**—Records and logs should be maintained so that if a compromise does occur, evidence of the attack is available to the organization. This information can assist in securing the network and host after the compromise and aid in identifying the methods and exploits used by the attacker. This information can be used to better secure the host or network in the future.

Electronic voting systems are critical security systems, and security needs to address the plethora of requirements previously identified. The following chapters of this dissertation, attempt to propose a number of controls and countermeasures according to these principles, that fall in the above categories, that attempt to defend the principles of security in remote electronic voting. The following recommendations of controls can assist in reducing a number

of previously identified threats and vulnerabilities.

4.2 Strong Authentication is required

At the core of information system security, is access control. Access to protected information must be restricted to people who are authorized to access the information. Managing an entity's admittance and rights to specific enterprise resources, ensures that valuable data and services are not abused, misappropriated or stolen. By preventing unauthorized access, organizations can achieve greater confidence in data and system integrity. Additionally, such mechanisms offer greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity (accountability).

Electronic authentication, is the process of establishing confidence in a users identity, electronically presented to an information system. During this process, an entity provides an authentication authority with a number or set of attributes that allows for the unique identification of the entity. Authentication is often mistakenly correlated with authorization, which involves permitting an entity to perform a defined action or to use a defined service after an entity has been authenticated. E-authentication presents a technical challenge when this process involves the remote authentication of individual people over a network, for the purpose of electronic government and commerce (NIST). Authentication mechanisms use any of three types of attributes to confirm a user's identity.

- Something a user ***knows*** (including passwords, PIN numbers, pass-phrases and mother's maiden name etc.)
- Something a user ***has*** (identity badges, physical keys, a driver's license, etc.)
- Something a user ***is*** (these authenticators, called biometrics, are based on a physical characteristic of the user, such as a fingerprint, the pattern of a person's voice, or a face/picture).

Two or more forms can be combined for more solid (strong) authentication, referred to as ***multi-factor authentication***.

To deliver complete on-line services to citizens, business partners, employees, and other entities, governments need to strongly authenticate the identity of users who wish to conduct transactions involving sensitive information, such as financial or personal information(United States General Accounting Office, 2003). Strong authentication and identification of citizens

in electronic government interactions is a growing necessity, as an increasing amount of security critical processes are being digitalized. Information and communication security is vital to the success of these initiatives, as it attempts to guarantee the confidentiality, integrity and availability of implicated data and communications. Today the most common way to authenticate such transactions is by means of passwords, but more secure solutions protecting privacy are increasingly needed (MEMO/10/681, 2010) .

High risk threshold applications, such as electronic government services, require strong multifactor authentication to ensure protection of data and communications. This need is addressed by electronic IDentification (e-ID) systems. The purpose of eID systems is to provide the means to reliably identify and authenticate citizens remotely over the Internet (T. Zefferer (AT-TUG), 2010). An e-ID infrastructure is understood as an Authentication Framework, that enables individuals to access various e-services offered by government and non-governmental entities, using a single dedicated identity profile and making use of multi-factor authentication techniques.

In terms of STORK project "Electronic Identity" is defined as (Gutierrez & Piñuela, 2009):

[…] a collection of identity attributes in an electronic form.

These attributes specify characteristics, like a name, a membership, a role or any other information suitable to uniquely identify a person or a thing. These attributes are combined with smart card technology, digital signatures and a user's "knowledge" of a pin number to generate multifactor authentication. An e-ID infrastructure is as strong and as effective as the authentication services ability to correlate an entity's provided credentials with an entity's valid credentials. Identification is usually based on unique identifiers being stored on the issued eID card and used by online systems to recognize users. Smart cards contain small chips, providing complex operations allowing secure communication over secure channels, digital signature or on-chip key generation. Phone based solutions are sometimes used that use the mobile device as a proof of possession authentication factor in multi-factor environments A SIM card in a phone can be regarded as a smart card fully integrated with reader and display in combination with networking functions(Ivkovic, Keskel, Knall, Leitold, & Martens, 2009).

The development of e-ID infrastructures varies considerably across Europe. From 2000 onwards, a number of countries have implemented e-ID card projects, with Italy and Finland

being the early adopters (2000 and 2003, respectively). Austria and Belgium followed in 2004, the Netherlands and Sweden in 2005, and Portugal in 2007, while Germany and Poland are currently starting their e-ID card rollout. Finally, a large number of countries including France, Hungary, Romania, Slovakia, Greece and others, are planning the implementation of an e-ID card (Patsos, Ciechanowicz, & Piper, 2010).

4.2.1 Certificates and Public Key Infrastructure

Public Key cryptography realizes the concept of digital signatures; it provides a practical, elegant mechanism for symmetric key agreement; and in combination with smart card technology currently enables the strongest available authentication of involved entities and secure communications. Public key cryptography has reached a stage of relative maturity, due to the intense scrutiny and research that has occurred in this area over the past two decades, currently incorporating many value added characteristics into the signing process; hash algorithms have given a solution to the computational efficiency of the signatures, digital certificates (Kohnfelder L, 1978) provide the means for effective identification of the signer, Public Key Infrastructure (PKI) architectures built the necessary trust relationships and finally time-stamping and notarization techniques provide additional proofs that add value and longevity to a digital signature (Adams, Cain, Pinkas, Zuccherato, 2001),(Lekkas, Gritzalis, 2004).

Public Key Infrastructure (PKI) is an essential security component of electronic trusted services. The development of robust and scalable PKI is an important task, which has been a field of active research for a number of years. A **Public Key Infrastructure** (**PKI**) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. A PKI infrastructure is comprised by several working units which can be easily collerated to the required services an e-Id infrastructure is required to provide.

These entities are defined as follows {Document not in library: (Sokratis Katsikas, 2001)} {Document not in library: (S. Gritzalis, Socratis Katsikas, Lekkas, Moulinos, & Polydorou, 2000)}:

The Certification Authority: The function of binding a specific unique cryptographic key pair to a given identity is performed by an authority, which in PKI terminology is called the Certification Authority (CA). The CAs role is to certify the key pair/identity binding by digitally signing a data structure that contains some representation of the identity and a

corresponding public key. This data structure is called a digital certificate.

The Public Key Repository or Directory: PKI in a distributed information system, benefits from the coupling with a directory. A directory is a set of objects with similar attributes, organized in a logical and hierarchical manner. A directory can be used to distribute (VeriSign, 2004)

- Certificates, for applications such as e-mail in which an end user certificate must be obtained before an encrypted message is sent.
- Certificate status information, such as certificate revocation lists (CRLs)
- Private keys, when portability is required in environments where users do not use the same machine every day. The directory stores encrypted private keys, which are decrypted at the remote workstation using a password provided by the user.

This repository is a point of reference for any individual wishing to validate a digital signature or to encrypt data addressed to another entity.

The Registration authority: The role of the Registration authority is to:

Establish and confirm the identity of an individual, as part of the initialisation process. (For example, the RA might verify the identity of an individual, through a combination of physical presence and identification documents, proving the individuals relation with the educational unit.)

- Distribute shared secrets to end users for subsequent authentication during an on-line personalisation process.
- Generate keying material on behalf of an end user.
- Perform certain key/certificate life-cycle management functions, such as to initiate a certificate revocation request, or a key recovery operation on behalf of an end-entity

The specified PKI services are as follows (Sokratis Katsikas, 2001) (S. Gritzalis, et al, 2000) (Keystone, 1998)

Registration- In order for a user to join the PKI environments, s/he must register with a certifying CA belonging to the PKI. The primary goal of this service, is to establish the reliable unique binding between a user and her/his public key. Functions supporting this service include: Initial request submission, Registration form's format validity checks on behalf of the TTP, end entity authentication and identification, and anonymity assurance.

Digital Signatures- Digitally signing a document is a process we have become accustomed to, as it provides for the electronic representation of the traditional signing process. Digital signatures are used to preserve the basic security characteristics of digital documents, such as integrity and authenticity, while acting as the principal verification method of the signer's intended meaning, as expressed in the respective document. The creation of a digital signature cannot be denied as an action (non-repudiation), since it can be algorithmically proven, using cryptographic techniques.

Encryption- Encryption is a basic service providing the cryptographic functions for protection of message confidentiality, in a computer network. Functions supporting this service include encryption and decryption of the message.

Time-stamping- Time-stamping is described as the process of attaching data and time to a document, in order to prove that it existed at a particular moment of time.

Non-repudiation- Non repudiation refers to a state of affairs where the purported maker of a statement is unable to successfully challenge the validity of the statement or contract. Non-repudiation involves the generation, accumulation, retrieval, and interpretation of evidence that a particular party processed a particular data item. The evidence must be capable of convincing an independent third party, potentially at a much later time, as to the validity of a claim. Functions supporting this service include initialization, revocation and dispute resolution and notary.

Key Management- Key management is a principal service within a PKI architecture. This service deals primarily with the handling of cryptographic keys in a proper, efficient, scalable and secure way.

Certificate Management. A digital certificate is an electronic token ensuring the binding between an entity and its public key. The functions supporting this service include generation, distribution, storage, retrieval, and revocation of digital certificates.

Information Repository- This service maintains the collection of data critical for the operation of the TTP system. It states the general means and fashion for storing, archiving and maintaining several types of data, ranging from organization's legal requirements, to system recovery needs.

Directory Services- In order to interact, a member of a PKI must have access to information about other PKI members. This is achieved by the use of Directory Services, which are supported by the following functions: update with new certificates, update with

revoked certificates, distribution, replication, caching, searching, retrieval (for certification purposes), retrieval (for cross-certification purposes), returning information.

Authorization- The PKI should enable requesting entities to delegate access rights at will to other PKI entities. This means that a PKI user who possesses a resource, may grant the right to another PKI user to access this resource. TTPs should ensure the granting of rights, including the ability to access specific information or resources.

Audit- In order to ensure that certain operational, procedural, legal, qualitative and several other requirements are complied with, so that trust is enhanced, an auditing service is required.

Quality assurance and trust enhancement services- It is expected that the potential users of PKI services would require products and services of a given quality to be delivered or be available by a given time, and to be priced so that best value for money is achieved. In order to achieve this level of quality, PKI services must be quality assured.

Customer oriented services- This group of PKI services includes services which directly involve users or that require some contact, or some kind of dealing or bargaining with the end user. Examples of such services are legal aspects and payment negotiations between a user and a TTP.

Implementing digital signatures, in combination with advanced cryptographic smart cards, minimises user side complexity, while maintaining reliability and security (multifactor authentication). Smart cards provide the means for performing secure communications with minimal human intervention. In addition, smart cards are suitable for electronic identification schemes ,as they are engineered to be tamper proof. (D. Spasic, 2005).

Public Key Infrastructures and specifically digital signatures provide invaluable tools towards enabling strong authentication in distributed environments, by ensuring data authenticity and integrity and most importantly by enforcing commitment and non-repudiation for the transacting parties. Within eID solutions, especially the creation of electronic signatures on the smartcard, is of vital importance. For a plethora of electronic government services, a citizen is required to digitally sign a petition or a document to ensure consent and non repudiation of communications. The concept of National PKI is conceived by a large number of governments, as the de facto infrastructure onto which policies, technology and security can be built upon, in order to provide authentication, identity verification, encryption and non-repudiation in electronic services(Patsos et al., 2010). A National PKI is primarily

focused on simplifying routine Government to Government (G2G), Government to Business (G2B) and Government to Citizen (G2C) transactions, while enhancing security horizontally(Patsos et al., 2010).

Research seems to conclude that in the context of electronic voting, there is no alternative to using PKI for voter authentication (Damgard, Groth, & Salomonsen, 2003). The main reason is that unless a private/public key pair is used, anybody who can verify authentication information can also fake it. In particular, universal verifiability of an election with a decent level of security is significantly simplified by using PKI (Damgard, Groth, & Salomonsen, 2003). PKI has been identified as a fundamental prerequisite to the deployment of any electronic voting information system, as most schemes that protect the confidentiality and integrity of data and communications require digital signatures. "I-voting will become fully electronic, from registration to tallying, only when a secure and uniform Public Key Infrastructure for digital signatures becomes available" (Burnester & Magkos, 2003). This is due to the fact, that most of the transactions performed during an e-voting session must be non repudiable, in order to guarantee the auditability and verifiability of the system. The only tool currently known that allows to satisfy such a property is the digital signature. Since all the voting protocols proposed use digital certificates and digital signatures, they all implicitly rely on Public Key (Curse, D. Bruschi, G. Poletti, & E. Rosti, 2003).

4.2.2 Need for interoperable security and services

Although the vision of using digital certificates for the verification and authentication of e-government services deployed across Europe, appears to be common-sense(Green Paper Lisbon Treat, the inherent perplexities and complexities are soon evident. The process of validating a digital signatures authenticity, relies upon a horizontal support infrastructure, that guarantees the uniqueness and originality of the signature, while correlating it to a specific individual(the signer). Cross-border digital signing, requires an infrastructure that can provide this service across borders, which at present is non existant. The vision expressed in the EU Ministerial Declaration of Manchester that "by 2010 all European citizens, businesses and administrations shall benefit from secure means of electronic identification (eID) that maximise user convenience while respecting data protection regulations" today seems to be a utopia. At present, the e-government services themselves are rarely, or not easily, available across borders.

It is safe to say that across Europe, all countries are not only at different stages of

maturity with regards to deployment of e-id infrastructures and respective PKI's, but also lack a common set of implementation mechanisms (Arora, 2008). Most notably, one can see the different underlying motivations and technical implementations across each country. While at a national level the schemes might operate as initially designed, attempting to use e-ID cards to address cross-border function's, has proved to be nearly impossible (Arora, 2008). There are several examples where different national eID solutions are usually not compatible with each other. Smartcard communication is usually performed using the PC/SC protocol and predefined application protocol data units (APDU). There is currently no common standard for defining the data that must be stored on an e-id smart card; across borders representation differs widely (T. Zefferer (AT-TUG), 2010).

All national e-id attempts have been primarily specified to work in a given national context; thus making systems highly interoperable. Some Citizen Cards (e.g. the Austrian Citizen Card) use different algorithms, which would very likely result in interoperability issues (Zefferer, 2010). Although most e-id infrastructures rely upon RSA cryptography, a few employ the ECDSA algorithm. The associated national PKI, is either public or privately owned and maintained, making use of several deployment models. For instance, in Spain, the public National Spanish Police Department (Ministry of Interior), is responsible for the PKI being associated with issued certificates being stored on eID cards. In contrast, in Estonia a private organization (Certification Center) maintains the associated PKI (T. Zefferer (AT-TUG), 2010).

A series of European Union initiatives and frameworks have been published, which are attempting to address the issue of offering common services and security solutions in an interoperable and scalable fashion. Notable examples include the Secure Identity Across Borders Linked (STORK) for Electronic Identities (e-ID), the eID Interoperability for PEGS project, the Pan European Public Procurement Office (PEPPOL) for public procurement, and the European Patient Smart Open Services (epSOS) for e-health services (IDABC, 2009). Additionally, attempting to overcome some of the prementioned e-Id interoperability difficulties, the European Citizen Card framework has been proposed. The ECC is an open application standard, defining logical data structure, security and privacy mechanisms of the data, interface and communication protocols. It is open, because it allows the governments to select a number of deployment options (Eurosmart, 2008). Although this framework provides an initial proposal upon which common solutions can be developed, at least as to common data structures with the e-id card, its adoption has been slow, as most countries are in the

process or have already deployed their e-id solutions. In addition, unfortunately, this framework has not been designed with scalability of services in mind, and lacks to support the generation of Zero-Knowledge proofs or ElGamal encryption algorithms, algorithms required for the deployment of any electronic vote casting service, limiting the solutions effectiveness only to current electronic government services (Meister, Huhnlein, Eichholz, & Araujo, 2008).

Even more critical to interoperability issues, involving smartcard communication and smart card data structures, is the interoperability at a PKI trust level. The electronic services for identification, authentication and signature creation purposes are based on public key procedures. The validation on these processes, requires a level of trust above the end user. This trust requires cross border cooperation, between the Certification Authorities of National PKI's. End user certificates, which are stored on the card and link user specific data (unique identifiers, etc.), with the corresponding public keys, are signed with the PKI's root certificate (or an intermediate certificate, which in turn is signed by the root certificate)(Figure 1). If this cross border cooperation is not achieved, it is not possible to effectively validate a citizen's signature, or authentication request successfully (T. Zefferer (AT-TUG), 2010). Differences exist either at a policy or functional level, placing serious limitations on cross border availability of these services. Unfortunately, in current implementations, the notion of trust is not clearly identified and either the researchers do not address it or it is considered as de facto granted. This certainly requires a common understanding of all identity management issues (legal technical organizational).

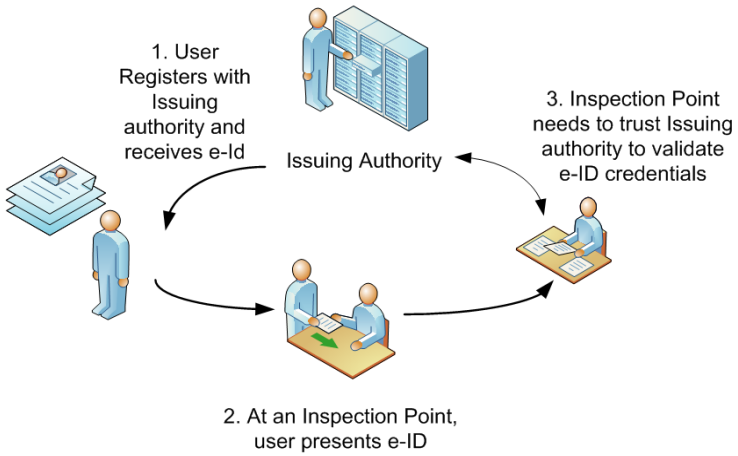

Illustration 40: Validation requires interoperable infrastructure

The deployment of a large Public Key Infrastructure, that shall effectively and proficiently escalate into a pan-european Electronic Identification Infrastructure, covering all needs of security for e-Government, is a highly complex task. Such an infrastructure is itself required to be highly interoperable, scalable and efficient. A common PKI solution,

encouraging agencies to work together, allows equitable cost sharing among agencies, while enhancing community confidence in electronic dealings. A homogenized security infrastructure provides consistency in e-Authentication across borders, while increasing trust and efficiency of services.

PKI scalability is a complex issue. Consider a simple example where certificates are issued by a central CA for a specific application. These certificates contain a predetermined maximum validity period. When a certificate is outdated, it becomes revoked and is added to the Certificate Revocation List (CRL) published by the CA. A user is required to check the validity of a certificate, by reviewing the CRL. Now consider scaling this to cross border services, millions of users, numerous CA's, applications and trust domains. Moreover, if these parameters are not carefully engineered, the size of the CRL may result in very inefficient lookup and update schemes(Varvitsiotis, 2000). This scheme quickly becomes inefficient.

From the above example, it becomes apparent that smooth scaling of a PKI community depends on many factors. The factors include(Varvitsiotis, 2000):

- *Number of users:* The PKI deployment architecture should enable performance, degradation should optimally be negligible, or in the worst case, a sub-linear (e.g., logarithmic) function of the user population, in order for the set-up to scale up reliably.
- *Number of CAs:* as the number of CAs (and the respective Certification server components) grows, special procedures have to be followed in order to allow interoperation between users certified by different CAs.
- *Length of certificate chains*: hierarchies of subordinate CAs have some administrative and interoperability advantages compared to a collection of unrelated CAs. However, verification of the resulting certificate chains may not be as efficient. Procedures need to be in place to effectively deal with large chain lengths.
- *Number of Directory server components*: the number of servers under different administrations is an important factor for complicated community set-ups, consisting of several server components. Performance should not degrade or in any way make the creation of more servers impractical.
- *The dynamics of user population*: users of a PKI community are not static. They may relocate, hence change their own DN. They may also request that their own

certificates be revoked (e.g., because of a private key compromise) or demand that some server certificates be revoked (e.g., because of administrative changes or service termination). Each of the above events requires revocation of a certificate. Beyond user dynamics, application dynamics also play an important role, possibly extending the lifetime of certificates and adding complex requirements to PKI functions.

Overall, an authentication mechanism, achieving cross border interoperability is required to fulfill a number of requirements,

– Technology compatibility

- Common Data formats-Semantics;
- Communication Protocol Compatibility;
- Algorithm usage compatibility;
- Card compatibility-Reader Compatibility;

– Policy Compatibility

- Registration procedures and requirements(identity proofing etc);
- Operational Requirements;

– Security Schema Compatibility

- Common understanding of security risk assessment analysis;
- Common definition of risk assessment criteria, typically combined with a consideration of potential damage in case of incidents; these should be the basis for determining security requirements, i.e. Authentication Assurance Levels;

– Legal Compatibility

- Privacy & Data Protection legal framework;
- Legal Data Signature Validity;

– PKI Compatibility

- Trust relationships must be established between issuing authorities;

- Deployment architecture compatibility;

– Directories must be complex free and achieve high compatibly(schema and protocol)

– Infrastructure must be able to achieve high scalability to respond to dynamics of user population

4.2.3 Leveraging the e-Passport Infrastructure

While the research community has been involved in time consuming recursive debates on how to implement a globally acceptable and trusted Public Key Infrastructure, it seems that the e-passports PK infrastructure, currently deployed in several countries provides a potentially friendly environment for achieving the necessary global trust. Electronic passports, or e-passports, are currently being issued and inspected across the globe, in accordance with International Civil Aviation Organization (ICAO) standards for Machine Readable Travel Documents (MRTD). Every e-Passport has an embedded electronic chip, that contains the holder's personal information and photo found in the passport. To achieve interoperability a common understanding between participants on data structures and communications was required. This was achieved in MRTD, as all MRTDs follow a standardized layout to facilitate reading of data on a global basis by both eye readable and machine readable means. In order to increase confidence in the MRTD scheme, the e-Passport chip is digitally signed to prevent unauthorized alteration and ensure authenticity. In order to verify a digital signature, border and other authorities need to access the e-Passport's public key. As electronic passports are designed to be of maximum use in facilitating international travel, successfully validating these documents at inspection points is critical. That is why it is crucial to share the public keys as widely as possible (ICAO, 2009).The aim of this process is to link the passports validity and authenticity back to the issuing authority.

To achieve this, a web of trust is set up between implicated parties. The inspecting entity accepts the e-passport as valid, because it trusts the authenticity of the respective signing authority. Basically, a chain of electronic certificates and signatures is created with one end securely anchored in the authority of the issuing state and the other end securely stored in the respective chip (Hartmann, Körting, & Käthler, 2009). The validity of these documents is checked by comparing the validity of the implicated certificates, usually at the top of the chain, with the certificate of the country's issuing authority. This validation, requires that the inspection entity has authenticated access to the certificate of the respective country, to validate against it, otherwise this process is broken. The ability for any implicated entity, to

validate the authenticity of a signature of a third parties certification authority, is critical.

The most important advantage offered by the e-passport infrastructure is the established worldwide trust; the e-passport PKI offers a global multilateral framework to verify the entire chain of certificates issued by each country. This is achieved either with cross country certification, or by using the ICAO Public Key Directory (PKD). Technically, a trust relationship is established when a Country decides to trust the root certificate, (the certificate of the CSCA) of another Country. First of all, a secure offline channel for the distribution of one's country's root CA certificate, to another country, must be established. This is achieved through out-of-band secure diplomatic means. Given that the whole infrastructure of a country trusts its own root certificate (i.e. the CSCA plays the role of a SPOT for this country), there are two alternative mechanisms to implement the web-of-trust.

- *Cross-certification*: The Country issues a cross-certificate, (signed by the home CSCA), for each root CA of all the countries it trusts. The cross-certificates are then distributed to the inspection systems of the Country, where the cross-certified countries will be trusted. This kind of trust link can be reciprocal or one-way.
- *ICAO Public Key Directory*: ICAO recognizing that the exchange of PKI certificates and certificate revocation lists must be reliable and timely, established the ICAO Public Key Directory. The ICAO PKD was established to support the global interoperability of e-Passport validation, and to act as a central broker to manage the exchange of certificates and certificate revocation lists. This central role is critical to minimize the volume of certificates being exchanged, to ensure timely uploads and to manage adherence to technical standards, guaranteeing interoperability is achieved and maintained (Overview - The ICAO Public Key Directory).

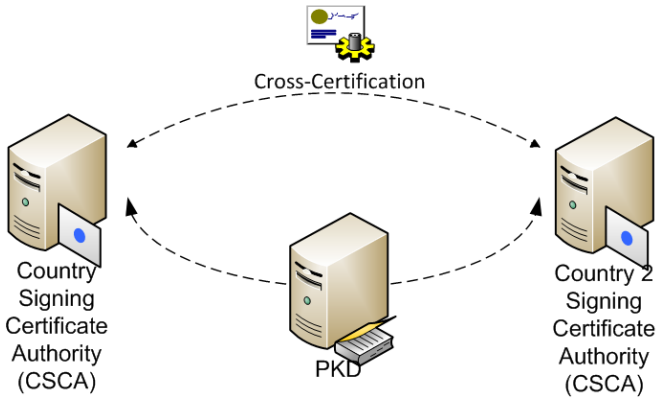

Illustration 41: The ICAO Public Key Directory

This de-facto trust infrastructure overcomes the basic drawback of the most commercial

or closed-groups PKIs; lack on interoperability. It is critical that e-id infrastructure's leverage this global trust framework, as it provides the required platform for global interoperability at a PKI level. In addition, leveraging the e-passport infrastructure achieves economies of scale and knowledge, according to the requirements set by recent initiatives, (as identified in previous section).

A strategic decision for the current implementation of e-passports, is the lack of citizen certificates, in order to facilitate a fast-track implementation and to avoid the complexity of managing client certificates and keys. However, it has all the characteristics of a full-scale PKI, with only one part missing from this implementation, i.e. the management of end-entity certificates. The X.509 digital certificates, which are issued for the ICAO PKI implementation, are restricted only to the authorities issuing the passports (i.e. the hierarchy of Country Signing CA and the subordinate Document Signing CA). Although the e-passport does not contain an X.509.v3 certificate and it is not designed for everyday Internet transactions, it exhibits all-but-one of the characteristics of a typical PKI-enabled smart card, containing a private key and the relevant digital certificate.

The e-passport member states PKIs, follow the standard proposed by ICAO and are deployed in a hierarchical architecture. A hierarchical architecture has been proven under real-world conditions to scale smoothly from hundreds to millions of users (HHS-IRM-2000-001); thus achieving the demanded scalability requirement. Trust operates in a hierarchical manner, starting at the country's highest certification authority. At the top of the hierarchy is the Country Signing Certificate Authority, which is responsible for issuing certificates for the subordinate Document Signer Certificate Authority, and for cross certification with other national CSCA. The Document Signing CA signs the passport's data, including a public key (Active Authentication key) stored in each passport. Leveraging existing software, procedures and policies, a subordinate **Identification Signing Certification Authority (ISCA)** can be deployed with minimal complexity and cost, that shall be delegated with the authority of issuing X509 certificates. This ISCA is deployed as a subordinate CA to CSCA inheriting cross country trust relationships. This enables certificates issued by the ISCA, to be automatically trusted by any other state or country that has been cross certified or has joined the ICAO PKD.

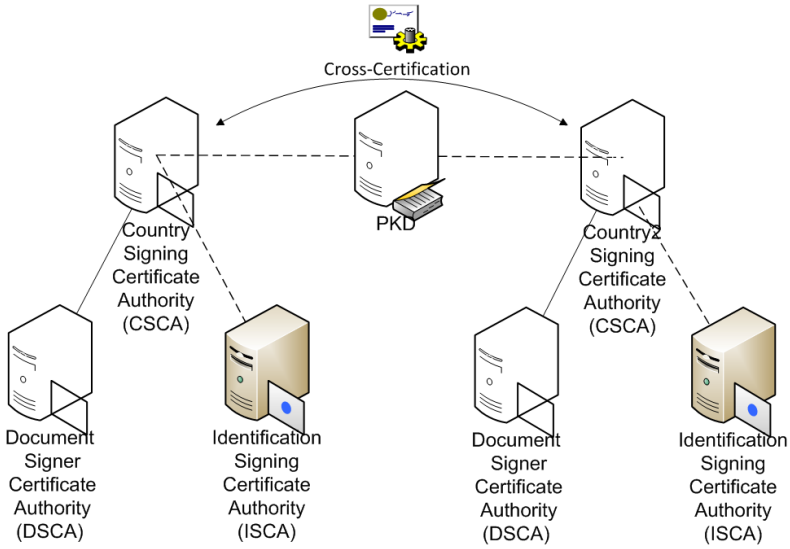

Illustration 42: The proposed infrastructure creates a subordinate Identification Signing Certification Authority that shall be delegated with the authority of issuing X509 certificates, while inheriting trust relationships from CSCA

The proposed ISCA can leverage the deployment of the e-passport infrastructure and be responsible for the creation of personal citizen certificates, as hard or soft tokens. Hard tokens offer greatest security, but a number of low security services may require soft tokens to increase process efficiency(Illustration 48).

- Personal Certificate- Hard: on smartcard, personal phone
- Personal Certificate- Soft: email, compact disc
- E-Government Services certificate: application certificate

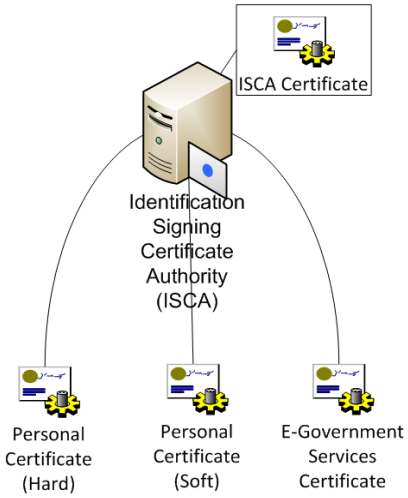

Illustration 43: Types of certificates

The uses of these certificates are identified below,

ISCA Certificate:

- Sign subordinate CA's certificate (if any)
- Sign Data in e-id card to guarantee authenticity
- Sign CRL

Personal Hard Certificate:

- Strong Authentication (multifactor) with electronic government service. This is the highest practical remote network authentication assurance. According to NIST strong multifactor authentication with hard tokens, (named Level 4) is the strongest available authentication method. Level 4 is similar to Level 3, except that only "hard" cryptographic tokens are allowed.
- Digitally sign documents and emails to ensure authenticity and non repudiation. Encrypt data to ensure confidentiality and integrity. Hard certificates are necessary for the most security sensitive electronic government services.
- Encrypted communications with electronic government services. Bootstrapping secure communication protocols, such as Internet key exchange (IKE) and SSL.
- Non repudiation of communications.

Personal Soft Certificate:

- Strong Authentication (multifactor) with electronic government service, provides multi- factor remote network authentication. At this level, identity proofing procedures, require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or password through a cryptographic protocol.(soft token)
- Digitally sign documents and emails to ensure authenticity and non repudiation. Encrypt data to ensure confidentiality and integrity.
- Encrypted communications with electronic government service. Bootstrapping secure communication protocols, such as Internet key exchange (IKE) and SSL. In both of these, initial set-up of a secure channel (a "security association") uses asymmetric key (public key) methods
- Non repudiation of communications

Extending the e-passport infrastructure can address a plethora of previously identified requirements, while adding value to the overall security of e-government. The deployment of the e-passport infrastructure enabled the development of policies and procedures that guarantee strict citizen identification and registration required for a secure e-id infrastructure. At the time of design and deployment of this architecture, secure procedures and policies were implemented, uniform to all member states, for addressing the security issues of the infrastructure and achieving safe passport issuance. These procedures include designing processes such as secure registration, deployments, contingency and recovery planning, and many more. These procedures equate to the required procedures for safe issuance of secure e-ids. These procedures increase the overall trust in the infrastructure.

Leveraging the e-passport infrastructure provides a plethora of additional benefits. Since the ID cards are accepted as travel documents within Schengen States, their profile is required to be in conformity with many ICAO specifications, common to the e-passport. The mandatory card services are passive authentication, BAC, EAC chip & terminal authentication referenced by the specific OIDs, plus Secure Messaging for the ICAO application (Eurosmart, 2008). By leveraging the e-passport PKI infrastructure, we achieve economies of scale and knowledge.

The global e-passports implementation seems to be an attractive PKI establishment, since:

- The passport as a digital identity is issued by governmental authorities, under very strict and reliable identification and issuance procedures for the citizens; due to the standardization of most of this process, member states are interoperable at policy procedures.
- The e-passports and electronic identity documents have common security profiles.
- The technology used throughout the world is compatible and, thus, interoperable. Due to the standardization of the PKI infrastructure it is highly interoperable and scalable, as common deployment models have been adopted across member states.
- High security procedures and operational models were defined during the deployment of e-passports, including the creation of high security facilities for the issuance of e-passports and for the protection of related data. The e-passport requirements are identical to the requirements of an e-id infrastructure at this

level.

- A worldwide Web-of-Trust is established through a reliable and secure exchange of countries self-signed certificates.
- The member states legal framework has been addressed to be compatible with the e-passports; thus providing compatibility for e-id cards (registration requirements, policy, digital signatures , etc)
- The e-passport member states PKIs, follow the standards proposed by ICAO and are deployed in a hierarchical architecture. A hierarchical architecture has been proven under real-world conditions to scale smoothly from hundreds to millions of users (HHS-IRM-2000-001)

Many enterprises currently operate independent directories, based on closed propriety protocols. As the number of applications and utilities relying on these directories are increasing, current practices are becoming inefficient. The directory service is the hub, around which a large distributed system revolves, but also generates trust between implicated parties in the authenticity of communicating parties. In numerous occasions, electronic communications between unknown entities are staggered, due to the lack of authenticity. Users, but also legal entities are often unable to initialize transactions, as they are unable to validate electronic credentials presented as proof of identity (e.g. email etc). There is a trust deficit in electronically presented credentials. These occurrences require providing credentials, issued from a trusted third party, that can be easily validated. Relying on information provided by a trusted directory would increase trust in all communications between member entities. As e-id credentials are issued under strict registration procedures and policies, identifying an entity's email and information in a trusted directory, enhances trust between communicating parties. An interoperable cross border PKI infrastructure can establish the goal of unifying information into a homogenous directory, maintained by member states, but accessible from a common gateway. Such a directory may simplify C2G, but additionally G2B interactions, as in many cases a citizen is required to prove his identity to a business to initialize transactions. The availability of a trusted directory, easily accessible and highly available, overcomes this requirement, enabling stronger and safer e-commerce as it guarantees the validity of credentials of implicated parties. But also on a citizen's side, interaction with web services can be verifiable, as directories contain lists of information of natural but also legal entities. Validating an e-services certificate would thus increase the

integrity of communications. It is critical to point out that although interoperability of directories is a requirement, integration of member states directories into a common global directory, may not be required due to privacy and security risks.

Revisiting the previously identified requirements for implementing an interoperable authentication mechanism and weighing these requirements against the characteristics available in the e-passport PKI infrastructure, already deployed by a number of member states, provides numerous benefits, identified in table 1.

Requirements	Achieved from the adoption of e-passport PKI	Achieved by extending the e-passport PKI
Communication Protocol Compatibility	X	
Card compatibility-Reader Compatibility	X	
Common Data formats-Semantics		X
Registration procedures and requirements	X	
Operational Requirements	X	
Common understanding of security		X
risk assessment analysis		
Common Security Profiles		X
Privacy & Data Protection legal framework		X
Legal Digital Signature Validity	X	
Trust relationships between CA	X	
PKI Architectural Compatibility	X	
PKI Algorithm compatibility	X	
Directories		X
Scalability	X	

Table 9: Extending e-passport infrastructure

This e-authentication infrastructure presents the essential platform upon which IS security can be built. Providing a secure identification and authentication of the voter is conditio sine qua non for e-voting systems to be used in public elections (Gritzalis, 2003).

4.3 Cryptography & Elections

Evolution in the field of cryptography has taken cryptographic algorithms out of the theoretical sphere and applied them as solutions to a number of information systems security

issues. These implementations of cryptography have made it possible to counter eminent threats and attacks on security critical systems. This technology is mature and can be relied upon to ensure the integrity and confidentiality of the communications and data.

Cryptography has the ability to provide more than confidentiality and integrity; especially in the context of elections. Voting requires public verification of a process that must remain secret. In elections there is a contradiction in critical system functional requirements between verifiability and anonymity. Any attempt to maintain a bidirectional on-line association between voter and votes cast is suspicious, because of the inability to protect such information in such an environment. This secrecy cannot be guaranteed by trusting an all-powerful third party: even the auditors cannot be made aware of how individual citizens vote. In addition, this audit must be convincing to mutually distrusting observers. Cryptography provides an opportunity to generate trust between involved parties of an election and present a means for greater transparency. Using cryptography, it is possible to operate on encrypted data in public, open for everyone to view, while maintaining privacy. Cryptography can provide verifiability, while maintaining ballot secrecy.

Cryptography is all important element in information and communication security with the ability to address a perplexity of issues surrounding electronic voting. A plethora of cryptographic schemes have been proposed which are presented in the following section.

4.3.1 Generic Cryptographic Requirements

Cryptography is concerned with the construction of schemes that should withstand abuse. Such schemes are constructed so as to maintain a desired functionality, even under malicious attempts aimed at making them deviate from their prescribed functionality(Goldreich, 2007).

Cryptographic schemes proposed for electronic voting must exhibit the desired functionalities of (Zuzana, 2002) (Caarls, 2010):

- **Coercion-resistance**: a voter should be unable to cooperate with a coercer to prove to him that she voted in a certain way. Uncoercibility and prevention of vote buying and extortion can be ensured by an e-voting system designed so that no voter can prove that she voted in a particular way (untraceability on the part of the voter).
- **Verifiability**: Among researchers in the field of electronic voting,it is widely assumed that trust in the vote counting process can only be assured if each voter

has the ability to verify that his/her vote was indeed counted(this is called universal verifiability) (Peralta, 2003).

Two different forms can be distinguished:

- Universal verifiability, meaning that anyone (voter, responsible election authority, or external auditors) can verify the election result after the announcement of the tally.
- Individual verifiability. Each eligible voter can verify that his vote was really counted.

- **Fairness**. No participant can gain any knowledge about the (partial) tally before the counting stage (the knowledge of the partial tally could affect the intentions of the voters who has not yet voted).
- **Robustness**. Faulty behaviour of any reasonably sized coalition of participants can be tolerated. No coalition of voters can disrupt the election and any cheating voter will be detected.
- **Receipt-freeness.** An election scheme is believed to be incoercible, if the voter cannot convince any observer how he has voted. This requirement prevents vote-buying, selling and coercion. Before the election, someone can bribe or coerce the voter to vote in a particular way. The coercer can order the voter how he should behave during the voting process (e.g. generates for him random bits). During the election, the coercer can observe the public communication between the voter and the authorities. After the election, he will want to see a proof that the voter really voted this way. In the scheme achieving privacy, the coercer alone or with reasonable coalition of participants cannot open the voter's vote. Thus the coercer will force the voter to show him his secret information. With it, he is capable of opening the ballot and seeing the vote. Incoercible scheme provides the voter with the ability to modify his secrets and to open his ballot in any desired way. Thus the voter can vote on his own will and he can feed the coercer with a false proof.
- **Eligibility**. Only eligible voters can cast the votes. Every voter can cast only one vote.
- **Privacy**. No coalition of participants (of reasonable composition) can gain any information about the voter's vote. By reasonable composition, we mean coalition

of at most t authorities and any number of voters. We say that information-theoretic privacy is achieved when the ballots of the voters are indistinguishable independent of any cryptographic assumption; otherwise we say that computational privacy is achieved.

Cryptographic design of voting schemes, which started in the early 80's, has proved to be very challenging due to the multitude and conflicting nature of properties such schemes need to satisfy. Most electronic voting schemes can be classified into three classes, the first comprises of protocols derived from Chaums seminal paper (Chaum, 1981), which heavily rely on asymmetric cryptography; the second class derives from Cohen's work(Cohen & Fisher, 1985) and is based on homomorphic encryption; and the third class combines the two approaches in order to gain the benefits from each (Bruschi, Poletti, & Rosti, 2003). All e-voting protocols seem to share a common structure. They are generally composed of two components; a component for the verification of user entities involved in the protocols, to guarantee voter eligibility and vote uniqueness and a second component, responsible for the cryptographic operations on the cast votes, in order to guarantee the security of the process (i.e., vote secrecy and voters' privacy). These protocols principally differ in the way the first component is implemented. For the second component, the protocols employ asymmetric cryptography and ultimately digital signatures for voter authentication and uniqueness. This is due to the fact that most of the transactions performed during an e-voting session must be non repudiable in order to guarantee the auditability and verifiability of the system+ (Bruschi, Poletti, & Rosti, 2003). As previously identified, the deployment of a Public Key Infrastructure is an essential prerequisite for the establishment of secure electronic elections.

An electronic voting scheme, consists of three main stages: initialization stage, voting stage, and counting stage.

Initialization stage. At this stage, authorities set up the system. They announce the elections, formulate the questions and possible answers, create a list of eligible voters, and so on. They generate their public and secret keys, and publish the public certificates.

Voting stage. Voters are casting their votes. The voter communicates with authorities through the channels he can use, forming a ballot containing his vote. Finally he sends his ballot to its destination.

Counting stage. Authorities use their public and secret information to open the ballots and

count the votes. They publish the result of elections.

The proposed cryptographic election schemes can be categorised according to the election phase in which the mechanisms are applied (this categorisation is introduced in (Melanie Volkamer, 2009)(R. Krimmer, Triessnig, & M. Volkamer, 2007)

Election Phase	Cryptographic Election Scheme
Initialisation Phase	Randomised Authentication Token
Voting Phase	Blind Signature Separation of Duty Benaloh's Model
Tallying Phase	Homomorphic Encryption Mix Nets Hardware Security Model

Table 10: Cryptographic election schemes categorized according to election phase

4.3.2 Cryptographic Schemes

In the following section we provide a description of each cryptographic protocol proposed and examine its benefits and drawbacks.

4.3.2.1 Randomized Authentication Token

A simple non cryptographic solution is based on the distribution of anonymous tokens to ensure election secrecy, prior to the election. The voter can use this election token to authenticate as an eligible voter without the system having knowledge of who he is.

4.3.2.2 Blind Signature Schemes

The concept of blind signatures was first introduced by Chaum (Chaum, 1982) as a method to digitally authenticate a message, without having knowledge of the messages content. A critical feature of blind signatures is their unlinkability: the signer cannot derive the correspondence between the signing process and the signature, which is later made public.

Electronic blind signatures work similar as physical blind signatures. Physical blind signatures can be made with an envelope, white paper and carbon paper: something secret is written on the white paper, next the carbon paper is placed on top of the white paper in the envelope, and the envelope is sealed. Next, the so called validator signs the envelope. Obviously the signer does not know what he has signed but on the secret document is his valid signature(Melanie Volkamer, 2009).

Completely Blind signatures (Schneier, 1996)

Bob is a notary public. Alice needs him to sign a document, without him having any knowledge of the contents of what he is signing. Bob is not interested in the contents of the document, just certifies that he notarized it at a certain time.

1. Alice takes the document and multiplies it by a random value. This random value is called the blinding factor.
2. Alice sends Bob the blinded document
3. Bob signs the blinded document.
4. Alice divides out the blinding factor, leaving the original document signed by Bob.

This protocol only works if the signature function and multiplication are commutative. This protocol does not permit Bob to view the contents of the document signed. If the blinding factor is truly random and makes the blinded document truly random, Bob is restrained from viewing the document. The blinded document signed in step 2, does not appear like the document Alice began with. The blinded document in step 3 looks nothing like the signed document at the end of step 4. Even in the possibility that Bob obtained the document with his signature on it, after the protocol has completed, there is no possibility for him to prove to himself or someone else that it is the document he signed in the particular protocol. If he signed a million documents during the execution of such a protocol, he has no knowledge during which instance he signed which document.

The properties of completely blind signatures are:

1. Bob's signature on the document is valid. The signature is proof that Bob signed the document. It will convince Bob that he has signed the document, if ever showed to him. All digital signatures properties also hold.
2. Bob cannot correlate the signed document with the act of signing the document. Even if he keeps record of every blind signature he makes, he cannot determine when he signed any given document.
3. Eve who is in the middle, watching the execution of the protocol, has even less information than Bob.

Blind signatures make use of the RSA algorithm. Bob has a public key, e, a private key, d, and a public modulus, n. Alice wants Bob to sign her message, m blindly.

1. Alice chooses a random value, k, between 1 and n. Then she blinds m by computing

$$t = mk^e \, mod n$$

2. Bob signs t

$$t^d = (mk^e)^d \, mod n$$

3. Alice unblinds t^d by computing

$$s = t^d / k mod n$$

4. And the result is

$$s = m^d \, mod n$$

The implementation for a voting protocol is possible in two different ways: either the e-vote itself is blinded or an authorisation token is (Melanie Volkamer, 2009):

- Blinded e-votes: each voter encrypts their vote and sends it to the validator. The validator checks if the voter is eligible to vote. If so the validator blindly signs the encrypted vote. The voter unblinds the received data and gets a signed e-vote which s/he sends to the voting authority(or tallier). The voting authority knows that that the e-vote was sent by an eligible voter (it is signed by the validator), but cannot detect the voters identity.
- Blinded authentication tokens: the voter sends a blinded anonymous authentication token (instead of the blinded e-vote) to the validator, together with some identification and authentication data. He receives a digital signature from the validator on this blinded token. In the next step, the voter computes the value for the signed authentication token and sends this data together with his e-vote to the tallier, which accepts the vote because of the digitally signed authentication token.

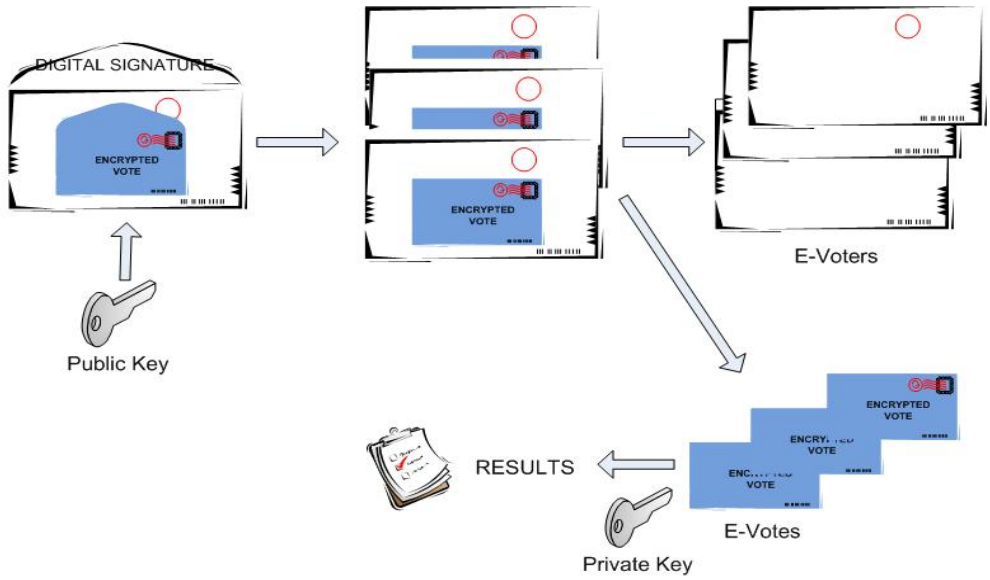

Illustration 44: Double envelopes

An advantage of blind signature election schemes, is that their communication and computation overhead is fairly small, even when the number of voters is fairly large. Furthermore, these schemes can easily be, and realize elections with multiple candidates. However, they only offer individual verifiability and require that every eligible voter should not abstain after the registration phase or else a corrupted validator can add extra votes on behalf of abstaining voters(Burnester & Magkos, 2003).

4.3.2.3 Separation of Duty

The separation of duty approach works with at least two voting servers, one inspecting the right to vote and another one storing the eligible e-votes. The voter authenticates himself to the first server. In case that he has the right to vote, he receives a random number generated by this first server. This random number is also sent to the second voting server, but without any information about the voter's ID. Now the voter uses this random number to authenticate himself as an eligible voter to the second voting server, to which he sends his vote in the next step. Again this second voting server can only check whether an eligible voter sent the e-vote but not who(Melanie Volkamer, 2009).

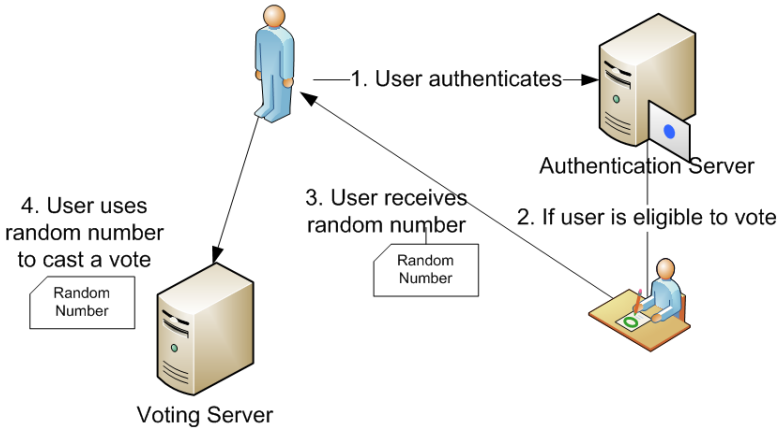

Illustration 45: Separation of Duty

4.3.2.4 Benaloh's Model

Benaloh's model proposed in (Benaloh, 1987) is based on a homomorphic secret sharing scheme: each voter shares his vote among n voting authorities. The shares are encrypted with the public key of the receiving authority, authenticated and posted to a bulletin board.

At the end of the election day each voting server adds all the received shares to get a share of the election result. Finally the shares of election results are combined to get the total election result. Results are universally verifiable.

Schemes of this type, although structurally simple, have a high communication cost: each voter must cast his/ her vote over n communication channels(Burnester & Magkos, 2003).

4.3.2.5 Homomorphic Encryption

This election scheme which has been proposed by Crammer (Cramer, Gennaro, & Schoenmakers, 1997), uses special features of homomorphic encryption algorithms to achieve universal verifiability in large scale elections, while maintaining privacy. Homomorphic Encryption is a special kind of encryption that supports the property that the sum of two encrypted numbers is always equal to the encryption of their sum.

An encryption function E is called homomorphic, if for some operations $\oplus, \otimes$, the following holds:

$$E(x \oplus y) = E(x) \otimes E(y)$$

this property is especially useful for tallying voting results; as the multiplication of the encrypted votes is an encrypted sum of the votes.

This essentially means that anyone can compute and verify the “encrypted sum” of a collection of encrypted values. Because the data is encrypted, this same person will not know what numbers are actually encrypted, either in the original values, or the final sum, but he will know that whatever the unencrypted values are, they maintain the sum/total relationship.

Instead of hiding the identity of the voters, this scheme hides the contents of the ballot itself. The ballot is submitted in a traceable manner, attached to the voter identity, so that the verifiability property is satisfied(Labrinoudakis et al., 2003). At vote counting, a ballot needs to be decrypted to reveal voter selections. This is avoided by encrypting the ballot using homomorphic encryption, since if the encrypted ballots are multiplied, they produce a result that is the encrypted election tally. For example, given ciphertexts C=EncK(M) and C'=EncK(M'), an additively homomorphic encryption scheme would allow to combine C and C' to obtain EncK(M+M')(Micciancio, 2010). For example, an electronic voting scheme may collect encrypted votes Ci=EncK(Mi) where each vote Mi is either 0 or 1, and then tally them to obtain the encryption of the outcome C=EncK(M1+..+Mn). Each voter encrypts his vote with the public encryption key of a voting authority and then publishes the encryption on a bulletin board, together with a proof of correctness (proof that the encryption contains a valid vote). At the end of the voting period, the authorities multiply all received encryptions to get an encryption of the tally. The authorities then jointly decrypt this to get the final tally. The final tally can be checked for accuracy by all parties; thus achieving universal verifiability. For robustness, the encryption procedure is distributed among n authorities using threshold cryptography.

A drawback of this scheme is its limited flexibility, as voters are essentially limited to a selection set of yes/no values.(Burnester & Magkos, 2003). In addition some implementations /(using el Gamal encryption) have a relatively high computational complexity.

4.3.2.6 Mix Nets

Mix nets have been introduced by Chaum in (Chaum, 1981) as a cryptographic alternative to an anonymous channel. A mix net is composed of several linked servers called mixes. Election schemes based on Mix Nets, take as input a sequence of scrambled messages and produce an output sequence of unscrambled messages, that correspond to some permutation of the original sequence. Mixes can be used to permute a variety of entities, such as ballots from

different voters, a number of ballots from a single voter etc.

The purpose of the mix is (Tsekmezoglou E., 2005):

- To hide the correspondence between the items in its input and those in its output
- To ensure that no item is processed more than once by attaching something like a timestamp, that is only valid for a particular batch.

In the original proposal, a vote is encrypted with the public key of each mix. It is then decrypted,shuffled and forwarded to the next mix. This is also referred to as the decryption mix. In the re-encryption net, all votes are re encrypted with the public key of the first mix and then randomized re-encryption takes place at each layer in a verifiable way (Burnester & Magkos, 2003).

Using only one Mix node, it is necessary to trust this particular component not to keep the information about the link between input and output messages. To reduce trust, whole Mix networks with n Mix nodes are implemented and incoming messages are encrypted with the public key of each Mix node (in reverse order). Messages are decrypted, shuffled, and forwarded from one Mix to the next one. Now, all Mix components need to collaborate in order to reveal the links between input and output messages of the MIX network, consequently, only one out of n Mix nodes needs to be trustworthy. As in any other system implementing the anonymisation during the tallying phase, the anonymisation mechanism is applied in the tallying phase. To do so, the encrypted e-votes (without any voter information) are sent through a Mix network. Assuming the Mix network works correctly, the decrypted output votes cannot be linked to the encrypted input votes (and, thus, the voters).

The operation of mixing is performed as follows (Rjaskova, 2002) (Illustration 51):

- The first authority takes the list of L possible votes (original list), permutes it in a random order, and re-encrypts each possible vote. It unveils the permutation only to the voter and no one else. To increase the security, the authority sends the permutation to the voter through an untappable channel. The created list, containing re-encrypted and permuted possible votes is published and handled to the next authority. Seeing just the original and created list, no one is able to say anything about the permutation mapping each item, from the original list to its re-encryption in the created list, unless this permutation is revealed to him by the authority.
- The next authority takes the handled list, and shuffles it in the same way as the first authority shuffled the original list: it permutes the list in a random order, re-encrypts

each item, unveils the permutation to the voter through the untappable channel and publishes the produced list.

- Successively, each authority takes the list handled by the previous authority, shuffles it in the manner described above, and handles the produced list to the next authority. The list produced by the last authority is called the final list. Only the voter can keep track of the permutations that have been sequentially applied to the original list by the authorities. Therefore, only he knows the permutation mapping each item from the original list to its re-encryption in the final list. The voter just selects one item from the final list as his vote

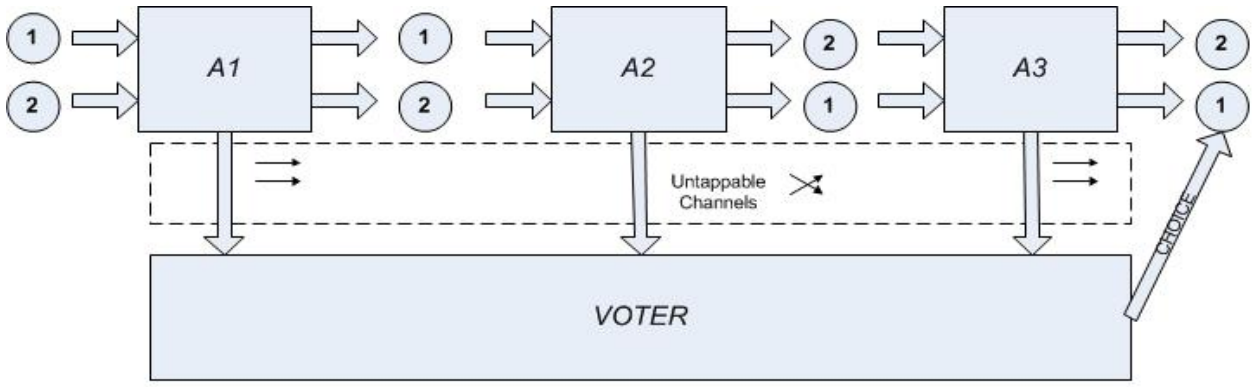

Illustration 46: Homomorphic Encryption election scheme

A useful property of mix-nets, specially in large scale elections, is their universal verifiability. Mix-nets are also quite efficient, provided that there are not too many mixes in the process. No election scheme based on mixes has been implemented so far (Burnester & Magkos, 2003).

4.3.2.7 Hardware Security Model

A **hardware security module** (often abbreviated to **HSM**) is a type of secure cryptoprocessor targeted at managing digital keys, accelerating cryptoprocesses in terms of digital signings/second and for providing strong authentication to access critical keys for server applications. These modules are physical devices that traditionally come in the form of a plug-in card or an external TCP/IP security device, that can be attached directly to the server or general purpose computer.

An HSM implementing decryption can be seen as a function which takes as input the encrypted e-votes and returns as output the decrypted result, while the decrypted votes are not

revealed. The Estonian remote electronic voting system uses such an HSM, but only to decrypt votes, that is, the tallying software sends encrypted e-votes to the HSM and receives the corresponding decrypted e-votes. The sum is computed outside the HSM. Here, the decryption key is protected, but the key to activate the HSM needs to be shared-analogous to the decryption key for homomorphic schemes in order to ensure that malicious key holders do not decrypt vote by vote with the HSM (and thereby compromise the secrecy of the vote) (Melanie Volkamer, 2009).

4.3.3 High Level Primitives

4.3.3.1 Threshold cryptography

All cryptographic voting systems use a special kind of encryption called randomized threshold public-key encryption. Threshold cryptosystems distribute functionality of cryptographic protocols to establish robustness(Burnester & Magkos, 2003). The public-key property ensures that anyone can encrypt using a public key. The threshold-decryption property ensures that only a quorum of the trustees (more than the "threshold"), each with his own share of the secret key, can decrypt.

4.3.3.2 Bulletin Boards

These are public channels that enable voters to communicate with the voting authorities in public view. Protocols using bulletin boards enable verifiability by posting to public bulletin boards in several stages. Often a voter is presented with a unique identifier when his/her vote is cast, that s/he can use to confirm the validity of the vote, against a web bulletin board at a later date. Communications are authenticated by using digital signatures.

4.3.3.3 Anonymous Channels

These are implemented to assure voter anonymity. Besides mix nets, several proxy based anonymous channel protocols have been proposed, such as the anonymizer(Community Connexion Inc, n d) and the LPWA(Burnester & Magkos, 2003) (Goldschlag, Reed, & Syverson, 1999).

4.3.3.4 Zero Knowledge proofs

These are prover verifier interactive protocols, in which the prover proves to a verifier the correctness of a statement, in such a way that the prover does not reveal anything the verifier could not learn by himself, apart that the fact that the statement is correct(Goldwasser, Micali,

& Rackoff, 1989).Zero knowledge proofs have been extensively used in election cryptographic protocols to prove the validity of encrypted votes in homomorphic elections, to prove the correctness of permutations in mix nets, to prove the correctness of encryptions in incoercible protocols, and to prove the correctness of blind signatures (Burnester & Magkos, 2003).

4.3.4 Which cryptosystems to use?

In reality, electronic voting implementations use a combination of the above cryptosystems. Often, an implementation may use blind signatures in combination with anonymous channels, where the channels will be implemented using MIX nets or be based on some physical assumption (Damgard, Groth, & Salomonsen, 2003). In such an example a voter would prepare his vote in clear-text and then interact with a validator server which would validate his eligibility to vote. If this is the case, the validator will blindly sign the vote. All voters then send their votes to a separate server responsible for counting. In order to preserve privacy, this is done over anonymous channels. Such a channel can be implemented as a mix net. The Estonian electronic voting system combines blind signatures and the principle of separation of duty to achieve privacy during vote casting.

A different approach could use a combination of homomorphic encryption, zero knowledge proofs and threshold cryptography (Damgard, Groth, & Salomonsen, 2003). In such an example, a voter simply publishes an encryption of his vote, represented as a number. This encryption makes use of public-key cryptosystem, i.e. there is a public key known by everyone that can be used for encrypting each vote. When casting a vote, the voter must prove his eligibility to vote. Furthermore he must prove knowledge of casting a valid vote without revealing the vote itself. This is achieved using zero knowledge proofs;thus not violating privacy. As this cryptosystem uses homomorphic encryption the votes can be "implicitly added" to get the encrypted tally. This tally can be decrypted securely with the secret key that has been shared between authorities (threshold cryptography).

Numerous protocols have been proposed, that combine these cryptographic protocols in ways that attempt to overcome each ones weaknesses(efficiency, scalability etc.). Although cryptography is one of the strongest tools available for securing information systems and data, cryptography is only a middle solution. Even with perfect mathematics, the data must exist in an unencrypted format at the endpoints(before and after encryption, before vote casting and during tallying). These are identified as weak points throughout electronic voting literature. In

the successive chapter, we shall attempt to identify ways of preserving the principles of security at these stages.

4.4 Chapter Summary & Conclusions

This chapter explored security controls that attempted to fulfill the predefined security requirements. Evolution in the field of cryptography has taken cryptographic algorithms out of the theoretical sphere and applied them as solutions to a number of information systems security issues. Cryptography is concerned with the construction of schemes that should withstand abuse. Cryptographic protocols provide an opportunity to generate trust between involved parties of an election. Cryptography is a crucial element of the overall system security, dealing with integrity, confidentiality, authenticity of communications and data and verifiability of elections. The design of cryptographic voting schemes, which started in the early 80's, has proved to be very challenging, due to the multitude and conflicting nature of properties such schemes need to satisfy. A number of election crypto-systems have been proposed and evaluated. Today this technology is believed to be mature, due to intense scrutiny that has occurred in the field over recent years. Within this context, Public Key Infrastructure is identified as the essential architecture upon which security and trust are built, in order to provide authentication, identity verification, encryption and non-repudiation in electronic transactions. The ability of the deployed e-passport PKI to extend and meet the correlating demands of an e-ID infrastructure have been explored and a high level solution is proposed.

Chapter 5

Countering the limitations

5 COUNTERING THE LIMITATIONS

Chapter Abstract: This chapter identifies the security requirements not addressed by cryptography and explores countermeasures that exhibit the required properties. Within this scope, cloud computing is explored, as currently a multitude of applications and services are being transported to this deployment model, ranging from electronic government services to word processing applications. We are currently witnessing events in which the clouds capabilities are being leveraged to perform malicious acts, such as using cloud instances as bots to perform DDOS or crack passwords. Diametrically opposed to this, cloud implementations are being implemented to achieve advanced security features, mostly due to the universality of the architecture, the resiliency and elasticity of services. In this section we explore cloud computing applicability to electronic government and electronic voting, evaluate the technology's benefits and detriments, while identify the unique security issues introduced by this innovative architecture and ways of overcoming these. This chapter provides recommendations of considerations, that can assist in reducing previously identified vulnerabilities.

5.1 Identification of limitations of cryptography

Cryptography by itself is fairly useless (Ferguson & Schneier, 2003). Currently a number of cryptographic schemes, attempt to provide a sense of security in e-voting. Cryptographic protocols provide an opportunity to generate trust between involved parties of an election. Cryptography is a crucial element of the overall system security, dealing with integrity, confidentiality, authenticity of communications and data and verifiability of elections. Unfortunately, a wide number of threats to e-voting security can circumvent cryptographic solutions, before they have been applied.

Bruce Schneier, a renown security expert and cryptographer, recently stated,

"*I have made a living as a cryptography consultant: designing and analysing security systems. To my initial surprise, I found that weak points had nothing to do with the mathematics. They were in the hardware, the software, the networks and the people. Beautiful pieces of mathematics were made irrelevant through bad programming, a lousy operating system, or someone's bad password.*"

Schneier paraphrases a famous roger Needman and Butler Lampson quotation thusly:

"*If you think technology can solve your security problems, then you do not understand the problems and you do not understand technology.*"

Cryptography is only a middle solution—even with perfect mathematics, the data must exist in an unencrypted format at the endpoints(before and after encryption). With traditional hardware and software architectures, a malicious payload on a voting client, can modify the voter's vote, without the voter or anyone else noticing, regardless of the kind of encryption or voter authentication in place. Essentially because the malicious code can do its damage before the encryption and authentication is applied to the data, the malicious module can then erase itself after doing its damage, so that there is no evidence to correct, or even detect the fraud. Although strong encryption is a very powerful tool for addressing issues of integrity, confidentiality and authenticity, additional technological implementations are required to address availability issues and enhance overall computer security.

Certain aspects rely upon the naïve assumption that integrity and secrecy are guaranteed over the Internet, since ballots would be encrypted prior to transmission. Unfortunately this is untrue. Without fully securing the vote system end-to-end, not only during distribution but also by monitoring the actual development of the balloting software to ensure that trapdoors or other bogus software is not inserted into encryption or other processes (Mercuri, 2001)

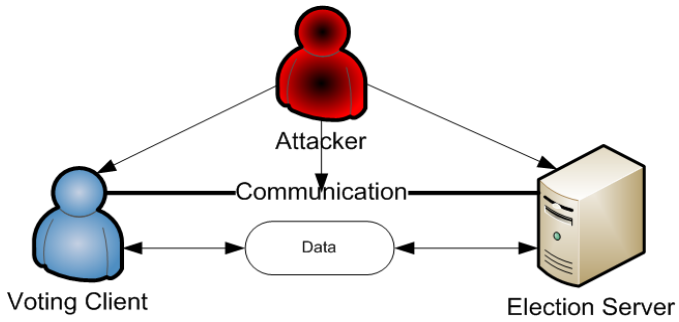

Illustration 47: I-Voting vulnerabilities

I-voting is more vulnerable to attacks than other forms of electronic voting (Burnester & Magkos, 2003) :

- at the voting client: worm-like viruses or trojan horses may alter the vote before any encryption or authentication is applied to the data. An attacker may remotely exploit security holes at the operating system or at the web browser(Rubin, 2001).
- At the communication level. During a spoofing attack, an attacker could feed a voter with a seemingly legitimate web page. This may be enough to change the voters vote. Communication may also be threatened by other network based

attacks(e.g. TCP SYN spoofing, IP fragmentation)

- At the election server. Attacks at this level are similar to attacks at the voting client. Denial of Service attacks are also possible. The bottleneck problem is similar to a DOS attack except that the jam is caused by an overwhelming number of legitimate contacts occurring simultaneously.

We shall review these issues in the consecutive chapters and attempt to provide recommendations of considerations that can assist in reducing these limitations.

5.2 Voting Client Integrity

In the field of computer and network security the principle of the weakest link is often quoted. This principle states that overall system security cannot be stronger than its weakest link. As security is often viewed as a chain, a single breaking point shall crumple its overall efficiency. An intruder must be expected to use any available means of penetration and shall attack a system at its most vulnerable point. The client's personal computer is identified as the weakest point in an e-voting environment (Jefferson, et al, 2004; Gritzalis, 2002; Cranor, 2003). Internet voting requires that the voting software run on a machine and possibly an operating system and web browser that is outside of the control of the election jurisdiction. (Jones, 2003)

Voters' home computers are most likely to be less defended than corporate ones, as they often run outdated virus protection systems, mis-configured firewalls, unpatched operating systems, and contain numerous applications from various vendors, making these machines especially susceptible to malicious attacks. The NIST guide to "Enterprise Telework and Remote Access Security guide for Federal IS" states that the primary threat against most telework client devices is malware, including viruses, worms, malicious mobile code, Trojan horses, rootkits, and spyware. Election integrity is closely related to the integrity of the voting client.

A number of requirements have previously been proposed to guard the integrity of the client's terminal (Gritzalis, 2002):

- Users should administer the system only from specific terminals, within a predefined time window, using a combination of strong authentication means, such as biometrics or smart cards.
- The minimum necessary software and hardware components should be installed on

the host of the voting system.

- The maximum possible level of operating system security enhancement should be applied to all machines of the voting system.

Additionally, the NIST guide to enterprise telework and remote access for Federal Information Systems states that, "telework client devices should have the same local security controls as other client devices in the enterprise – OS and application security updates applied promptly, unneeded services disabled, antimalware software and a personal firewall enabled and kept up-to-date, etc"(NIST800-46, p. 4-2).

A number of solutions have been proposed that attempt to overcome this issue. These attempts can be distinguished between a fat-client approach, a thin-client (the applet solution) approach, and a Web browser solution (Volkamer, 2009).

Web Browser Solution

This approach makes use of the web browser on the client computer to communicate with the voting server. This approach does not include any kind of Java applet. The main security mechanisms in this approach run on the voting server side. The only assumed security functionality is SSL.

Using SSL, it is possible to ensure confidentiality and integrity of the exchanged messages. Moreover, the authenticity of the voting server can be ensured (with the help of the voter who needs to check the voting server's certificate). (Volkamer, 2009) This solution benefits from a usability perspective, as there is no requirement for the user to install any software. Web browser based solutions also offer cross platform portability.

However, there are critical disadvantages to this approach. Firstly, the remote electronic voting system has no possibility to check the trustworthiness of the vote-casting device, for example, whether there is a virus or Trojan Horse on the vote-casting device which affects the communication between the voter and the voting server. Moreover, an (un-patched) Web browser could weaken the trustworthiness by well-known exploits.

The second disadvantage is caused by the poor Web browser functionality. Thus, most of the proposed voting protocols cannot be implemented, because they require security functionality on the client-side. For the same reason, this approach can only be used in combination with secrets as authentication techniques. The only disadvantage from the

usability point of view, is the necessity for the voter to check the certificate of the voting server. This might be new for many voters, even if they use SSL on a daily base.(Volkamer, 2009). Finally the software used for vote casting is not contained or able for audit in case of error or disaster.

Fat-Client Solution

A **fat/heavy client** or **thick client** is a computer in client–server architecture or networks, which typically provides rich functionality independent of the central server. This approach is called fat-client, because the client side voting software is loaded with security functionality and cryptographic algorithms. In this approach, client side voting software needs to be installed and executed on the voting terminal in order to cast a vote. Fat client software often comes in the form of a bootable clean cds, which attempt to convert any standard PC into a secure terminal. These bootable cs bypass the users operating system and load a specific secure installation.

Any available voting protocol can be implemented using the fat-client approach, thus, in contrast to the Web browser solution, this solution does not exclude any voting protocol nor any authentication technique. In addition, a fat-client can include a virus scanner or similar security software in order to verify the trustworthiness of the vote-casting device, before starting the vote casting process.

On the downside, this approach limits cross platform portability and accessibility of the solution. Additional disadvantages of this approach are the distribution, installation, and maintenance of the client-side voting software. Delayed updating of software can propose a significant threat to the client system, especially when using bootable cds that are not updatable after distribution.

Thin-Client Solution

A thin client (sometimes also called a lean or slim client), is a computer that depends heavily on a server to fulfil its traditional computational roles. The Web browser solution is from a usability and maintenance aspect preferable, while from a security point of view the fat-client is advantageous. A mix of both strong points is provided by the thin-client approach. It often implements a Java applet running in the Web browser. This Java applet is the client-side voting software, which provides the necessary security functionality on the client-side.

A number of requirements specifically concerned about the voting clients integrity restrict the use of some of the above solutions.

- Protection Against Malicious Software Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. (voting Standards)
- Operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.
- The system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software. (Voting Standards 1)

Different approaches to implement a security function to meet the client side security requirements have been proposed, while most of them address the problem but do not satisfactorily solve it for the described security problem definition(Melanie Volkamer, 2009) :

- The Swiss and GI guidelines provide voters with guidelines on how to improve the security of their vote casting clients. This approach can reduce the risks created by malware, but many voters are not likely to be able to follow the instructions(Volkamer, 2009). Moreover, such an approach is useless against malicious voters installing malware on purpose.
- Otten (Otten, 2005) proposes a secure voting operating system based on Knoppix. Voters are required to boot their vote-casting device from CD. This approach also does not solve the malicious voter problem, but it prevents attacks caused by malware.
- Helbach (Helbach & Schwenk, 2007) (Oppliger, Schwenk, & Helbach, 2008)proposes code sheets to overcome the problem with malicious clients. This code sheet is sent via ordinary mail and contains for each candidate a voting TAN, and a confirmation TAN12. The voter enters a corresponding voting TAN instead of choosing a candidate on the PC screen. To verify the correctness, he compares the received and displayed confirmation TAN with the one on the code sheet. The disadvantages of this approach concerns the user-friendliness (which decreases in particular for complex ballots implementing) and the fact that the requirement O.T.ProofGen can only be ensured if vote updating is applied(Melanie Volkamer, 2009).

- Another approach proposes to use an appropriate security architecture based on a security kernel and on Trusted Computing elements. Such a solution is the only one that could efficiently prevent the described threat. However, currently, there are still open problems with Trusted Computing and it is not easy to know-how to integrate the Trusted Computing elements in a Common Criteria evaluation (Volkamer, 2009).

What is essentially required to ensure the integrity of the voting client efficiently is a solution that can exhibit the benefits of a "fat client solution", combined with the usability, portability, updatability and accessibility of a thin client solution.

5.3 Election server availability

Availability applies both to data and to services (that is, to information and to information processing), and it is similarly complex. We can construct an overall description of availability by combining these goals. We say a data item, service, or system is available if (Pfleeger & Pfleeger, 2006):

- There is a timely response to our request.
- Resources are allocated fairly, so that some requesters are not favoured over others.
- The service or system involved follows a philosophy of fault tolerance, whereby hardware or software faults lead to graceful cessation of service, or to workarounds, rather than to crashes and abrupt loss of information.
- The service or system can be used easily and in the way it was intended to be used.

In elections, availability is (because of the universal requirement) as critical as other properties. Attacks at the communication level and at the election server can be categorized as attacks on the systems availability.

The availability of a voting system is defined as the probability that the equipment (and supporting software) needed to perform designated voting functions will respond to operational commands and accomplish the function. The voting system shall meet the availability standard for each of the following voting functions.

System availability is measured as the ratio of the time during which the system is operational (up time) to the total time period of operation (up time plus down time). Inherent availability (AI) is a the fraction of time a system is functional, based upon Mean Time

Between Failure (MTBF) and Mean Time to Repair (MTTR), that is:

$$AI = (MTBF)/(MTBF + MTTR)$$

Mean Time to Repair (MTTR) is the average time required to perform a corrective maintenance task during periods of system operation. Corrective maintenance task time is active repair time, plus the time attributable to other factors that could lead to logistic or administrative delays, such as travel notification of qualified maintenance personnel and travel time for such personnel to arrive at the appropriate site.

Corrective maintenance may consist of substitution of the complete device or one of its components, as in the case of precinct count and some central count systems, or it may consist of on-site repair.

Voting systems are required to achieve at least **ninety nine percent** availability during normal operation (Federal Election Commission- Voting System Standards). This standard encompasses, for each function, the combination of all devices and components that support the function, including their MTTR and MTBF attributes.

A DDOS attack against a voting server can render the e-voting system unavailable to eligible voters. A solution given to requiring 99% availability, is extending the internet vote casting period. “Since the Internet is vulnerable to a denial of service attack of significantly long duration, the voters must be able to cast their vote over a period of several days or weeks” (Peralta, 2003).

This solution has proved to be effective (see Estonia), but as the field of computer science is evolving, innovative deployment architectures must be explored. Such an innovative deployment architecture is cloud computing. The idea, the concept, and the term, that is cloud computing, has recently passed into common currency and the academic lexicon in an ambiguous manner, as cloud dust is being sprinkled on an excess of emerging products. Exorcising complexity and protecting against the caprice of the moment, in the following section we explore the notion behind the hype of cloud computing and evaluate its relevance to electronic government and electronic voting information systems.

5.4 Cloud Computing

Currently a multitude of applications and services are being transported to cloud computing, ranging from electronic government services to word processing applications. We

are witnessing events in which the cloud's capabilities are being leveraged to perform malicious acts, such as using cloud instances as bots to perform DDOS or crack passwords. Diametrically opposed to this, cloud implementations are being implemented to achieve advanced security features, mostly due to the universality of the architecture, the resiliency and elasticity of services. In this section, we explore cloud computing applicability to electronic government and electronic voting, evaluate the technology's benefits and detriments, while identify the unique security issues introduced by this innovative architecture and ways of overcoming these.

5.4.1 Cloud computing Architecture

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST, 2009). The name cloud computing was inspired by the cloud symbol that is often used to represent the Internet in flow charts and diagrams. A distinct migration to the clouds has been taking place over recent years, with end users maintaining a growing number of personal data, including bookmarks, photographs, music files, etc. on remote servers accessible via a network.

Throughout computer science history, numerous attempts have been made to shift users from computer hardware needs and from time-sharing utilities envisioned in the 1960s, and the network computers of the 1990s, to the commercial grid systems of more recent years. This abstraction is steadily becoming a reality, as a number of academic and business leaders in this field of science are spiraling towards cloud computing. Cloud computing is an innovative IS architecture, visualized as what may be the future of computing, a driving force demanding from its audience to rethink their understanding of operating systems, client server architectures, and browsers.

Cloud computing is empowered by virtualization technology, a technology that actually dates back to 1967, but that for decades was available only on mainframe systems. In its quintessence, a host computer runs an application known as a hypervisor; this application creates one or more virtual machines, which simulate physical computers so faithfully, that the simulations can run any software, from operating systems, to end-user applications (Naone, 2009). The software “supposes” it has physical access to a processor, network, and disk drive. Virtualization is a critical element of cloud implementations and is used to provide

the essential cloud characteristics of location independence, resource pooling, and rapid elasticity (explained in detail in the following section). Differing from traditional network topologies (e.g. a client server), cloud computing is able to offer flexibility and alleviate traffic congestion issues.

At a low level, a hardware layer, a number of physical devices, including processors, hard drives and network devices, are located in data centers, independent from geographical location, which are responsible for storage and processing needs. The combination of software layers, the virtualization layer, and the management layer allows for the effective management of servers. The virtualization layer allows a single server to host many virtual servers, each of which can operate independently of the others. The management layer monitors traffic and responds to peaks or drops with the creation of new servers or the destruction of non-necessary ones. Beyond the software layers are the available service models, which are:

1) Infrastructure as a Service (IaaS). IaaS provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources, and allows the consumer to deploy and run arbitrary software, which can include operating systems and applications.

2) Platform as a Service (PaaS). PaaS provides the consumer with the capability to deploy consumer-created or acquired applications, which are produced using programming languages and tools supported by the provider, onto the cloud infrastructure.

3) Software as a Service (SaaS). SaaS provides the consumer with the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices, through a thin client interface, such as a Web browser (e.g., Web-based email).

Four deployment models have been identified for cloud architecture solutions and are described below.

1) Private cloud. The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise.

2) Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise.

3) Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

4) Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). (The NIST Definition of Cloud Computing, 2009).

Cloud computing is viewed as one of the most promising technologies in computing today, inherently able to address a number of issues. The recent increase in the use of full virtualization products and services, has been driven by many benefits (NIST 800-125). In general, servers using full virtualization, can benefit more of the computer's processing and memory resources than servers running a single OS instance and a single set of services. Recent advances in CPU architectures have enabled full virtualization as more processing power is available than in previous years, and similar advances are expected to continue to be made both by CPU vendors and virtualization software vendors. Also, CPU architecture changes have made full virtualization more secure by strengthening hypervisor restrictions on resources(NIST 800-125).

A number of key characteristics of cloud computing have been identified (Sun Microsystems, 2009; Reese, 2009; The NIST Definition of Cloud Computing, 2009; Rajkumar, 2009):

1) Flexibility/Elasticity. Users can rapidly provision computing resources, as needed, without human interaction. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out or up.

2) Scalability of infrastructure. New nodes can be added or dropped from the network as can physical servers, with limited modifications to infrastructure set up and software.

3) Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous platforms (e.g., mobile phones, laptops, and PDAs).

4) Location independence. There is a sense of location independence, in that the customer generally has no control or knowledge over the exact location of the provided resources.

5) Reliability. Reliability improves through the use of multiple redundant sites, which makes cloud computing suitable for business continuity and disaster recovery.

6) Economies of scale and cost effectiveness. Cloud implementations, regardless of the deployment model, tend to be as large as possible in order to take advantage of economies of scale. Large cloud deployments can often be located close to cheap power stations and in low-priced real estate in order to lower costs.

7) Sustainability. Sustainability comes about through improved resource utilization, more efficient systems, and carbon neutrality.

8) Open free software. The need for openness and interoperability is a driving force for designing and implementing cloud infrastructures, and for moving towards open source software solutions. The massive scale of many clouds, combined with the need for many software licenses, encourages the use of free software in the development of cloud architectures. To prevent vendor lock-in, open APIs, open data formats, and standards implemented through open-source reference models are vital requirements.

9) Advanced Security Technologies. Cloud implementations often contain advanced security technologies, which are mostly available due to the centralization of data and universal architecture. The homogenous, resource-pooled nature of the cloud enables cloud providers to focus all of their security resources on securing the cloud architecture. At the same time, the automation capabilities within a cloud, combined with the large focused security resources, usually result in advanced security capabilities.

In its quintessence, cloud computing has the capability to address a number of identified deficiencies of traditional architectures, but maintaining a perspicacious vision is essential in a field that is evolving exponentially. Cloud computing is not a panacea and many believe it to be little more than market-driven hype. Cautiousness is necessary, so as not to be carried away by the caprice of the moment. Progress requires its audience to rethink their understanding of solid notions such as, the network and personal computers.

Recently, the U.S. federal cloud computing initiative was published, which is a service oriented approach, whereby common infrastructure information and solutions can be shared across the U.S. government (NIST, 2009). The overall objective is to create a more agile federal enterprise using cloud computing architecture, by which services can be reused and provisioned on demand to meet business needs. This endeavor can be viewed as an opening step into computing clouds, which is primarily focused on applications dealing with less sensitive data. These initiatives hold the capacity to expand into the building blocks of a universal e-Government solution, supported by cloud infrastructure, whereby computing

resources and tools can be uniformly shared between agencies and citizens, while increasing participation. Presently government use of cloud environments focuses mainly on information sharing and communications, rather than data processing. Beyond strictly communications, the US federal government is exploring methods to leverage cloud technology in a number of application-oriented ways (Paquette, Jaeger, & Wilson, 2010). Some agencies have begun to use the cloud for information processing; in other words, they are using it as an application and processing server rather than simply a repository. The US Defence Information Systems Agency (DISA) first awarded contracts to Hewlett-Packard, Apptis, Sun Microsystems and Vion for on-demand (a.k.a. software-as-a-service, or SAAS) data storage and processing services in 2006, under the aegis of its Defense Enterprise Computing Center (Mark, 2008). This service has matured into DISA's Rapid Access Computing Environment (RACE) (Beizer, 2009) and serves more than 3 million DOD users, with 18 processing centers, 1,400 applications, 180 software vendors, 18,000 copies of executive software, 45 mainframes, and more than 4,500 servers (Beizer, 2008) . Its operations are typical of a transaction system: the customer (usually an in-house or contractor developer) submits a credit card or purchase order number through a front-end portal, (developed in this case in Cluster Resources' Moab software) and describes the work to be performed and the environment needed. Upon purchase approval, the requestor purchases a computing environment. Access security is managed by public key infrastructure (PKI) credentials, or common access cards (Paquette, Jaeger, & Wilson, 2010).

Cloud computing has the capability to evolve beyond meeting the business needs of e-Government agencies and towards providing to numerous identified e-citizens related shortages. In the 1960s, John McCarthy, speaking at the MIT Centennial, stated that computation may someday be organized as a public utility “Cloud computing is a reincarnation of the computing utility of the 1960s but is substantially more flexible and larger scale than systems of the past”, says Google executive and Internet pioneer Vint Cerf. The vision of computing, offered to all, when paired with initiatives such as e-Inclusion and One Laptop Per Child, presents an opportunity to overcome economic disparities and geographical differences in society, steering towards an all-inclusive digital e-citizen platform.

The appearance of cloud computing, demands that we rethink our current understanding of personal computers, operating systems, and network architectures. Clusters of Web servers assembling, conjuring clouds of massive computational resources, could inevitably one day

meet all individuals' needs. The opportunities for e-Government are enormous, and providing a personalized online desktop system, which would be accessible via a "web browser" or a custom-made operating system, is just around the corner. Barriers to the wide adoption of e-Government solutions may be abolished all together, as purchasing hardware to upgrade a personal computer to meet with growing requirements, may one day be a remnant of the past, as all computational needs could be met through a "dumb" terminal over a network. Clouds can enhance electronic participation by providing the means for wider citizen involvement, bringing down barriers experienced by digitally or socially excluded groups.

Cloud computing provides a single access point towards a gateway of interaction with government information, personal information and government representatives, presented through an online desktop application for all citizens. Through SaS, a surplus of applications can be provided, including social networking and collaboration tools, cryptographic functions, electronic voting functions, information services, email, etc., thereby linking supportive infrastructure with services supplied.

The U.S. Federal cloud computing initiative provides a high-level overview of the key functional components for cloud computing services for the Government.

- Citizen Adoption (Wikis, Blogs, Social Networking, Collaboration and Participatory Tools)
- Government Productivity (Email /IM Services, Office Automation etc)
- Government Enterprise Applications(Business Applications, Core Mission Applications, Legacy Applications)

As initiatives across the globe are attempting to improve organisational processes and cooperation between federal institutions and businesses, it is crucial to unify tools and infrastructure into a common platform. Cloud computing offers an operational model that can digitally amalgamate geographically remote data centres into a common infrastructure, providing a principal gateway to government related services and data. Cloud computing leverages existing infrastructure and provides public services, while using fewer resources, reducing carbon emissions, and contributing to wider carbon-reduction targets.

Federal institutions adopting a cloud computing operating model, benefit from the concentration of data; centralization leads to greater consistency and accuracy. Unifying remote data centers into a universal solution overcomes problematic issues of data

consistency, (federal agencies maintaining out-dated archives, several data formats in use etc.). The risks that are involved with the adoption of proprietary software and data formats for the long term survival of data are enormous. The adoption of proprietary standards and software models, which lock data into a specific model, can jeopardize system security, privacy, and interoperability. The creation of a truly competitive computing marketplace that allows for portability and easy switching between providers, requires a triumph of open APIs, open data formats, and standards that are implemented through open-source reference models.

The centralization of data and application solutions holds the capacity to provide additional tools, thereby enhancing timely communications and control. Reducing the time required to access both data and required applications, not only across the federal structure but also between business partners, generates stronger collaboration. Leveraging existing remote infrastructures into a common IS reduces installation and monitoring time and expenses, and focuses on improving quality. By centrally managing, developing, implementing, and assessing IS's costs can be amortized across the federal structure.

It is imperative to follow a methodological framework for the assessment and analysis of electronic government proposals, as there are many technical, organizational, and institutional elements to be considered. This paper adopts a framework proposed by J. Montagna (Montagna, 2005), which enhances previous works done by several scholars, that allows determining whether proposed initiatives are suitable for governmental action and determines the benefits provided in a multidimensional approach. This framework also evaluates initiatives regarding the dimensions characterizing e-Government actions, products (Table 11), time (Table 12), distance (Table 13), interactions (Table 14), and procedures.

Performance Criteria	Product
Efficiency	-Uniform access to data and applications
Effectiveness	-Improved data quality -Improved quality of services
Strategic Benefits	-Uniformity of solution -Introduction of new services -Integration of existing infrastructure deployments
Transparency	Constant evaluation and control of services and application usage,reduction of expenses

Table 11: Characterizing e-Government products

Performance Criteria	Time
Efficiency	-Reduction of time required to access applications and data -Reduction of time required for installations and modifications -Reduction of monitoring time
Effectiveness	-Applications and resources available on demand
Strategic Benefits	-Timely opinion and expression -Possibility of real time cooperation across agencies
Transparency	-Timely control

Table 12: Characterizing e-Government actions according to time

Performance Criteria	Distance
Efficiency	-Overcomes geographical difficulties -Cross agency and boundaries cooperation -Reduced distribution and delivery cost -Improved data quality due to centralization and uniformity -Improved data accuracy due to centralization and uniformity
Effectiveness	-Improved communication and interaction
Strategic Benefits	-Introduction of new services independent of geographical location -Hybrid centralization
Transparency	-Access services and data independently from geographical location

Table 13: Characterizing e-Government actions according to distance

Performance Criteria	Interaction
Efficiency	-Reduced deployment cost -Reduced interaction costs -Increase of cooperation -Increase of participation
Effectiveness	-Generation of relationships -Enhanced accessibility
Strategic Benefits	-New communication and operation channels -More information and accurate information available
Transparency	-Active participation -Breakdown of barriers

Table 14: Characterizing e-Government actions according to interactions

Adopting a cloud infrastructure for electronic government presents a number of business drivers.

1. Performance. The cloud computing model increases cross-agency collaboration, as tools and data can be deployed upon demand, reducing any additional overhead.

Business and citizen related tasks can benefit from increased computational resources, available due to the elasticity of cloud computing services. The architectural characteristics can support the deployment of additional "citizen to citizen" and "business to business" tools, which can increase participation and electronic governance performance. The centralization of data, improves data quality and availability, increasing the efficiency of related business processes.

2. Cost efficiency. Cloud computing proposes many cost effective gains and business drivers. Cloud computing deployments benefit from economies of scale, as purchasing hardware is performed in a large scale and data centers can be deployed at geographical locations, with lower overheads, (such as real estate, electricity, etc.). Due to the elasticity of services provided, energy efficiency and power savings reduce overall expenditure. The cost of human resources may additionally be reduced, as it will not be required for all agencies to staff technical teams and powerful management automation characteristics can alleviate the load put on administrative teams. Furthermore, the use of open source software solutions can minimize costs, which, in turn, can reduce the need for multiple licenses in the cloud.
3. Scalability. In addition to cloud infrastructure's ability to scale to demand, either horizontally or vertically though virtualization, hardware servers can be added to the infrastructure in a complex free manner.
4. Resiliency and business continuity. Deploying data centers at multiple geographical locations – often referred to as availability zones – guarantees availability of services, if a specific data center fails. In the instance of a disaster, sophisticated network rerouting ensures business continuity.
5. Maintainability. Centralization of IT infrastructure simplifies monitoring and maintenance tasks.
6. Security. The cloud computing model provides a plethora of information and communication security benefits, including centralization and unification of the security infrastructure.

This rapid transition towards the clouds, has fuelled concerns on a critical issue for the success of information systems, communication and information security. From a security perspective in the following section, we identify a number of uncharted risks and challenges that have been introduced from this relocation to the clouds, deteriorating much of the

effectiveness of traditional protection mechanisms. Firstly we evaluate cloud security by identifying unique security requirements and secondly we present a viable solution that attempts to eliminate these potential threats. The following section proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment.

5.4.2 Cloud Computing Security

Trust in a cloud environment depends heavily on the selected deployment model, as governance of data and applications is outsourced and delegated out of the owner's strict control. In traditional architectures, trust was enforced by an efficient security policy, which addressed constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people. In a cloud deployment, this perception is totally obscured. In the case of public or community clouds, control is delegated to the organisation owning the infrastructure. When deploying on a public cloud, control is mitigated to the infrastructure owner to enforce a sufficient security policy, which guarantees that appropriate security activities are being performed to ensure that risk is reduced. This introduces a number of risks and threats, as essentially security is related to trusting the processes and computing base implemented by the cloud owner. It is crucial to differentiate between deployment models, as a private cloud, where the infrastructure is operated and managed on premise by a private organization, does not introduce additional unique security challenges, as trust remains within the organization. In such a situation, the infrastructures owner remains the data and process owner.

Most importantly the cloud environment deteriorates the perception of perimeter security. *Perimeter security* is a set of physical and programmatic security policies that provide levels of protection on a conceptual borderline, against remote malicious activity. Traditionally, it is believed that any connectivity to systems or organizations outside of an organization provides an opening for unauthorized entities (personnel or processes) to gain access or tamper with information resources. Upon this static conceptual boundary, security controls were deployed to protect the Information System within it. In a cloud computing model, the perimeter becomes fuzzy, weakening the effectiveness of this measure. The emergence of cloud service models, is expected to lead to a deconstruction of the application services as they are already delivered in existing "closed" service provisioning environments (Altmann et al., 2010). From the traditional viewpoint of perimeter security, the cloud appears outside the trust borderline

and should be viewed with suspicion, but this adversely leads to not trusting essential business processes and services that have been outsourced. It has become impossible to place a virtual moat around an organizations castle, as an abundance of services have been outsourced. The ability to clearly identify, authenticate, authorize and monitor who or what is accessing the assets of an organization is essential to protecting an IS from threats and vulnerabilities. Separation is the key ingredient of any secure system, and is based on the ability to create boundaries between those entities that must be protected and those which cannot be trusted(Sherman, 1992).

5.4.2.1 Unique threats to a cloud environment

Cloud computing due to its architectural design and characteristics imposes a number of security benefits, which include centralization of security, data and process segmentation, redundancy and high availability. While many traditional risks are countered effectively, due to the infrastructures singular characteristics, a number of distinctive security challenges are introduced. Cloud computing has "unique attributes that require risk assessment in areas such as availability and reliability issues, data integrity, recovery, and privacy and auditing" (Gartner, 2008)

5.4.2.1.1 Confidentiality in the cloud

The threat of data compromise escalates in the cloud, due to the increased number of parties, devices and applications involved, that leads to an augmented number of points of access. Delegating data control to the cloud, inversely leads to an increment in the risk of data compromise, as the data becomes accessible to an augmented number of parties. A number of concerns emerge regarding the issues of multi-tenancy, data remanence, application security and privacy (Cloud Security Alliance, 2010).

Multi-tenancy refers to the cloud characteristic of resource sharing. Several aspects of the IS are shared including, memory, programs, networks and data. Cloud computing is based on a business model in which resources are shared (i.e., multiple users using the same resource) at the network level, host level, and application level. Although users are isolated at a virtual level, hardware is not separated. With a multi-tenant architecture, a software application is designed to virtually partition its data and configuration, so that each client organization works with a customized virtual application instance. Multi-tenancy, is relative to multitasking in operating systems. In computing, multitasking is a method by which multiple tasks, also known as processes, share common processing resources such as a CPU. Multi-

tenancy, as multitasking, presents a number of privacy and confidentiality threats. Object re-usability is an important characteristic of cloud infrastructures, but reusable objects must be carefully controlled lest they create a serious vulnerability. Data confidentiality could be breached unintentionally, due to data remanence. Data remanence is the residual representation of data that have been in some way nominally erased or removed. Due to virtual separation of logical drives and lack of hardware separation between multiple users on a single infrastructure, data remanence may lead to the unwilling disclosure of private data. But also maliciously, a user may claim a large amount of disk space and then scavenge for sensitive data.

Data confidentiality in the cloud can be correlated to user authentication. Protecting a user's account from theft is an instance of a larger problem of controlling access to objects, including memory, devices, software etc. Electronic authentication is the process of establishing confidence in user identities, electronically presented to an information system. Lack of strong authentication can lead to unauthorized access to users account on a cloud, leading to a breach in privacy.

Software confidentiality is as important as data confidentiality to the overall system security. Software confidentiality refers to trusting that specific applications or processes will maintain and handle the user's personal data in a secure manner. In a cloud environment, the user is required to delegate "trust" to applications provided by the organization owning the infrastructure. Software applications interacting with the user's data must be certified not to introduce additional confidentiality and privacy risks. Unauthorized access can become possible through the exploitation of an application vulnerability or lack of strong identification, bringing up issues of data confidentiality and privacy. In addition, the cloud provider is responsible for providing secure cloud instances, which should ensure users privacy.

Privacy is the desire of a person to control the disclosure of (personal) information. Organizations dealing with personal data are required to obey to a country's legal framework, that ensures appropriate *privacy* and confidentiality protection. The cloud presents a number of legal challenges towards privacy issues involved in data stored in multiple locations in the cloud, additionally increasing the risk of confidentiality and privacy breaches. Instead of its data being stored on the company's servers, data is stored on the service provider's servers, which could be in Europe, Asia, or anywhere else. This tenet of cloud computing conflicts with various legal requirements, such as the European laws that require that an organisation

know where the personal data in its possession is at all times.

5.4.2.1.2 Integrity in the cloud

A key aspect of Information Security is integrity. Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and hardware. *Data Integrity* refers to protecting data from unauthorized deletion, modification or fabrication. Managing an entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated or stolen. By preventing unauthorized access, organizations can achieve greater confidence in data and system integrity. Additionally, such mechanisms offer greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity (accountability). *Authorization* is the mechanism by which a system determines what level of access a particular authenticated user should have to secured resources controlled by the system. Due to the increased number of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data.

A cloud computing provider is trusted to maintain data integrity and accuracy. The cloud model presents a number of threats including sophisticated insider attacks on these data attributes.

Software Integrity refers to protecting software from unauthorized deletion, modification, theft or fabrication. Deletion, modification or fabrication can be intentional or unintentional. For instance, a disgruntled employee may intentionally modify a program to fail when certain conditions are met or when a certain time is reached. Cloud computing providers implement a set of software interfaces or APIs, that customers use to manage and interact with cloud services. In addition to previously mentioned threats, the security of cloud services depends heavily on the security of these interfaces, as an unauthorized user gaining control of them could alter, delete or fabricate user data. In the cloud, responsibility for the protection of the software's integrity is transferred to the software's owner or administrator. Hardware and network integrity is an additional issue that needs to be addressed by the cloud provider, as he is burdened with protecting the underlying hardware from theft, modification and fabrication.

5.4.2.1.3 Availability in the cloud

Availability refers to the property of a system being accessible and usable upon demand

by an authorized entity. System availability includes a systems ability to carry on operations even when some authorities misbehave. The system, must have the ability to continue operations even in the possibility of a security breach. Availability refers to data, software but also hardware being available to authorized users upon demand. Leveraging users from hardware infrastructure demands, generates a heavy reliance on the ubiquitous network's availability. The network in now burdened with data retrieval and processing. The cloud owner needs to guarantee that information and information processing is available to clients upon demand. Cloud computing services present a heavy reliance on the resource infrastructures and network availability at all times.

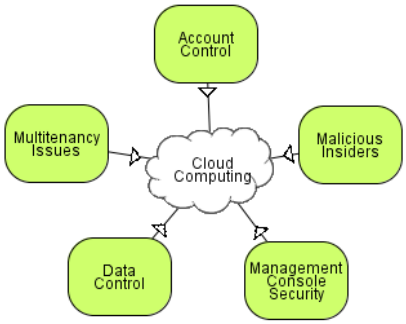

Illustration 48: Categorization of threats

Understanding and clearly documenting specific user requirements is imperative in designing a solution targeting at assuring these necessities. Verifying identities many of which share common fundamental security requirements, and determining specific needs for data protection and information security can be one of the most complex elements of IS design. This multiuser distributed environment, poses unique security challenges, depending on the level at which the user operates, application, virtual or physical (Table 15)

Level	Service Level	Users	Security Requirements	Threats
Application Level	Software as a Service (SaS)	End Client applies to a person or organization who subscribes to a service offered by a cloud provider and is accountable for its use	○ Privacy in multi-tenant environment ○ Data protection from exposure(remnants) ○ Access Control ○ Communication Protection ○ Software Security ○ Service Availability	○ Interception ○ Modification of data at rest and in transit ○ Data interruption(Deletion) ○ Privacy Breach ○ Impersonation ○ Defacement ○ Session hijacking ○ Traffic flow Analysis ○ Exposure in network
Virtual Level	Platform as a Service (PaS)	Developer-Moderator applies to a person or organization that deploys software on a cloud infrastructure	○ Access Control ○ Application Security ○ Data security, (Data-in-transit, Data-at-rest, Remanence) ○ Cloud management control security ○ Secure Images ○ Virtual Cloud Protection ○ Communication Security	○ Programming flaws ○ Software Modification ○ Software Interruption (Deletion) ○ Impersonation ○ Session hijacking ○ Traffic flow Analysis ○ Exposure in network ○ Defacement ○ Connection Flooding ○ DDOS ○ Impersonation ○ Disrupting communications
	Infrastructure as a Service (IaS)			
Physical Level	Physical Datacenter	Owner applies to a person or organization that owns the infrastructure upon which clouds are deployed	○ Legal not abusive use of cloud computing ○ Hardware Security ○ Hardware Reliability ○ Network protection ○ Network resources protection	○ Network Attacks ○ Connection Flooding ○ DDOS ○ Hardware Interruption ○ Hardware Theft ○ Hardware Modification ○ Misuse of infrastructure ○ Natural Disasters

Table 15: User-specific security requirements.

The security objectives within a distributed system are essentially (Sherman, 1992):

- to ensure the availability of information communicated between or held within participating systems;
- to maintain the integrity of information communicated between or held

within participating systems, i.e. preventing the loss or modification of information due to unauthorized access, component failure or other errors;

- to maintain the integrity of the services provided, i.e. correct operation;
- to provide control over access to services or their components to ensure that users may only USC services for which they are authorized;
- to authenticate the identity of communicating partners (peer entities) and where necessary (eg. for banking purposes) to ensure non-repudiation of data origin and delivery; and
- where appropriate, to provide secure interworking with the non-open systems world.

While adding,

- To ensure the confidentiality of information held on participating systems
- Clear separation of data and processes on the virtual level of the cloud, ensuring zero data leakage between different applications
- To maintain the same level of security when adding or removing resources on the physical level.

5.4.2.2 Trusted Third Party

In (Zissis & Lekkas, 2011), we claim that employing Trusted Third Party services within the cloud, leads to the establishment of the necessary Trust level and provides ideal solutions to preserve the confidentiality, integrity and authenticity of data and communications(Polemi, 1998). In cryptography, a Trusted Third Party (TTP) is an entity which facilitates secure interactions between two parties, who both trust this third party. The scope of a TTP within an Information System is to provide end-to-end security services, which are scalable, based on standards and useful across different domains, geographical areas and specialisation sectors. The establishment and the assurance of a trust relationship, between two transacting parties, shall be concluded as a result of specific acceptances, techniques and mechanisms. The Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content. Introducing a Trusted Third Party, can specifically address the loss of the traditional security boundary, by producing trusted security domains. As described by Castell, «A Trusted Third Party is an impartial organisation delivering business confidence, through commercial and technical security

features, to an electronic transaction. It supplies technically and legally reliable means of carrying out, facilitating, producing independent evidence about and/or arbitrating on an electronic transaction. Its services are provided and underwritten by technical, legal, financial and/or structural means" .

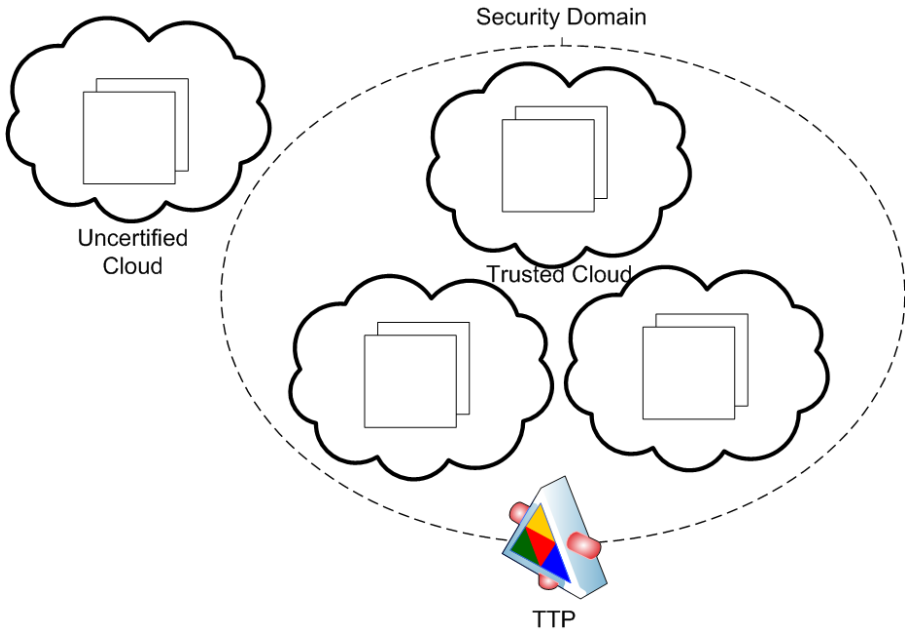

Illustration 49: TTP to enable Cloud Federations

This infrastructure, leverages a system of digital certificate distribution and a mechanism for associating these certificates, with known origin and target sites, at each participating server. TTP services are provided and underwritten not only by technical, but also by legal, financial, and structural means (Castell, 1993)(Commission of the European Community, 1994). TTPs are operationally connected through chains of trust (usually called certificate paths), in order to provide a web of trust forming the notion of a Public Key Infrastructure (PKI). The role of the PKI infrastructure in the context of electronic voting, can efficiently be executed by the e-passport infrastructure, extended to meet e-ID requirements as proposed in previous chapter.

PKI deployed in concert with Single-Sign-On (SSO) mechanisms are ideal for distributed environments, such as cloud environments, where users navigate between an abundance of cross-organization boundaries. In a single sign-on environment, a user does not need to repeatedly enter passwords to access resources across a network, instead the user signs on once, using a password, smartcard, or other authentication mechanism, and thereby obtains access to multiple resources on different machines. PKI-based Single-Sign-On mechanisms are indispensable within a cloud environment, since they provide the means for a smooth, transparent strong authentication across different physical resources. SSO in concert with PKI, enhances complex free, authorization and

authentication processes. In practice, this results in enhancing the security of the whole infrastructure, among other evident technical issues, because a sufficient level of usability is assured.

The trusted third party can be relied upon for:

- Low and High level confidentiality;
- Server and Client Authentication;
- Creation of Security Domains;
- Cryptographic Separation of Data;
- Certificate-Based Authorization;

5.4.2.2.1 Low and High level confidentiality

Securing data travelling over the network is a hard and highly complex issue, while the threat of data modification and data interruption is continuously rising. A cloud environment increases this complexity, as it does not only require protection of traffic towards the cloud, but additionally between cloud hosts, as they lack a traditional physical connection. PKI enables implementing IPSec or SSL for secure communications.

IPSec is an IP layer protocol, that enables the sending and receiving of cryptographically protected packets of any kind (TCP, UDP, ICMP, etc), without any modification. IPSec provides two kinds of cryptographic services. Based on necessity, IPSec can provide confidentiality and authenticity, or it can provide authenticity only (Alshamsi & Saito, 2004). IPsec users are able to authenticate themselves to the peer entity, using PKI certificates in a way that enhances scalability, because only the trusted CA certificate(s) need to be transmitted beforehand. SSL protocol generates end to end encryption by interfacing between applications and the TCPIP protocols, to provide client-server authentication and an encrypted communications channel between client-server.

Due to the cloud environments unique characteristics, communications are required to be protected between users and hosts, but also from host-to-host. Choosing IPSec or SSL depends on the diverse needs and security requirements. IPSec is compatible with any application, but requires an IPSec client to be installed on each remote device (PC, PDA, etc.) to add the encryption. In contrast, SSL is built into every browser, so no special client software is required. As the cloud environment promotes use by heterogeneous platforms, it is

unacceptable to require users to install an IPSec client for encryption. In addition, as cloud services are mostly accessed through browsers, SSL has many benefits for client to host communications. On the other hand, IPSec supports using compression, making it a more efficient choice for host to host communications. This paper proposes implementing IPSec for encrypting communications for Host-to-Host communications and SSL for Client-to- Cloud communications.

5.4.2.2.2 Server and Client Authentication

In a cloud environment, a Certification authority is required to certify entities involved in interactions, these include certifying physical infrastructure servers, virtual servers, environments users and the networks devices (Illustration 55). The PKI certification authority is responsible for generating these required certificates, while registering these within the trust mesh. In other words, a Certification Authority builds the necessary strong credentials for all the physical or virtual entities involved in a cloud and it therefore builds a security domain with specific boundaries within the otherwise fuzzy set of entities of a cloud.

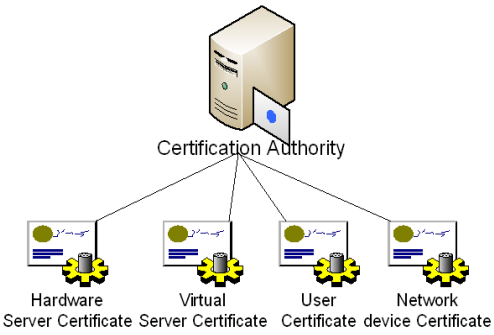

Illustration 50: Certificate Categories

Digital signatures in combination with SSO and Ldap, implement the strongest available authentication process in distributed environments, while guaranteeing user mobility and flexibility. The signing private key, can be used to authenticate the user automatically and transparently to other servers and devices around the network whenever he/she wants to establish a connection with them.

While the cloud is becoming the common operating platform, every service is going to require a secure authentication and authorization process. As the conceptual boundary between an organisations own service's and outsourced services becomes "fuzzy", the need to adopt Single Sign On solution is critical. Users require to make use of applications deployed on their virtual "office", without having to repeat the authentication process on each service (application) provider or maintain numerous passwords, but make use of a single strong authentication process that authorizes them to use services across trusted parties. "*Eight years ago, it was all about securing*

applications within the enterprise through identity management. Today we talk about securing applications in the cloud with identities originating within the enterprise" (Cloud Identity Summit, 2010).

Shibboleth is standards-based, open source middle-ware software, which provides Web Single Sign On (SSO) across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner (Internet 2, 2007). Shibboleth technology relies on a third party to provide the information about a user, named attributes. In the proposed system architecture, this is performed by the TTP LDAP repository. It is essential to distinguish the authentication process, from the authorization process. During the authentication process, a user is required to navigate to his home organisation and authenticate himself. During this phase, information is exchanged between the user and his home organisation only. After the successful authentication of a user, according to the user attributes/credentials, permission to access resources is either granted or rejected. The process in which the user exchanges his attributes with the resource server, is the authorization process during which no personal information is leaked and can only be performed after successful authentication (Illustration 56).

To maximize interoperability between communicating parties, it is a necessity to adopt widely used standards. Security Assertion Mark-up Language (SAML), is an XML-based standard for exchanging authentication and authorization of data between security domains. The primary function of the Shibboleth system is to support identity federation between multiple sites using the SAML protocol standard. The Shibboleth and SAML design processes, have been coupled to insure that Shibboleth is standards-based (Internet 2, 2010).Because of this design, on a software level, a major part of the Shibboleth system is the OpenSAML libraries, which are also widely used. Both the OpenSAML libraries and the Shibboleth software are developed by the Shibboleth team and released as open source. Shibboleth's added value lies in support for privacy, business process improvement via user attributes, extensive policy controls, and large-scale federation support via metadata.

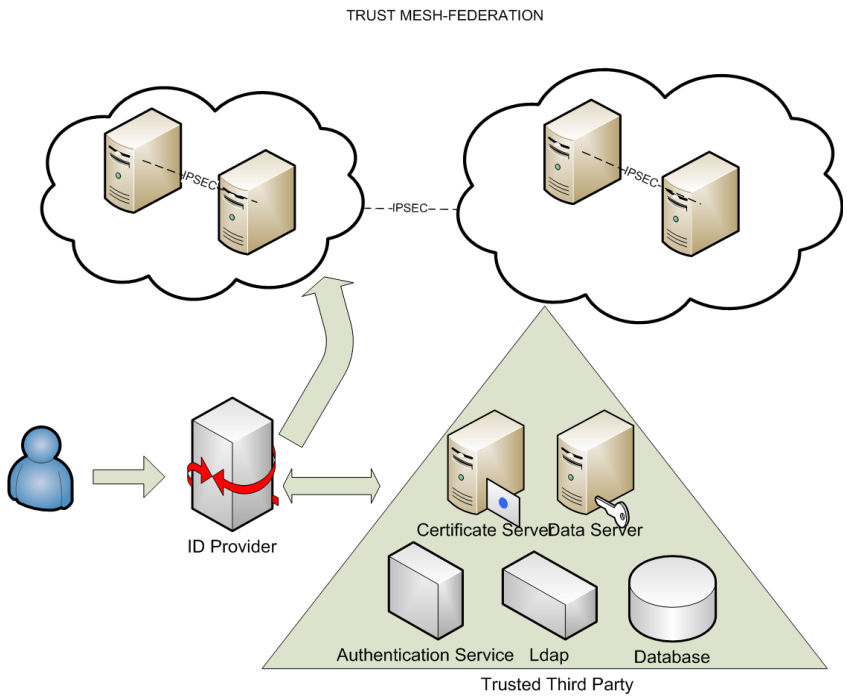

Illustration 51: Authentication in the Trusted Environment

5.4.2.2.3 Creation of Security Domains

Introducing federations, in association with PKI and Ldap technology, leads to efficient trust relationships between involved entities. A federation is a group of legal entities that share a set of agreed policies and rules for access to online resources (UK Federation Information Centre, 2007). A federation provides a structure and a legal framework that enables authentication and authorization across different organizations. Cloud infrastructures can be organized in distinctive security domains, (an application or collection of applications that all trust a common security token for authentication, authorization or session management) enabling "Federated clouds". Federated Clouds are a collection of single Clouds that can interoperate, i.e. exchange data and computing resources, through defined interfaces. According to basic federation principles, in a Federation of Clouds, each single Cloud remains independent, but can interoperate with other Clouds in the federation through standardized interfaces. A federation provides a structure and a legal framework that enables authentication and authorization across different organizations(Stanoevska-Slabeva, Wozniak, & Ristol, 2009).

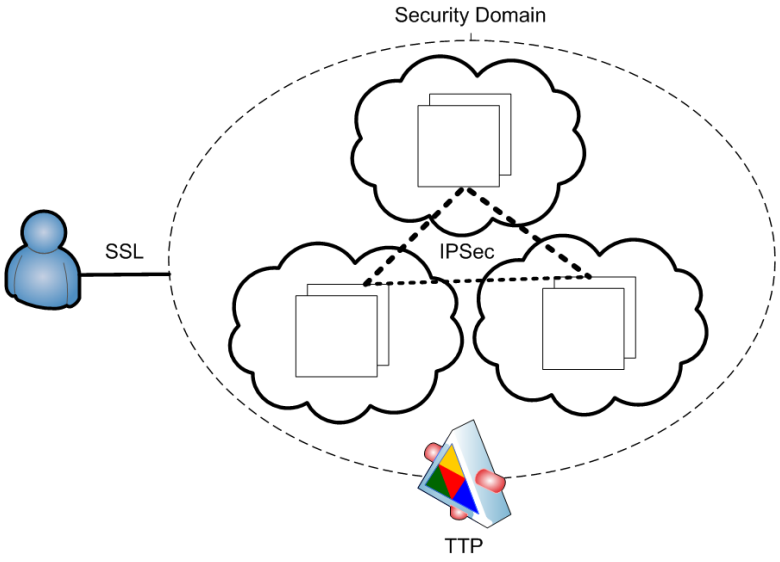

Illustration 52: Security Domains

5.4.2.2.4 Cryptographic Separation of Data

The protection of personal information or/and sensitive data, within the framework of a cloud environment, constitutes a crucial factor for the successful deployment of SaS and AaS models. Cryptographic Separation in which processes, computations and data are concealed in such a way that they appear intangible to outsiders (C. Pfleeger & S. Pfleeger, 2006). Confidentiality and integrity, but also privacy of data can be protected through encryption. If sensitive data is encrypted, a user that accidentally or maliciously gains access is unable to interpret it. Each level of sensitive data can be stored in a table of encrypted under a key unique to the level of data sensitivity. Using a combination of asymmetric and symmetric cryptography (often referred to as hybrid cryptography) can offer the efficiency of symmetric cryptography while maintaining the security of asymmetric cryptography.

5.4.2.2.5 Certificate-Based Authorization

A cloud environment is a virtual net of several independent domains. In a cloud environment, the relationship between resources and users is more ad hoc and dynamic, resource providers and users are not in the same security domain, and users are usually identified by their characteristics or attributes rather than predefined identities. Therefore, the traditional identity-based access control models are not effective, and access decisions need to be made based on attributes(Lang, Foster, Siebenlist, Ananthakrishnan, & Freeman, 2008). Certificates issued by a PKI facility can be used for enforcing access control in the Web environment. An example is the use of an extended X.509 certificate, that carries role

information about a user . These certificates are issued by a certification authority that acts as a trust centre in the global Web environment (Joshi, Aref, Ghafoor, & Spafford, 2001). Attribute certificates, contain an attribute-value pair and the principal to whom it applies. They are signed by attribute authorities that have been specified in a use-condition certificate. Attribute based access control, making access decisions based on the attributes of requestors, resources, and the environment, provides the flexibility and scalability that are essential to large-scale distributed systems, such as the cloud.

5.4.2.3 Assessment

Trust essentially operates in a top-down fashion, as every layer needs to trust the layer immediately below it, and requires a security guarantee at an operational, technical, procedural and legal level, to enable secure communications with it (Illustration 58). A trusted certificate serves as a reliable electronic "passport", that establishes an entity's identity, credentials and responsibilities. Trust can be viewed as a chain, from the end user, to the application owner, who in turn trusts the infrastructure provider (either at a virtual or hardware level according to the selected service model). A Trusted Third Party, is able to provide the required trust by guaranteeing that communicating parties are who they claim to be and have been scrutinized to adhere to strict requirements. This process is performed through the certification process, during which an entity requiring certification is required to conform with a set of policies and requirements. TTP is an ideal security facilitator in a distributed cloud environment, where entities belonging to separate administrative domains, with no prior knowledge of each other, require to establish secure interactions.

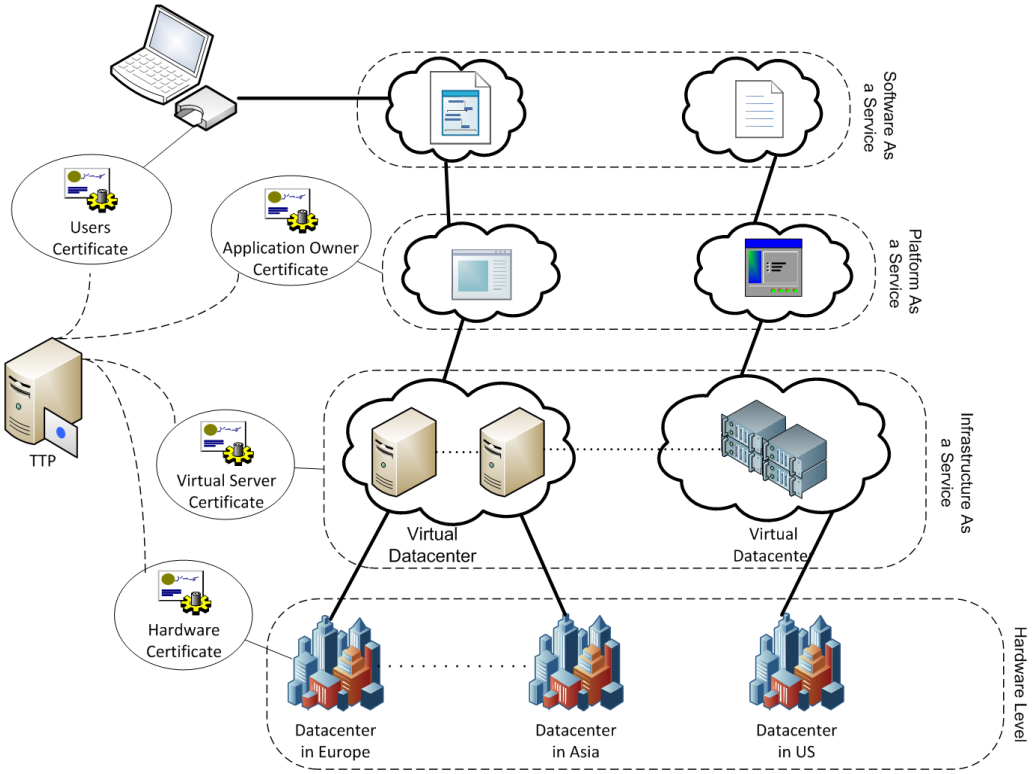

Illustration 53: Trust essentially operates in a top-down fashion, as every layer is required to trust the layer immediately below it.

An end user is required to use his personal digital certificate to strongly authenticate himself with a cloud service and validate his access rights to a required resource. This certificate is used in combination with the service provider's certificate (PaS or IaS level) to create a secure SSL connection between them, thus encrypting exchanged data and guaranteeing their security through the cloud infrastructure(Illustration 59). The user is able to encrypt all personal data stored on the cloud to counter previously identified confidentiality risks. As cloud infrastructure's host a number of services, several applications can be mounted on a virtual server, each requiring separate digital certificates for SSL communications (different ports can be used to support more than one SSL connections to a virtual server).

The application provider can use his own certificate to authenticate himself in communications with the cloud, but also use this certificate to encrypt and decrypt application data. These certificates can be enhanced, to carry role information about a user or process (extended X.509 certificates. At the lowest level, the hardware infrastructure owner, makes use of a digital certificate to communicate security between devices and virtual servers, but also for authentication purposes if required.

Key management is a critical issue in cloud infrastructures, as the virtualisation of

services obscures the identification of the physical key storage location, disabling traditional protection mechanisms. Keys, are principally stored and protected at a hardware infrastructure level. In such an environment, deploying tamper-proof devices for key protection is essential e.g. user smarts cards coupled with Hardware Security Module as part of the virtual deployment.

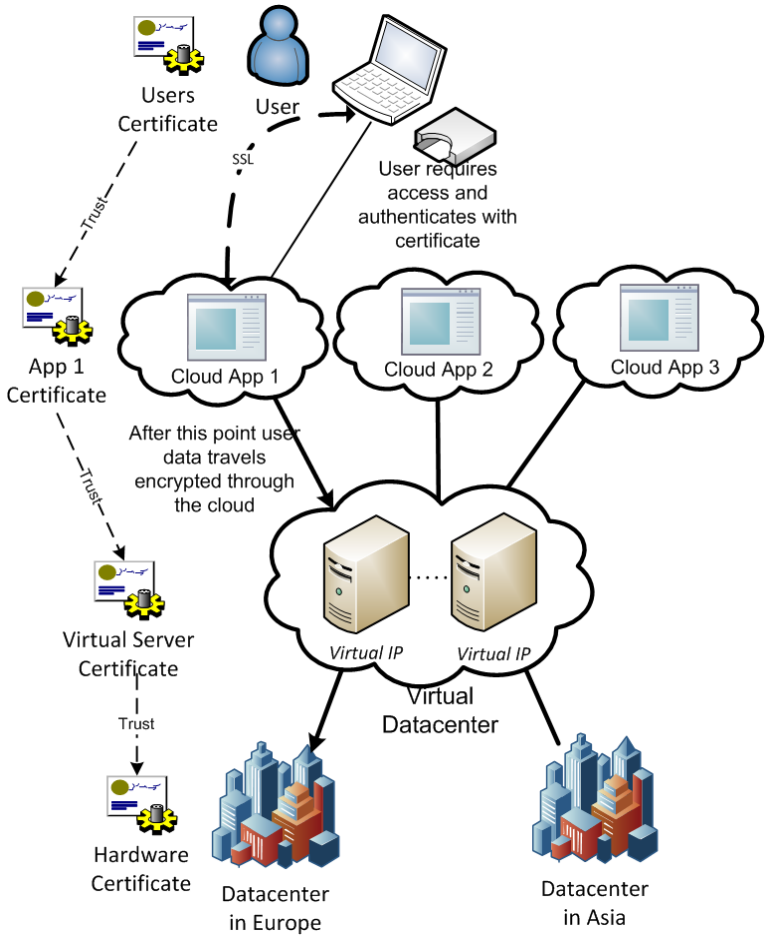

Illustration 54: A user authenticates himself with a cloud service using his personal certificate which in combination with the service providers certificate is used to secure and encrypt all communications.

5.4.3 A cloud Solution to e-voting

Leveraging existing infrastructure into a dynamically responsive cloud, overcomes several deficiencies of traditional implementations. Cloud computing implementations can be viewed as having a server side and a client side (NIST SP 800-144, 2011); with emphasis typically placed on the former. Providing citizens with "hardened" operating systems (OS), on a bootable read-only removable media, with pre-configured cloud access client software, eliminates a plethora of threats. Enabling electronic vote casting, by minimizing threats

through offering citizens “desktop as a service” (a container of a collection of virtual objects, software, hardware, configurations etc., residing on the cloud, used by a client to interact with remote services).

There are several reasons for deploying desktop virtualization. It allows changes to be made to an OS and subsequently revert to the original if needed, such as to eliminate changes that negatively affect security. Desktop virtualization also supports better control of OSs to ensure that they meet the organization’s security requirements. This control, can be asserted by creating a high-assurance platform, that constantly updates the guest OS, to have the exact versions of the programs that it is authorized to have, and no other programs(NIST SP 800-125). Organizations considering the use of desktop virtualization, should determine which scenarios require the enforcement of security by managed virtualization solutions and which scenarios do not require centralized management. Desktop virtualization, can be used to improve security by providing a well-secured guest OS image for the desktop environment(NIST SP 800-125). Another benefit of using managed guest OS images, is that they can be updated by the organization as needed without requiring user intervention. However, image distribution can be problematic, because a single guest OS image can be many gigabytes in size, making it difficult to download.(NIST SP 800-125).

A user can bypass loading a PCs vulnerable OS, by inserting a hardened minimal OS on distributed removable media, thereby overstepping both compromise and threat, which is then used as a gateway to the cloud. Trusted operating systems (TOS), are security-modified or -enhanced OSs that include additional security mechanisms not found in most general-purpose OSs. A growing number of pre-hardened OS and Web server packages are being distributed today. These packages include an OS and Web server applications, that are modified and pre-configured to provide high security.

Authenticating a client over a secure channel, for a time-limited session required to perform vote casting, provides a control to a severe vulnerability.

Cloud computing places the user’s terminal within the systems’ “security perimeter”, which is maintained, updated, and monitored by security experts. Due to its identified characteristics, cloud computing architecture attempts to propose an effective and efficient way of countering a plethora of threats, identified as barriers to electronic voting. In collaboration with a deployed Public Key Infrastructure (PKI), which serves as an authentication and cryptographic layer, cloud computing offers the benefits of placing the

voter inside the "security perimeter". Enabling e-voting through "desktop as a service" makes developing and maintaining common information security foundations an achievable goal. Centralization of security is crucial, as it provides a uniform and consistent way to manage the risk to individuals, organizational operations, organizational assets, whole organizations, and entire nations, from the operation and use of information systems (NIST SP 800-53). Additionally, by centrally managing the development, implementation, and assessment of the common security controls, designated by the organization, security costs can be amortized across multiple information systems.

A cloud unique desktop as-a-service, has the following characteristics:

- It is centrally maintained and monitored as part of a uniform protection scheme, which puts "client computers" behind professional security protection hardware, software, and personnel.
- Only authorized and authenticated software can be executed on the desktop instance due to management restrictions that can prevent many threats.
- Updates are rolled out centrally, increasing effectiveness and time of deployment.
- It is transparent and open to scrutiny.
- All source code used in the electoral process is contained for inspection.
- Policies and procedures are in place to protect from insider attacks, corruption, and hardware and software failures.

5.4.4 Controlling hardware-specific threats

On many occasions, attacks on sophisticated information systems have boiled down to deliberate assaults on hardware equipment. An attack against an electronic election could essentially be carried out by destroying the physical servers used in an election. A key characteristic of cloud architecture, is geographical independence. The lack of knowledge of a server's location provides an interesting physical security benefit, as it becomes nearly impossible for a motivated attacker to use a physical vector to compromise the system. Additionally, data dispersal in the cloud "slices" information through sophisticated algorithms and stores data across different geographical locations. These technological characteristics contribute to high redundancy and availability achieved in the cloud (Reese, 2009).

High risk cloud infrastructures, have the ability to realize distinct but overlapping

availability zones. An availability zone can be conceptually mapped to a physical data center, with the security feature of having distinct physical infrastructures. Spanning virtual servers on multiple availability zones achieves geographical redundancy. Virtualization technology enables the inexpensive generation of redundancies, which span data centers and enable rapid recovery in the occurrence of disaster.

5.4.5 Controlling software-specific threats

Personal computers are often overloaded with software, developed by many different vendors. At any point an employee could consciously leave a backdoor, thereby creating opportunities for attacks against an electronic voting system. Backdoors, when placed in software, could be activated when a user tries to cast a vote (time-bombs), thereby invisibly monitoring or subverting the voting process. Providing a certified hardened OS on a bootable media, creates a secure fat client, open to extensive audits, generating unparalleled client side trust. This fat client, would then be used to access the cloud desktop. In the cloud, it is possible to forbid uncertified software modifications, as updates and installations would be performed centrally to avoid threatening the systems integrity. Additionally, software installations can be restricted at a management level, eliminating the threat of installing malicious software on the system. In the event of a successfully deployed attack, that modifies/deletes a voter's vote, all implicated software is contained and open to extensive audits. It is a fundamental requirement of an e-voting system that all operations related to electronic voting, be logged and monitored. (Gritzalis, 2002). If e-voting clients and the physical environment are carefully supervised, such as with polling place voting, then e-voting may be feasible even with an Internet connection between clients and election servers. (Burnester & Magkos, 2003) (California Internet Voting Task Force, 2000). A remote desktop on a cloud computing infrastructure (virtual instance), government owned and centrally monitored, would be open to extensive audits and to public scrutiny due to the adoption of open APIs, open data formats and open source models (Wardley, 2009).

In addition to the risk from pre-installed applications, there is a threat from remote attackers. Such an attacker might gain control of a computer without being detected. For example, an attacker could exploit a security vulnerability in the software on a voter's computer. One of the identified benefits of cloud computing, is the centralization of information and uniformity of security infrastructure, which can offer the ability to accurately address identified vulnerabilities rapidly across all clients. In addition, providing a "desktop

within the clouds," makes it possible to overcome the exploitation of any vulnerability that could have been identified on a standard bootable OS, or on the application contained within it after distribution. Updates can be rolled out effectively, as soon as the vulnerability has been identified, overcoming the drawback of "publishing day to update". The cloud provides a user interface, that allows both the user and the IT administrators to easily manage the provisioned resources throughout the life cycle of the service request, effectively changing the installed software; removing servers; increasing or decreasing the allocated processing power, memory, or storage; and even starting, stopping, and restarting servers. These are self-service functions, that can be performed 24 hours a day and take only minutes to perform. By contrast, in a non-cloud environment, it could take hours or days for someone to have a server restarted or hardware or software configurations changed. (IBM, 2009)

An attacker could attempt to exploit a vulnerability identified in a server. In a traditional data center, rolling out security patches across an entire infrastructure is time consuming and risky. Due to the virtualization characteristics of cloud computing, increased efficiency is achieved. Virtual servers or instances are launched from a machine image. A machine image is a prototype, which is copied onto a virtual server's hard drive, every time an instance is launched. Updates and modifications are performed on a single image, which is successfully used to re-launch the virtual servers. In the cloud, rolling out a patch or update across the infrastructure, takes three steps:

- Patching of machine images with new security updates,
- Testing the results, and
- Re-launching virtual serves.

Virus attacks impose an immense threat to such a system and traditional anti-virus software would not be able to efficiently defend the system from such attacks. Specific anti-virus tools can be provided as an additional cloud service, to enhance end users' security coverage. A pure cloud anti-virus solution, relies on a detection set that resides on Internet servers, or "in the cloud". A lightweight desktop agent is used to query this detection set. E-voting systems are targets of system-specific viruses; it is imperative that effective solutions are created that can immediately deal with identified malicious code, preventing the propagation throughout the system. Cloud anti-virus programs, reduce the publishing delay to zero and allow for quicker innovation. They are more efficient and faster, providing security experts the ability to fine-tune their detection logic. After the identification of malicious code,

server images can be hardened to protect against it and new server instances loaded. A proposed solution makes use of a Network Identification System and a centralized Host Intrusion Detection System, which respectively monitors the system servers and network for anything unusual.

5.4.6 Controlling network specific threats

Attacks can be directed at a network's availability, or one of its services, but normally such attacks are focused on any IT services of which the network is an agent. Common attacks falling into this category, include denial of service attacks, attempts to breach a firewall, and attempts to breach a router. Denial of Service (DoS) and distributed Denial of Service (DDoS) attacks, involve attempts to make a computer resource unavailable to its intended users. Commonly, these attacks involve simply saturating the target machine with external Internet requests. One of the most critical characteristics of cloud computing, is its elasticity due to the virtualization of servers. Information systems using a cloud computing infrastructure are able to respond to peaks in traffic, with the creation of additional virtual servers.

Availability in the cloud, is believed to be higher due to elasticity. The key differentiator between downtime in the cloud and downtime in a physical environment, lies in how rapidly the infrastructure will respond to failure. Even though a physical server may be more reliable than a virtual server in the cloud, the cloud enables inexpensive creation of redundancies, that span data centers. This gives the cloud infrastructure the ability to respond rapidly to failure (Reese, 2009).

Elasticity, in combination with network filtering techniques, available through a uniform security solution, can provide an effective and efficient response to network attacks, such as DDoS. Network intrusion detection systems, can provide adequate protection on the "systems perimeter". A simple non technical solution has been proposed for protecting against DDOS attacks. The polling phase could be designed to last for several days, even weeks, which would make Denial of Service attacks unattractive.

Table 16: Proposal of controls combined with cloud architecture

		Characteristics of Cloud Computing Architecture														
		Centralization/ Unified Security Architecture							*Economies of scale*	*Location independence*	*Open Free Software / Centralization*	*Reliability*				
	Compliance with NIST Security Control Classes	***AC:** Access Control, **IA:** Identification and Authentication, **SC:** Systems and Communications Protection, **AU:** Audit and Accountability, **CP:** Contingency Planning*							**CP:** Contingency Planning		**AU:** Audit and Accountabili	CP: Contingency Planning				
Identified Treats e-Voting		On-Demand User Security Controls	Controlled execution enviroment	Encryption at rest and in transit	Perimeter security (IDS, firewall, one time authentication)	Hypervisor Protection Against Network Attacks	Real-Time Detection of System Tampering	Advanced Honeynet Capabilities	Low-Cost Disaster Recovery and Data Storage Solutions	Provision of data zones (e.g., by country)	Disclosability/Transparency	Data Fragmentation and Dispersal	Fault Tolerance and Reliability	Rapid Re-Constitution of Services	Automated replication	VLAN capabilities
	Hardware modification								×		×		×	×		
	Hardware substitution								×		×		×	×		
	Hardware interception								×		×		×	×		
	Software modification															
	o Trapdoors	×	×		×		×		×		×	×	×	×	×	
	o EasterEggs	×	×		×		×		×		×	×	×	×	×	
	o Logic bombs	×	×		×		×		×		×	×	×	×	×	
	o Information leaks	×	×		×		×		×		×	×	×	×	×	
	o Virus	×	×		×		×		×		×	×	×	×	×	
	o Trojan horse	×	×		×		×		×		×	×	×	×	×	
	Software Deletion	×	×		×		×		×		×	×	×	×	×	
	Software Theft	×	×	×	×		×		×		×	×	×	×	×	
	Malicious code on client	×	×		×				×		×	×	×			
	Man in the middle-*Replay*			×	×											
	Impersonation/ Spoofing			×	×						×					
	Falsification of messages			×	×		×				×					
	DNS attack			×	×	×				×	×		×			×
	DDOS			×	×	×				×	×		×			×
	Coonection Flooding				×	×		×		×						×
	Traffic Redirection			×							×					
	Session Hijacking			×												
	Eavesdropping			×	×		×	×								×
	Wiretapping			×			×	×			×					×
	Misdelivery			×			×									
	Exposure within network			×	×	×	×				×					×
	Traffic flow analysis			×	×	×	×	×								
	Man in the middle-*Replay*			×	×											

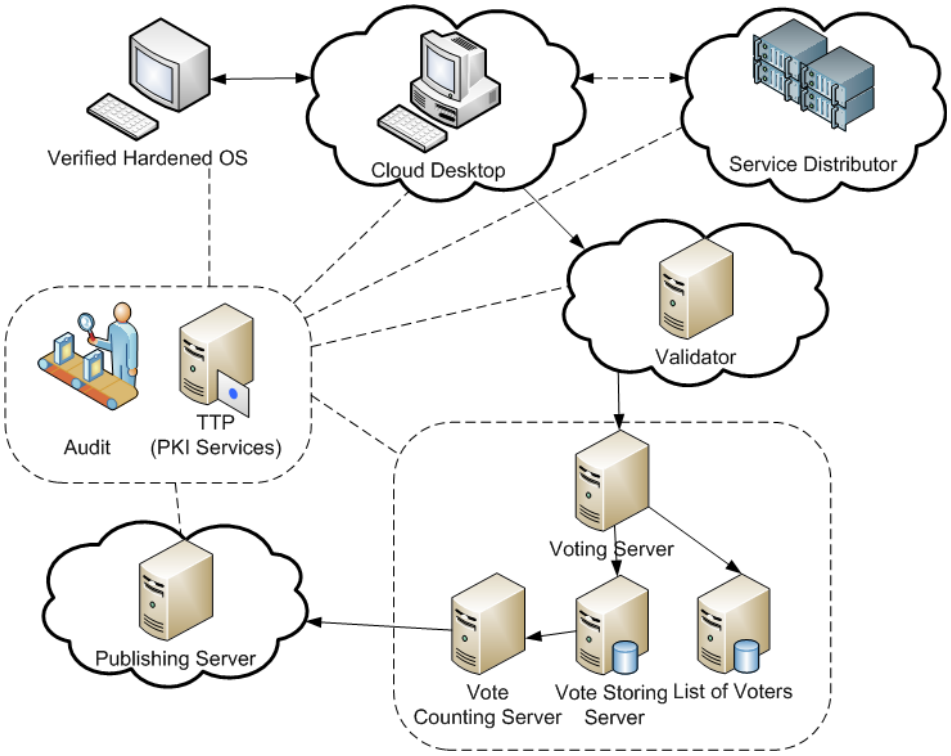

Illustration 55: High Level Design of the proposed e-voting system. This illustration describes the cloud elements of the proposed solution(Cloud desktop, validator and publishing server), while pictorially showing the implication of the TTP(PKI) Services and the Audit Services.

5.5 Recommendations of controls for safeguarding elections

Digital signatures and blind signatures based on PKI infrastructure, allow for a horizontal infrastructure for both authentication and integrity features. PKI and encryption applications can make use of the cloud feature of the architecture, to provide hybrid solutions, enhanced by back-end security modules such as Hardware Security Module (HSM) devices. The cloud can offer a secure vote casting terminal and provide an edge due to flexibility, over traditional client server model to increase availability. Public key encryption is used to encrypt data in transit, ephemeral data on virtual instances, data storages, and network traffic.

The Serve security report (Jefferson, et al., 2004), summarized a number of specific threats to electronic voting systems and points out the inefficiency of traditional architecture countermeasures to control these. In the following table (Table 17), the threats identified are weighed against the controls imposed by a cloud computing infrastructure.

Threat	Traditional Architecture Countermeasures	Cloud Architecture Proposed Solution Controls
Trojan horse attack on PC to prevent voting	can mitigate risk with careful control of PC software; reason for failure may never be diagnosed	Contained environment/Software modifications disabled/Client security applications/HIDS/Auditability
On screen electioneering	voter can do nothing to prevent this; requires new law	On screen electioneering can be prevented by making it technically infeasible to gain access onto the voter's terminal. Disabled though desktop as a service, only encrypted communications permitted
Spoofing of system (various kinds)	none exist; likely to go undetected; launchable by anyone in the world	Encryption / Authentication/ Digital Signatures/ Perimeter Security/ Client Desktop is within security perimeter
Client tampering	none exist for all possible mechanisms. Too difficult to anticipate all attacks; most likely never diagnosed.	Client environment centrally protected monitored/ contained/ within security perimeter/ auditability
Insider attack on system servers	none within SERVE architecture; voter verified ballots needed; likely undetected	Transparency, Openness, Data Fragmentation and Dispersal, Cryptography
System-specific virus	virus checking software can catch known viruses, but not new ones; likely to go undetected	Real time detection of system tampering/ On demand user security controls/
Trojan horse attack on PC to change votes or spy on them	can mitigate risk with careful control of PC software; harder to control at cybercafe, or other institutionally managed networks; attack likely to go undetected	Real time detection of system tampering/ Client environment centrally protected monitored/ contained/ within security perimeter/ auditability
DDOS	Network Filtering	Elasticity in combination with network filtering techniques , management layer is able to monitor traffic 24/7 , centralized approach

Table 17: Combination of controls

Essentially securing an Information System (IS), involves identifying unique threats and challenges, which need to be addressed by implementing the appropriate countermeasures. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process, to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability).

This section attempts to propose controls that are intended to meet the previously identified requirements. The controls attempts to diminish the threat or repel it.

NIST Special Publication 800-53

5.5.1 Recommendation's for addressing security requirements for the remote Electronic Voting System

1. The remote electronic voting system shall unambiguously identify and authenticate the voter before storing his vote in the e-ballot box.

   - ✔ **USER IDENTIFICATION AND AUTHENTICATION:** Control: The information system uniquely identifies and authenticates users, using multifactor authentication.
   - ✔ **DEVICE IDENTIFICATION AND AUTHENTICATION:** Control: The information system identifies and authenticates specific devices, before establishing a connection.
   - ✔ **AUTHORIZATION AND MONITORING:** Control: The organization authorizes, monitors, and controls all methods of remote access to the information system.
   - ✔ **ACCESS ENFORCEMENT** Control: The information system shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

2. The remote electronic voting system shall store in the e-ballot box only e-votes cast from eligible voters. Any other access to the e-ballot box shall be denied.

   - ✔ **ACCESS CONTROL POLICY AND PROCEDURES:** Control: The election officials develop/review/update a formal eligible voter lists from which authentication and authorization permissions are generated.
   - ✔ **UNSUCCESSFUL LOGIN ATTEMPTS:** Control: The information system enforces a limit of consecutive invalid access attempts by a user during a time

period. The information system automatically , *delays next login prompt according to* when the maximum number of unsuccessful attempts is exceeded. Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

- ✔ **NON-REPUDIATION:** Control: The information system shall provide the capability to determine whether a given individual took a particular action.
- ✔ **NON-REPUDIATION (**2): Control: The Information system shall employ digital signatures and timestamps to store in an e-ballot only the latest vote cast by a voter.

3. The remote electronic voting system shall ensure the data protection law with respect to the transmission of any personal data.
   - ✔ **DATA PROTECTION:** Control: The organization shall employ cryptography to protect the confidentiality and integrity of transmitted data
4. The remote electronic voting system shall protect the confidentiality of the transmitted authentication information.
   - ✔ **COMMUNICATION PROTECTION:** Control: The organization shall employ cryptography to protect the confidentiality and integrity of communications.
   - ✔ **AUTHENTICATOR FEEDBACK:** Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
5. The remote electronic voting system shall ensure the confidentiality of the transmitted e-votes during the polling phase.
   - ✔ **COMMUNICATION PROTECTION:** control: the organization shall employ cryptography to protect the confidentiality and integrity of communications.
   - ✔ **DATA PROTECTION:** Control: The organization shall employ cryptography to protect the confidentiality and integrity of transmitted data
6. The remote electronic voting system shall ensure that protocol messages cannot be deleted undetected.

- ✔ **SOFTWARE AND INFORMATION INTEGRITY:** Control: The information system detects and protects against unauthorized changes to software and information. The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization shall employ automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification. The organization employs centrally managed integrity verification tools.
- ✔ **AUDITABLE EVENTS.** The organisation shall monitor and store events that affect the confidentiality, integrity and availability of data and communications.
- ✔ **PROTECTION OF AUDIT INFORMATION:** Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

7. The remote electronic voting system shall verify the freshness, authenticity, integrity, and format correctness of all messages before processing them.
   - ✔ **INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY** Control: The information system checks information for accuracy, completeness, validity, and authenticity.
   - ✔ **NON-REPUDIATION:** Control: The Information system shall employ digital signatures and timestamps to verify the validity, authenticity and integrity of all messages.
   - ✔ **SESSION AUTHENTICITY:** Control: The information system provides mechanisms to protect the authenticity of communications sessions.

8. The remote electronic voting system shall delete any records related to the voter's voting process from the vote-casting device when finishing the voting process.
   - ✔ **VOTING TERMINAL INTEGRITY** Control: The information system provides the facility to voters to perform vote casting through services such as desktop as a service. After vote casting is complete, the desktop can be wiped clean.
9. The remote electronic voting system shall not provide any information in the transmitted protocol messages, which allows to construct the link between a particular voterand his vote.
   - ✔ **COMMUNICATION PROTECTION:** Control: The organization shall employ

cryptography to protect the confidentiality and integrity of communications.

10. The remote electronic voting system shall ensure that neither the vote itself nor the number of chosen voting options (including an empty ballot), nor a spoilt vote (for example,by using the length of the protocol messages) can be linked to a particular voter. In addition, it shall be ensured that the sequence of messages does not reveal the link.

    - ✔ **ELECTION ENCRYPTION**: Control: The organisation shall employ the appropriate election encryption scheme which will protect voters privacy(e.g. digital signatures, homomorphic encryption etc.)

11. The remote electronic voting system shall ensure that voters are not able to construct a receipt proving their vote. Neither information sent to, displayed on, sent from, nor intermediate results calculated on his vote-casting device or protocol messages sequences shall serve as proof.

    - ✔ **ELECTION ENCRYPTION**: Control: The organisation shall employ the appropriate election encryption scheme, which will allow the voter to verify his vote has been received successfully, but will not reveal any information on the voter choice.

5.5.2 Recommendation's for addressing security requirements for the Tallying Phase

1. The voting server shall protect the integrity and authenticity of e-votes after the polling phase.

- ✔ **SOFTWARE AND INFORMATION INTEGRITY:** Control: The information system detects and protects against unauthorized changes to software and information. The organization employs integrity verification applications on the information system, to look for evidence of information tampering, errors, and omissions.

2. The tallying software shall verify the integrity and authenticity of e-votes.

- ✔ **INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY:** Control: The tallying software checks information for accuracy, completeness, validity, and authenticity according to predefined information schema.

3. The tallying software shall protect the integrity and authenticity of election

data as soon as the tallying is completed.

- ✔ **SOFTWARE AND INFORMATION INTEGRITY** Control: The information system detects and protects against unauthorized changes to software and information. The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions.

4. The tallying software shall ensure that its operations and data are unaffected by other applications.

- ✔ **APPLICATION PARTITIONING** Control: The information system separates user functionality (including user interface services) from information system management functionality.

5.5.3 Recommendation's for addressing security requirements for the Voting Server

1. The voting server shall communicate only with the authentic and unaltered client-side voting software.

- ✔ **CLIENT SIDE AUTHENTICITY Control:** The organisation shall employ digital signatures to ensure authenticity of communicating parties. The Organisation shall only establish communications with authentic terminals.

2. The voting server should be tamper-resistant and tamper-evident.

- ✔ **SOFTWARE AND INFORMATION INTEGRITY:** Control: The information system detects and protects against unauthorized changes to software and information. The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization shall employ automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification. The organization employs centrally managed integrity verification tools.

- ✔ **SERVER INTEGRITY:** Control: The voting server shall employ techniques to protect its integrity. The voting server will have all unnecessary Services, Applications, and Network Protocols removed or disabled.

- ✔ **Auditable Events.** The organisation shall monitor and store events that affect the confidentiality, integrity and availability of data and communications.

3. The voting server shall implement an access control policy for the poll worker interface which

    - restricts all activities to particular user-roles and

✔ **LEAST FUNCTIONALITY:** Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of services

✔ **APPLICATION PARTITIONING:** Control: The information system separates user functionality (including user interface services) from information system management functionality.

    - requires physical presence.

✔ **IDENTIFICATION AND AUTHENTICATION OF ORGANIZATIONAL USERS** Control: The information system uniquely identifies and authenticates organizational users by employing strong authentication techniques which require physical presence. (e.g. Digital Signatures and Hardware devices.)

4. The voting server should not store any information which could link the voter with his vote after the completion of the voting process. Where any information which could link the voter to his vote is stored on the voting server, it shall only be accessible to those with appropriate authority.

✔ **INFORMATION REMNANCE:** Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

5.5.4 Recommendation's for addressing security requirements on the Client-Side

1. The client-side voting software, shall ensure that its operations and data are unaffected by other applications running on the vote-casting device.

✔ **Voting terminal protection:** control: the information system provides the facility to voters where they can perform vote casting through services such as desktop virtualisation.

✔ **VOTING TERMINAL Protection (2)** Control: The organization enforces explicit controls on voter client software .

2. The client-side voting software shall only communicate with the authentic and unaltered voting server.

   - ✔ **TRUSTED PATH:** Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication*]. A trusted path is employed for high-confidence connections
   - ✔ **CLIENT SIDE AUTHENTICITY Control:** The organisation shall employ digital signatures to ensure authenticity of communicating parties. The Organisation shall only establish communications with authentic terminals.

3. The client-side voting software shall protect the voter from influence during voting

   - ✔ **VOTING TERMINAL Protection (3) Control:** The information system provides the facility to voters where they can perform vote casting through services such as desktop virtualisation.
   - ✔ **VOTING TERMINAL Protection (4) Guest OS Monitoring Control:** The Information system is fully aware of the current state of each guest OS it controls
   - ✔ **VOTING TERMINAL Protection (5) SPAM PROTECTION** Control: The information system implements spam protection on voting client. **The organization centrally manages spam protection mechanisms.**
   - ✔ **VOTING TERMINAL Protection (6) MALICIOUS CODE PROTECTION** Control: The information system implements malicious code protection on voting client. **The organization centrally manages malicious code protection mechanisms.**

5.5.5 Recommendation's for addressing Operational security Requirements for the Remote Electronic Voting System

1. The remote electronic voting system shall ensure that no voter loses his voting right, without having cast a vote.

   - ✔ **VOTER PROTECTION** Control: vote updating The information system will permit a voter to cast a vote as many times as he/she wishes, but only the last vote cast will be counted (either electronic or providing the voter with the possibility of going to the polling station on the last day). The voter may

cancel any previous cast votes by casting a new vote.

- ✔ **SOFTWARE AND INFORMATION INTEGRITY** Control: The information system detects and protects against unauthorized changes to software and information. The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions.

2. The remote electronic voting system shall prevent voter interactions in case of exceptions and malfunctions.

3. The remote electronic voting system shall provide a confirmation to the voter regarding the status of his vote – at least the information that his e-vote has been successfully stored.

   - ✔ **CRYPTOGRAPHIC VERIFIABILITY**: Control: The organisation shall employ the appropriate election encryption scheme which will allow the voter to verify his vote has been received successfully, but will not reveal any information on the voter choice.

4. The remote electronic voting system shall provide feedback to the poll workers in form of error messages, in case of exceptions, malfunctions, and breakdowns. Where a voter is in the voting process at that time he shall also get a feedback.

5. The remote electronic voting system shall prevent data loss during normal operations and in case of exceptions, malfunctions, and breakdowns.

   - ✔ ALTERNATE STORAGE SITE Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.
   - ✔ ALTERNATE PROCESSING SITE Control: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within, when the primary processing capabilities are unavailable.

6. The remote electronic voting system should be available during the whole polling phase.

   - ✔ **SERVICE AVAILABILITY PROTECTION** Control: The information system protects against or limits the effects of the following types of denial of service attacks. The IS system design makes use of cloud computing, load balancers,

reverse proxies and intrusion detection and prevention systems to guard system availability. A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy. Control Enhancements: (1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks. (2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

- ✔ I**NFORMATION SYSTEM RECOVERY AND RECONSTITUTION:** Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

7. The remote electronic voting system shall be robust against power outage at the voting server, unexpected user activity, environmental effects (for instance, mechanical, electromagnetic, and climatic) to the voting server, and network problems.

   - ✔ **POWER EQUIPMENT AND POWER CABLING:** Control: The organization protects power equipment and power cabling for the information system from damage and destruction. The organization employs redundant and parallel power cabling paths. The organization employs automatic voltage controls for [*Assignment: organization-defined list of critical information system components*].
   - ✔ **PHYSICAL ACCESS CONTROL :**Control: The organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides.
   - ✔ **EMERGENCY POWER:** Control: The organization provides a long-term uninterruptible power supply to facilitate an orderly shut-down of the information system in the event of a primary power source loss.
   - ✔ **TELECOMMUNICATIONS SERVICES:** Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions, within a *defined time period,* when the primary

telecommunications capabilities are unavailable. Control Enhancements: Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services. The organization obtains alternate telecommunications service providers that are separated from primary service providers, so as not to be susceptible to the same hazards. The organization requires primary and alternate telecommunications service providers to have contingency plans.

- ✔ **FIRE PROTECTION** Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.
- ✔ **TEMPERATURE AND HUMIDITY CONTROLS** Control: The organization organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system. an alarm or notification of changes potentially harmful to personnel or equipment.
- ✔ **WATER DAMAGE PROTECTION** Control: The organization protects the information system from damage resulting from water leakage by providing master shut-off valves that are accessible, working properly, and known to key personnel. The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.
- ✔ **INFORMATION LEAKAGE** Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.
- ✔ **LOCATION OF INFORMATION SYSTEM Components** Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
- ✔ **ALTERNATE WORK SITE** Control: The organization:a. Employs an alternate work site.
- ✔ **CONTINGENCY PLAN** Control: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated

officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

8. The remote electronic voting system shall ensure that in case of exceptions, malfunctions, and breakdowns, no voter loses his right to cast a vote nor get the possibility to cast two votes.

   - ✔ I**NFORMATION SYSTEM RECOVERY AND RECONSTITUTION** Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state, after a disruption or failure.
   - ✔ **VOTER PROTECTION** Control: vote updating The information system will permit a voter to cast a vote as many times as he/she wishes, but only the last vote cast will be counted (either electronic or providing the voter with the possibility of going to the polling station on the last day). The voter may cancel any previous cast votes by casting a new vote.
   - ✔ **ALTERNATE STORAGE SITE** Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.

9. The remote electronic voting system shall be capable to determine whether a particular voter cast a vote, and his e-vote was successfully stored, in case of exceptions, malfunctions, and breakdowns.

10. The remote electronic voting system shall be capable of resuming operations without a disruption of services after a security failure

    - ✔ **CONTINGENCY PLAN** Control: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.
    - ✔ **INFORMATION SYSTEM RECOVERY AND RECONSTITUTION** Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

5.6 Chapter Summary & Conclusions

As a wide number of threats to e-voting security can circumvent cryptographic solutions, before they have been applied, this chapter investigated controls and design principles with the ability to assist in reducing a number of previously identified threats and vulnerabilities. Within this scope, we explore cloud computing, as currently a multitude of applications and services are being transported to this deployment model, ranging from electronic government services, to word processing applications. In this section we investigated cloud computing applicability to electronic government and electronic voting, and evaluated the technology's benefits and detriments, while identifying the unique security issues introduced by this innovative architecture. Finally this chapter included an overall attempt to propose a plethora of controls or design principles, that are intended to prevent, deter, deflect, detect or recover from security threats on electronic voting.

Chapter 6

Increasing Trust

6 INCREASING TRUST

Abstract: Transparency and audit ability may be one of the most decisive rudiments of such a system, as it is directed in increasing citizen's confidentiality Public trust can be fostered through transparency and openness of all aspects of the electoral system and by implementing various recommendations and guidelines at an international level. Electronic voting information systems require strict scrutiny and continuous supervision. The complexity of these information systems restricts a large number of the electorate from having the ability to supervise the process. To overcome this issue and enhance trustworthiness, electronic voting systems need to be reviewed prior to their adoption and continuously after their deployment. Certification is a crucial element in increasing openness, as an IS is officially evaluated and tested to abide to a minimum set of requirements defined by a country or state. But more important than the certification itself is the disclosabiltity of the official certification results. Apparently, to ensure public confidence and follow the principle of transparency and reproducibility, the voting software source code, the configuration as well as the list of all hardware and software components of the e-voting system need to be open to public scrutiny. Approaching the issue from information's systems security perspective and taking into account relations with the open source initiative, it is evaluated that for electronic voting to harness the power of scientific review and secure coding, security must not depend on obscurity. Evidently for electronic voting to profit from all benefits of disclosing system software, it will have to incorporate features of the open source design process.

6.1 Transparency

Voter confidence is the level of certainty in a particular voters mind, that his/her desired election choices were actually transcribed as intended, into the equivalent computer-readable indicators. Public confidence on the other hand, is the level of acceptance of the general public, taken as a whole, that the reported election results actually represent the collective choices of the voters. The level of public confidence includes the sum of all individual voter confidences, plus other factors, such as assurance of computer program correctness, the announcement of audit results and reports of election difficulties and their causes (Saltman, 2003). Confidence in an electronic voting system can thus be seen as the sum of individual verifiability, universal verifiability, the results of the official certification of the system, the

results of official and unofficial audits and the reports on system-specific failures. We have addressed the issue of verifiability by implementing cryptographic protocols with the ability to respect voter privacy. What is necessary is to increase the transparency of the electoral processes.

Throughout history, transparency was a critical issue in democracy. The need for surveillance was invoked early on in the French Revolution, in reaction to the tendency of representatives to claim autonomy for themselves, to transform themselves into "a kind of defacto aristocracy". Surveillance is required to enhance trust, as a disconnection during election cycles occurs, as after the ballot box is closed the power is vested in the representatives. In classical Athens, as described by Aristotle, various officials were assigned the task of supervising the work of other officials (either chosen by lot or elected). There were overseers (euthynoi), auditors (logistai), supervisors (exetastai),and public ombudsmen (synegoroi) (Rosanvallon, 2008). Montesquieu, devoted considerable attention to the ephoroi, which etymologically means" those who look at, observe, or oversee" the powers that be. Rousseau, also appreciated their role and dedicated an entire chapter of the Social Contract to the Roman censors, who were responsible for auditing public accounts and had jurisdiction over certain kinds of law suits.

Electronic voting information systems, require strict scrutiny and continuous supervision. The complexity of these information systems restricts a large number of the electorate from having the ability to supervise their process. To overcome this issue and enhance trustworthiness, electronic voting systems need to be reviewed prior to their adoption and continuously after their adoption, by what today we would call overseers,supervisors, auditors but also the public ombudsmen, analogously .

The EU commission identifying the growing need for transparency in electronic elections published the "Guidelines on transparency of e-enabled elections". Fostering transparent practices in member states is a key element for building public trust and confidence. Being transparent about the e-voting system, the processes surrounding different electoral procedures and the reasons for introducing e-voting, will contribute to voters' knowledge and understanding, thereby generating trust and public confidence(Directorate General of Democracy and Political Affairs, 2005). Although transparency, through the availability of documents to voters and stakeholders, is important, it will not be possible for everybody to understand an e-voting system. In order to have confidence in the electoral process, voters rely on others who are in a position to understand the materials and the processes. It is

therefore essential that stakeholders have as much access as possible to relevant documents, meetings, activities etc. Acting in a transparent manner towards these specific and important groups, will boost public trust and confidence, because without transparency, states cannot guarantee that an e-enabled election was conducted according to the democratic principles of free and fair elections.

In the following sections, we explore methods of increasing trust in electronic voting IS, through increasing the transparency of these.

6.2 Certification

The credibility and trustworthiness of an electronic voting system is supported by a combination of measures designed to increase its openness. According to the EU commission, "system certification plays a dual role: firstly, reassuring the commissioning party that the technical specifications of the system components correspond to the specifications assigned to them; and secondly, provided certification is made public, it is a major element in creating a climate of trust around the voting procedure"(GENERAL, AND, AFFAIRS, & INSTITUTIONS, 2009), Certification is a crucial element in increasing openness, as an IS is officially evaluated and tested to abide to a minimum set of requirements defined by a country or state. *Product certification* or product qualification is the process of certifying that a certain product has passed performance, and quality assurance tests or qualification requirements stipulated in regulations such as a building code and nationally accredited test standards, or that it complies with a set of regulations governing quality and minimum performance requirements (Ascent World, 2010). Requirements include software and hardware preconditions, but also functional, accessibility, usability and security requirements. Certification defines a minimum set of security objectives, which every remote electronic voting system has to ensure and a set of assumptions to the environment, in which the system is used.

The electoral authorities would only agree to voting machines that, according to several technical analyses, comply with detailed conditions previously set up. This process would be quite similar to the certification of industrial products, but here there are some specific features, because we are not trying to check only whether a device is technically correct. We are also trying to compensate for the lack of citizen control that exists where voting procedures accept computer components. Moreover, ordinary industrial products generate external evidences of their performance, but electronic voting solutions cannot provide these external data because

they must also guarantee the secrecy of the vote.

The certification procedure requires focus on several important issues,

- which authority is responsible for the certification process?
- which criteria shall be selected upon to accurately define a electronic voting requirements?
- which components need to be checked to cover electronic voting efficiently?
- which agent will conduct the technical analysis? Should the analysis be performed by public or private bodies?
- what shall be the availability of the certification procedure documents(public or private)

Following the patterns of the ordinary industrial certification processes, these policies are usually very opaque.

In the US, the US Election Assistance Commission has assumed federal responsibility for accrediting voting system test laboratories and certifying voting equipment through the Voting System Certification & Laboratory Accreditation Program. The purpose of the program is to independently verify that voting systems comply with the functional capabilities, accessibility, and security requirements necessary to ensure the integrity and reliability of voting system operation, as established in the Voluntary Voting System Guidelines (VVSG). The Voluntary Voting System Guidelines (VVSG), are guidelines adopted by the United States Election Assistance Commission (EAC) for the certification of voting systems. Within this program the National Institute of Standards and Technology (NIST) will recommend labs for accreditation through its National Voluntary Laboratory Accreditation Program (NVLAP). Certification is only voluntary and each state has ultimate jurisdiction over certification, though most states currently require national certification for the voting systems(WIKI). Federal voting standards require voting system vendors to share their source code, with a testing laboratory selected by the vendor, and the testing labs are supposed to check that the system complies with the federal standards. However, the testing labs have come under growing criticism for missing security and reliability problems in deployed voting systems, and many experts have expressed concerns about the ability of the testing labs to ensure that voting systems are fit for use.

Over the past several months, the state of California conducted the most comprehensive

security review yet of electronic voting machines. Security experts analysed machines from three different manufacturers, performing both a red-team attack analysis and a detailed source-code review. Serious flaws were discovered in all machines, and as a result the machines were all decertified for use in California elections.

The Sequoia voting machine model, was previously evaluated and certified as being secure. The Red Team test tells a very different story. Researchers were able to surreptitiously load a trojan horse onto the system by using a USB flash drive partitioned and formatted in a manner that would enable it to trigger Windows auto-run functionality. The trojan horse was designed to monitor device events and automatically modify Sequoia's election results cartridges. Sequoia's voter SmartCards attempt to prevent forgery, by using checksumming, but the "hash is stored on the SmartCard itself," says the Red Team report. "Therefore, once the contents are modified it is trivial to recompute the correct checksum, making the card appear legitimate." Sequoia's physical security failed as well. Despite the presence of locks and seals intended to prevent tampering, researchers were able to access security-critical parts of the system "by simply unscrewing a few screws." The researchers also found vulnerabilities in the version of Microsoft SQL Server 2000 used to store the data.

In some cases—particularly with the Diebold vote tabulation server—researchers found significant discrepancies between the configuration of the machines as provided by the vendors and the configuration as described in the official documentation. The researchers evaluating the Diebold machines also found that the version of Windows 2000 Server, distributed with the servers was not properly patched and was vulnerable to exploits publicly available on the Internet. The Red Team also "noted that most standard Windows logging capabilities were either disabled or enabled in a very limited state in the configuration provided by Diebold," meaning that "most malicious actions taken by attackers would not be traceable."

The most critical flaw that the Red Team discovered in Diebold's Windows set-up, was the presence of "evidence that Diebold technicians created a remotely-accessible Windows account that, by default configuration (according to Diebold documentation), can be accessed without the need to supply a password." The Red Team overview report concludes that "the red teams demonstrated that the security mechanisms provided for all systems analyzed, were inadequate.

Because testing labs are paid and selected by the vendor, who makes the equipment being

tested, testing labs are surely aware that withholding approval too frequently might send vendors to competing testing labs with a reputation for more lenient treatment. Elsewhere in the software industry, a similar “race to the bottom” has been observed in labs that test compliance to international computer security standards. Unfortunately, at present there are few checks and balances that can be used to hold testing labs accountable if they fail to serve the public interest(Wagner, 2007).

Although certification is a critical component of trustworthiness, its actual effects will largely depend on the disclosure of its final findings. Openness refers not only to source code, but also to design methods, disclosability of audits and certification results. Disclosability of audits is often referred to as auditability. Auditability is the determination of whether the data on which an audit is based are available to be applied, so that a conclusive determination of correctness of reported results can be made. Each decision plays a critical role on the trustworthiness of an IS. It is worth noting, that, except for some slight nuances, in all the cases which have been observed, the decision taken was to restrict to the maximum the access to the documentation produced by the technical analysis(Barr at, 2008).

6.3 Openness

Recently in France, an interesting conundrum brought this issue to light, when public authorities had to take a position regarding a request by which a citizen expressly demanded the disclosure of the certification reports, related to the three authorized voting companies. On February, 3rd 2006 the French Ministry of the Interior refused to grant such a claim following the criteria provided by the CADA –Commission d’art aux Documents Administratifs. The CADA is an advisory body, whose mission consists precisely on deciding, in the light of the regulations on the access to public information, which documents can be actually disclosed and, on the basis of different criteria, which must be handled in a different way. This Commission recommended not to disclose the requested documentation, arguing that it could be detrimental to "le secret industriel et commercial ... [et] compromettre le bon déroulement des élections" (the commercial and industrial secrecy ... [and] endanger the correct electoral management)(Barrat, 2008).

The EU Recommendation to member states addresses the issue, “To ensure public confidence and follow the principle of transparency and reproducibility, the voting software source code, the configuration as well as the list of all hardware and software components of the e-voting system (see also Rec (2004)11, paragraph 69) should be part of the audit

trail."(GGIS 2010).

Several e-voting companies use proprietary software, which has the disadvantage that in most cases the rights holder does not make the source code available to the general public (or makes it available only partially or temporarily). In some cases, a few selected experts are given the possibility to review the source code. However, this is most likely to be governed by strict rules, for example non-disclosure agreements barring the electoral authority from revealing anything about the content of the source code, or its conclusions or recommendations. (Caarls, 2010).

Recognising the issue, the field of computer science has attempted to approach the issue with alternative methods. To increase trust in source code, often researchers, scholars and implementers reveal the source code to the public to scrutinize. Publicly disclosing software has fuelled concerns over the years, as it is primarily in opposition to designing software through obscurity; it is an approach that has been used by locksmiths for centuries. An important decision when defining an e-voting strategy is whether to use open-source or proprietary software. In General electronic voting software is one of the most opaque pieces of software, treated as a black box.

To anyone unfamiliar with information systems security, it appears paradoxical that open, fully disclosed source code, evidently increases overall system security, as the most obvious way in securing a system would be by keeping it secret.

There are at least three levels of openness, each with its own benefits, drawbacks, and peripheral issues:

1. Public disclosure of algorithms and protocols.
2. Public disclosure of source code .
3. Public or open contribution of source.

Every one of these levels of openness, has its own implications on security. Each also has associated costs, that are often overlooked in discussions that focus only on benefits. The acclaimed down side of any open process, for the development and review of security systems, is that open review might reveal security flaws and render users of flawed mechanisms, subject to attack. This argument is usually derided in the security community as "security through obscurity."

It is a widely accepted principle in software security to never assume your secrets are

safe. Kerckhoffs principle, which dates back to the 19th century, states that systems should be designed so that their security does not rely upon the secrecy of their design or implementation (Kerckhoffs, 1883) (Wagner, 2007). The reason is simple; if the is a leak of information about how the system works can compromise its security, then the system is fragile. (Hall, 2006). Security through obscurity, means that some sort of secrecy or obfuscation is an important part of the security model. Keeping secrets is hard, and is almost always a source of security risk. Information security experts and cryptographers believe that software engineers should "demand open source code for anything related to security" (Schneier, 1999). Security through obscurity is the failure point of most types of computer systems because it provides:

- False sense of security.
- Limited verification.
- Vulnerabilities known by the wrong people.

The claim that security through obscurity has negative implication on system security, has its roots in cryptography, where algorithms have historically been designed to resist even an adversary that gained knowledge of the cryptographic algorithm. It seems to escape public knowledge that the baton used in relay races originates from the Spartan tool of military communication encryption. As early as the fifth century BC, they employed a device called the "skytale". The earliest apparatus used in military cryptology and one of the few ever devised in the whole history of the science of transposition ciphers (Kahn, 1967,1973). The skytale consists of a staff of wood around which a strip of papyrus, or leather, or parchment is wrapped close-packed. The secret message was written on the parchment down the length of the staff; the parchment is then unwound and sent on its way. The disconnected letters make no sense unless the parchment is re-wrapped around a baton of the same length, as the first words then leap from loop to loop, forming the message. Cryptography did not try to hide the existence of a message, but only the context, as it was assumed that adversaries would be able to gain possession of the message but not understand it. Cryptography, secret writing, is the strongest tool for protection against many kinds of security threats. Well disguised data cannot be read, modified, or fabricated easily. Cryptography is rooted from higher mathematics: Group and field theory, computational complexity, and even real analysis, not to mention probability and statistics (Pfleeger & Pfleeger, 2006).

An encryption algorithm is only believed to be secure when:

1. It is based on sound mathematics.
2. It has been analysed by competent experts and found to be sound. A review by critical, outside experts is crucial.
3. It has stood the test of time. A new algorithm gains popularity people continue to review its foundations. Although a long period for successful use and analysis in not a guarantee of a good algorithm, the flaws in many algorithms are discovered relatively soon after their release.

All encryption algorithms are open to public scrutiny and their strength relies on higher mathematics. Even with the knowledge of the algorithms design, it must be computationally infeasible to break, thus making it secure. Many developers find it exciting to write their own cryptographic algorithms, sometimes banking on the fact that if they are weak, security by obscurity will help them. Weak or flawed encryption provides only the illusion of protection and security. The RC2 and RC4 encryption algorithms were supposed to be RSA Security trade secrets and were not open to public scrutiny. They were both reverse engineered and posted anonymously to the Internet (Barnum & Gegick, 2005).

6.4 Open source

Open source is a concept often related simply to the free distribution of software. Open source is an approach to design, development, and distribution, offering practical accessibility to a product's source (goods and knowledge). Before open source became widely adopted, developers and producers used a variety of phrases to describe the concept; the term open source gained popularity with the rise of the Internet, which provided access to diverse production models, communication paths, and interactive communities. The open source design approach, involves concurrent input from diverse sources, with different approaches and priorities, and is directly opposed to centralized models of development. The principles and practices are commonly applied to the peer production development of source code for software, that is made available for public collaboration. The result of this peer-based collaboration is usually released as open-source software; however open source methods are increasingly being applied in other fields of interest.

Open source software (OSS), is defined as computer software for which the source code is freely available for review and scrutiny and is made available under a license which conforms with the open source definition. OSS is often viewed as having better quality higher reliability and more flexibility, with the additional benefit of being distributed for free. Proponents of

open source software argue that due to the characteristic of openness, permitting peer review, massive parallel debugging leads to arguably securer code, than closed system software. This is often referred to as “Linus’s Law”: “Given enough eyeballs all bugs are shallow”. The many eyeballs code review assertion, has been criticized for its effectiveness.

Evidently, success of an open source project is in accord with the characteristics of the project itself. Paraphrasing Raymond,(Raymond,2001) “The best OSS projects are those that scratch the itch of the best coders”. Additionally high profile projects have the potential to motivate a greater developer community, as increasing programmers status is a core incentive. Linus’s Law has been proven effective in some high profile open source projects. (Robbins, 2005) As opposed to traditional software design methods, open source design begins only with a vision of what the final product should be; requirement analysis is an ad hoc procedure (Joseph Feller, 2005). A prototype is rapidly put into the community for circulation and the creative process begins. Release Early, Release Often. Open source projects are not subject to the economic concerns or contractual agreements that turn releases into major events in traditional development (Robbins, 2005). Additional requirements or features can come from any member of the community reviewing the product. A core group of respected developers can guide this process and review the proposals by other members of the community. Implementation and testing is often going on in parallel with system specification. Often there will be competing designs and implementations, at most one of which will be selected for inclusion in the OSS project. The process lacks most of the crucial elements of traditional project management, such as project plans, system level designs, schedules and defined processes. The parallel debugging and testing feature in open source software design is captivating. Changes or fixes to a bug are sent to the core design team through a preselected reporting channel. After a rigorous design process and approval of the updates, they are assigned to developers with specific details to be updated in each module. After changes are performed, additional code inspections, feature tests, integration, system tests and finally release to the customer follows.

Vincent Rijmen, a developer of the winning Advanced Encryption Standard (AES), encryption algorithm, believes that the open source nature of Linux provides a superior vehicle, to making security vulnerabilities easier to spot and fix, “Not only because more people can look at it, but, more importantly, because the model forces people to write more clear code, and to adhere to standards. This in turn facilitates security review” (Rijmen, 2000). In reference to Linus Law and to openness, it is believed that programmers involved in open

source projects, code carefully, knowing that their code will be heavily commented and reviewed. Additionally, commercial deadlines can impose pressures as deadlines approach that cause programmers to work less carefully.

Proponents of open systems, often counter argue, that additionally to friendly eyes reviewing software, many hostile can find weaknesses and use them to their own advantage. Whitfield Diffie, the co-inventor of public-key cryptography, is chief security officer and senior staff engineer at Sun Microsystems. “As for the notion that open source's usefulness to opponents outweighs the advantages to users, that argument flies in the face of one of the most important principles in security: A secret that cannot be readily changed should be regarded as a vulnerability. If you depend on a secret for your security, what do you do when the secret is discovered? If it is easy to change, like a cryptographic key, you do so. If it's hard to change, like a cryptographic system or an operating system, you're stuck. You will be vulnerable, until you invest the time and money to design another system. This has long been understood in cryptography, where the principle of openness was articulated as far back as the 1870s (though it took over a century to come to fruition).” (Whitfield Diffie, 1998)

Additionally, it is often stated that the second point is that a few expert eyes are better than several random ones; a dedicated organization with responsibility for the software is a better custodian than the many eyes of the open-source community. An immense argument in favor of open source processes is their massive parallel debugging.

In particular, there seems to be an increasing tendency among the mass-market proprietary software developers to rush to market, whether the product is ready or not—in essence, letting the customers be the beta testers. Furthermore, efforts to reduce costs often seem to result in lowest-common-denominator products. Indeed, satisfying stringent requirements for security and reliability (for example), is generally not a goal that yields maximum profits (Neumann, 2005). Then a straightforward economic analysis can in principle tell us the right time to roll out a product for beta testing. Alpha testers are more expensive, being paid a salary; as time goes on, they discover fewer bugs and so the cost per bug discovered, climbs steadily. At some threshold, perhaps once bug removal starts to cost more than the damage that bugs could do in a beta release product, alpha testing stops. Beta testing is much cheaper; testers are not paid (Anderson, Open and Closed System Are Equivalent, 2005). Typically, commercial software firms can ask users only to point at the problems: beta testers do not fix the bugs, they just report them. It is also interesting to note that most commercial companies do not discourage their employees from working on open source

projects (Raymond, 2001).

Elias Levy, is the former moderator of one of the most popular security discussion groups – Bugtraq, Advocates derive their dogmatic faith in the implicit security of Open Source code from the concept of "peer review," a cornerstone of the scientific process in which published papers and theories are scrutinized by experts other than the authors. The more peers that review the work, the less likely it is that it will contains errors, and the more likely it is to become accepted. So does all this mean Open Source Software is no better than closed source software when it comes to security vulnerabilities? No. Open Source Software certainly does have the potential to be more secure than its closed source counterpart. But make no mistake; simply being open source is no guarantee of security. (Levy, 2000)

Electronic voting information systems have a very high attack profile as a lot is at stake, including political power and large amounts of money. It is evidently obvious, that relying on keeping system source code and design secret, against such attacker profiles, is inapplicable protection. Insider attacks make obscurity an irrelevant security measure. It must be assumed that an attacker can obtain information about every system aspect -- assume the attacker has access to all source code and all designs. Even if this is not true, it is trivially easy for an attacker to determine obscured information. An example of such is that of the FBI spy Richard P. Hanssen, who carried out the ultimate insider attack against U.S.classified networks for over 15 years. Hanssen was assigned to the FBI counterintelligence squad in 1985, around the same time he became a traitor to his country. Even the most secure networks are often amenable to insider attacks. Several studies show that the most common threat to companies is the insider attack, where a disgruntled employee abuses access. (Howard, 2002)

At any point, an employee could consciously leave a backdoor to permit attacks on an electronic voting system. Backdoors, placed in software, could be activated when a user tries to cast a vote, can invisibly monitor, or subvert the voting process. “The prevalence of so-called EasterEggs in many popular software packages, demonstrates that this is a real possibility. (Easter Eggs are cute extras that a software developer adds to the application without authorization, for fun. One well-known example: Microsoft's Excel 97 spreadsheet application contains a full-fledged flight simulator, that can be launched using a secret sequence of keystrokes.)” (MIT, 2001).It is an undeniable fact the disclosed source code is the only protection to insider attacks of this nature.

Outsider attacks from well funded and organized threats, are equally as difficult to protect

from, using obscurity, as insider attacks. Tools such as decompilers and disassemblers, allow attackers to obtain sensitive information that may be stored in binary files. Also, inside attacks, which may be accidental or malicious, can lead to security exploits. Using real protection mechanisms to secure sensitive information should be the ultimate means of protecting your secrets. (Barnum & Gegick, 2005). Users don't want their personal data leaked. Keys must be kept secret to avoid eavesdropping and tampering. Many people make an implicit assumption that secrets in a binary are likely to stay secret, maybe because it seems very difficult to extract secrets from a binary. However keeping the "secrets" secret in a binary is incredibly difficult. One problem is that some attackers are surprisingly good at reverse engineering binaries.

Disclosing electronic voting software, firmware and hardware to public scrutiny is the single process of generating a trustworthy voting platform. Disclosed and open source software, supports random access to the system, by allowing a greater sphere of individuals the ability to scrutinize the detailed workings of a voting system. In the case of publicly available source, this access is available to all members of the public. Openness is necessary for the processes of trial and the elimination of error (Kantrowitz, The Weapon of Openness, 1992).It is important to clarify that open source software is not the same as disclosed source software. Vendors may choose to continue to use traditional software development processes and subsequently disclose the resulting source code, without any need to adopt any of the other distinguishing features of open source software. Source code disclosure policies, licensing terms, and software development processes are three separate matters, and while open source software takes a particular stance on all three topics, it is source code disclosure that matters most to elections (Hall, 2006).

Trust in electronic voting system is a crucial factor; as a threat to the trust in electronic elections can pose a threat to the trust in our electoral processes and evidently our state of governance. Security through transparent operations is the only guarantee that can maintain trust in a system. Election security has to be viewed as a component of national security, since the very legitimacy of democratic government depends on elections that are fair, open, trustworthy, and seen to be so (MIT Serve, 2001). Electronic Voting requires a higher level of security than e-commerce, “e-commerce grade security is not good enough for public elections”.

Evidently for electronic voting to profit from all benefits of disclosing system software, it will have to incorporate features of the open source design process. High reliability theory

advocates that building a highly reliable system, requires high levels of technical competence acquired through an environment that rewards error reporting and promotes continuous system improvement such as the reporting procedures implemented in open source design process (Moynihan, 2004).The open source method could potentially lead to a more robust product. The term robust here is used in Neumann's sense—that is, an intentionally inclusive term embracing meaningful security, reliability, availability, and system survivability in the face of a wide and realistic range of potential adversities (Neumann 1999), (Krishnamurthy, 2005).

It is crucial for electronic voting systems to ensure interoperability and portability. The adoption of proprietary standards and software models, which lock data into a specific model, can jeopardize system security, privacy, and interoperability. "Software and hardware of an e-voting system require ongoing maintenance. This is in addition to the procedures required for a specific event, for example, the creation of ballot papers. It is important for member states not to be over dependent on just one or two vendors for all of these actions, since this could result in a vendor-lock-in. If considering outsourcing, it is essential that those who are responsible for the elections understand what is being outsourced, why it is being outsourced and what methods and processes the vendor intends to undertake." To prevent vendor lock-in, open APIs, open data formats, and standards implemented through open-source reference models, are vital requirements. Open standards for electronic ballot formatting, transmission and storage offer tremendous potential that has yet to be effectively exploited in the marketplace. (Jones, 2003)

The question of a single, open standard, usable by all the different e-voting systems, is a further possible solution to the distrust expressed by the various players in the electoral process. The proposal put forward by OASIS, which comprises government representatives, researchers, enterprises and electoral service providers, is to promote a standard facilitating data exchange, between hardware, software and service providers. EML (Election Mark-up Language) is an attempt to take up this challenge by ensuring the harmonious, robust and reliable interoperability of all the systems involved in the electoral system. The standard, which is now at its version 5.0, was designed for use in either public or private elections, either comprehensively, covering the entire process, or selectively for the registration on electoral lists, the voting itself, vote counting or the communication of results. It is a case of providing common interfaces at "critical" stages in the voting procedure in order to certify the relevance, conformity and validity of the data exchanged. One of the advantages of using EML as a standard, is that it gives users greater freedom to call on the services of more

different hardware and software suppliers, and thus escape the pressure to use one proprietary programme. The transparency requirement, particularly in respect of software used by voting system suppliers, which is specific to political elections, is more compatible with open-source software than with proprietary systems. To that extent, recognising the EML as an ISO standard is one of the priority objectives of OASIS, which is actively working towards this goal, backed up by the many experiments of voting with EML, which have been conducted since 2003 in the USA and Europe, particularly under the European e-Poll project. (GENERAL, AND, AFFAIRS, & INSTITUTIONS, 2009)

Overall, using an open source design process to designing electronic voting systems will evidently lead to (Hall, 2006) (Joseph Feller, 2005) (Pfleeger & Pfleeger, 2006) (Howard, 2002):

- Securer System. Will evidently lead to a securer system due to mass parallel testing debugging and monitoring.
- Less Complex & Higher Quality. Complex design is never easy to understand, and is therefore more likely to include subtle problems that will be missed during analysis. Complex code tends to be harder to maintain as well. And most importantly, complex software tends to be far buggier.
- Transparency. Clear and complex free source code ,publicly available, promotes transparency. Historically, one of the abiding principles of election administration has been that the best way to demonstrate that the election is honest is by inviting public scrutiny and being open and transparent about all aspects of the election.
- Usability. A not so obvious point of simplicity is usability.
- Accountability. Design and test teams can be held accountable for not performing duties.
- Evaluation. Source code disclosure would enable independent analysis of voting software.
- Promote Interoperability. Source code disclosure would eliminate one barrier to interoperability between equipment from different vendors, potentially enhancing competition between vendors
- Increased Accuracy. An efficiently and effectively operating system will operate as expected introducing increased accuracy into the electoral results.

6.5 Chapter Summary & Conclusions

Transparency and audit ability may be one of the most decisive rudiments of such a system, as it is directed towards increasing citizen's confidentiality Public trust can be fostered through transparency and openness of all aspects of the electoral system and by implementing various recommendations and guidelines at an international level. Electronic voting information systems, require strict scrutiny and continuous supervision. The complexity of these information systems restricts a large number of the electorate from having the ability to supervise the process. To overcome this issue and enhance trustworthiness, electronic voting systems need to be reviewed prior to their adoption and continuously after their deployment. Certification is a crucial element in increasing openness, as an IS is officially evaluated and tested to abide to a minimum set of requirements defined by a country or state. But more important than the certification itself, is the disclosabiltity of the official certification results.

Although certification can enhance openness, it is only one side of the coin. Certification labs have often come under growing criticism for missing security and reliability problems in deployed voting systems, and many experts have expressed concerns about the ability of the testing labs to ensure that voting systems are fit for use. Additionally, in many cases, certification documents have been restricted to public view, due to disclosability agreements. Apparently, to ensure public confidence and follow the principle of transparency and reproducibility, the voting software source code, the configuration, as well as the list of all hardware and software components of the e-voting system, need to be open to public scrutiny.

Approaching the issue from information's systems security perspective and taking into account relations with the open source initiative, it is evaluated that for electronic voting to harness the power of scientific review and secure coding, security must not depend on obscurity. Evidently, for electronic voting to profit from all benefits of disclosing system software, it will have to incorporate features of the open source design process.

Chapter 7

Conclusion

7 CONCLUSION

Over recent years, interest in the field of electronic voting has been growing, as countries globally are exploring methods of using ICT to increase election accuracy, speed and transparency, while openning democratic processes to a broader audience. A number of countries have experimented with electronic voting solutions and have concluded to abandon its implementation, until further developments in the field are made, while others have succeeded in implementing fully electronic vote casting systems without failures. Approaches and conclusions seem to differ widely, while the Netherlands have decided to revert to traditional voting, abandoning voting machines, France has authorised the latter since 2003 but is refusing to implement e-voting in areas other than professional elections, which is also the case in Portugal; Austria successfully conducted its first e-voting legally binding election in 2009, Switzerland has amended its legal regulations to enable remote e-voting, Estonia has held two consecutive legally binding remote e-voting elections, while the United Kingdom, despite its very many "pilot runs" (150 since 2002), has suspended any further experimentation until 2010, officially for reasons of electoral timetables (GGIS, 2009).

It is a common fact, that globally, Information Systems and Communication Technologies are silently being integrated into different stages of the electoral process, thus it is becoming a necessity that we explore methods that enable secure electronic voting, while researching controls with the ability to reduce threats. The basic question in electoral administration no longer focuses on whether ICT should be accepted in the electoral process, but rather on what kind of technology should be implemented, to what extent and what protection mechanisms should be applied.

It is now clear, that the success of an electronic voting system is evidently dependent on the issue of trust and its dimensions, as fears on e-voting are often voiced on security issues, but also on the sociological and political implications. Such trust can be assessed in political terms, sociological, but also as trust in the technology that abides and is regulated by a legal framework.

Trust assessed in political terms, is the so-called political trust. Political trust happens when citizens appraise the government and its institutions, policy making in general and/or the individual political leaders as promise-keeping, efficient, fair and honest. If such trust exists, voters are then very likely to have confidence in new e-enabled elections. Information and Communication Technologies (ICT) have been considered vital for political systems.

ICT's were recognized to have tremendous administrative “potential” , ICTs could help create a networked structure for interconnectivity, efficiency and effectiveness , interactivity, decentralization, transparency, and accountability.

Political trust does not emerge, nor does it operate, in vitro. Social trust, which refers to citizens’ confidence in each other, as members of a social community, is inseparable from the notion of political trust. Increasing social trust, is associated with increasing political participation, especially in the form of voting. Electronic voting is an e-participation method with the capacity of widening participation in the electoral process. It is seen as bringing a social improvement in it by widening the circle of citizens involved in politics and political decision-making. E-voting systems have the potential to be more usable than paper, especially for people with disabilities such as visual impairment or reduced kinetic ability. As Ms Gabriele Kucsko-Stadlmayer, the Venice Commission representative, pointed out, the main disadvantages of remote e-voting, particularly the shortcomings in terms of system security, are much less serious, given that e-voting enables population groups, previously excluded from the electoral process (eg persons with disabilities, soldiers and other citizens abroad) to exercise their voting rights.

The notion of trust in an organisation could be defined as the customer’s certainty that the organisation is capable of providing the required services accurately and infallibly. A certainty which also expresses the customer’s faith in its moral integrity, in the soundness of its operation, in the effectiveness of its security mechanisms, in its expertise and in its abidance by all regulations and laws, while at the same time, it also contains the acknowledgement of a minimum risk factor, The notion of security refers to a given situation where all possible risks are either eliminated or brought to an absolute minimum. Electronic voting Information systems demand, to be treated as security critical information systems, with a complexity higher than traditional information systems. As no IS is totally secure, a combination of measures need to be applied, that can address a number of the identified threats (i.e. integrity, confidentiality, authenticity, and availability of data and communications), effectively enabling secure electronic voting.

This dissertation has approached the issue of electronic voting as security critical process. This research attempts to approach the issue from an inter-disciplinary scope, while focusing on security issues, as deploying a system in a secure manner requires meeting technical and procedural levels of assurance, in respect to social and regulatory frameworks. From an Information and Communication Security perspective, a structured analysis has been adopted

to identify vulnerabilities, involved in the digitalization of government transactions and the electoral process, exploring the notion of trust and transparency within this context. A number of information security risks, vulnerabilities and threats have been documented, leading to the identification of a set of requirements, which should be met when designing an e-voting system. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process, to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability).These requirements lead to the development of a design framework, with proposals for consideration, that can assist in reducing these vulnerabilities. The research methodology adopted towards achieving this goal, is based on software engineering and information systems design approaches.

Evolution in the field of cryptography, has taken cryptographic algorithms out of the theoretical sphere and applied them as solutions to a number of information systems security issues. Cryptography is concerned with the construction of schemes, that should withstand abuse. Cryptographic protocols, provide an opportunity to generate trust between involved parties of an election. Cryptography is a crucial element of the overall system security, dealing with integrity, confidentiality, authenticity of communications and data and verifiability of elections. The design of cryptographic voting schemes, which started in the early 80's, has proved to be very challenging, due to the multitude and conflicting nature of properties such schemes need to satisfy. A number of election crypto-systems have been proposed and evaluated. Today this technology is believed to be mature, due to intense scrutiny that has occurred in the field over recent years. Within this context, Public Key Infrastructure is identified as the essential architecture upon which security and trust are built, in order to provide authentication, identity verification, encryption and non-repudiation in electronic transactions. The ability of the deployed e-passport PKI, to extend and meet the correlating demands of an e-ID infrastructure have been explored and a high level solution has been proposed.

Unfortunately though, cryptography is not enough; as a wide number of threats to e-voting security can circumvent cryptographic solutions, before they have been applied. Within this framework, cloud computing is explored, as currently a multitude of applications and services are being transported to this deployment model, ranging from electronic government services to word processing applications. We evaluate the technology's benefits and

detriments, while identify the unique security issues introduced by this innovative architecture and ways of overcoming these. We proposes a high level electronic governance and electronic voting solution, supported by cloud computing architecture and cryptographic technologies, additionally identifying issues that require further research. Overall, this dissertation has attempted to propose a plethora of controls or design principles, that are intended to prevent, deter, deflect or detect security threats on electronic voting , but also to increase transparency to achieve greater auditability.

Public trust can be fostered through transparency and openness of all aspects of the electoral system and by implementing various recommendations and guidelines at an international level. Electronic voting information systems, require strict scrutiny and continuous supervision. The complexity of these information systems, restricts a large number of the electorate from having the ability to supervise the process. To overcome this issue and enhance trustworthiness, electronic voting systems need to be reviewed prior to their adoption and continuously after their deployment. Certification, is a crucial element in increasing openness, as an IS is officially evaluated and tested to abide to a minimum set of requirements defined by a country or state. But more important than the certification itself is the disclosabiltity of the official certification results.

Although certification can enhance openness, it is only one side of the coin. Certification labs have come under growing criticism for missing security and reliability problems in deployed voting systems, and many experts have expressed concerns about the ability of the testing labs to ensure that voting systems are fit for use. Additionally, in many cases, certification documents have been restricted to public view, due to disclosability agreements. Evidently, to ensure public confidence and follow the principle of transparency and reproducibility, the voting software source code, the configuration, as well as the list of all hardware and software components of the e-voting system, need to be open to public scrutiny.

It is crucial that further research is conducted in the field of electronic voting security, through official trials and pilots, before any solution is adopted for legally binding elections, as the integrity of the electoral system is at stake. A number of issues can be identified as open, thus requiring further research,

Open Issues,

- Efficiency, effectiveness and speed of cryptographic schemes for large scale elections. Although proposed cryptographic schemes are able to guard the

principles of security, these may deter system usability and accessibility. A devastating majority of Internet users, either business or social, seem to lack the basic ability, knowledge or even willingness to effectively use cryptographic applications, in a way that can successfully deter imminent threats. As when users fail to manage their private keys securely or when they fail to validate each other‟s public keys rigorously, then authenticity and privacy guarantees weaken and overall security deteriorates. The design of an e-voting solution must achieve high usability stands. Additionally, these crypto-systems must be thoroughly tested and evaluated to guarantee their ability to perform successfully under high demand.

- Availability of e-voting system. Denial of service and distributed denial of service attacks, project an important issue for high profile internet accessed IS. A **denial-of-service attack** (**DoS attack**) or **distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a computer resource unavailable, simply by saturating the target machine with external communications requests. Cloud computing architecture increases resilience of the IS, due to the multitude of servers and IDS deployed, giving the system an edge against traditional architecture, but does not propose a perfect remedy. Network filtering is the best, though still imperfect remedy to DDOS. Further research is required in ways of protecting Is against DDOS and DOS attacks.

- Cloud Computing Security. As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through the adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered, as the characteristics of this innovative deployment model, differ widely from those of traditional architectures. From a security perspective, a number of uncharted risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. Further scrutiny is required in this innovative field before the adoption of such solutions for security sensitive information systems. Future work should also focus on improving the availability and quality of such services provided.

- Authentication Credentials. An additionally important issue, which diminishes overall system security, includes the selling of voter authentication credentials. “How should the system protect against wide selling of authentication

credentials?" remains an open question. A partial solution suggested to counter this threat, includes permitting voters with the ability to cast valid vote by visiting an election hall thus canceling previously cast e-vote/s, thus making e-vote selling unattractive, as the e-vote can not be guaranteed.

Chapter 8

Bibliography

8 BIBLIOGRAPHY

44 U.S.C. § 3542. (n.d.). *United States Code: Title 44,3542. Definitions | LII / Legal Information Institute*.

ACEEEO. (2005). Recommendations on the Implementation of E-voting. *Global Election Organizations and General Assembly Meeting of the Association of Central and Eastern European Election Officials (ACEEEO)*. Siófok, Hungary.

Adida, B. (2006). *Advances in Cryptographic Voting Systems*. *Electrical Engineering*. Massachusetts Institute of Technology.

Alshamsi, A., & Saito, T. (2004). A technical comparison of IPSec and SSL. *Cryptology*.

Altmann, J., Rana, O., Tserpes, K., Aisopos, F., Kyriazis, D., & Varvarigou, T. (2010). *Economics of Grids, Clouds, Systems, and Services*. (J. Altmann & O. F. Rana, Eds.) (Vol. 6296, pp. 16-33-33). Berlin, Heidelberg: Springer Berlin Heidelberg. doi: 10.1007/978-3-642-15681-6.

Artz, D., & Gil, Y. (2007). A survey of trust in computer science and the Semantic Web. *Web Semantics: Science, Services and Agents on the World Wide Web*, *5*(2), 58-71. doi: 10.1016/j.websem.2007.03.002.

Ascent World. (2010). ISO Product Certification. Retrieved April 30, 2011, from http://iso.ascentworld.com/product-certification/.

Barnum, S., & Gegick, M. (2005a). Separation of Privilege. *Build Security In*. Retrieved April 26, 2011, from https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/principles/357-BSI.html.

Barnum, S., & Gegick, M. (2005b). Least Common Mechanism. *Build Security In*. Retrieved April 26, 2011, from https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/principles/350-BSI.html.

Barrat, J. (2008). The Certification of E-Voting Mechanisms. Fighting against Opacity. In Robert Krimmer & R. Grimm (Eds.), *3rd international Conference on Electronic Voting 2008.Lecture Notes in Informatics*.

Beizer. (2008). DISA debuts self-service computing. *FCW*. Retrieved April 28, 2011, from

http://fcw.com/Articles/2008/07/14/DISA-debuts-selfservice-computing.aspx.

Beizer, D. (2009). USA.gov will move to cloud computing. *FCW*. Retrieved April 28, 2011, from http://www.fcw.com/Articles/2009/02/23/USAgov-moves-to-the-cloud.aspx.

Bekkers, V., & Zouridis, S. (1999). Electronic service delivery in public administration: Some trends and issues. *International Review of Administrative Sciences*, *65*, 183−196.

Benaloh, J. (1987). *Verifiable Secret Ballot Elections*. Yale University.

Blind, P. K. (2007). BUILDING TRUST IN GOVERNMENT IN THE TWENTY-FIRST CENTURY: Review of Literature and Emerging Issues. *7th Global Forum on Reinventing Government Building Trust in Government* (pp. 1-31). Vienna, Austria.

Bruschi, Danilo, Poletti, Giusi, & Rosti, Emilia. (2003). E-vote and PKI's: a need, a bliss or a curse? In Dimitris Gritzalis (Ed.), *Secure Electronic Voting (Advances in Information Security)*. Kluwer Academic Publishing.

Buchstein, H. (2004). Online Democracy, Is it viable?Is it desirable?Internet Voting and Normative Democratic theory. In N. Kersting & H. Baldersheim (Eds.), *Electronic Voting and Democracy: A Comparative Analysis* (p. 328). Palgrave Macmillan. Retrieved November 28, 2010, from http://www.amazon.co.uk/Electronic-Voting-Democracy-Comparative-Analysis/dp/1403936781.

Burnester, M., & Magkos, E. (2003). Towards secure and practical e-elections in the new era. In Dimitris Gritzalis (Ed.), *Secure Electronic Voting (Advances in Information Security)*.

Caarls, S. (2010). *E-voting handbook, Key steps in the implementation of e-enabled elections*. Strasbourg.

California Internet Voting Task Force. (2000). *A Report on the Feasibility of Internet Voting*.

Capgemini. (2009). *8th Benchmark Measurement of European eGovernment services*. Brussels.

Castell, S. (1993). *Code of practice and management guidelines for trusted third party services*.

Chaum, D. (1981). Untraceable electronic mail, return address, and digital pseudonyms. *Communication of the ACM* (pp. 84-88). ACM Press.

Chaum, D. (1982). Blind signatures for untraceable payments. *Advances in Cryptology, CRYPTO'82, Lectures Notes in Computer Science,* (pp. 199-203). Springer-Verlag.

Cloud Identity Summit. (2010). Secure the cloud now, Cloud identity summit. *Cloud Identity Summit*. Retrieved November 10, 2010, from http://www.cloudidentitysummit.com/.

Cloud Security Alliance. (2010). *Top threats to cloud computing*.

Cohen, J., & Fisher, M. (1985). *A Robust and Verifiable Cryptographically Secure Election Scheme*.

Commission of the European Community. (1994). *Green paper on the security of information systems,* .

Community Connexion Inc. (n.d.). *The Anonymizer*. Retrieved from http://www.anonymizer.com.

Council of Europe. (2004). Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. *BMJ (Clinical research ed.)*, *340*, c3033. Retrieved from http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2933870&tool=pmcentrez&rendertype=abstract.

Cramer, R., Gennaro, R., & Schoenmakers, B. (1997). A Secure and Optimally Efficient Multi-Authority Election Scheme. *EUROCRYPT'97*.

Cranor, L. (2003). In search of the perfect voting technology: no easy answers. In Dimitris Gritzalis (Ed.), *Secure Electronic Voting (Advances in Information Security)* (pp. 17-30). Springer. Retrieved November 25, 2010, from http://www.amazon.com/Secure-Electronic-Advances-Information-Security/dp/1402073011.

Curse, A., Bruschi, D., Poletti, G., & Rosti, E. (2003). E-VOTE AND PKI'S: A NEED, A BLISS OR. In Dimitris Gritzalis (Ed.), *Secure Electronic Voting*. Kluwer Academic Publishing. Retrieved February 20, 2011, from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.115.7287.

Curtin, M., & Neumann, P. G. (2001). *Developing Trust: Online Privacy and Security* (p. 312). Apress.

CyberVote Project. (2000). *Report on electronic democracy projects, legal issues of Internet voting and users requirements analysis*.

Damgard, I., Groth, J., & Salomonsen, G. (2003). The theory and implementation of an electronic voting system. In Dimitris Gritzalis (Ed.), *Secure Electronic Voting (Advances*

in Information Security). Kluwer Academic Publishing.

Deutsch, K. W. (1963). *Nerves of Government*. Free Press.

DiCaterino, A., & Pardo, T. (1996). *The World Wide Web as a universal interface to government services.*

Directorate General of Democracy and Political Affairs. (2005). *Guidelines on transparency of e-enabled elections*. Strasbourg.

DIRECTORATE GENERAL OF DEMOCRACY AND POLITICAL AFFAIRS. (2009). Meeting to review developments in the field of e-voting since the adoption of Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. *Council of Europe's Forum for the Future of Democracy on the theme of e-democracy* (pp. 1-8). Strasbourg.

DIRECTORATE GENERAL OF DEMOCRACY AND POLITICAL AFFAIRS. (2010). *Guidelines on transparency of e-enabled elections*. *October.* Strasbourg.

Election Assistance Commission. (2005). *VOLUNTARY VOTING SYSTEM GUIDELINES. Volume I. Voting System Performance Guidelines*.

Estonian National Electoral Committee. (2011). *Statistics about Internet Voting in Estonia*. Tallinn. Retrieved from http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics.

Ferguson, N., & Schneier, B. (2003). *Practical Cryptography* (p. 8). Indianapolis,Indiana: Wiley Publishing.

Flew, T., & Young, G. (2005). From e-Government to Online Deliberative Democracy. *Oxford Internet Institute Summer Doctoral Program, Chinese Academy of Social Sciences* (pp. 1-11). Beijing.

Gartner. (2008). *Assessing the security risks of cloud computing*.

Gerlach, B. J., & Gasser, U. (2009). Three Case Studies from Switzerland :

Ghere, R. K., & Young, B. A. (1998). The cyber-management environment: Where technology and ingenuity meet public purpose and accountability. *Public Administration and Management: An Interactive Journal, 3(1)*. Retrieved from http://www.pamij.com/gypaper.html. .

Goldreich, O. (2007). *Foundations of Cryptography: Volume 1, Basic Tools* (p. 396). Cambridge University Press.

Goldschlag, D., Reed, M., & Syverson, P. (1999). Onion Routing for Anonymous and Private Communications. *Communications of the ACM*, *42*(2), 39-41.

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. *Siam Journal on Computing - SIAMCOMP*, *18*(1), 186-208.

Gritzalis, D. (2002a). Principles and requirements for a secure e-voting system. *Computers & Security*, *21*(6), 539-556. doi: 10.1016/S0167-4048(02)01014-3.

Gritzalis, D. (2002b). Principles and requirements for a secure e-voting system. *Computers & Security*, *21*(6), 539-556. doi: 10.1016/S0167-4048(02)01014-3.

Gritzalis, S., Katsikas, Socratis, Lekkas, D., Moulinos, K., & Polydorou, E. (2000). Securing The Electronic Market: The KEYSTONE Public Key Infrastructure Architecture. *Computers & Security*, *19*(8), 731-746.

Gutierrez, A., & Piñuela, A. (2009). *STORK Glossary and Acronyms*.

Heeks, R. (2001a). Building e-governance for development: A framework for national and donor action. *The University of Manchester, Institute for Development, Policy and Management Information, Systems, Technology and Government: Working Papers Series*.

Heeks, R. (2001b). Understanding e-governance for development. *The University of Manchester, Institute for Development, Policy and Management Information, Systems, Technology and Government: Working Papers Series*, *11/2001*.

Helbach, J., & Schwenk, J. (2007). Secure Internet Voting with Code Sheets. *E-Voting and Identity – First International Conference, VOTE-ID 2007. LNCS, vol. 4896* (p. 166–177). Springer, Heidelberg.

Howard, M., & LeBlanc, D. (2002). *Writing Secure Code* (2nd ed.). Redmond: Microsoft Press.

Ikonomopoulos, S., Labrinoudakis, C., Gritzalis, Dimitris, Kokolakis, S., & Vassiliou, K. (2002). Functional Requirements for a Secure Electronic Voting System. *IFIP Conference Proceedings; Vol. 214, ,IFIP TC11 17th*.

Internet 2. (2007). Shibboleth. Retrieved November 10, 2010, from http://shibboleth.internet2.edu/.

Internet 2. (2010). FAQ on SAML and Shibboleth relationship. *Shibboleth, Internet 2*. Retrieved November 10, 2010, from http://shibboleth.internet2.edu/.

IP/09/343. (2010). *Better high-speed internet access needed to revitalise Europe ' s rural regions , says Commission*. *Romania*. Brussels.

IP/10/1328. (2010). *Digital Agenda : household survey reveals more Europeans on-line but concerned about costs and security*. *October* (pp. 10-12). Brussels.

ISACA. (2006). *CISA Review Manual 2006. Information Systems Audit and Control Association.*

Jones, D. (2003). The evaluation of voting technology. In Dimitris Gritzalis (Ed.), *Secure Electronic Voting (Advances in Information Security)*. Kluwer Academic Publishing.

Joshi, J. B. D., Aref, W. G., Ghafoor, A., & Spafford, E. H. (2001). Security models for web-based applications. *Communications of the ACM*, *44*(2), 38-44. doi: 10.1145/359205.359224.

Katsikas, Sokratis. (2001). The Role of Public Key Infrastructure in Electronic Commerce. *ejeta*. Retrieved from http://www.ejeta.org/first-issue/ejeta-2001.12.31.22.46.37.pdf.

Keystone. (1998). *KEYSTONE project, KEYSTONE deliverable 9.1: Final project report*.

Klaus, D., & Weddeling, S. (2006). Online Voting Project – New Developments in the Voting System and Consequently Implemented Improvement in the Representation of Legal Principles. *Electronic Voting 2006 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.5 and E-Voting.CC* (pp. 213-222).

Krimmer, R. (2010). The Use of E-Voting in the Federation of Students Elections 2009. *4th International Conference on Electronic Voting*. Bregenz.

Krimmer, R., Triessnig, S., & Volkamer, M. (2007). The Development of Remote EVoting around the World: A Review of Roads and Directions. In A. Alkassar & M Volkamer (Eds.), *E-Voting and Identity – First International Conference, VOTE-ID 2007.*

Krimmer, Robert, & Schuster, R. (2008). The E-Voting Readiness Index. In Robert Krimmer & R. Grimm (Eds.), *3rd international Conference on Electronic Voting 2008* (pp. 127-136). Castle Hofen, Bregenz, Austria.

Labrinoudakis, C., Gritzalis, Dimitris, Tsoumas, V., Karyda, M., & Ikonomopoulos, S. (2003). Secure electronic voting:the current landscape. In Dimitris Gritzalis (Ed.), *Secure Electronic Voting (Advances in Information Security)S*. Kluwer Academic Publishing.

Lang, B., Foster, I., Siebenlist, F., Ananthakrishnan, R., & Freeman, T. (2008). *Attribute based*

access control for grid computing.

Macintosh, A. (2004). *Working Group 4 to the European Commission.* Retrieved from Retrieved 03 05, 2004, from http://www.eu-forum.org/summit/docs/WG4e-democracy-FINAL RESULTS.doc.

Mark, R. (2008). Do federal agencies belong in cloud computing networks? *eWeek*. Retrieved April 28, 2011, from http://www.eweek.com/c/a/Government-IT/Should-Feds-Climb-on-the-Cloud/.

McClure, C. R., & Bertot, J. C. (2000). The Chief Information Officer (CIO): Assessing its impact. *Government Information Quarterly*, *17*, 7-12.

Mcgaley, M. (2008). *E-voting: an Immature Technology in a Critical Context*. *PhD Thesis*. National University of Ireland.

Mcgaley, M., & Gibson, J. P. (2006). A Critical Analysis of the Council of Europe Recommendations on e-voting. *EVT'06 Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop*.

Mell, P., & Grance, T. (2011). *NIST SP 800-145. The NIST Definition of Cloud Computing (Draft). Recommendations of the National Institute of Standards and Technology*.

MEMO/10/681. (2010). *Digital Agenda: eGovernment Action Plan - what would it do for me?* Brussels.

Mercuri, R. (2001). Electronic Vote Tabulation Checks and Balances. University of Pennsylvania: Bell&Howell Information and Learning Company.

Micciancio, D. (2010). A First Glimpse of Cryptography's Holy Grail. *Communications of the ACM*, *53*(3), 56.

Mitrou, L, Gritzalis, D, & Katsikas, S. (2002). Revisiting legal and regulatory requirements for secure e-voting. *IFIP SEC 2002* (pp. 469-480.). Cairo, Egypt.

Mitrou, Lilian, Gritzalis, Dimitris, Katsikas, Sokratis, & Quirchmayr, G. (2003). e-Voting:Constitutional and legal requirements and their technical reflection. In Dimitris Gritzalis (Ed.), *Secure Electronic Voting (Advances in Information Security)*. Kluwer Academic Publishing.

Monnoyer-Smith, L. (2008). *Council of Europe Forum for the Future of Democracy, "e-democracy", Workshop No 3 "ICT in electoral processes."* Madrid, Spain.

Moynihan, D. P. (2004). Building Secure Elections: E-Voting, Security, and Systems Theory. *Public Administration Review*, *64*(5), 515-528. doi: 10.1111/j.1540-6210.2004.00400.x.

Nagarajan, A., & Varadharajan, V. (2011). Dynamic trust enhanced security model for trusted platform based services. *Future Generation Computer Systems*, *27*(5), 564-573. doi: 10.1016/j.future.2010.10.008.

NIST. (2006). *DRAFT HFP Section of VVSG. Usability and Accessibility Requirements*. Retrieved from http://vote.nist.gov/VVSG-HFP.pdf.

NIST 800-60. (2008). *Guide for Mapping Types of Information and Information Systems to Security categories*.

Oppliger, R., Schwenk, J., & Helbach, J. (2008). Protecting Code Voting Against Vote Selling. *LNI*, *128*, 193–204.

Otten, D. (2005). Mehr Demokratie durch Internetwahlen? *Vortrag gehalten im Nixdorf Forum in Paderborn*.

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, *27*(3), 245-253. doi: 10.1016/j.giq.2010.01.002.

Patsos, D., Ciechanowicz, C., & Piper, F. (2010). The status of National PKIs – A European overview. *Information Security Technical Report*, *15*(1), 13-20. doi: 10.1016/j.istr.2010.10.007.

Paul, R. (2009). Netherlands says “nee” to electronic voting. Retrieved April 19, 2011, from http://arstechnica.com/hardware/news/2008/05/netherlands-says-nee-to-electronic-voting.ars.

Peralta, R. (2003). Issues, non issues, and cryptographic tools for internet-based voting. In Dimitris Gritzalis (Ed.), *Secure Electronic Voting (Advances in Information Security)*. Kluwer Academic Publishing.

Pfleeger, C., & Pfleeger, S. (2006). *Security in Computing* (4th ed.). Prentice Hall.

Polemi, D. (1998). Trusted third party services for health care in Europe. *Future Generation Computer Systems*, *14*(1-2), 51-59. doi: 10.1016/S0167-739X(98)00008-9.

Prisajganec. (2010). ELECTRONING VOTING: NECESSITY OR FICTION. Retrieved from www.nispa.org/files/conferences/2010/.../201006230944530.dimeski.doc.

Project, E. S. V. (2010). Student Vote. Retrieved October 30, 2010, from http://www.eu-studentvote.org/centreen.htm#.

Ralston, A., Reilly, E. D., & Hemmendinger, D. (2003). Information Systems. *Encyclopedia of Computer Science, 4th edition*. John Wiley and Sons Ltd.

Reese, G. (2009). *Cloud Application Architectures: Building Applications and Infrastructure in the Cloud (Theory in Practice (O'Reilly))* (p. 208). O'Reilly Media. Retrieved April 29, 2011, from http://www.amazon.com/Cloud-Application-Architectures-Applications-Infrastructure/dp/0596156367.

Republique Et Canton De Geneve. (n.d.). History and results of the tests and official ballots. *2010*. Retrieved November 23, 2010, from http://www.geneve.ch/evoting/english/historique.asp.

Rosanvallon, P. (2006). *Democracy past and future (political thought / political history)* (p. 312). Columbia University Press.

Rubin, A. (2001). *Security considerations for remote evoting over the Internet*.

Russian Federation. (2010). Ways, means and methods of electronic voting current conditions: the Russian approach to e-voting. *Third meeting to review developments in the field of e-voting since the adoption of Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting*. Strasbourg: Directorate General of Democracy and Political Affairs DIRECTORATE OF DEMOCRATIC INSTITUTIONS.

Saltman, R. (2003). Public confidence and auditability in voting systems. In Dimitris Gritzalis (Ed.), *Secure Electronic Voting (Advances in Information Security)*. Kluwer Academic Publishing.

Saltzer, J. H., & Schroeder., M. D. (1975). The Protection of Information in Computer Systems. *Proceedings of the IEEE 63, 9* (pp. 1278-1308).

Schneier, B. (2000). The Process of Security. *Information Security Magazine*.

Schäuble, W. (2007). No Title. *German Minister of Interior, Statement at eGovernment Conference*. Berlin.

Seibert, H., & Loof, A. (2010). *Internet usage in 2010 – Households and Individuals*. Retrieved from http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF.

Sherman, R. (1992). Distributed systems security. *Computers & Security*, *11*(1), 24-28. doi: 10.1016/0167-4048(92)90216-E.

Spanish Government. (2010). ELECTORAL MANAGEMENT: E VOTING AND ICTS. CURRENT SITUATION, Contribution by Spain. *Third meeting to review developments in the field of e-voting since the adoption of Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting*. Retrieved from http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/E-voting 2010/Biennial_Nov_meeting/GGIS(2010)12_Spain e-voting report E.asp#TopOfPage.

Stanoevska-Slabeva, K., Wozniak, T., & Ristol, S. (2009). *Grid and Cloud Computing: A Business Perspective on Technology and Applications* (Springer.).

Strehlow, R. A., Wright, S. E., & Materials, A. S. for T. and. (1993). *Standardizing terminology for better communication: practice, applied theory ...* (p. 390). ASTM International. Retrieved February 15, 2011, from http://books.google.com/books?id=AS2OP1MK8ngC&pgis=1.

T. Zefferer (AT-TUG). (2010). *STORK Work Item 3.3.5 Smartcard eID Comparison*. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1384.

Tsekmezoglou, E., & Iliadis, J. (2005). A Critical View on Internet Voting Technology. *eJeta*, (4). Retrieved from http://www.ejeta.org/fourth-issue/ejeta-2005.12.25.00.08.19.pdf.

UK Federation Information Centre. (2007). *UK Federation Information Centre Report*.

UK Govenrment. (2007). *The Government ' s response to the Electoral Commission ' s recommendations on the May 2007 electoral pilot schemes Introduction The Government ' s responses to the key recommendations from the Electoral Commission ' s evaluations E-voting* (pp. 1-9).

Varvitsiotis, A. P. (2000). Scaling issues in large PKI communities. *Future Generation Computer Systems*, *16*(4), 361-372. doi: 10.1016/S0167-739X(99)00060-6.

Viega, J., & McGraw, G. (2001). *Building Secure Software: How to Avoid Security Problems the Right Way* (p. 528). Addison-Wesley Professional.

Volkamer, Melanie. (2009). *Evaluation of Electronic Voting* (Lecture No.). Springer.

Volkamer, Melanie, & Hutter, D. (2004). From Legal Principles to an Internet Voting System.

Electronic Voting in Europe - Technology, Law, Politics and Society (pp. 111-120).

VoterAction. (2008). *Glossary of election terms for Pennsylvania*. Seattle.

Wagner, D. (2007). *WRITTEN TESTIMONY BEFORE THE COMMITTEE ON HOUSE ADMINISTRATION, ELECTIONS SUBCOMMITTEE*.

Weldemariam, K. S. (2010). *Using Formal Methods for Building more Reliable and Secure e-voting Systems*. *Technology*. University of Trento.

Wikipedia. (2010). Information security. Retrieved April 20, 2011, from http://en.wikipedia.org/wiki/Information_security.

Yildiz, M. (2007). E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly*, *24*, 646–665.

Zissis, D., & Lekkas, D. (2011). Addressing cloud computing security issues. *Future Generation Computer Systems*. Elsevier B.V. doi: 10.1016/j.future.2010.12.006.

Zissis, D., Lekkas, D., & Papadopoulou, A.-E. (2009). Competent Electronic Participation Channels in Electronic Democracy. *Electronic Journal of eGovernment*, *7*(2), 195-208. Retrieved from http://www.ejeg.com/issue/download.html?idArticle=174.

Zuzana, R. (2002). *Electronic Voting Schemes*. Comenius University, Bratislava.

APPENDICES

A,B & C

APPENDIX A TERMS

Terms

Accessibility	
Accountability	information, selectively kept and protected, so that actions affecting security can be traced to the responsible party (audit).
AUDIT:	
Auditabillity	the determination of whether the data on which an audit is based are available to be applied so that a conclusive determination of correctness of reported results can be made.
Authentication	Electronic authentication is the process of establishing confidence in user identities electronically presented to an information system.
Authenticity	ensuring that the involved data, transactions, communications or documents (electronic or physical) are genuine.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission,
Availability	ensuring timely and reliable access to and use of information.
Backdoors	
Ballot	the legally recognised means by which the voter can express his or her choice of voting option;
Ballot	
Certification	the process of certifying that a certain product has passed performance and quality assurance tests or qualification requirements stipulated in regulations such as a building code and nationally accredited test standards, or that it complies with a set of regulations governing quality and minimum performance requirements
Chain of trust	a process in computer security which is established by validating each

	component of hardware and software from the bottom up. It is intended to ensure that only trusted software and hardware can be used while still remaining flexible.
Cloud computing	a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Coercion-resistance	a voter should be unable to cooperate with a coercer to prove to him that she voted in a certain way.
Compartmentalise	Principle of least privilege works better if basic access structure is not "all or nothing". Minimize the amount of damage that can be done to a system by breaking up the system into as few units as possible while still isolating code that has security privilege
Complete Mediation	Rather than providing direct access to information, mediators that enforce access policy should be employed. Common examples of mediators include file system permissions, proxies, firewalls, and mail gateways.
Confidentiality	preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Control	See countermeasure
Countermeasure	Countermeasure a security countermeasure refers to a way to detects, prevent, or minimize losses associated with a specific IS threat
Defense in Depth	Security mechanisms (defenses) need to be layered so that compromise of a single security mechanism is insufficient to

	compromise an entire host or network;
Digital certificate	an electronic token ensuring the binding between an entity and its public key.
EasterEggs	
Election Privacy	No coalition of participants (of reasonable composition) not containing voter himself can gain any information about the voter's vote.
electronic ballot box	the electronic means by which the votes are stored pending being counted;
Electronic Democracy	Electronic Democracy is identified as the electronic representation of democratic processes
Electronic government	utilizing the Internet and the World-Wide-Web for delivering government information and services to citizens"
Electronic Voting	In general, two types of e-voting can be identified : • e-voting supervised by the physical presence of representatives of governmental or independent electoral authorities, like electronic voting machines (DRE) at polling stations or municipal offices, or at diplomatic or consular missions abroad; • remote e-voting within the voter's sole influence, not physically supervised by representatives of governmental authorities, like voting from one's own or another person's computer via the internet (i-voting), by touch-tone telephones, by mobile phones (including SMS), or via Digital TV, or at public open-air kiosks - which themselves are more venues and frames for different machines, such as; PCs or push-button voting machines, with or without smart card readers.
Eligibility	Only eligible voters can cast the votes. Every voter can cast only one vote.
Fairness	No participant can gain any knowledge about the (partial) tally before the counting stage (the knowledge of the partial tally could affect the intentions of the voters who has not yet voted).
Flexibility	A system is flexible if it allows a variety of ballot questions formats including open-ended questions, is compatible with a variety of standards platforms and technologies, is accessible to

	people with disabilities.
Grid Systems	grid systems
Hardware Security Module	a type of secure cryptoprocessor targeted at managing digital keys, accelerating cryptoprocesses in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.
Individual verifiability.	Each eligible voter can verify that his vote was really counted.
Information security	Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction
Information System	Information System is a collection of people, procedures, and equipment designed, constructed, operated, and maintained to collect, record, process, store, retrieve, and display information.
Information technology	Information technology (IT) is defined as "a microelectronics-based combination of computing and telecommunications used for the acquisition, processing, storage and dissemination of vocal, pictorial, textual and numerical information"
Infrastructure as a Service (IaaS).	IaaS provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources, and allows the consumer to deploy and run arbitrary software, which can include operating systems and applications.
Integrity	guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
Least Privilege	Least Privilege—This principle dictates that each task, process, or user is granted the minimum rights required to perform its job. By applying this principle consistently, if a task, process, or user is compromised, the scope of damage is constrained to the limited resources available to the compromised entity.

Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some
Mobility	a system is mobile if there are no restrictions(other than logistical ones) on the location from which a voter can cast a vote therefore enabling voters to cast their vote from any geographical location.
Non-repudiation	the generation, accumulation, retrieval, and interpretation of evidence that a particular party processed a particular data item.
Open Access	access to material via the internet in such a way that the material is free for all to read, and possibly to use (or reuse) to various extents.
Open source	an approach to design, development, and distribution, offering practical accessibility to a product's source (goods and knowledge).
Open source software (OSS)	computer software for which the source code is freely available for review and scrutiny and is made available under a license which conforms with the open source definition.
Platform as a Service (PaaS)	PaaS provides the consumer with the capability to deploy consumer-created or acquired applications, which are produced using programming languages and tools supported by the provider, onto the cloud infrastructure.
Reliability	Reliability is often related to availability, but is a slightly different concept. Reliability can be considered as having two aspects; hardware and software reliability. Hardware reliability- Reliability engineering involves all aspects of design, development, and fabrication that minimize the chance of equipment breakdown. The success of complex missions such as space probes depends heavily on reliability engineering, since the failure of a single component, such as an O-ring on a space shuttle, can result and has resulted in total loss of the system. Software reliability is defined as the probability that a software

	fault that causes deviations from the required output by more than a specified tolerance, in a specified environment, does not occur during a specified exposure period
Remote Access	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).
reversible vote	"reversible vote" or "vote updating" or "provisional voting". The voter may cancel any previous cast votes by casting a new vote.
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk management	the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization
Robustness	Faulty behaviour of any reasonably sized coalition of participants can be tolerated. No coalition of voters can disrupt the election and any cheating voter will be detected.
Robustness	the ability of a computer system to cope with errors during execution or the ability of an algorithm to continue to operate despite abnormalities in input, calculations, etc.
Scalability	indicating a systems ability to meet rising demands while maintaining performance level.
sealing:	protecting information so that it cannot be used or interpreted without the help of other information or means available only to specific persons or authorities;

Separation of Privilege	A system should ensure that multiple conditions are met before granting permissions to an object.
Smart-cards	Smart-cards
Software as a Service (SaaS)	SaaS provides the consumer with the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices, through a thin client interface, such as a Web browser (e.g., Web-based email).
Tally	
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Assessment	Formal description and evaluation of threat to an information system.
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Time-stamping	the process of attaching data and time to a document in order to prove that it existed at a particular moment of time.
Transparency	; an electronic voting system is necessary to be treated as a white box or open system
Trusted operating systems (TOS)	security-modified or -enhanced OSs that include additional security mechanisms not found in most general-purpose OSs.
Uncoersibility	Uncoersibility is defined as the voter not having the power to prove to a third party what his/her vote was
Universal verifiability	anyone (voter, responsible election authority, or external auditors) can verify the election result after the announcement of the tally.
usability	
vote	the expression of the choice of voting option;

voter	a person who is entitled to cast a vote in a particular election or referendum;
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Acronyms

(AES)	Advanced Encryption Standard
ACEEEO	
API	
CA	Certification Authority
DDOS	Distributed Denial of Service
DFA	Design for all
DOS	Denial of Service
DREV	Direct Recording Electronic Voting
EAC	Election Assistance Commission
EML (	Election Mark-up Language
EVM	Electronic Voting Machines
FISMA	Federal Information Security Management Act
FVAP	Federal Voting Assistance Program
HAVA	Help America Vote Act
HIDS	Host Intrusion Detection System
HSM	Hardware Security Module
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies
IS	Information System
NIS	Network Identification System a

NIST	NIST
OASIS	
OS	operating system
PaaS	Platform As a Service
PKI	Public Key Infrastructure
RA	Registration authority
SaaS	Software As a Service
SERVE	Secure Electronic Registration and Voting Experiment
TCSEC	Trusted Computer System Evaluation Criteria
UCD	user-centered design
UD	Principles of Universal Design
VOI	voting over Internet

APPENDIX B

SUPPORTIVE PUBLICATIONS

8.1 Peer-reviewed Journal Articles

[J01] Zissis, D, Lekkas, D, and Papadopoulou. A.E, “Competent Electronic Participation Channels in Electronic Democracy.” Electronic Journal of e-Government Volume 7 Issue 2 2009, (pp195 - 208)

[J02] Dimitrios Zissis and Dimitrios Lekkas, "Securing e-Government and e-Voting with an open cloud computing architecture", Government Information Quarterly, Volume 28, Issue 2, April 2011, Pages 239-251, Elsevier, 2011

[J03] Dimitrios Zissis and Dimitrios Lekkas, "Addressing Cloud computing Security Issues", Future Generation Computer Systems: The International Journal of Grid Computing and eScience, Special Issue on Infrastructure and Network-aware Grids and Service Oriented Architectures, 2011. Doi:10.1016/j.future.2010.12.006

[J04] Argyris Arnellos, Dimitrios Lekkas, Dimitrios Zissis, Thomas Spyrou, John Darzentas. Fair Digital Signing: The Structural Reliability of Signed Documents, 2011c (Forthcoming)

8.2 Conference Publications

[C01] Dimitrios Zissis, Dimitrios Lekkas, Thomas Spyrou, Security Services in e-School and their role in the evaluation of educational processes, International Conference on Institutional Evaluation Techniques in Education, ICIETE, Samos 2007

[C02] Dimitrios Zissis, Anastasia-Evangelia Papadopoulou, Dimitrios Lekkas, "Enhancing security in the integration of e-Government: The e-School initiative", In 4th International Conference on Web Information Systems and Technologies, WEBIST’08, Madeira - Portugal, May 2008

[C03] Dimitrios Zissis, Dimitrios Lekkas, Anastasia-Evangelia Papadopoulou, "Competent electronic participation channels in electronic democracy", In 8th European Conference on e-Government - ECEG’08, Lausanne, Switzerland, July 2008

[C04] Dimitrios Zissis and Dimitrios Lekkas, "The security paradox, disclosing source

code to attain secure electronic elections", Proceedings of the 9th European Conference on e-Government, p. 741, University of Westminster, London, UK, 29-30 June 2009.

[C05] Dimitrios Zissis, Dimitrios Lekkas and Panayiotis Koutsabasis, "Cryptographic Dysfunctionality-A Survey on User Perceptions of Digital Certificates", In 7th International Conference in Global Security Safety and Sustainability(ICGS3)/4th International Conference on e-Democracy, Thessaloniki, August 2011(Submitted).

[C06] Dimitrios Lekkas and Dimitrios Zissis, "Leveraging the e-passport PKI to achieve interoperable security for e-government cross border services", In 7th International Conference in Global Security Safety and Sustainability(ICGS3)/4th International Conference on e-Democracy, Thessaloniki, August 2011(Submitted).

8.3 Book Chapters

[B01] Dimitrios Zissis, Dimitrios Lekkas, Argyris Arnellos, "A systems theory approach to electronic voting complexity", E-Governance and Civic Engagement: Factors and Determinants of E-Democracy, IGI Global, 2012 (Accepted for publication)

APPENDIX C

SUMMARY IN GREEK

Η διατριβή εντάσσεται στην ευρύτερη γνωστική περιοχή της «Σχεδίασης Πληροφοριακών και Επικοινωνιακών Συστημάτων» με έμφαση στην ειδικότερη γνωστική περιοχή της «Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων. Η εργασία όπως υποδηλώνει ο τίτλος της έχει ως αντικείμενο την μελέτη και ανάπτυξη μεθοδολογιών και τεχνολογιών που αποσκοπούν στην ασφαλή σχεδίαση συστημάτων ηλεκτρονικών ψηφοφοριών μέσω διαδικτύου. Η υλοποίηση της εκπόνησης της διδακτορικής διατριβής αφορούσε αρχικά τον καθορισμό των βασικών στοιχείων που αποτελούν τις αρχές λειτουργιάς των συστημάτων ηλεκτρονικών ψηφοφοριών, την καταγραφή, καθώς και την ανάλυση λεπτομερών απαιτήσεων χρήσης που ήταν απαραίτητα για την πλήρη κατανόηση της θεματικής περιοχής. Η καταγραφή αυτή προσεγγίστηκε υιοθετώντας μια διεπιστημονική μεθοδολογία που αποσκοπούσε στην κατανόηση του προβληματικού χώρου ολιστικά. Στην συνέχεια μελετήθηκαν και προσδιορίστηκαν οι λειτουργικές απαιτήσεις και προδιαγραφές του Πληροφοριακού Συστήματος (ΠΣ). Ακολούθησε η εμβάθυνση στον θεματικό χώρο επικεντρώνοντας στα προβλήματα και τις απαιτήσεις από την σκοπιά της σχεδίασης ασφαλών πληροφοριακών και επικοινωνιακών συστημάτων. Σε αυτό το πλαίσιο, εντοπίζονται και αναλύονται συγκεκριμένα προβλήματα (κίνδυνοι) που αφορούν τα συστήματα ηλεκτρονικών ψηφοφοριών μέσω διαδικτύου και προτείνονται μέσα προστασίας, καθώς και σχεδιαστικές επιλογές, που αποπειρώνται να διασφαλίσουν την διαθεσιμότητα, την ακεραιότητα, την αυθεντικότητα και την εγκυρότητα του ΠΣ. Με στόχο την μείωση της συνολικής επικινδυνότητας του πληροφοριακού συστήματος, προτάθηκαν μέσα προστασίας που αξιοποιούν Υποδομές Δημόσιου Κλειδιού για την ασφαλή και αυθεντικοποιημένη προσπέλαση των πόρων του πληροφοριακού συστήματος, υποδομές νεφουπολογιστικής για την διασφάλιση της ακεραιότητας αλλά και της διαθεσιμότητας του, καθώς και σχεδιαστικές επιλογές που αποσκοπούν στην αύξηση της συνολικής εμπιστοσύνης προς αυτό. Τελικά προτείνεται ένα συνολικό σχεδιαστικό πλαίσιο για την ασφαλή σχεδίαση και ανάπτυξη συστημάτων ηλεκτρονικών ψηφοφοριών μέσω διαδικτύου.

Πιο συγκεκριμένα, η διδακτορική διατριβή περιλαμβάνει αρχικά την εισαγωγή (Κεφάλαιο 1ο) στην οποία περιγράφεται το αντικείμενο, οριοθετείται το πρόβλημα, η θεματική περιοχή, μεθοδολογία προσέγγισης και οι στόχοι της διατριβής.

Το δεύτερο κεφάλαιο αποτελεί το θεωρητικό υπόβαθρο της διατριβής στο οποίο θεμελιώνονται οι βασικές έννοιες που σχετίζονται με την θεματική περιοχή. Θεμελιώνονται θεωρητικά οι έννοιες του Πληροφοριακού Συστήματος (ΠΣ), της ηλεκτρονικής διακυβέρνησης, συμμετοχής, ηλεκτρονικές ψηφοφορίες καθώς και μελετώνται κάποια παραδείγματα (case studies) αυτών.

Στο επόμενο κεφάλαιο (Κεφάλαιο 3) μελετάται το θέμα των ηλεκτρονικών ψηφοφοριών από μια διεπιστημονική προσέγγιση αναδεικνύοντας τα πολύπλοκα προβλήματα αυτής της θεματικής περιοχής. Μελετήθηκαν και προσδιορίστηκαν οι λειτουργικές απαιτήσεις και οι συγκεκριμένες προδιαγραφές του ΠΣ. Ακολούθησε η εμβάθυνση στον θεματικό χώρο επικεντρώνοντας στα προβλήματα και τις απαιτήσεις από την σκοπιά της σχεδίασης ασφαλών πληροφοριακών συστημάτων. Σε αυτό το πλαίσιο, εντοπίζονται και αναλύονται συγκεκριμένα προβλήματα (κίνδυνοι) που αφορούν τα συστήματα ηλεκτρονικών ψηφοφοριών μέσω διαδικτύου.

Στο Κεφάλαιο 4, προτείνονται μέσα προστασίας και σχεδιαστικές επιλογές που αποπειρώνται να μειώσουν την συνολική επικινδυνότητα του ΠΣ. Σε αυτό το κεφάλαιο προτείνονται μέσα προστασίας που αξιοποιούν την κρυπτογραφία, και ειδικότερα τις Υποδομές Δημόσιου Κλειδιού, για να επιτευχθεί η ασφαλής και αυθεντικοποιημένη προσπέλαση των πόρων του πληροφοριακού συστήματος.

Στο Κεφάλαιο 5, μελετάται η νεφοϋπολογιστική (cloud computing), μια αρχιτεκτονική υποδομή κατανεμημένης υπολογιστικής ισχύος στον Ιστό, η οποία αποτελεί πρόσφατη εξέλιξη της υπολογιστικής τεχνολογίας, και αναδεικνύονται τα οφέλη που μπορεί να προσφέρει στην ηλεκτρονική διακυβέρνηση καθώς και συγκεκριμένα στα ΠΣ ηλεκτρονικών ψηφοφοριών. Στην συνέχεια προτείνεται μια ένα συνολικό σχεδιαστικό πλαίσιο με προτάσεις για μέσα προστασίας που αποπειρώνται να διασφαλίσουν την διαθεσιμότητα, την ακεραιότητα, την αυθεντικότητα και την εγκυρότητα του ΠΣ.

Στο επόμενο κεφάλαιο (Κεφάλαιο 6) αναλύεται και προσδιορίζεται η έννοια της εμπιστοσύνης στα πλαίσια του ΠΣ και προτείνονται τρόποι αύξησης της συνολικής εμπιστοσύνης προς αυτό. Σε αυτό το πλαίσιο μελετώνται τα συστήματα και οι πρακτικές ανάπτυξης και διάθεσης λογισμικού ανοιχτού κώδικα καθώς και οι τρόποι πιστοποίησης του ΠΣ.

Στο τελευταίο κεφάλαιο, παρατίθενται τα συνολικά συμπεράσματα της συγκεκριμένης διδακτορικής διατριβής. Με στόχο την μείωση της συνολικής επικινδυνότητας του

πληροφοριακού συστήματος, προτάθηκαν μέσα προστασίας που αξιοποιούν Υποδομές Δημόσιου Κλειδιού για την ασφαλή και αυθεντικοποιημένη προσπέλαση των πόρων του πληροφοριακού συστήματος, υποδομές νεφουπολογιστικής για την διασφάλιση της ακεραιότητας αλλά και της διαθεσιμότητας του, καθώς και σχεδιαστικές επιλογές που αποσκοπούν στην αύξηση της συνολικής εμπιστοσύνης προς αυτό. Συνοπτικά, προτείνεται ένα συνολικό σχεδιαστικό πλαίσιο για την ασφαλή σχεδίαση και ανάπτυξη συστημάτων ηλεκτρονικών ψηφοφοριών μέσω διαδικτύου.