Multi-Level Trust in E-Government Certification Practice

Amel MEDDEB[1], Arbia RIAHI[1] and Manel ABDELKADER[1]

National Digital Certification Agency, 3 bis rue d'Angleterre, Tunis RP 1000, Tunisia

Abstract. Trust management has been addressed recently to provide networked systems with the appropriate mechanisms to perform any conformance checking with respect to a security policy in e-business and e-government. Trust management is an important issue for the deployment and success of e-government. Besides, public-key infrastructures manage trust in data exchanges through email, over the web and using other electronic means. The principal elements used for maintaining that trust are the contents of the certificates and the security safeguards established in the environments where various parties are involved. These two elements are derived from the business requirements, according to the stipulations of the certificate policy and the applicable regulation. We show in this paper the need to introduce the paradigm of multi-level trust in e-government systems, and propose a solution that provides X.509 standards with the modifications to allow multi-level trust certificate management, publication, and efficient use.

1 Introduction

The role that information and communications technologies (ICT) are playing in our daily lives becomes more pronounced. ICT applications help the improvement of the effectiveness and efficiency of government and change its relationship with the citizens by improving its process and management. E-government refers to the use of information technology to overcome the physical bounds of traditional and physical based systems while offering better quality of service to citizens and enterprises [1]. Its adoption aims to enhance government services to benefit citizens and enterprises through the use of web-based Internet applications. To protect transactions and privacy in e-government, on-line security is essential. Consequently, new problems related to security and privacy of data networks have emerged.

Various reliable features need to be made available to help a rapid and efficient deployment of e-government. These features are made up of mechanisms of authenticating users accessing the government network, guaranteeing the integrity of messages, ensuring the non-repudiation of the intervening parties, and controlling access to sensitive information [2]. An effective approach to contribute to the establishment of trusted communication between e-government parties is the use of Public Key Infrastructure (PKI). Through the use of X.509 digital certificates, PKI verifies the identity of the parties involved in on-line transactions, ensures that data has not been altered in transit, prevents parties from repudiating having sent (or received) a message, and guarantees confidentiality of sensitive data.

Riahi A., Meddeb A. and Abdelkader M. (2004).
Multi-Level Trust in E-Government Certification Practice.
In *Proceedings of the 1st International Workshop on Electronic Government and Commerce: Design, Modeling, Analysis and Security*, pages 13-23
DOI: 10.5220/0001405100130023

Access policies to government services can not be managed easily. According to a specific policy, each entity may be granted a set of permissions to perform specific actions on certain targets. The architecture, services, and roles performed by the government agencies are very divergent in their nature and the way they should be protected. For example, the protection provided for a given transaction may vary based on the importance of the transaction itself, the data it includes (e.g., amount of money, priority, privacy, etc.), and the site it accesses. Consequently, many levels of trust need to be made available in an e-government environment. However, once we get into details, it becomes increasingly evident that the trust model conforming X.509 is not particularly appropriate for e-government [3,4]. One major shortcoming of the X.509 certificates is that they are not flexible and offer only one level of trust. Therefore, it can not fulfill the requirements of e-government needs.

This paper proposes a multi-trust model integrating the X.509 certificate model in an e-government environment. It provides the modifications needed by relevant functions, and organizes an appropriate LDAP hierarchy for the publication of multi-trust certificates. Our contribution is three-fold. First, it keeps the main features of the X.509 (e.g., use of global names, certificates and revocation procedure). Second, it organizes conceptually various layers where certificates offering the same level of trust are located, while allowing certificates to handle more than one trust level. Finally, it describes and justifies the modifications to the main functions of certificate management. The remaining part of this paper is organized as follows. In the second section, we address the different requirements that must be fulfilled by a PKI to respond to the different needs of the e-government and cope with the provision of various levels of trust. The third section presents the modifications that should be introduced to a PKI to add the multi-trust model. In the fourth section, a strategy of analysis is presented to ensure an adequate choice of a PKI architecture in an e-government environment with multi-trust levels, and estimate the cost of adding new features. The last section presents a case study of a model allowing a reduced set of trust levels.

2 Requirements for e-government PKI

In an e-government environment, many issues need to be addressed when establishing a PKI [1]. These issues include the following tasks:
* Provide public certification services (including certificate public archives for verification) and customized registration authorities (RAs).
* Provide technical specifications for government PKI standard documents (including documents such as Certification Policy and Certificate practice Statements).
* Issue and manage certificate services (publishing, revocation, renewal, time stamping, and validating certificates).
* Provide application programming interface (API) for data encryption, digital signature, and digital envelope and many other on-line services.
* Address PKI Interoperability and trust paths including interconnection issues between Certification Authorities (CA), Cross certification policy, Cross-border interoperability with other governments (eg. Bridge CA, Strict hierarchy).

* Consider Information management issues related to digitally signed documents such as legal archiving and on-line consulting.

As said before, within the frame of government projects, access rights to different departments are not managed in the same manner. Diversity of applications, services and policies from an e-government environment to an other may lead to considerable variability of security requirements and access control needs. Different levels of trust must be allocated to the intervening individuals and departments, while keeping some of the centralization feature and dividing the e-government environment into two main domains: public, where citizens and enterprises can access and interfere, and private, where access, authentication, and authorizations is strictly handled.

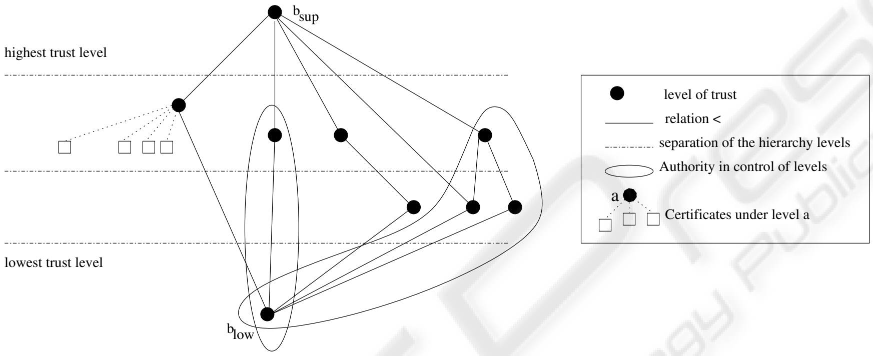
b_{sup}
highest trust level
lowest trust level
b_{low}
level of trust
relation <
separation of the hierarchy levels
Authority in control of levels
a
Certificates under level a

Fig. 1. The trust levels in an e-government

The public domain represents the interface with citizens accessing services. To benefit from a service, certain requirements must be defined by the service provider and fulfilled by the service applicants. According to these requirements, the offered services can be classified into different categories based on the users need and constraints. The private domain contains a set of resources internal to the departments themselves. Access rights to these resources by the personnel are managed in different ways according to their importance and confidentiality and the sensitivity of the resource they may access. Thus, these resources may be assembled into different categories. To fulfill the e-government needs, the concept of PKI must be adapted. Different levels of trust must be defined according to the users access rights and service constraints. In this trend, the classical architecture and functions of PKI must be modified to satisfy these needs. Since it is widely used, the X.509 standard will be kept for the adopted certificate structure. The contents of the deployed adapted X.509 certificates should be made in order to support multi-levels of trust. The trust levels defined in a given e-government environment should be linked using a relational order, say $\preceq$. Thus, when $\Lambda = \{n_1, ..., n_{level}\}$ designates the set of authorized levels defined in a given e-government environment, the following constraint should be kept always true in the sequel:

$$\forall n \in \Lambda,\ \forall m \in \Lambda :\ \exists b \in \Lambda,\ b = lub(n, m)\, in\, (\Lambda, \preceq) \tag{1}$$

Equation 1 means that the ordered set $(\Lambda, \preceq)$ is a lattice; that is, any pair (n, m) of trust levels should have a least upper bound $b \in \Lambda$ such that $(n \preceq b)$ and $(m \preceq b)$, and that any level b' satisfying: $(n \preceq b')$ and $(m \preceq b')$, should satisfy $(b \preceq b')$. Moreover, the need for uniform procedure have led us to consider that the lattice $(\Lambda, \preceq)$ should be a complete lattice, in the sense that any finite ordered sequence of trust levels in $(\Lambda, \preceq)$, say $n_1 \preceq n_2 \preceq ... \preceq n_p$, should have a least upper bound b_{sup}. In addition, we assume that the lattice $(\Lambda, \preceq)$ should have a lowest element b_{low} satisfying: $\forall n \in \Lambda : \ b_{low} \preceq n$.

All these assumptions have been considered for the need to provide an environment where a set of uniform rules can apply for conforming certificates and CAs. According to this, many features can be concluded. First, this implies that the e-government has a central (or root) authority, which is the highest element in $(\Lambda, \preceq)$. Second, this means that different levels of trust can exist in $(\Lambda, \preceq)$and could not be compared with each other. This states that departments occurring in the e-government can manage their own trust levels with no need to compare them to the other departments. Third, this states that all department in the e-government agree on a minimal level of trust. The lattice structure is partially depicted in Figure 1 which shows the link between certificates and levels of trust and organizes the trust levels under the control of entities called CAs. Let us now assume that citizens and enterprises accessing any service in the e-government should be able to do it and that all identification, access control, or authentication procedure should be based on a unique proof provided by the applicant. In the sequence we will provide a digital certificate enhancement to contain the multi-level trust need by the e-government services.

3 Management of multi-trust in e-government

3.1 Multi-trust certificate structure

Table 1. Certificate policies extension syntax

id-ce-certificatePolicies OBJECT IDENTIFIER ::= { id-ce 32 }
anyPolicy OBJECT IDENTIFIER ::= { id-ce-certificatePolicies 0 }
CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation PolicyInformation ::= SEQUENCE { policyIdentifier CertPolicyId }
CertPolicyId ::= OBJECT IDENTIFIER

To manage multi-trust, $n_{level}(> 1)$ levels must be defined within a PKI framework. This condition is expressed in the certificate through the Certificate Policies Extension as specified in Table 1. These extensions are used to indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used [5]. The value of the `CertificatePolicies` field is a set of integers contained in $N = \{n_1, n_{level}\}$. Each value of these integers corresponds to a trust level of the certificate. At the verification level, access can be granted to applicant according to the value of this field. Thus, when a citizen or an enterprise is assigned a given subset of trust levels, the subset is reported in `PolicyInformation` in the `CertificatePolicies` extension. Each level of trust is introduced by a `policyIdentifier` defined by the e-government PKI.

In the following, we will present the modifications to be introduced within the framework of an e-government PKI that supports multi-trust levels. In this PKI, each principal (entity or organization) p possesses a a subset N_P of trust levels. The representation of N_P contains only the maximal element assigned to entity p. This means that whenever $n \in N_P$ and m is a trust level lower than n, then m is allowed to entity p. However, for the sake of simplicity we assume that subset N_P is at least reduced to the minimal element in Λ, say $\supseteq \{b_{low}\}$. The value of $"b_{low}"$ expresses that no trust level is attributed to entity p, since no interaction can be defined with any domain.

3.2 Hierarchical LDAP

The LDAP repository presents an important role during the verification process in PKIs. The modifications in the structure of the certificates used in the PKI have a direct impact on the architecture and the management of the LDAP. The introduction of different levels of trust in the certificates should be appearing in the LDAP to facilitate the access and the treatments done by the applications of the e-government for the certificate verifications. LDAP can be considered as a set of clusters indexed by the set Λ We can assume, for the sake of verification simplicity, that a certificate marked by a subset of trust levels N_P occurs in all clusters indexed by N_P.

Each CA, present in the e-government PKI, defines its LDAP repository to publish the certificates and the certificate revocation lists it generates. LDAP architecture should distinguish the different levels of trust defined in the certificates. Two cases should be examined. First, LDAP defines a hierarchical data structure. It presents a single root node under which can be defined different subordinate nodes for any depth chosen by the administrator. This architecture can be exploited to emphasize the levels of trust defined in the certificates generated by a CA. Then, under the root of each LDAP repository, the information related to the certificates holders are classified by organization. Among these information, we distinguish the levels of trust mentioned in the digital certificates. Figure 2 gives an overview of the LDAP architecture. Second, certificate retrieval and verification in the LDAP should present the ability to read the levels of trust of the certificate and to realize the searches using the attribute specifying the trust level. In this trend, we can adopt the approach of Klasen and Gietz [6,7] which proposes the extraction of the different attributes of the X.509 certificate and their storage as researchable attributes in the LDAP repository.

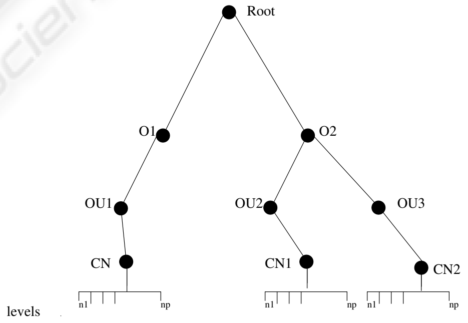

Fig. 2. The LDAP architecture for multi-trust PKI

3.3 Trust level verification

The trust level verification is initiated by the applications defined in the e-government environment. When a citizen desires to benefit from a service, he presents its certificate to the given service. The latter extracts the level of trust, by which it is concerned, from the certificate. Then, it verifies its existence in the corresponding LDAP repository. At the LDAP level, the research starts by the determination of the common name and the level of trust. Next, the existence of the asked certificate is verified. In addition, the certificate is searched in the certificate revocation list of that level.

4 PKI organization

4.1 Registration

During the registration process, user applies for a certificate with a given trust level. RA must define a set of procedures for user identity verification related to each trust level. When applying for a certificate, concerned entities must submit certain information. The correspondence between the provided information and the required certificate level of trust must be defined and verified by RA. If this correspondence is verified, the RA generates a certificate request containing the user's public key and the certificate information including information related to the trust level. If the correspondence can not be verified, RA must contact the applicant to review the level of trust that he/she applies for. In situations where an applicant wants to add a new level of trust, the following four cases have to be considered.
First, if the user with a trust level n_D in some domain requires to upgrade his trust level inside that domain. Then, a new trust level n'_D will be assigned to him under the condition that there exist a direct relation between n'_D and n_D expressed by $n'_D \geq n_D$. The first certificate with the trust level n_D must be revoked before the generation of the certificate with the new level of trust.
Second, if a user belongs to many different domains, then he can have a certificate that contains as many trust levels as many domains to which he belongs.
Third, if the trust level in some domain of a given user must be modified and there is no direct relationship between the old trust level and the required one (n'_D), then the user gets a new certificate with the trust level n'_D in addition to his old certificate. One of these certificates can be presented in function of the level of trust required by a given application.
Fourth, if we consider the case of CA, the trust level is denoted n_{CA}. For each $n \in \{b_{low}, b_{sup}\}$, CA can only issue certificates to entities with a trust level $n_{entity} < n_{CA}$. This means that a given CA in the considered environment can not issue certificates to entities with a higher trust levels than that it owns.
Illustrative example. If an employee is working for one department and he/she has been promoted without changing his/her workplace, then he/she can benefit from a higher level of trust in that department. His certificate must be replaced by a new certificate with a higher level of trust (see first case). However, if an employee works for $n_{user-domain}(> 1)$ departments, he/she can require a certificate with $n_{user-domain}$ trust levels. The way this is done proceeds first by choosing the maximal levels of trust,

then defining a subset N_P contains these levels, and finally mark the correct certificate with N_P (see second case). Finally, if we consider the case of an employee involved into two independent e-government domains ; then two certificates must be generated. The first certificate is used in the first domain which requires a given trust level ; whereas the second certificate will be used in the second domain that defines dissimilar trust requirements. Specific values of trust must be attributed to each certificate but are independent since each certificate will be used in a separate context. This means that one certificate can be kept in use but may not cover all potential activities of the certificate holder (see third case).

4.2 Generation

The generation process takes place once CA receives the certificate request. The number of `PolicyIdentifier` fields is equal to the number of the trust levels. These fields are added when the request file is generated as specified in 3.1. The standards PKCS are slightly modified accordingly. CA authenticates the origin of the certificate request and, then signs the certificates with the requested trust levels. After its generation, the certificate publication starts at this level of the PKI. For the commodity of servers management, we propose that, at least, every certificate authority publishes certificates it generates on a publication server it manages.

4.3 Revocation

Revocation process occurs when any information in the certificate is modified. It is preferable to customize the periodicity and the priority of certificate revocation and CRL issuance according to the level of trust. A set of procedures is defined for each level of trust. Certificates with high level of trust need strong authentication (eg. physical presence).

If it is a concern of priority, then the trust level must be taken in consideration. Certificates with a low level of trust can be gathered in bundles and revoked together. Authentication through passwords is enough to authenticate their holders. The lasting period of revocation request can be set in function of certificate levels of trust. Certificates with a high level of trust must be revoked immediately if the applicant can be correctly authenticated. If this requirement can not be fulfilled at the moment of application, certificates are suspended at the revocation request reception and then revoked after applicant authentication. Certificates with a high level of trust are prior to be revoked. A new CRL must be issued after each certificate revocation and then made available for e-government entities. Periodicity of CRLs issuance and publication vary in function of the trust level. Thus, a set of rules must be clearly defined by the PKI to handle certificate revocation and CRLs in function of the relevant level of trust.

4.4 Verification

The verification process can be divided into two parts. First the verifier must construct the trust chain beginning from the end user's certificate until the root CA. Then, the verifier must verify whether each certificate in the chain is valid. Second, the trust level in the certificate must be verified to check whether the certificate holder has the right to access a given resource in a given environment. When accessing the LDAP server to verify a user's certificate, the common name and the trust levels of the certificate holder are extracted. The verification is performed when examining the corresponding entries in the LDAP hierarchy to check whether the level of trust assigned to the end entity is exact and whether the certificate is valid (by examining the CRL).

4.5 Publication

The publication process is initiated by the CA. In the publication server, the information related to each entry are classified under its relevant organization name and organization unit name. When a request is sent to the server to add up one entry, the server must extract the level(s) of trust from the certificate to be published. These levels must appear as researchable attributes in the repository content.

5 Strategy of analysis

In the proposed model of PKI with multi-trust support, the compliance with X.509 standard is kept unchanged. Our model can be implemented based on the existing PKI platforms. In fact, to adopt the suitable solution to implement the PKI, we must analyze and compare the existing products in order to compare the cost of adding the new features to the existing platforms. To this end, a set of criteria and comparison rules must be built to distinguish between them. When evaluating PKI products, the NSS group considers the following sets of criteria: certificate support, revocation methods, scalability, security, PKI topologies, registration mechanisms, directory support, smart card/token support, key management, management interface, interoperability, third party application support, price, etc. [8]

Available platforms do not support multi-trust levels. The strategy analysis presented in [8] does not invoke sufficient parameters to evaluate the PKI products . Effectively, conformity with law requirement is not considered in [8]. We have added to these criteria some other criteria that we found appropriate to consider to achieve a better solution for multi-level trust integration. Among those criteria, we can mention the audit of functions related to multi-level management, LDAP hierarchy verification and certificate modification.

On the technical level, to ensure that multi-trust is supported in a given PKI, different conditions must be verified. First, adding extensions must be allowed by the PKI. Second, the maximum number of trust levels permitted by the PKI must meet the e-government needs. Third, the verification at the LDAP level must permit the string matching technique. Once fulfilled, these requirements can guarantee the support of multi-trust level certificates. As we seen before, the other modifications that we introduced to the classical PKI are related to practices and rules which can be developed outside the PKI software.

6 Case study : a two-color model

6.1 Certification Policy establishment

In an e-government environment, the majority of citizens interact with two domains : their job domain and the remainder part of the government. Some citizens, but not all, have more than one job. Their percentage can be considered very small. So, we can admit that each entity is characterized by two levels of trust $\{n_I, n_E\}$, where : $n_I \in \{b_{low}, b_{sup}\}$ refers to the level of trust assigned to the entity inside the department to which he/she belongs while $n_E \in \{b_{low}, b_{sup}\}$ refers to the trust level of that entity outside the same department. We assign the following levels of trust for the following particular cases : (1) Jobless end-users : (b_{low}, n_E), (2) CAs : (n_I, b_{low}).

Here, the value of "b_{low}" is assigned when no trust level can be attributed because no interaction can be defined between the certificate holder and some domain. For the first case mentioned above, no department can be affected to jobless users. So, the value of "b_{low}" is affected as a trust level of that user inside some department. However, in the case of CA, no external relationship are defined, the value of "b_{low}" is assigned to that authority outside its scope of operation.

6.2 PKI functions

During the registration process, a user applies for a certificate with a given trust level (n_I, n_E). A verification process must be performed by RA. If this succeeds, RA generates a certificate request containing the user's public key and the certificate information including trust level parameters. If the applicant wants to add a new level of trust, then the following case have to be considered.

First, if the user possesses a trust level (n_I, n_E) requires to upgrade the trust level defined in his department. A new trust level (n'_I, n_E) will be assigned to him provided that there exists a direct relation between n'_I and n_I expressed by $n'_I > n_I$. The first certificate with the trust level (n_I, n_E) must be revoked before the generation of the certificate with the higher level of trust.

Second, if a user belongs to two different departments, then he can have a certificate that corresponds to each department to which he belongs. For example, if a user works for $n_{user-dept} > 1$ departments, then he can require $n_{user-dept}$ certificates.

Third, if the trust level assigned to a given user outside his department ; two cases are conceivable. (1) If there is a direct relationship between the requiered level n'_E and n_E such as $n'_E > n_E$, the user gets a new certificate with the trust level (n_I, n'_E) and the old certificate is revoked. (2) If not, the user gets a supplementary new certificate with the required trust level. One of these certificates can be presented in function of application requirements.

Fourth, if we consider the case of CA, the trust level is denoted (n_{CA}, b_{low}). For each $n \in \{b_{low}, b_{sup}\}$, CA can only issue certificates to entities with a trust level (n_I, n_E) with $n_I < n_{CA}$ and $n_E < n_{CA}$. This means that a given CA in the considered environment can not issue certificates to entities with a higher trust levels.

After the certificate generation, the CA ensures its publication in its LDAP repository. The architecture of the latter is organized in a such a way that two fields are assigned to the trust levels. In this nomenclature, the management of the LDAP server and certificate verification become easier due to the use of two levels of trust only. When a user desires to accede to a particular application or resource, a verification process of his presented certificate must be performed. Depending on the minimum required trust level, the application extracts the significant parameter in the couple (n_I, n_E) and verifies the access rights attributed to the end-user.

6.3 Implementation issues

For the purpose of multi-level trust PKI implementing, the use of open-source software can fulfill the suggested requirements. For example, the use of `openssl` [1] with its cryptographic functionalities can be a satisfying option for a standard solution. Moreover, `openssl` is worldwide used and can be easily manipulated. Thus, the different PKI roles can be separated from each other according to the environment requirements (RA, CA, end-user). In addition, the printable fields in a X.509 can be specified in such a manner to insert the trust level information corresponding to the certificate holder. We must notice that, with `openssl`, the certificate authority manager has to intervene only on some specific points. Time can be then saved efficiently. Another characteristic of `openssl` that may encourage its use in a large-scale environment is the possibility of databases building to manage users certificates, keys, and other active elements of certification. Up to here, `openssl` can be used to perform the following functions of the PKI : registration (key and request generation), certificate generation and revocation.

The publication and verification of certificates are two essential functions when implementing a multi-level trust PKI in the e-government environment. For the publication purpose, an open-source solution such as `openldap` [2] is available for use. On its own, `openldap` offers a complete publication service for certificates and CRLs with hierarchical structure. However, one shortcoming of `openldap` is the rigidity of matching. `openldap` does not use the same encoding used in the X.509 certificate. Thus, it is unable to perform a research using attributes existing inside the X.509 certificates. To overcome this insufficiency, new attributes must be added in the repository as searchable parameters and as they are listed in the certificate. The `openldap` as it is currently defined does not present this possibility.

In this trend, two solutions can be adopted. First, an intelligent database for certificates can be built to support different types of encoding formats and new requests can be added to interact with the database. This approach can remedy to the limited set of request predefined in the LDAP protocol. The second solution consists of building an external module for conformity testing. This can be achieved without modifying the repository structure but requires a verification rules building to manage accesses to the repositories and to involved applications requested by certificate holders.

7 Conclusion

The world is moving toward more complex and open PKIs structures. In addition, e-government requirements in term of trust become more and more pronounced. People

[1] http://www.openssl.org

[2] http://www.openldap.org

can have multiple certificates, which may belong to different PKIs and may be used in environments having variable security requirements. Similar situations may lead to a considerable cost for users in term of time, money and complexity. Thus, the limited expressiveness of current certificate becomes a concern to manage multi-trust levels in different e-government domains.

We have attempted in this paper to propose a model that integrates the concept of multi-level trust through the use of X.509 certificates. We have also adapted it to the need of managing access control and authentication in e-government. Then, we have considered the main modification needed by a PKI to handle digital certificates marked with a subset of trust levels. We finally presented a case study in an e-government environment in which two trust levels are defined.

References

1. Boudriga, N., "Technical Issues in Securing E-government," *IEEE international conference on systems, men, and cybernetics (SMC02)*, Tunisia, 2002.
2. Benabdallah, S., Guemara El Fatmi, S., Boudriga, N., "Security Issues in E-Government Models: What Governments Should do ?," *IEEE international conference on systems, men, and cybernetics (SMC02)*, Tunisia, 2002.
3. Chadwick, D.W.*, An X.509 Role Based Privilege Management Infrastructure*, Business Briefing - Global InfoSecurity 2002, World Markets Research Centre Ltd, ISBN: 1-903150-52-3, 2001.
4. Chadwick, D.W., Otenko, A., "The PERMIS X.509 Role Based Privilege Management Infrastructure," *Future Generation Computer Systems*, 936 (2002) 113, 2002. Elsevier Science BV.
5. Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," RFC 3647, 2003.
6. Chadwick, D.W., Ball, E., Sahalayev, M.V., "Modifying LDAP to Support X.509-based PKIs," *Working Conference on Database and Applications Security to be held August 4-6 2003 Colorado.*
7. Chadwick, D.W., "Internet X.509 Public Key Infrastructure Operational Protocols : LDAPv3," *Internet Draft <draft-ietf-pkix-ldap-v3-05.txt>*, 2002.
8. NSS Group Report "Public Key Infrastructure," *Group Test Edition 6 - 2003.*