A User-Centric Approach to eCertificate for Electronic Identities (eIDs) Management in Mobile Environment

Michele Schiano di Zenise[1], Andrea Vitaletti[1], David Argles[2]
[1]*University of Rome "Sapienza", Italy*
[2]*University of Southampton, United Kingdom*
michele.zenise@gmail.com, andrea.vitaletti@dis.uniroma1.it, da@ecs.soton.ac.uk

Abstract

The use of electronic documents is constantly growing and the necessity to implement an ad-hoc eCertificate which manages access to private information is not only required but also necessary. This paper presents a protocol for the management of electronic identities (eIDs), meant as a substitute for the paper-based IDs, in a mobile environment with a user-centric approach. Mobile devices have been chosen because they provide mobility, personal use and high computational complexity. The inherent user-centricity also allows the user to personally manage the ID information and to display only what is required. The chosen path to develop the protocol is to migrate the existing eCert technologies implemented by the Learning Societies Laboratory in Southampton. By comparing this protocol with the analysis of the eID problem domain, a new solution has been derived which is compatible with both systems without loss of features.

1. Introduction

Recently, improvements in technology have made possible the creation of new support, usually electronic, for personal data management that is more efficient and reliable than those existing previously. Electronic identity (eID) aims to replace paper-based documents, thereby providing transportability, a support stronger than paper. Consider, for example, a cup of coffee which falls on our passport. In some contexts, the possibility exists to set personally the information to be made public, thus supporting a user-centric approach to sensitive information management. On the other hand this type of support has a wide variety of issues bound mainly to security. In this sense, the provision of an ad-hoc eCertificate which manages the access to reserved information is not only required, but also necessary. Moreover to gain maximum advantage from eID, we may think to use it on a mobile device. This idea adds other security issues to existing problems and at the time of writing this paper, only a few limited solutions have been proposed.

The Learning Societies Laboratory in Southampton's School of Electronics and Computer Science is developing *eCert* [1], an innovative project focused on the creation of an eCertificate that guarantees prevention of forgery, provision of privacy and interoperability between different systems, particularly in the field of ePortfolios (EP). These EPs are electronic versions of paper-based portfolios and their management has some common points with eIDs. So, eCert seems a valid candidate to solve the eID problem. However, eCert is a web-based protocol, so how can we make suitable use of this technology to provide a solution to the mobile eID problem? This paper proposes a possible user-centric approach to the problem with two main goals:

- to adapt the eCert protocol to make it suitable for eID;
- to migrate the methodology from the web to a mobile environment.

The following discussion demonstrates how these goals may be achieved.

2. Underlying technologies

Consider the following situation: UserX goes out clubbing and has to certify his age to enter. Observe that with paper ID, users are forced to disclose all the sensitive information on the ID, not only the age. Unfortunately his wallet is untidy and it contains a lot of smart cards, other IDs, but not that one that the UserX needs. Disconsolate, UserX comes back home. eCert for eID managed in mobile devices proposes itself as the tool able to be always available and to provide a huge variety of ID in order to avoid the previous scenario. The eID exploits and leverages some key technologies, such as:

- eCertificate as policy for key management;
- ePortfolio to understand and underpin the choice about eCert;
- eID to understand what it is and the related requirements;

- Mobile agents as means to reach a big part of the population and to provide portability, mobility, scalability, data management and identification and control.

In the following we briefly discuss the role of these technologies in our proposed solution.

2.1. eCertificate

The word eCertificate is often used as synonymous with the concept of Public Key Infrastructure (PKI). A PKI provides a secure infrastructure based on authentication and proof of content. Specifically in cryptography, PKI denotes the authentication managed by CA (certification authority): each user receives a public key bound with its unique identity through the registration and issuance process provided, usually, by the certification authority. The link between unique identity and the public key identifies unambiguously for each user a certainty in:

- quality of information sent and received;
- source and destination;
- time and timing characterizing information;
- privacy;
- legal trustworthiness;

Thus PKI ensures confidentiality, integrity and availability with consideration to possible changes of hardware, software, data, policy and people.

2.2. ePortfolio

The Southampton eCert project is focused on providing user-centric control of personal data within the context of ePortfolios (EPs). The term ePortfolio identifies a digitalized collection of artifacts that represent an institution, group or an individual. The EP possibilities go beyond the previous definition: it can be used as an administrative tool (to manage and organize work), to monitor access to private information and it can be used as a means for exchanging ideas and feedback. The structure of an ePortfolio (collection of files) isn't directly linked to the eID structure, which is a collection of text-line information, but its idea is quite close to that of eID: both EP and eID have to find an electronic and secure way to certify, set and show the users' private information. This feature underpins the eCert protocol which is designed to manage ePortfolios, providing security in this field of e-Learning.

2.3. eID

Just as the ePortfolio is proposed as a substitute of the paper-based portfolio, the eID guarantees the same functionalities as an ID card. Usually an eID is a plastic smart-card (like a bank card) that provides personal user identification through a microchip containing information. The electronic side of this support consists of authentication and requires a document to be signed with a digital signature. This paper presents a secure protocol for eID management which is completely electronic: it allows the user to set a scope for his information, provide security through the migration of the eCert protocol, and mobility through the use of mobile devices.

2.4. Mobile agents

We envision a mobile solution based on mobile agents (MAs) implemented on mobile phones. A MA is a software agent which can transport its state between different environments without loss of features. More specifically a mobile agent is autonomous, self-taught (with respect to its environment) and mobile.

Security problems for MA include the protection of the Agent Execution Environment (AEE) from malicious agents, of agents from a malicious AEE, of one agent from another, of an AEE from another AEE, of the communication to and from the AEE, and of the host from the AEE. In order to solve these problems we could use the principles shown in [3]:

- *for the most natural applications of MA, the participants cannot be assumed to trust one another,*
- *any agent-critical decisions should be made on neutral (trusted) hosts,*
- *unchanging components of the state should be sealed cryptographically.*

The eCert central system provides the same features. Thus the migrated eCert technology is sufficient to guarantee these principles in practice.

2.5. Current system

There are many examples of eID applications. They include the following:

Identification eID: is a government-issued document for online and offline identification. Usually this type of document allows digital signing and uses a chip which contains the same information legible on the card plus information for the identification like signature key and certificates. Examples are the biometrical passport [4] and the italian CIE [5] (electronic identity card): the first one is a combination of paper and electronic ID that provides the same features described above.

Access badge (private eID): is used for entry to reserved areas managed by automated access control. It can be equipped with various technologies, but usually uses barcodes or magnetic stripes to carry an identification number. An example of this type is the IDcard [6] for the students of Southampton University. This card provides authentication for all the universitary stuff, including the public transport.

Financial eID: can be defined as a "middle way" between the previous two. The mechanism of authentication is close to an access badge (authentication through an automated control with magnetic stripe) but the new eIDs belonging to this group has a chip that contains all the private information of the user. Moreover the process of authentication is made stronger by the use of a personal secure number (PIN). Bank cards [7] are typical examples of this category.

Each type of eID analyzed provides security, authentication, and has a track record in the security field. Moreover they use the same cryptography model that the developers would use for the project, so we have to think: what is the innovation inside the project? Why could it become a useful tool for the day life? The answers are: mobility and customizability. None of the previous eID examples allow the user to set a scope for his data and no one has an implementation usable by mobile. The project shown in this paper aims to reach both this goals and, in this sense, it's a very innovative project.

3. eCert protocol

The eCert project is a UK government-sponsored project [8]. At the heart of this project is an eCertification protocol which is being developed to address security issues which originally arose as a concern within the field of ePortfolios. The current phase of the project involves the completion of a demonstrator system, and the beginning of the implementation of the protocol within a UK ePortfolio system and an Australian system. For this reason, it seems a good idea to leverage the UK government user-centric structure of eCert for ePortofolios to achieve the creation of a new protocol with similar features but focused on eID in the mobile environment.

3.1. Overview

eCert divides the system actors into three categories and for each of them it defines the relationships shown in figure1:

the issuer is the entity that manages, provides and issues the eCert, after the user identification;

the owner is the entity that, if identification succeeds, receives eCert. Then he is able to set his information and finally he can distribute them;

the reviewer is the entity that views the information provided by the owner and he checks if they are valid.

The actors interact each other through the processes shown in figure. The owner and the issuer are bound by the issue relation which is the act to provide an eCert and it contains the request (r) (the act to request an eCert) and the ack (a) (act to send an eCert). The owner is then linked to the reviewer by the distribute relation which is the act of disseminating the information. Finally the reviewer communicates with the issuer through the verify relation which is the act of checking the validity of information. It contains a request (r) requesting the checking process and ack (a) confirming the document's validity and showing the eCert).

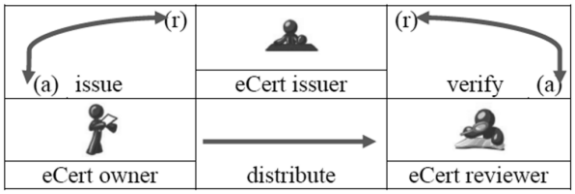

Figure 1. eCert actors and relations

eCert aims to secure the whole e-certificate system, not just the eCertificate itself. We now show how to reach this goal.

3.2. Structure and functionalities

The eCert structure provides central services, but requires user-orientated storage. It is composed of:

- central system (online service): provides the management and the verification for all the issuers that use the system. This solution is able to guarantee a unique standard for all the institution;
- issuer side: signs the documents with his private key, encrypts whole the document with owner's public key and provides the needed updates for the central system (e.g. revokes a document that it was withdrawn);
- owner side: sets the info's access through an access token contained into the XML metadata and sends the eDocument to reviewer;
- reviewer side: uses the online service for verifying the genuiness of the eDocument.

Figure2 shows the structure. The eCert policy provides also the following functionalities that aim to solve the problems related to the chosen architecture:

- each owner has one and only one system ID that acquires at the moment of first registration into the system and it has a lifetime-duration. It must be attached in each owner's information;
- the issuers have to be certified to avoid that fake issuers are present into the system. Moreover all the member that belong to an issuer have to be certified also;
- owner: system ID → 1:1;
- system ID: eCert → 1:many;
- owner's public key must to be known only by owner and central system;

- the central system has to maintain a revocation list for all issued eCerts that may be uploaded by the institutions.

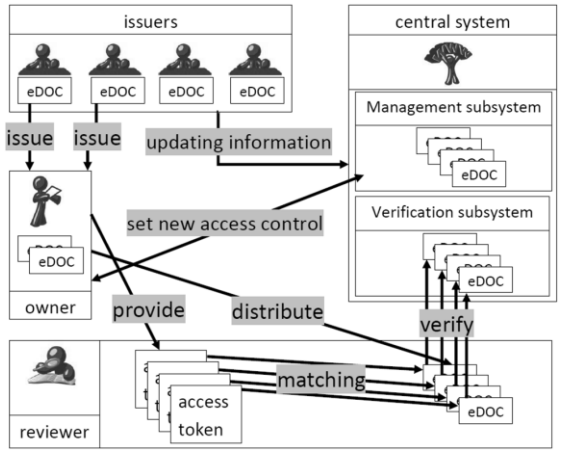

Figure 2. eCert system

3.3. Advantages and disadvantages

eCert provides a unique, secure and trusted system for the management of data in a web environment with a secure user-centric approach. This user-centric focus is key to this project and a further advantage would be to consider this protocol as a possible candidate for a future national level standard. On the other hand, the protocol is thought to manage ePortfolio in the web environment: a reverse engineering process to adapt the system is needed. Even if the ideas of EP and eID are quite close, their structure is different: eCert is not able to manage eID. Furthermore, the issue process is different in terms of the data transmitted and the execution environment. These issues will now be analyzed.

4. Design

The idea of an eID managed in mobile environments constitutes a powerful and innovative tool to manage personal identity in an easy and comfortable way, but it offers many security challenges as that to guarantee security in the whole the process. In order to do this it is clear that:

- reviewer has to be able to verify the identity and the validity of the document shown;
- the owner has to be able to show only the information that he wants to show (in this case date of birth) and he has to be able to manage the access to this information;
- the issuer has to be trusted to manage a huge quantity of information and to sign its document with the eCert policy.

Apart from the security and adaptation issues, we have to consider a technical problem related to the mobile environment: to find a good and quick way to pass the eID to the reviewer. Two possible solutions were considered, NFC [9] and qr code [10]. Although the two means are equally efficient, the increasing popularity of qr codes and the availability of a qr reader within mobile devices support the choice of the qr code over NFC.

Figure 3 gives the use case diagram for eID eCert:

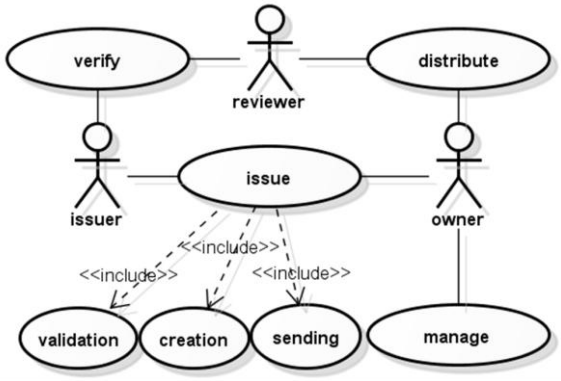

Figure 3. Use case diagram

4.1. eID vs eCert

The review of the underlying technologies identified that the idea of EP is quite close to eID in that both need to find an electronic and secure way to certify and show the users' information. Although eCert provides secure eCertificates in the web environment, studies on eCert and in the literature point out that it can't be directly applied to eID for two reasons; differences in the file structure and the existence of a personal account. eCert is a stand-alone system, but it has been created to manage EPs and this feature is evident in the structure of the managed files.

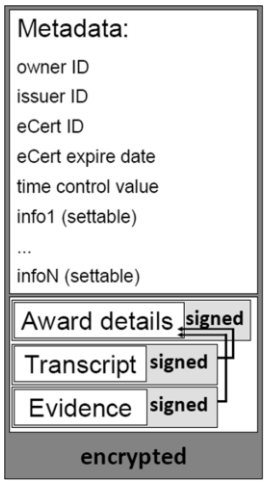

Figure 4.a) eCert file

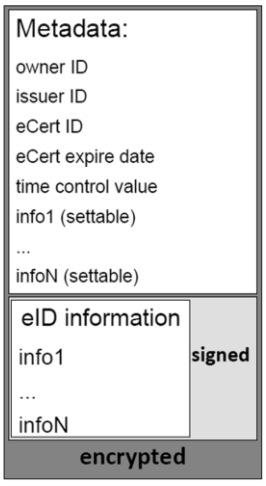

Figure 4.b) eID-eCert file

The eCert files are a collection of files, individually signed, and encrypted together with

metadata that makes it possible to set a file's scope. Instead the eID files are a collection of line-text information gathered in a single signed file and encrypted together with metadata that makes it possible to set the scope of this information. This problem is related to the code of the issue process: a recoding is sufficient to make the system able to recognize the eID file. Thus, the recoding aims to make able the system to use the structure in figure 4.b) instead the structure in figure 4.a). Note that with the notation "settable" we set the visibility for that element of the file: other files in the case of eCert, and text-line information in the case of eID.

The second difference is related to the nature of the information: the original protocol allows the issuing institution to have an account for each eCertificate owner in order to manage his information. In the eID, this step is unnecessary because it is reasonable to think that personal information like DOB (date of birth) is valid for a person's life-time. This issue mans we need to find a way to supply the lack of an account and thus, secure the eID-eCert on mobile devices. We therefore need a new encryption method to straighten the issue process between issuer and owner without using an intermediary account. In this sense, AES-128 [11] seems the best possible choice.

4.2. Using eCert's solutions in eID

In order to guarantee security, eCert employs additional features beyond the basic architecture with a central service and no central storage. Some of these must be maintained for the eID system.

About the assertion techniques:

- an XML signature can be used to encapsulate the documents in order to have an issuer's secure signature;
- XML metadata: the ownership information of an eCert can be stored in XML metadata and meanwhile the employee can create an eCert through the XML signature method;
- revocation lists: a check of information status is required. In fact if the key has been compromised or the information has been withdrawn, the system has to deny the access;
- auto request: the Certificate validation processes has to start automatically before the verification results are ready;
- timestamp: can also be added the XML Signatures to improve the security.

Concerning the privacy techniques, we may use the eCert signature method [1].

Regarding the lifetime validation techniques, the eCert central system provides a verification service for eCertificates issued throughout the UK. It would be ideal for solving the lifetime validation issue. Adopting this solution, we need to take care to consider the mass of stored data: in fact it implies that all the issued information should be stored in the central system.

5. Development

In the following, we are using the name eID to indicate the data to protect, eID-eCert for the protected data, [ ]a to indicate that eCert is encrypted by a's private key and ( )a to indicate eCert is encrypted by a's public key. The issuer and the central system have the same cryptographic method, so all encrypted data sent by the owner is accessible by the central system.

5.1. Issue process

The issue process for eID exploits the same validation and creation processes as eCertificate. After the validation, the issuer gathers the owner's information, sets an initial (default) access control and applies his signature (with his private key). This component is the eID. After this, the issuer creates an AES-128 key, updates the central system revocation list and sends this key to the owner that acquires it as his private key. Finally, the issuer creates [eID]owner = eID-eCert and sends it to the owner. Note that the key and the eID-eCert must be sent in two separate messages.

5.2. Manage process

The owner logs in to access the management system sending his key. If the validation of his identity succeeds, the owner is able to interact with the central system and update the eID-eCert. The central system is able to verify ownership, revocation, modification and validation of eID-eCert. The central system creates two new key pairs ( )access; [ ]access: the first one is used as access key to view the eCert, and the second one is used to apply a new signature to the eID. The new eID-eCert will have a new access control set by the owner. The next step is the creation of the qr codes. One can assume that the owner doesn't have the needed IT skills to proceed in this operation, so the best solution is to make the central system able to create these codes. The system generates qr_code{access key} and qr_code{[eID]owner}. The system must send the two codes in two separate messages in order to avoid possible attacks like the "man in the middle" attack. In this way the owner has both items of required information enveloped into a qr code, which is easily and quickly presentable to the reviewer.

5.3. Distribute and verify process

The owner forwards qr_code{access key} and qr_code{[eID]owner} to the reviewer. The latter one

uploads eID-eCert to central system and uses the access key to certify his authorization. The central system decrypts the eID-eCert and verifies revocation, modification and validation. If the checking is positive, the central system enables the reviewer to view the eID, otherwise it sends an error message. We call the act of giving the information to the reviewer "sending", but actually the owner shows, not send his data: in fact the reviewer, through the use of a barcode reader, scans the barcodes and, gets back the contained information on his phone.

5.4. Implementation

eID-eCert has been implemented on the Android [12] platform in Java. This platform is open source and in future its market could be a good testbed for this work. The methodology used for the development of the protocol is Agile [13]. It has been very useful to understand the real user requirement and to improve it through a constant flow of feedback given by the developers of original protocol and by experts in security field. This new protocol turns out to be very powerful and applicable in a wide variety of scenarios (e.g. to prove own personal age, but also as substitute for digital access cards for reserved areas). As for with all the new protocols, it will be prone to bugs, new and inherited from previous versions of eCert: these are matter for future work.

6. Conclusions and future work

Initial results indicate a real possibility of using eCert to manage eID in the mobile environment supporting the user-centric management of sensitive information.

Figure 5. The result

We can distinguish between two types of possible improvement: the first one is related to the improvement of the code and the second one related to improvement of the protocol methodology. In relation to the methodological issues, it will be advisable to find a way to reduce the use of the central system (by reducing message exchange and the access into the DB) and, most importantly, to make an identification picture for each eID available, in order to improve security and privacy. Moreover, a mechanism could be developed that allows for the detection of the type of CA to which the issuer is referred, reducing the work of the central system (verification process).

We plan to evaluate the usability of our system by real testbeds. A possible testbed is related to the access to alcoholic drinks: we should be able to certify age so that the salesman can be sure of that. Another way is to release a beta version on the Android market and wait for the feedback in order to improve the protocol. Finally we plan to submit the protocol to a group of security experts following the methodology of think aloud [14] and to make improvements based on any suggestions offered.

7. References

[1] Chen-Wilson, L. and Argles, D.”Towards a framework of a secure e-Qualification certificate system” *ICCMS*, 2010, Sanya, China.

[2] George Lorenzo and John Ittelson, “An overview of E-Portfolio” July 2005.

[3] Vu Anh Pham and Ahmed Karmouch, “Mobile Software Agents: An Overview”, *IEEE Communications Magazine*, 1998, Volume 36 Issue 7.

[4]http://www.direct.gov.uk/en/TravelAndTransport/Passports/Applicationinformation/DG_174159/, accessed 30dec2010.

[5]http://www.servizidemografici.interno.it/sitoCNSD/pagina.do?metodo=homePage&servizio=navigazione, accessed 30dec2010.

[6]http://www.soton.ac.uk/sais/idstudio/idstudio.html, accessed 30dec2010.

[7]http://www.unicreditbanca.it/it/privati/conti/genius/one/?idc=14626, accessed 30dec2010.

[8]http://www.jisc.ac.uk/whatwedo/programmes/aim/ecert.aspx, accessed 30dec2010.

[9]http://www.nfc-forum.org/specs/spec_list/#refapps, accessed 30dec2010.

[10]http://www.denso-wave.com/qrcode/index-e.html, accessed 30dec2010.

[11] NIST, Announcing the Advanced Encryption Standard (AES), *Federal Information Processing Standards Publication 197*, 2001.

[12]http://developer.android.com/index.html, accessed 30dec2010.

[13]http://agilemanifesto.org/, accessed 30dec2010.

[14] Maarten W. van Someren, Yvonne F. Barnard, Jacobijn A.C. Sandberg, “*The think aloud method - A practical guide to modelling cognitive processes*”, Academic Press, London, 1994.