This is an HTML working draft that led to an article publication. A reference to this work should always be done using the following citation:

Zisis D., **Lekkas D.**, Spyrou T., "Security services in e-School and their role in the evaluation of educational processes", *International Conference on Institutional Evaluation Techniques in Education, ICIETE'07*, Samos, Greece (July 2007)

SECURITY SERVICES IN E-SCHOOL AND THEIR ROLE IN THE EVALUATION OF EDUCATIONAL PROCESSES

Dimitris Zissis, Dimitrios Lekkas, Thomas Spyrou.

Dept. of Product & Systems Design Engineering, University of the Aegean

{dzissis, dlek, tsp} @aegean.gr

Abstract

This paper presents the e-School initiative which is involved in the integration of daily business processes conducted by primary and secondary level educational services in Greece. It deals with the aspects of security services in e-School and their role in the evaluation of educational processes. In addition it describes the way in which cryptography is used to ensure the authentication, integrity and confidentiality of information and examines the benefits gained.

Introduction: The e-School Initiative

The e-School initiative is involved in the integration of daily business processes conducted by primary and secondary level educational services in Greece. E-School offers the platform for the digitalisation of the administrative tasks of the educational processes by means of Information and Communication Technology (ICT). The objective of this initiative is the achievement of high level services and simultaneously the establishment of conditions for easier access and exploitation of services offered via the Internet. The main aim is the improvement of citizen services followed by expense reduction. This is achieved through the simplification of bureaucratic mechanisms and the reduction of response time.

E-School supports the adoption of an infrastructure development model to provide electronic services which include:

- The publication of official documents and information of the educational services (e.g. student grades and evaluation results)
- An interactive environment to provide information to individuals through the use of WebPages, electronic mail etc. (e.g. online accomplishment of various administrative tasks, such as the lesson attendance and the students registry)
- A transaction environment providing the ability to submit applications and follow up the related workflow

- Combined services that include the implementation of centralised facilities that offer unified services for various education levels and sectors.

Public Key Infrastructure in Educational Services

Emphasising on the perspective of security in e-School, cryptography is called upon to ensure the authentication, integrity and confidentiality of information. A security infrastructure provides a horizontal level of service for the entire system and must be accessible by all applications and sub-systems in the network that require security (Lekkas, Zissis, et al., 2007). The security solution provided makes use of Public Key Infrastructure (PKI) and evidently digital signatures (Gritzalis S. 2006, Lekkas D. 2002). The provision of security services in e-School is based on Public-key cryptography. PKI realises the concept of a digital signature; provides a practical, elegant mechanism for symmetric key agreement; and enables strong authentication of involved entities and secure communication. The underlying concepts of public-key cryptography, along with a number of the fundamental algorithms, have reached a stage of relative maturity. This is due to the intense scrutiny and research that has occurred in this area over the past two decades. Such a pervasive security infrastructure has many and varied benefits, such as cost savings, interoperability (inter and intra enterprise) and consistency of a uniform solution (Carlisle Adams, 2002). PKI provides technically sound and legally acceptable means to implement:

- Strong Authentication: The control of authenticity, the process of identification of parts involved in electronic transactions or exchange of information with electronic means.
- Authorisation: The authenticated access to resources, database and informative systems, according to the user's permission rights and the roles
- Data Confidentiality: The protection of information either locally stored or in transmission from unauthorised access.
- Data Integrity: The protection of information either locally stored or in transmission from unauthorised modification.
- Non-Repudiation: Ensuring that no part of an electronic transaction can deny its attendance in it

Administrative transactions

The e-School electronic system offers a number of applications that increase the effectiveness and ease of the administrative process. These features involve automation of student registry, grade management, absence management, courses & department management, human resource management, functional unit and time scheduling. Digital signatures are implemented as to ensure security in electronic communications between parties involved in e-School (e.g. secure email, client authentication, virtual private networks). Ensuring safety of electronically exchanged messages, encourages trusted communications between administration units but also between individuals. According to current legislation (Directive 1999/93/EC , Decision 248/71, FEK Issue 603/B/16-5-2002) a digitally signed document can be used as an official document. The wide use of digital signatures in documents by educational and administrative units of e-school will aim at the progressive suppression of printed forms. The certification

services contribute considerably in the creation of an environment of trust for the collaboration between citizens, companies, public administration and educational units. A number of transactions that target in improving the educational processes are implemented. These transactions are designed to provide useful feedback on a processes progress towards its set goals and how it can be improved. A diverse variety of online anonymous forms offer the opportunity to individuals to evaluate a process and for administration to obtain quantitative and qualitative data from a selection of sources. Online dialogue is considered as an important instructional strategy for building an online learning community (Sue D. Achtemeier, 2003), and cooperation between students.

Educational transactions

E-School offers students a wide range of facilities' that improve the effectiveness of education provided and student involvement in the process. These include access to online up to date personal information, effective communications and access to available resources such as course information and course evaluations. The deployment of digital signatures builds the necessary trust among all involved entities (Lekkas D. 2003) and enables students and parents to gain authorised and secure access to available information, (grades, transcripts, absent sheets, etc). In addition, time consuming traditional processes like registration can be completed through the e-School system. Students make use of provided information archives, giving them the ability to obtain a broader approach to educational material. In addition the means are provided to improve computer aided education by improving student-to-instructor relationship (Virtual Office Hour, providing media for communication) and student-to-student relationship (learner-to-learner collaboration, providing media for communication) (Woochun Jun, 2001)

PKI Design and Development

PKI infrastructure is comprised by several working units, as follows:

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 an *Identity Certificate.* The possession of a digital certificate enables its holder to securely communicate with another unknown entity (person or server) without prior agreement (e.g. exchange of cryptographic keys). (Carlisle Adams, 2002)

The Certificate Repository: this robust, scalable, on-line repository system contains a list of all issued certificates binding them to individual identities. The LDAP-based directory service of e-School will play the role of certificate repository. This repository will be the point of reference for any individual wishing to validate a digital signature or to encrypt data addressed to another entity.

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

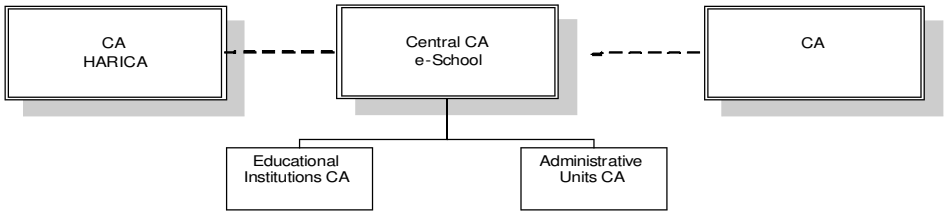
- Establish and confirm the identity of an individual as part of the initialisation process. (For example, the RA might verify the identity of an individual through a combination of physical presence and identification documents proving the individuals relation with the educational unit.)
- Distribute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

PKI e-School is designed to contain a Central CA unit which is in hierarchically elevated position, than following CA authorities implemented by educational institutions and administrative units. Each unit independently implements the CA that certifies its final users. Trust operates as a chain from the top to the bottom.

Figure 1. Hierarchical Model of trust



International practice (University of the Aegean, 2005) has proven that hierarchical structure provides the largest possible flexibility and scalability with the lowest cost, when implemented within a single organisation or administrative domain. This model is advisable practice for private sector corporations and for the public sector. Interoperability with other existing or under development PKI structures is crucial on selecting a flexible mechanism able to connect these. The concept of Cross certification has arisen in the PKI environment to deal with the need for forming trust relationships between formerly unrelated PKI installations. The proposed model permits two Certification Authorities to achieve a bilateral agreement of *cross certification* and in this way ensure that entities belonging to ones field of trust will accept certificates published by the second and/or reversely.

The Greek government is taking steps towards the implementation of electronic government, e-School assures interoperability with existing PKI infrastructures in the public sector and future projects. At present PKI infrastructures in use include:

- HARICA: Hellenic Academic and Research Institutions Certification Authority). Aim of HARICA is the creation of infrastructure that ensures communication between Academic and Research institutions of Greece.
- Public Administration Network “SYZEFKSIS”

A critical element of PKI e-School is the interoperability with the other elements of the e-School system due to its pervasiveness.

Technical and Organisational Considerations and Deployment

Such security infrastructure provides a complete solution ensuring security for large systems. End users interact with the PKI/CA system through web services. It must be strongly pointed out though, that end user key loss breaches the essence of security entirely. It is crucial that individuals receive instructions for the protection of their cryptographic keys. The registration authority is functional only when necessary and is not accessible through the internet. The certificates

developed by the registration authority are transferred safely with detachable memory drives to the registration authority. Although the system operates in a protected environment it is open to inside attacks. Trusted personnel dealing with elements of the system must have a clear understanding of the system. Hardware requirements for educational units are minimised to Internet Access and Personal Computer. Required software for the implementation of Certification authorities is provided.

The PKI infrastructure is deployed after the Key Ceremony is completed. In this important process step the Central CA is created and its privates keys. Trusted personnel following a written protocol can only perform such an action and only after the successful completion of this step are the descending CAs created independently and evidently final users obtain certificates and private keys. The educational and administrative units included in the e-School system individually create the Certification Authority of their unit with provided software.

The e-Schools systems overall security relies heavily on the protection of PKIs sensitive components in protected facilities. These components are protected in high-security environments to avoid unauthorised access, modification or destruction. Physical and procedural safeguards are established to encounter risks. Although all measures of minimizing risks are in place contingency plans for recovery of disaster exist.

Benefits for the Evaluation Processes

The e-School evaluation process offers a number of benefits which include Global accessibility: Classrooms, families, parents and individual students have the ability to participate in the evaluation processes, through authenticated channels. Participation is independent of location, ethnical and behavioural characteristics.

Global Trust: PKI is based on the establishment of trust relationships between individuals, roles, servers and applications. The PKI of e-School builds the necessary trust infrastructure between students, teachers, administrators as well as web-servers, applications and education authorities (e.g. ministry of education and pedagogical institute) that encourages the participation of all parties in the evaluation processes.

Secure data collection: The security services of e-School PKI offer the technical and legal tools for a reliable, undeniable and confidential collection of data regarding the educational evaluation. For example, a student evaluating an instructor needs a secure mechanism that assures:

- students data will remain confidential,
- student may participate only once in the process,
- the authenticity (originality and integrity) of the data can be proved at a later stage,
- the student can undeniably prove participation in the process,
- the student cannot deny participation in the process,
- the student can prove the time of the data acquisition, subject a time-stamping service is used.

Automated evaluation processes: Data acquired by evaluation processes in different schools and locations can be securely stored in central facilities. PKI-enabled storage assures the originality and the confidentiality of the data. Secure

data storage assures that the value of the stored data remains high for long periods and consequently they can be used in automated procedures producing reliable and globally acceptable results in large scales.

Conclusion

The e-School initiative provides the foundation for evolutionary changes in the approach taken towards traditional education provided by second level education. Traditional educational practices and interactions between involved parties are optimised through the implementation of ICT permitting instructors and students to focus on the primary goal of education. Enabling student and parent participation in the evaluation process creates the opportunity for administration to obtain quantitative and qualitative data from a variety of sources.

References

- Fielding, A.H. and Bingham, E. (2004) “Tools for Computer-Aided Assessment”, *Learning and Teaching in Action* (LTiA) 2(1)
- Carlisle Adams, S. L. (2002). *Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Editio,* Addison Wesley.
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
- Regulation on the Provision of Electronic Signature Certification Services", Decision 248/71 (FEK Issue 603/B/16-5-2002)"
- Gritzalis S. (2006) “Public Key Infrastructure: Research and Applications”, International Journal of Information Security, 5(1).
- Lekkas D. (2002), ”Information and Communication Systems Security using Trusted Third Party services” Ph.D. Thesis, University of Aegean,
- Lekkas D., Zissis D., Papadopoulou A., Goudosis A., Kostis T. (2007) “Study on user requirements, implementation requirements, initial structure and transition of the e-School PKI/CA service” as part of the project “Design and Implementation of the e-School advanced services and infrastructure”
- Lekkas D., (2003) “Establishing and managing trust within the Public Key Infrastructure”, Computer Communications, 26(16) pp.1815-1825
- Achtemeier S.D., Morris L.V., Finnegan C.L. (2003). Considerations for Developing Evaluations of Online Courses”, *Journal of Asynchronous Learning Networks*, 7(1).
- University of the Aegean (2005), “PKI Survey – PKI services in the Public Sector of the EU Member States”, e-Europe 2005
- Woochun Jun, Le Gruenwald, (2001). An Evaluation Model for Web-Based Instruction. *IEEE Transactions on Education* 44(2), pp.9