Enhancing security in the integration of e-Government: The e-School initiative

Dimitrios Zissis, Anastasia-Evangelia Papadopoulou, Dimitrios Lekkas

Dept. Of Product & Systems Design Engineering University of The Aegean

Lekkas@aegean.gr, Dzissis@aegean.gr, Dpsd03040@syros.aegean.gr

Keywords: Security, e-School, e-Government, Public Key Infrastructure, Lightweight Directory Access Protocol, Shibboleth, Single Sign On, Identity management

Abstract: This paper presents a security infrastructure design which is implemented to ensure safety in the e-School initiative that can escalate to meet the requirements of the entire electronic government system. The e-School initiative offers a number of ways that increase the effectiveness of education, student involvement in the process and is an element of the e-Government effort in Greece. A combination of existing technologies comprises the security solution presented, including Public Key Infrastructure, Shibboleth, Smart cards and Lightweight Directory Access Protocol. In this system, Pki is responsible for binding a public key to an entity, Ldap is the repository of keys and certificates and SSO is a method of access control that enables a user to authenticate once and gain access to the resources of multiple independent web services.

1 INTRODUCTION

Member countries of the European Union are speeding into the digitalization of government services, with countries currently offering a surplus of interactive services which are increasing in availability and sophistication.

International attempts to develop integrated customer oriented administrative services represent efforts to alleviate the problems of bureaucracy and improve the provision of administrative services.

Since the launch of the European Strategy for the development of e-Government, with the “e-Europe 2002” initiative presented in March 2000 at the Lisbon European Council, a change of focus has occurred. The original target to “supply services through the internet” has evolved into “the impact of e-Government programmes in delivering better services to their citizens, more efficient in an inclusive society" which emphasizes on the quality of the services provided and the extent to which online services are meeting user needs.

Identified as a major aspect, is the "safe access to services European Union wide" by "establishing secure systems for mutual recognition of national electronic identities for public administration websites and services (European Commission, 2006).

The necessity of an interoperable and scalable security and identity infrastructure has been identified by all implicated parties focusing on the effectiveness of solutions provided.

2 E-GOVERNMENT IN GREECE

On the 25th of April 2006 the European Commission adopted the i2010 e-Government Action Plan (Accelerating e-Government in Europe for the Benefit of All).

The Action Plan defines five priorities which set the future targets to be met by all involved countries:

1. No citizen left behind**:** advancing inclusion through e-Government so that by 2010 all citizens benefit from trusted, innovative services and easy access for all;

2. Making efficiency and effectiveness a reality — significantly contributing, by 2010, to high user satisfaction, transparency and accountability, a lighter administrative burden and efficiency gains;

3. Implementing high-impact key services for citizens and businesses — by 2010, 100% of public procurement will be available electronically (with 50% actual usage) making an agreement on cooperation for further high-impact online citizen services;

4. Putting key enablers in place — enabling citizens and businesses to benefit, by 2010, from convenient, secure and interoperable authenticated access across Europe to public services;

5. Strengthening participation and democratic decision-making — demonstrating, by 2010, tools for effective public debate and participation in democratic decision-making.

Since 2001 Capgemini (Capgemini, 2006) has been officially responsible for measuring the progress of online public service delivery in member states of the European Union. Capgemini produces yearly surveys that have been identified as the only available data concerning e-Government "measured scientifically over a longer period of time" (Alabau, 2004).

The survey launched in September 2007 (Capgemini, 2007) which included the twenty seven Member States of the European Union—plus Norway, Iceland, Switzerland and Turkey produced attention-grabbing data. Greece achieved the twenty first place for online sophistication and the twenty third place for online availability placing the country in the overall ranking of twenty first place.

Previous projects implemented in Greece and specifically the online income tax system-TAXIS and the e-Passport system have gained an exceptional score in previous surveys. This year's survey points out the appealing scoring results of the National Portal, providing citizens with the ability to submit various forms electronically.

Capgemini has previously identified as an important issue the lack of "central e-identification infrastructure for e-government in Greece" and that "no plans for e-ID cards have been issued" (Capgemini, 2006).

The current Capgemini report states "We note that a single eID system is not available and relatively few services offer legally binding authentication" (Capgemini, 2007). This proposal for the adoption of a wide horizontal security infrastructure can be expanded to cover all needs of electronic government system in Greece.

Steps are been made in this direction for which emphasis is made on system interoperability, so that all existing and under development elements of eGovernment can benefit from the proposed design. The security infrastructure proposed as a solution in the e-School initiative may be expanded and scaled into a national electronic identification system that will face deficiencies.

3 THE E-SCHOOL INITIATIVE

The e-School initiative relates to the development of digital information management services in Primary and Secondary education in Greece. This initiative aims to provide an Information and Communication Technology - infrastructure for the digitalization of the administrative tasks of the educational processes, achieving a high level of electronic services and offering easier access via the Internet.

Digitalizing document processing, exchanging procedures through digital signatures and providing secure mechanisms for the authorization and authentication of end users, results in the simplification of bureaucracy, the reduction of response time, and therefore, the reduction of expenses.

E-School provides a Public Key Infrastructure - based system for secure electronic services which include (Lekkas, Zissis, etc, 2007):

- 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 lesson attendance and 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.

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).

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). (Lekkas, Zissis, et al., 2007).

4 NEED FOR HORIZONTAL SECURITY THROUGHOUT ELECTRONIC GOVERNMENT

Electronic Government services are being rapidly deployed throughout Europe. Security is the main concern in this process, creating the need for an interoperable secure infrastructure that will meet all current and future needs. It is a necessity that such an infrastructure will provide a horizontal level of service for the entire system and must be accessible by all applications and sub-systems in the network (Lekkas, Zissis, et al., 2007).

Delivering electronic services will largely depend upon the trust and confidence of citizens. For this aim, means have to be developed to achieve the same quality and trustworthiness of public services as provided by the traditional way. (R. Traunmüller, 2003)

Regarding the level of systems design, some fundamental requirements, as far as security is concerned, have to be met:

- Identification of the sender of a digital message.
- Authenticity of a message and its verification.
- Non-repudiation of a message or a data-processing act.
- Avoiding risks related to the availability and reliability.
- Confidentiality of the existence and content of a message (R. Traunmüller, 2003)

The solution provided makes use of coexisting and complementary technologies which ensure safety throughout all interactions. Such a system provides assurances of its interoperability by using widely recognised standards and open source software. This evolutionary infrastructure design is based on a collaboration of existing cutting edge technologies in a unique manner. Public key infrastructure, Single sign On techniques and Ldap collaborate effectively guaranteeing efficient and secure communications and access to resources.

4.1 Public Key Infrastructure

A Public Key Infrastructure (PKI) based on asymmetric keys and digital certificates, is the fundamental architecture to enable the use of public key cryptography in order to achieve strong authentication of involved entities and secure communication. PKI have reached a stage of relative maturity due to extensive research that has occurred in the area over the past two decades, becoming the necessary trust infrastructure for every e-business (e-commerce, e-banking, e-cryptography). (Lekkas, Zissis, etc, 2007).

The main purpose of PKI is to bind a public key to an entity. The binding is performed by a certification authority (CA), which plays the role of a trusted third party. The user identity must be unique for each CA. The CA digitally signs a data structure, which contains the name of the entity and the corresponding public key besides other data. (Wikipedia).

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).

4.2 Smart Cards

A PKI smart card is a hardware-based cryptographic device for securely generating and storing private and public keys, digital certificates and performing cryptographic operations.

Implementing digital signatures in combination with advanced cryptographic smart cards minimises user side complexity while maintaining reliability and security (Only an identity in possession of a smart card, a smart card reader and the Personal Identification Number (PIN) can use the smart card).

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)

4.3 Lightweight Directory Access Protocol

The lightweight directory access protocol, or LDAP, is the Internet standard way of accessing directory services that conform to the X.500 data model. LDAP has become the predominant protocol in support of PKIs accessing directory services for certificates and certificate revocation lists (CRLs) and is often used by other (web) services for authentication. A directory is a set of objects with similar attributes organized in a logical and hierarchical manner. An LDAP directory tree often reflects various political, geographic, and/or organizational boundaries, depending on the model chosen. LDAP deployments today tends to use Domain name system (DNS) names for structuring the topmost levels of the hierarchy. The directory contains entries representing people, organizational units, printers, documents, groups of people or anything else which represents a given tree entry (or multiple entries). (O'Reilly OnLamp)

4.4 Single Sign On

Single Sign On (SSO) is a method of access control that enables a user to authenticate once and gain access to the resources of multiple independent software systems. Shibboleth is standards-based, open source middleware 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. (Internet2). Shibboleth is a Security Assertion Mark Up Language with a focus on federating research and educational communities.

Key concepts within Shibboleth include:

- Federated Administration: The origin campus (home to the browser user) provides attribute assertions about that user to the target site. A trust fabric exists between campuses, allowing each site to identify the other speaker, and assign a trust level. Origin sites are responsible for authenticating their users, but can use any reliable means to do this. (Intenet2)
- Access Control Based On Attributes: Access control decisions are made using those assertions. The collection of assertions might include identity, but many situations will not require this (e.g. accessing a resource licensed for use by all active members of the campus community or accessing a resource available to students in a particular course). (Internet2)
- Active Management of Privacy: The origin site (and the browser user) controls what information is released to the target. A typical default is merely "member of community". Individuals can manage attribute release via a web-based user interface. Users are no longer at the mercy of the target's privacy policy. (Internet2)

5 DESIGN AND DEVELOPMENT

The e-School approach can effectively and proficiently escalate into a national Electronic Identification Management Infrastructure covering all needs of security for e-Government in Greece. A collaboration of independent technologies presented previously leads to an evolutionary horizontal infrastructure.

Introducing federations in e-government, in association with PKI and Ldap technology, will lead 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). These policies enable the members to establish trust and shared understanding of language or terminology. A federation provides a structure and a legal framework that enables authentication and authorization across different organizations. In the e-School the underlying trust relationships' networks of the federation are based on Public Key Infrastructure (PKI) and certificates enable mutual authentication between involved entities. This is performed using SSL/TLS protocol and XML digital signatures using keys contained in X.509 certificates (Young, 2007) obtained from e-school Certification Authorities. An opaque client certificate can contain information about the user's home institution and, optionally, the user's pseudonymous identity.

Shibboleth technology relies on a third party to provide the information about a user, named attributes. Attributes are used to refer to the characteristics of a user and not the user straightforward: a set of attributes about a user is what is actually needed rather than a name with respect to giving the user access to a resource (Internet 2). In the e-School system architecture, this is performed by the ldap repository which is also responsible for the association of user attributes. Additionally Ldap contains a list of all valid certificates and revoked certificates. Digital signatures are used to secure all information in transit between the various sub-systems.

This infrastructure leverages a system of certificate distribution and a mechanism for associating these certificates with known origin and target sites at each participating server. User side complexity is guaranteed to be minimum without any cutbacks on the overall security and reliability.

The model presented in this paper offers the advantages of each single technology used and deals with their deficiencies through their combined implementation:

- Hybrid PKI hierarchical infrastructure delegates the trust to subordinate CAs permitting the creation of trust meshes, under a central CA, between independent organizations. Interoperability is simply addressed.
- PKI supports single sign on with the use of Shibboleth. Shibboleth coordinates with PKI to develop enhanced, complex free, authorization and authentication processes.
- The user becomes part of the designed system using Single Sign On (SSO) technology, that simplifies the access to multiple resources with only one “gain access procedure”. 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. Providing a security infrastructure is not enough, the user must also be able to make use of the security features. Otherwise, the designed service will fail due to the fact that users’ behaviour is often the weakest link in a security chain.
- The combination of the above mentioned techniques creates strong trust relationships between users and e-Government services, by implementing a “zero-knowledge” procedure of a very strong authorization. Zero-Knowledge is an interactive method for one entity to prove the possession of a secret without actually revealing it, resulting eventually in not revealing anything about the entity’s personal information. The combined techniques mitigate the problem of memorizing many passwords and reduce the vulnerability of using the same password to access many web services.

5.1 Authentication Process

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 site and authenticate himself. During this phase information is exchanged between the user and his home site only; with all information on the wire being encrypted. 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.

The PKI-Shibboleth-Ldap collaboration process is explained in detail below (Note that **messages** in ***italics*** are communicated using Digital Signatures):

M1: User browser attempts to enter resources on the service provider.

M2: Services Provider contacts WAYF if user authenticated.

M3: WAYF messages Idp (user authentication).

M4: (Internal) message sent to authentication Service which requires user to authenticate.

M5: Ldp requires user to authenticate

M6: User submits authentication data to Idp, which are internally passed to the authentication service.

M7: The authentication Service messages Ldap with authentication data.

M8 & M9: Ldap communicates with PKI.

M10: Ldap approves/ disapproves authentication data.

M11: Idp authenticates user.

M12: User attempts to enter resources on Service Provider.

M13: SP requests attributes from Idp.

M14: Attributes sent from Idp to SP.

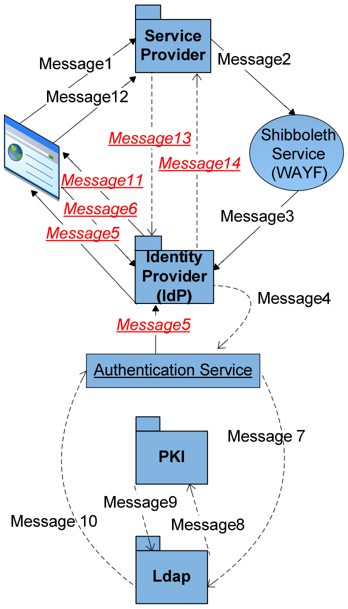

Figure 1: PKI - LDAP - Shibboleth Collaboration

5.2 User Authorization

User Authentication is performed only once when the user identifies himself inside the trust mesh. Once authenticated inside the trust mesh, users are not required to re-authenticate themselves. When a user navigates to a resource store inside the trust mesh, the authorization process is executed. During this process the service provider requires from the users Identity Provider to present the users access credentials. The Identity provider, after successfully identifying the user and checking if he is previously authenticated, retrieves user credentials for the required resource. If user has not previously been authenticated, the authentication process is initialized. The Shibboleth Identity provider contains four primary components the Attribute Authority (AA), the Handle Service (HS), attribute sources, and the local sign-on system (SSO). Shibboleth interacts with the Ldap infrastructure to retrieve user credentials.

From the Identity Providers point of view, the first contact will be the redirection of a user to the handle service, which will then consult the SSO system to determine whether the user has already been authenticated. If not, then the browser user will be asked to authenticate, and then sent back to the SP URL with a handle bundled in an attribute assertion. Next, a request from the Service Provider's Attribute Requester (AR) will arrive at the AA which will include the previously mentioned handle. The AA then consults the ARP's for the directory entry corresponding to the handle, queries the directory for these attributes, and releases to the AR all attributes the requesting application is entitled to know about that user. (Internet 2)

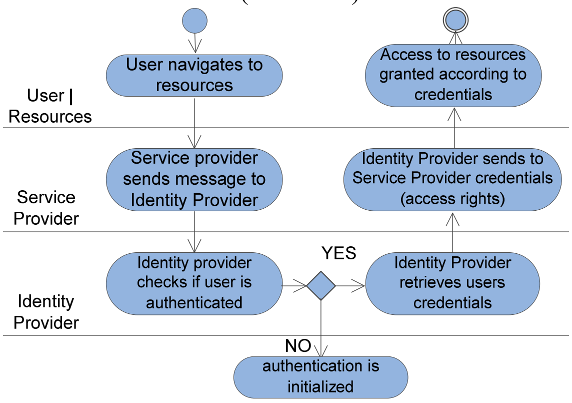
User | Resources
Service Provider
Identity Provider
User navigates to resources
Access to resources granted according to credentials
Service provider sends message to Identity Provider
Identity Provider sends to Service Provider credentials (access rights)
Identity provider checks if user is authenticated
YES
Identity Provider retrieves users credentials
NO
authentication is initialized

Figure 2: User Authorization (UML 2 Activity Diagram)

This process can be viewed as (Internet 2):

1. User attempts to access Shibboleth-protected resource on Service Provider site application server.
2. User is redirected to a Where Are You From (WAYF) server, where the user indicates their home site (Identity Provider).
3. User is redirected to the Handle Service at their Identity Provider. Handle service checks with SSO if user has been previously authenticated. If not authentication is initialized. User authenticates at their IdP, using local credentials.
4. Handle service generates unique ID (Handle) and redirects user to Service Provider site's Assertion Consumer Service (ACS). ACS validates the supplied assertion, creates a session, and transfers to Attribute Requestor (AR).
5. AR uses the Handle to request attributes from the IdP site's Attribute Authority. The attribute authority responds with an attribute assertion subject to attribute release policies; SP site uses attributes for access control and other application-level decisions.

This handle is used to identify a user to service providers in pseudonymous manner. It is pointed out that the user does not exchange any personal information with the service provider, which only receives an authorization ticket/access credentials.

5.3 Considerations about establishing and achieving goals

Project evaluation was based on a wide range of goals regarding different aspects: technological or technical, security, usability, scalability and interoperability were some of the issues taken into consideration.

From a technical point of view the set goal was to create a Hybrid PKI infrastructure, combining PKI with SSO (Shibboleth), Ldap and smart cards, keeping the advantages of each technology and eliminating their weak points.

The main goal established in the security field was the protection of personal information and privacy, while achieving strong authentication and authorization of users.

Usability was an issue addressing both sides: users and organizations. Users should be able to access the needed information and services, without considering how to achieve this or wasting time in complicated authorization/authentication processes. On the other side, organizations should be able to manage their member-user lists and information easily.

Scalability was essential for future implementation of required features in the infrastructure when new parameters and requirements arise.

Eventually, setting an interoperability goal for the e-School initiative with other infrastructures was a major concern in order to contribute effectively in the integration of e-Government in Greece.

The above discussed prerequisites were confronted in the way analyzed below:

- No need to leak personal information over the wire. No need to transmit personal information about users, only user attributes in transit inside the trust mesh. This is achieved by authenticating the user using a third party service (zero-knowledge) and not by the Service that gives access to the user in order to navigate to a resource. The Service receives information only about the users' credentials so they can get access to resources.
- Strong authentication process: Digital signatures in combination with shibboleth and Ldap, implement the strongest available authentication process.
- Strong authorization process: Digital signatures in combination with shibboleth and Ldap, implement the strongest available authorization process.
- Minimized end user complexity: Smart cards and SSO technology implement security in a user friendly way.
- Central user database: No need for each organization to create a user database, only one main database necessary with user information and attributes.
- Implementing hybrid-hierarchical architecture assures the ability to expand and scale to meet wider needs.
- The use of several widely-implemented standards, Secure Sockets Layer, and Lightweight Directory Access Protocol assure interoperability. Implementations of other solutions using such standards will be able to communicate with the proposed infrastructure readily, fostering the ability to interoperate (Internet2).

6 E-SCHOOL INTEROPERABILITY WITH ELECTRONIC GOVERNMENT AND CONSIDERATIONS

Current e-government attempts internationally are evolving and learning from mistakes of the past. Until recently attempts to implement electronic government procedures were viewed purely as technological attempts, setting aside operational and social aspects. A systemic approach strategy is necessary for electronic government to meet its set future goals (P.Georgiadis, 2007).

A systemic approach is nowadays considered to be a given researching procedure in confronting the reality. The characteristic element of this approach is its inter-scientific merge of different fields of studies that facilitate the selection and organization of accumulated knowledge in finding acceptable solutions (especially in complicated systems and problems). This approach, in contrary to the analytical approach does not consider the individual elements of a system to be independent. It focuses on the relations and the interdependencies between those elements, in order to study a system as whole, as an entity. (Joël de Rosnay, 1979)

A system is possible to have relations to other systems. We can also consider and study these systems as whole in order to control the output (result), given the requirements. Due to the nature of the systemic approach, the interoperability of the sub-systems is easier to define (Goguen,Varela, 1979). Being one of the pioneer security infrastructures in Greece concerning eGovernment, e-School design was approached making use of a systemic point of view. With the systemic approach is guaranteed that current and future eGovernment projects' interoperability is achieved.

According to recent studies (RONAGHAN, S. A., 2002) (WAUTERS, 2002) (R. Traunmüller, 2003), online access to public services is not used by citizens / business partners as expected. Experiences show that this is due to a number of factors among which the following loom particularly large:

- Neglect of stakeholder expectations and focus, so resulting in limited take-up of e-Services.
- Neglect of the specifics of the Governmental realm and the business processes at Stake.
- Neglect of interoperability and integration on various levels.

Inter-organisational workflows, cross-border process standardisation of public services and process models integrating the external view of customers (service oriented) with the internal view of public administrations (competence oriented) are among the requirements to implement integration on the process level. (R. Traunmüller, 2003)

Evidently all attempts must stress on interoperability and the added value that such a system will bring to the organization implementing it. Consequently all information systems of electronic government should be considered from start as critical operational infrastructures which are effectively designed and productively managed under the terms of adding operational value. (P.Georgiadis, 2007).

7 CONCLUSIONS

Internationally numerous governments are becoming available online daily. As unattached efforts of addressing electronic government are implemented globally, the need for an interoperable horizontal security infrastructure is stressed. The effective security infrastructure design presented in this paper is a solution which makes use of coexisting and complementary open source technologies and standards. Provides secure and effective communication supported by ease of use for the end user. Scalability and interoperability is an advantage of this design suitable to meet the needs of electronic government.

ACKNOWLEDGEMENTS

The e-School project was funded by grants of the 'Information Society SA' and the 'Ministry of National Education and Religious Affairs'.

REFERENCES

Alabau, A. (2004). *The European Union and its eGovernment development policy following the Lisbon strategy.* Retrieved 2007, from e-Democracy Centre (External Publications, Valencia Polytechnic University):http://edc.unige.ch/edcadmin/images/european_union_e-government_development_policy.pdf

Capgemini. (2006, June). *Online Availability of Public Services: How Is Europe Progressing? Web Based Survey on Electronic Public Services.* Retrieved 2007, from Europe's Information Society, Measuring Progress Section of the Europe's Information Society, eGovernment Benchmarking Reports (6th Report): http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/online_availability_2006.pdf

Capgemini. (2007). *The User Challenge Benchmarking The Supply Of Online Public Services.* Retrieved 2007, from Europe's Information Society, Measuring Progress Section of the Europe's Information Society, eGovernment Benchmarking Reports (7th Report): http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf

European Commision. (2006, April 25). *eGovernment: Commission calls for ambitious objectives in the EU for 2010 [Press Release].* Retrieved from http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/523&format=HTML&aged=1&language=EN&guiLanguage=en

European Commision. (2006, April 25). *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All.* Retrieved 2007, from European Commision's Archival Policy Records: http://ec.europa.eu/transparency/archival_policy/docs/moreq/action_plan_i2010_en.pdf

European parliament and council. (2000, January 1). Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures. *Official Journal of the European Communities , L 013*, pp. 0012 - 0020.

Georgiadis, P. D. (2006, June 3). *Electronic Government Systemic against mechanistic approach.* Retrieved 2007, from On-Line Magazine, Tech-Insight [Online exclusive], Issue 10, 3rdArticle: http://www.computer-engineers.gr/modules/Magazine/pdf/10/10_techinsights.pdf

Goguen, J. A., & Varella, F. J. (1979 , January). Systems and distinctions: Duality and complementarity. *International Journal of General Systems , 5* (1), pp. 31 - 43.

Gritzalis, S. (2006, January). Public Key Infrastructure: Research and Applications. *International Journal of Information Security , 5* (1), pp. 1-2.

Internet 2. (n.d.). *Shibboleth.* Retrieved 2007, from Internet 2: http://shibboleth.internet2.edu/

Lekkas, D. (2993). Establishing and managing trust within the Public Key Infrastructure. *Computer Communications , 26* (16), pp. 1815-1825.

Lekkas, D. (2003). Information and Communication Systems Security using Trusted Third Party services, Ph.D.Thesis. University Of the Aegean.

Lekkas, D., & Zissis, D. (2007). Security services in e-School and their role in the evaluation of educational processes. Samos, Greece: ICIETE conference proceedings .

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"* .

O'Reilly. (n.d.). *O'Reilly OnLamp (LAMP: The online opensource web platform)*. Retrieved 2007, from An introduction to LDAP: http://www.onlamp.com/pub/a/onlamp/2001/08/16/ldap.html

Regulation on the Provision of Electronic Signature Certification Services", Decision 248/71 (FEK Issue 603/B/16-5-2002)". (2002).

Ronaghan, S. A. (2002). *Benchmarking e-Government: a Global Perspective – Assessing the Progress of the UN Member States.* Final Report of the Global Survey of E-Government by UN and the American Society for Public Administration.

Rosney, J. (1979). *The Macroscope: A New World Scientific System.* HarperCollins Publishers.

Spasić, D. (2005). PKI Smart Card Technology. *XL International Scientific Conference on Information, Communication and Energy Systems and Technologies. Volume 2*, pp. 464-467. Niš, Serbia and Montenegro: ICEST 2005.

Traunmiiller, R., & Wimmer, M. A. (2003). E-Government at a Decisive Moment: Sketching a Roadmap to Excellence. *Second International Conference on Electronic Government* (pp. 1-14). Prague, Czech Republic: Springer.

Uk Federation Information Centre. (n.d.). *Uk Federation Information Centre*. Retrieved 2007, from Uk Federation Information Centre: http://www.ukfederation.org.uk/

Wauters, P. K. (2002). *Web-based Survey on Electronic Public Services.* Brussels: Directorate General Information Society.

Wikipedia encyclopedia. (n.d.). *Public Key Infrastructure*. Retrieved 2007, from Wikipedia encyclopedia: http://en.wikipedia.org/wiki/Public_key_infrastructure

Young, I. A. (2007, June 1). *Technical Recommendations.* Retrieved 2007, from UK Access Management Federation for Education and Research: http://www.ukfederation.org.uk/library/uploads/Documents/technical-recommendations-for-participants.pdf