INTEGRATED SECURITY SYSTEM FOR E-GOVERNMENT

BASED ON SAML STANDARD

Jeffy Mwakalinga, Prof Louise Yngström

Department of Computer and System Sciences
Royal Institute of Technology / Stockholm University
Forum 100, S-164 40 Kista, Sweden
Email: **jeffy@dsv.su.se**, **louise@dsv.su.se**
Tel: +468 161 721
Fax: +468 703 90 25

ABSTRACT

This paper describes an integrated security system for electronic-government services. Many governments are transforming manual government services to electronic government services. This transformation is in most cases done without involving users of the services. This makes users of these services have little trust in the e-government. Security is in most cases not addressed from the early stages of e-government development. Some governments depend on security solutions from private vendors and these governments do not have full control of security. E-government services have different levels of classification and so they require different types of authentication and authorization methods. Most e-government systems today use one form of authentication in all types of services without considering the different sensitivity levels. All countries have different levels of e-literacy and users with low levels of e-literacy do not understand some of today's e-government security systems. This security system provides multiple authentication methods. Some e-government services require simple authentication while other highly classified transactions demand strong authentication. This security system provides multiple authorization schemes, information integrity schemes and digital signature schemes. These schemes can be configured to accommodate different e-literacy levels. The system integrates a registration system, a certification system, an authorization system, and a smart card system. It bases on the Security Assertion Markup Language (SAML) standard, which is an XML-based framework for exchanging security information. The system can be integrated in existing e-government systems and can be built-in in new e-government systems. Information of different levels of classification can be stored in same websites and can be accessed through multiple authentication and authorization methods. This system enables the society to perform secure e-government transactions and accommodates different e-literacy levels.

KEY WORDS

Attribute certificate, integrated security system, e-literacy, assertion, and anonymity.

INTEGRATED SECURITY SYSTEM FOR E-GOVERNMENT

BASED ON SAML STANDARD

1 INTRODUCTION

Provision of electronic government services is one of the main goals of many governments in the digital world. It is cheaper to provide government services electronically than manually [1], and it reduces corruption practices, since one cannot bribe a server. An e-government service costs a government between US $1 and US $7, while a non e-government service costs a government between US $ 2 and US $ 200 [2]. The United Nations recommends development of e-government, in part three of the e-government handbook for developing nations [1], to consider the following challenges and opportunities in the design of e-government programs. These programs include "infrastructure development, law and public policy, digital divide (e-literacy and accessibility), trust (privacy and security), transparency, interoperability, records management, permanent availability and presentation, education and marketing, public/private competition/collaboration, workforce issues, cost structures and benchmarking" [1]. Privacy according to this handbook [1] involves protecting personal information that the government collects about individuals, while security is involved with protecting e-government sites from attacks and misuse. An example of laws involving personal information protection can be found in the Personal Information Protection and Electronic Documents Act [3]. This work is dealing with ways of providing security in e-government services.

There are different types of communications in e-government: government agencies to government agencies; government agencies to and from citizens; government agencies to and from business organizations [4], government agencies to and from international organizations and other countries. Willingness of citizens and other parties to use e-government services will depend on the trust that they have on the services. E-government services can be public or classified. There are four categories of e-government information and services [21] e-management, e-service, e-commerce and e-Decision making / e-democracy. An evaluation of the Australian local e-government indicated that there was progress in e-management but little progress in the e-service, e-democracy, and e-commerce areas. These services have different levels of classifications: high, medium, low, and these levels can in turn be broken into intermediary levels. The challenges in e-government services' security [1][4] include identifying users, authenticating users, storing public and classified information in same websites, checking authorizations, auditing, signing transactions, resolving conflicts, keeping copies of information, and so on. Hence, e-government security systems should be able to meet the following requirements: should provide multiple authentication methods, authorization, credential issuance and revocation [5], audit, confidentiality, conflict resolution, accountability, availability, platform independent, privacy, information integrity, anonymity, scalability, single sign on and so on.

The challenges and requirements were analyzed to find ways of providing security services in e-government. The e-government security systems are to support small countries like Namibia with a population of about two million people as well as big countries like China with a population of over 1.275 (2003) billion people. Study was made to find ways of managing e-government services and information of different levels classifications. The study included the issue is e-literacy. There are different levels of e-literacy in every country. The different levels of e-literacy and services with different levels of sensitivity can be solved by having multiple authentication methods, authorization methods, privacy provision methods, conflict-resolution schemes, and so on. Different e-literacy levels may require complicated computation to be performed on the e-government websites and leave only light and user-friendly procedures on the e-government client's side. A study was made of what the technology has to offer in these areas.

The remaining sections are organized in the following way:

The second section covers related work; the third section is about the e-government security system; section four briefly discusses the conclusions.

2 RELATED WORKS

This section discusses SAML [6] system, the integrated security system [14] and the challenges of an on-line authentication system.

2.1 SECURITY ASSERTION MARKUP LANGUAGE (SAML) STANDARD

SAML [6] is a flexible Extended Markup Language (XML) based framework for exchanging security information about users on the Internet. SAML supports single sign on, which enables users to visit different sites without needing to login every time. The security information is represented in forms of assertions about subjects. Assertions contain authentication information, attributes of subjects and information about authorization decisions on resources as shown in Figure 33. Assertions are issued and managed by SAML authorities and they include authentication authorities, attributes authorities, and policy decision points. Clients can request for assertions from the SAML authorities. Requests and responses are in XML formats. The protocol used for carrying the requests and responses is the Simple Object Access Protocol (SOAP) over HTTP. SOAP [7] is an XML based protocol that is used to exchange information in open environments. An assertion contains the following elements: major version, minor version, assertion ID, issuer, issuer instant, conditions, advice, XML signature [8], statement, subject statement, authentication statement, authorization decision statement, and an attribute statement.

The SAML architecture has the following components: a credentials' collector, an authentication authority, an attribute authority, a policy decision point, a system entity (subject) and a policy enforcement point. The authentication authority, attribute authority, and policy decision points make decisions basing on policies. A system entity logs in a domain and the authenticating authority authenticates the entity basing on the credentials supplied. The result of this process is stored in an authentication assertion. A reference to this assertion is created and it is in the form of a ticket and it is sent to the entity. The entity can supply this ticket to different websites and will be authenticated basing on the

ticket. If a website needs authorization information, the website contacts the attribute authority and requests for an attribute assertion. This assertion is sent to the policy decision point, which issues the authorization decision assertion. This assertion is then sent to the policy enforcement point on the website. The website will grant access to the requested resources depending on the authorization decision assertion.

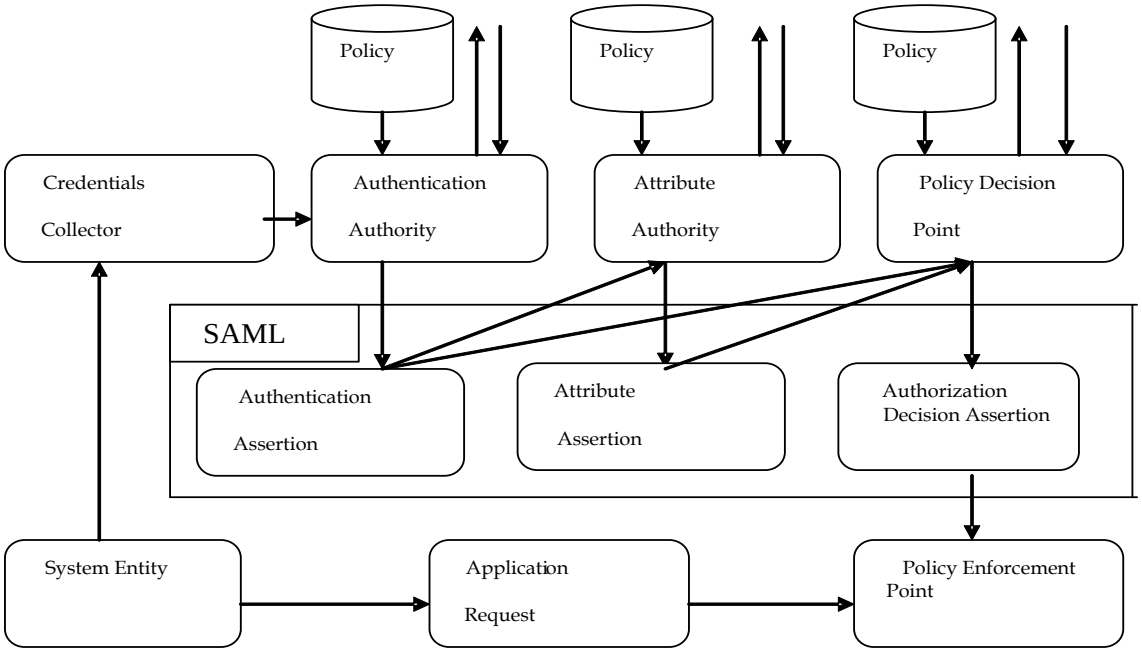

FIGURE 33: SAML ARCHITECTURE

2.2 INTEGRATED SECURITY SYSTEM (ISS)

This is an integrated security system [9] of various individual security systems, which are often used as separate systems. The components of this system include a registration (X500) [19] system, a certification system, a smart cards system, and an authorization system as shown in Figure 34. This system is supported by a security platform, which has different security mechanisms, which can be updated or changed whenever necessary. The main functions of this system are to provide identification of users, users' authentication, non-repudiation, confidentiality, delegation, information integrity, and authorization. Authentication is provided through public key certificates. Authorization and delegation are provided using attribute certificates [14]. An attribute certificate is a certificate that carries authorization and delegation information. It contains a reference to the authentication tokens for validation purposes. Non-repudiation is provided using smart card systems and signature schemes. Users in need of registration services, a smart card, a public key certificate, and authorization attributes usually identify themselves multiple times and perform registration procedure at four different administration stations in non-integrated security systems. In this system identification of users, verification of users' identities and registration of users is done once per user and all relevant security data are shared among the four security sub-systems. The same administrator registers the

client, issues a digital certificate, and issues an attribute certificate and a smart card to the client. The administrator can visualize all the data and can perform updates and other management operations from the same interface. The system offers functional integration of data and security administration procedures and visual integration through a common security administration interface.

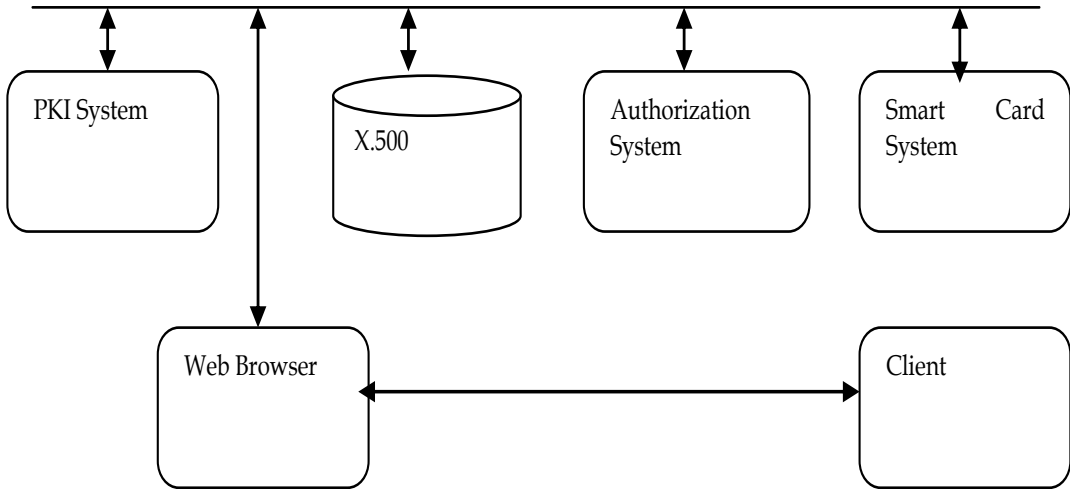

FIGURE 34: ARCHITECTURE OF INTEGRATED SECURITY SYSTEM

2.3 THE CHALLENGES OF AN ON-LINE GOVERNMENT SERVICES

One of challenges of e-government according to [10] is providing user-friendly systems for e-government clients. Clients today in US are forced to keep multiple passwords that are needed just in a single session. The second challenge is that e-government in US [10] is depending on multiple systems from different private vendors. In some cases authentication systems of different forms, and authorization systems of different forms come from different vendors and administrators have to use different platforms. The third challenge is to provide multiple authentication schemes. Some services demand strong authentication while others demand simple authentication schemes. Today many government agencies are forced to use only one type of authentication for the different types of services. The forth challenge is that the security perimeter of the US government was formally "well defined as inside and outside" [10], but it is not the case today. This complicates the management of security of e-government because the security perimeter of the government is no longer well defined today. The reason for this change is the expansion of e-business technology, which makes the government deal with security in different platforms and in different applications like web services. The US government is planning to create a special net GOVNET [4] that will not be connected to the global Internet for government agencies. This is aimed at protecting government agencies from security problems that are present today in the Internet. It will be interesting to see how the e-government services will be provided to clients when e-government clients are using the normal global Internet while the government is using GOVNET that is not connected to the global Internet.

3 E-GOVERNMENT SECURITY SYSTEM

3.1 ARCHITECTURE OF THE SYSTEM

The system contains the following components: an e-government website, an integrated security system, a SAML server, a controller, an e-government client, an e-citizen system, an e-regional system and ministries' systems as shown in Figure 35. The functions of the web site include directing e-government clients to different services, policy enforcements, protecting messages, informing the SAML server the required authentication and authorization types before accessing resources and before transactions, backup operations, and other administrational procedures. The integrated security system manages digital certificates, smart cards, attribute certificates, registrations, and policies. The ISS acts as an assertions' authority [6]. The SAML server manages authentication assertions, attribute assertions and authorization decision assertions. The controller performs anonymity services. Anonymity can be provided when performing services like electronic voting, survey, e-democracy issues, and other issues.

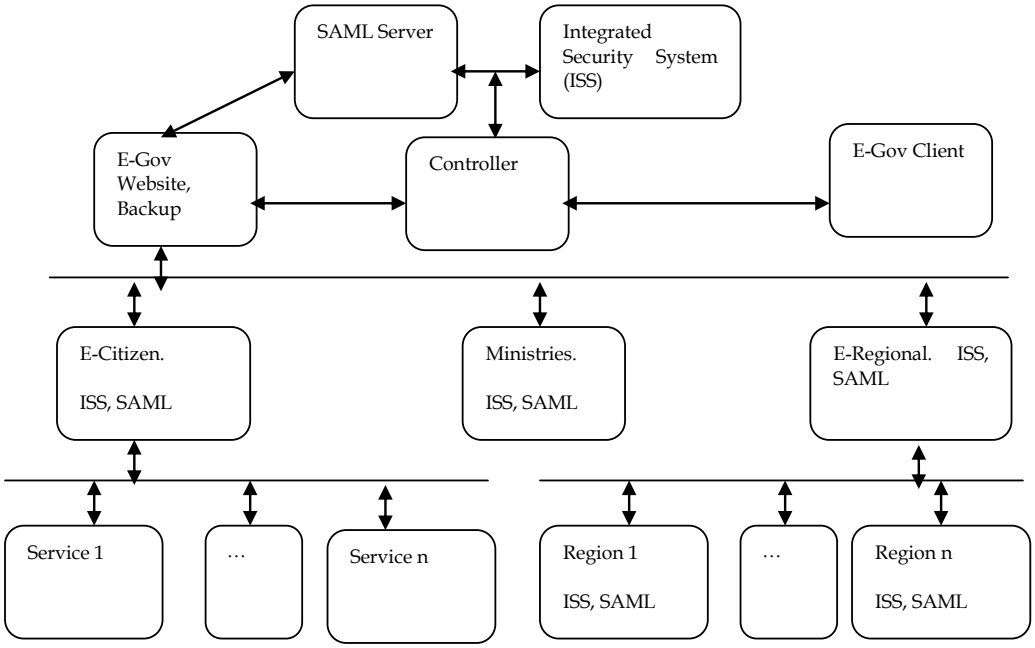

FIGURE 35: ARCHITECTURE OF E-GOVERNMENT SECURITY SYSTEM

The controller performs operations like identifying and authenticating an e-government client. After user identification and authentication, the controller removes the original IP address and then sends the message to the desired destination servers with controller's IP address as source [18]. Another function of the controller is to check the validity of requests. The controller collects credentials of clients. For every serious request, there is a denial of service cookie [11] that is a function of an IP address and a secret code of a client. This reduces non-availability (partially) problem of the e-government website.

E-citizen system offers a variety of public and classified e-government services to citizens. Public services require no authentication while classified services can require

simple or strong authentication with or without authorization. All transactions are protected using the configured security mechanisms. There is a policy file that specifies the types of authentication and authorization needed for each service. If a client desires to perform e-government services at a specific ministry, she will be directed to that ministry. Every ministry has a number of integrated security systems and SAML servers at different sections depending on the size of the ministry. Every ministry has its own policies basing on the sensitivity of the information and services it offers. E-regional is a system that deals with local e-government services. The regions or states are in turn divided into districts. All these regions and districts can have ISS and SAML systems to facilitate effectiveness in the management of services in local governments.

When an e-government client desires to access the e-government website, the controller collects credentials and sends them to the integrated security system. If it is the first time, the client performs identification and authentication procedures and if successful, she is registered in the directory. The information is shared by all e-government sub-systems. The client is then issued with a digital certificate, an attribute certificate [14] and a smart card if desired. A denial of service cookie [11] is sent to the client. If the client has already been registered, the controller checks whether the request is valid and then sends the credentials to the integrated security system. This system prepares authentication assertions, attribute assertions and authorization decision assertions. The assertions are signed by the integrated security system using XML signature [12] and then protected by XML encryption [8] and integrity. All the messages between the ISS and the SAML server are transmitted using the SOAP [7] protocol. The SAML server has to verify the signatures in the assertions from the ISS. The World Wide Web Consortium (W3C) has developed XML [15] Key Management Specification (XKMS) [16] for locating, validating and registering keys. This protocol is used by SAML to validate the keys used for signing and encrypting assertions from ISS. The reference to the each assertion is in the form of tickets [13]. The tickets are then sent to the client who forwards the tickets to the e-government website. The website checks the validity of tickets with the SAML server before granting access. The client can use these tickets to access the resources on the different e-government servers without needing to sign in again. SAML provides single sign on. The decision to grant services will depend on the roles indicated on the tickets. The ticket that refers to the attribute assertion contains an attribute certificate [14] or just a username, a role and other attributes. The authentication assertion contains the following authentication tokens: a username, a challenge response value, an X509 certificate, a password or a combination of these.

3.2 Security Services

3.2.1 Multiple Authentication Methods

This system supports simple authentication and strong authentication. The reason for supporting multiple authentications is that services have different levels of sensitivity and also to accommodate clients with different e-literacy levels. Services with low levels of sensitivity can be configured to require simple authentication. E-government services with high sensitivity levels can be configured to require strong authentication. Simple authentication can be password based, challenge-response based, or biometrics based. The default mechanisms for supporting password and challenge response in this system include Lamport's hash and Encrypted Key Exchange (EKE) [11]. Lamport's hash is a

password protocol in which a password is hashed *n* times and then sent to a server. The number *n* is specified in the policy file. One for every authentication reduces the number *n*. When *n* is 0, a new password has to be set. EKE is a strong password protocol that bases on Diffie-Hellman [11]. EKE enables e-government clients and e-government websites to create session keys and mutually authenticate each other. Strong authentication bases on digital certificates and secret keys. Parties mutually authenticate each other by proving to each that they possess private keys and secret keys.

3.2.2 Multiple Authorization Methods

Authorization in this system is role based, identity based, or a combination of these types. Before checking whether a client is authorized to access a resource or to perform a transaction the client must be authenticated first. Authorization tokens have references that can be used to verify the identity of clients. Authorization bases on tickets and attributes certificates [14].

3.2.3 Multiple Non-repudiation schemes

This system supports non-repudiation schemes with public key technology and also with secret key technology. The e-government website and the e-government client sign all the messages between them by using private keys. Providing non-repudiation using secret keys involves a third trusted party. In this system, the controller is configured as a default notary. However, it can be configured to use other trusted non-government agencies to act as third parties.

3.2.4 Multiple Integrity Schemes and Availability

This system supports multiple integrity schemes. It supports mechanisms that use secret keys as inputs and those that produce digests without taking keys as inputs. The default systems in this system are Secure Hash Algorithm -1 (SHA-1) [11] and HMAC [11]. SHA-1 takes a message and produces a message digest that is 160 bits long. HMAC takes a message and a secret key and creates message authentication code of 128 bits or 160 bits long. Availability is partially provided though the use of denial of service cookies.

3.2.5 Audit, Privacy, Confidentiality and Anonymity

All the signed transactions between the e-government websites and e-government clients are stored in the directory and in a backup database. Clients and e-government servers sign all the transactions. Transactions that are not signed are not processed and they are sent back to clients for signing. Timestamps are attached to all the transactions. These records are kept in this way to be used in conflict resolution and accountability matters. All the messages between e-government clients and e-government websites are protected by using the configured protocols. The default protocol is Secure Socket layer (SSL) [17]. In addition, in this protocol client authentication is mandatory in this security system. Anonymity is provided in cases of e-voting, survey projects and other specialized transactions. Anonymity is provided [18] as described in section 3. Client's data will be protected in accordance with the personal information protection laws of the government.

3.3 Advantages and Validation of the System

This system enables a government to control of all the security services and does not depend on different private vendors as discussed in the related work section 2.3. It provides multiple authentication methods, authorization schemes, privacy protection methods, information integrity schemes, and non-repudiation methods. This makes

services with different levels of classification require different types of security services. This security system is platform independent. The system is scalable. The administrator can manage public key certificates, smart cards, authorization attributes, and users' registration from one interface of the ISS, which is simple and efficient. This system is using standards and mechanisms that have been analyzed and tested by experts. X.509 certificate and strong password protocols are used for authentication for sensitive e-government services. The system is using multiple authentication methods and in some cases, it may be recommended to use authentication methods that are not very strong to accommodate clients that have low e-literacy levels, but this will depend on the government policies. The same applies to authorization schemes. Standardized algorithms provide digital signature schemes and encryption schemes and they can be replaced whenever necessary. The security platform supports updates and removal of undesired mechanisms. This security system is using standards like SAML, XML, and SOAP to provide platform independency. The system can be built-in in any e-government systems and it can also be integrated in already existing e-government systems.

3.4 LIMITATION OF THE SYSTEM

The system does not provide Denial of service security service. It does not support e-government wireless services' security. The system has not yet been implemented and so there are no results on performance. It is assumed that the government using this security system supports the public key infrastructure.

4 CONCLUSION

This work has highlighted security issues that need to be considered in designing e-government security systems. E-government services have different levels of sensitivity and they should be accessed through multiple authentication and authorization methods. The e-government security system should accommodate all clients regardless of their e-literacy levels. The system can be applied to any e-government architecture with minor adjustments. Future work includes extension to wireless technology, implementation of the system, and analysis of the system's performance.

REFERENCES

[1] UN Project of InfoDev and the Centre for Democracy & Technology, The e-government handbook for developing countries, 2002, www.cdt.org

[2] Prathiba M, Data Protection Law an E-business and E-government perception, IITC 2003 conference proceedings, ISBN 955-8974-00-5, 2003, pp122-128

[3] BILL C6, Canadian Personal Information Protection and Electronic Documents Act [3], http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6TOCE.html , 2000

[4] National Institute of Standards and Technology, E-government Strategy, www.nist.gov, 2002

[5] RSA Security Inc, Enabling e-government, www.rsasecurity.com**,** 2003

[6] OASIS standard 2003, Assertions and Protocols for the OASIS Security assertion Markup Language (SAML) 2003, www.oasis-open.org

[7] Simple Object Access Protocol (SOAP), May 2000, http://www.w3.org/TR/SOAP

[8] W3C Recommendation, XML Encryption Syntax and Processing, www.w3c.org/TR/2002/REC-xmlenc-core-20021210
[9] Mwakalinga Jeffy, Security Management of Global and Integrated Security System, ISRN SU/KTH/DSV/R—02/30—SE
[10] RSA Security Inc, www.rsasecurity.com, 2003
[11] Kauffman C., Perlman, R., Speciner, M., Network Security Private Communications in a Public World, ISBN 0-13-046019-2, 2002
[12] W3C Recommendation, XML Signature Syntax and Processing, www.w3c.org/TR/2002/REC-xmlsig-core-20020212, 2002
[13] Peldius Mark, Security Architecture for Web Services, DSV, Royal Institute of Technology, Stockholm, Sweden. 2004.
[14] Mwakalinga, J., Rissanen, E., Muftic, S., Authorization System in Open Networks Based on Attribute Certificates, IITC 2003 conference proceedings, ISBN 955-8974-00-5, 2003, pp 59-67
[15] Extensible Markup Language (XML), http://www.w3.org/XML/
[16] W3C Recommendation, XML Key Management Specification (XKMS) version 2, www.w3c.org/TR/xkms2, 2003
[17] The Secure Socket layer,
http://home.netscape.com/security/techbriefs/ssl.html, 2002.
[18] Pascual, Alberto E., Anonymous and Untraceable Communications, IMIT, The Royal Institute of Technology, Stockholm, Sweden. The June 2000,www.imit.kth.se/~aep
[19] CCITT REC. X.500-X.521 | ISO/IEC STANDARD 9594:1993
[20] Finne, A., Authorization for Secure Group Applications based on Web Services, DSV, The Royal Institute of technology, Stockholm, Sweden
[21] Shackleton, P., Fisher, J., Dawson, L., Evolution of Local Government E-Services: the applicability of e-business Maturity models, Proceedings of the 37th HICSS conference, 2004, ISBN 0-7695-2056-1