CS4200

Software Requirements Specification
for
eID
(Electronic Identity)

Version 1.0

Supervised by
Dr. Chandana Gamage
Dr. Shantha Fernando

Prepared By
Group CNWIS-G2
Buddika Malalasena (050262X)
Skandhakumar Nimalaprakasan (050293R)
Ramanan Sathananthasarma (050357T)
Kanaganayagham Shayanthan (050427J)

Department of Computer Science and Engineering
Faculty of Engineering
University of Moratuwa
Sri Lanka

Table of Contents

Revision History

Date	Reason For Changes	Version
29 May 2008	Initial Submission	1.0

1. Introduction

1.1. Purpose

This is the Software Requirements Specification(SRS) document that describes the software requirements of the the project eID (**e**lectronic **id**entity), which is the electronic replacement for traditional ID cards. This will be the electronic counterpart to the existing national identification card (NIC), with more diverse uses other than functioning as a mean to prove identity of a person. In day to day life a holder of eID will be able to use many e-government services and other online service using eID as the mean for authentication. This SRS will cover the user and system requirements of the project. The basis for scope, design, construction as well as planning and estimates will be based on the requirements stated here.

1.2. Document Conventions

The following font styles are used in this document:

- Major Headings – 18pt, Times New Roman, Bold
- Sub Headings - 14pt, Times New Roman, Bold
- Other Headings - 12pt, Times New Roman, Bold
- All other text - 12pt, Times New Roman

1.3. Intended Audience and Reading Suggestions

This document is intended towards a general audience with interest on the eID project. Specifically the government authorities and policymakers would find useful information from this about the eID project. Also the staff members of the Department of Computer Science and Engineering, University of Moratuwa, mainly the project supervisor, project coordinator, project evaluation panel, and the development team of the project could be using this for various purposes.. The supervisor will refer to the SRS whenever needed during the progress of the project. I will be using this through out the software process as the actor of all the roles.

1.4. Project Scope

The intention of this project is to implement an eID framework which could be a replacement for traditional paper based ID cards, with extra features supporting online and e-government services. Primary objective of eID project is to make an eID, that could be used not only in the electronic world, but also in the normal offline world. This needs an eID solution that could be accepted by different users, with providing facilities to support diverse services.

Three major components of the eID project are identified as follows:

A) eID Card

B) Back End Infrastructure

C) Front End Infrastructure

These three components can be considered as three different entities, but with total interoperability.

1.5. References

Research Papers

- *Advanced Applications for e-ID Cards in Flanders, ADAPID Deliverable D2, Requirements Study*, April 2006. Available at https://www.cosic.esat.kuleuven.be/adapid/docs/adapid-d2.pdf, Last accessed on 15 May 2008.
- *A Methodology for Anonymity Control, in Electronic Services Using Credentials*, Vincent NAESSENS, June 2006
- *Identity in Digital Government, A report of the 2003 Civic Scenario Workshop*, Jean Camp, Kennedy School of Government, Harvard University
- *Electronic ID-cards and Anonymity*, Jan Enlund, Department of Electrical Engineering, Helsinki University of Technology. Available at http://www.tml.tkk.fi/Opinnot/Tik-110.501/1999/papers/electronic_id/Electronicidandanonymity.htm, Last accessed on 15 May 2008.

2. Overall Description

2.1. Product Perspective

eID, short for **e**lectronic **id**entity, is the electronic counterpart to national identification card (NIC), driving license, passport, and other membership cards. In the changing world, which is moving more towards the online based services in public and private sectors, a person can present an eID electronically to prove his or her identity or their right to access information or services online. From an electronic identity perspective, one person is usually involved in multiple sectors (e.g. taxation, social security, education, telephony services, banking services) and also often fulfills different roles (e.g. a civil servant, a lawyer or a driver) depending of the context. Therefore, the corresponding data should be managed/accessed in an independent way.

2.2. User Classes and Characteristics

This projects will have two distinct concerned parties as system users. The end uses who will be holders will be using the eID in the daily life, and the issuing authorities and government will be concerned about how eID could be used for the benefit of their services for public. An individual who possesses an eID will be able to get multiple uses from it. The main one being identification in the offline world and authentication in the online world. For any individual who is used to traditional ID cards, the eID won't look too alien as it will also provide a similar printed interface with basic identification data. On the other hand as this is going to be interfaced to PCs and most of the other possible devices via USB interface, any user familiar with these equipments will be comfortable using the eID. In the user point of view acceptance is the key for the success of any system. This is the main reason for having a traditional ID like card as eID instead of a USB token device which could provided most of the electronic requirements. By this the user is given more uses out of his one eID, which ranges from e-government services and other online based services.

e-government can be defined as the use by government agencies of information technologies that have the ability to transform relations with citizens, businesses, and other arms of government These technologies can serve a variety of different ends such as better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. Dealing with this content-rich electronic identity will require adequate legal provisions in terms of data protection and personal control over personal data by the individual. The using of eID in e-government services provides greater advantages to the government, which is also the issuing authority of eIDs. Government will have greater control over eID system, and the closer relationship will lead to more diverse usage of eID in various different services specially online and also offline.

2.3. Operating Environment of the System

The operation of eID system will be in socio-technical environment. The acceptance of eID will be the main challenge as people might reject change. Also there are many concerns that will have to be looked into specifically on eIDs. Electronic transaction and related security will be a main concern for the acceptance. Also privacy will be an important aspect of the eID system as many users will be concerned about this. The eID system will operate in a social environment with ethical diversity and people with different educational backgrounds and believe systems. This will need the eID system to be appealing ad acceptable by a heterogeneous society, which could be highly challenging concerning all desires.

The technical aspect of the operating environment will be a very scalable software hardware system. This will involve high performance and durable hardware as will as operating systems, databases and other support software to be highly secure and reliable.

2.4. User Documentation

The eID being a very new product for the general person, there is a need for extensive documentation for all users. The different users of the system, such as normal citizen, system administrators, e-government service developers and other service developers, will be needing different documents explaining different functionalities of the system. Specially the general public, who will be the end users will need easy to understand documents preferably in their local languages.

3. System Features

3.1. Identification and Authentication

The eID serves as identification token for citizen to prove his identity, which is very similar to traditional ID cards. But in contrast to traditional ID, eID will be a mean for identifying a person in the online world as well, proving authentication for online based services. This is the main requirement of an eID and this has the highest priority of all functional requirements.

3.1.1. Off-line Identification

The traditional IDs provide identification with physical presence of the card owner. The authentication is performed by checking the visual appearance of the holder and the picture on the card. An eID will also have similar printed card with holder's picture and other basic details on it. This could be used as the same way as the existing ID cards. The migration from paper-based to eIDs enables extended functionalities in authentication. Personal data stored in the eID can be read much more efficiently when a citizen uses it to identify in person. The eID enables authorities to verify a person's identity by connecting to to the central authenticating server or by reading information from the digital data stored in the eID.

3.1.2. On-line Identification

The eID can also be used for identification and authentication in online applications apart from the offline world. In e-governance services authenticating a citizen to access an online service is crucial and eID provides means to do this effectively. The card will have electronic signature of the holder and that are signed by the issuing authority. This data would be read from the card directly by the authenticating service and authentication would be done. This authenticating service could be used by approved authorities and and other service providers. Citizens may use the card to gain access to e-government services, sign online contracts and access other web based services and applications.

3.2. Enhanced Security

3.2.1. Confidentiality

Confidentiality in eIDs is to keep information secret from entities those are not authorized to have access to it. Keeping information in the card in digital form secret and the transactions secure from entities that do not have any need on it, is an effective measure to prevent illegitimate use of the data. Confidentiality is particularly relevant when sensitive data that would be saved in the eID (such as ethnicity, personal details or health related information) is concerned. The confidentiality of the information should be protected, so that unauthorized third parties are not capable of eavesdropping on the communication between the eID holder and the services that the eID is used by the citizen. There are many available cryptographic algorithms that provide confidentiality, and eID would use public-key encryption schemes to achieve this. One of the main problems of storing encryption/decryption keys in the eID card is that the card may get lost, making it impossible to decrypt data. In order to solve this problem, some back-up or key escrow mechanism needs to be implemented.

3.2.2. Integrity

Integrity in eIDs is the quality which ensures the data in eID could not be subjected to any sort of manipulation such as insertion, deletion, substitution etc. Cryptographic methods such as message authentication codes (MACs) and digital signatures would be used for achieving data integrity. The integrity of the data contained in the eID card is protected by a digital signature generated by the card issuing authority. Anybody who has access to the card can read out the information it contains: public key certificates, personal data of the card owner, etc., if they posses relevant access level. However, only the card issuer can modify the contents of the card.

3.2.3. Authentication

Authentication serves to demonstrate the integrity and origin of what is being pretended. The security and reliability of authentication mechanisms may vary dependent on the desired authentication level. The stronger the authentication, the higher the confidence that an entity corresponds with the claimed set of attributes. During the authentication process, one makes often use of credentials. Authentication is often achieved by proving something you know (e.g., PIN or password), something you have (eID) and/or something you are (biometrics). In the case of the eID, authentication in the current version is performed by “something you have” (i.e., the physical eID card) and “something you know” (the PIN to the card).

3.2.4. Non-repudiation of origin

Non-repudiation is the concept of ensuring that an action cannot later be denied by one of the entities involved. With regard to digital security, non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. Non-repudiation of origin and delivery are very important for assuring legal effectiveness to actions done in a digital context (e.g., signing a contract). As the user may obtain official statements with legal value, it should not be possible for the server to deny having produced the document. Therefore, the server may have to produce some signature on the information in order to ensure non repudiation properties. The current version of the eID provides non-repudiation by using digital (qualified) signatures.

3.2.5. Access control – Authorization

Access control is restricting access to resources to privileged entities. Access control works at a number of levels: There are access control mechanisms that work at application level and for the user they are expressed as a very reach and complex security policy. Usually, authorization is used in the context of authentication. Permission is granted or denied based on the result of data or entity authentication, and on the allowed activities, as defined within the system. Once an entity is authenticated, it may be authorized to perform different types of access, each of which is referred as a role.

3.3. Privacy Maintenance and Data Protection

The meaning of privacy differs from one to another. But in common most people don’t want themselves to be continuously traced via the usage of the eID services. Also in terms of autonomy, the fear of having a person's actions recorded and reported may prevent individuals from using the system to the full capacity and this might lead the failure of the system as a whole. This privacy issue had led to the failure of some eID schemes in countries including Australia.

The eID card offers a range of opportunities to perform operations upon personal data. It will be important to determine who is in control of these operations. There will be several data controllers, so it is important to know who is responsible for which operation. While being able to prove the identity to the low enforcement authorities and to access the services available with the eID, the individuals should be able to keep the privacy of their personal information from third parties.

3.3.1. Trust Requirements

A system or party is trusted when an expectation rests on it to behave in a determined way or achieve a determined result, and where the relying system or party acts on this assumption. More generally, trust is a quality of a relationship between two or more entities, in which an entity assumes that another entity in the relationship will behave in a fashion agreed beforehand, and in which the first entity is willing to act on this assumption.

Whether or not to trust depends on a natural person's decision. It is possible, but not necessary, that several entities trust each other mutually in a certain context. Trust decisions of legal persons depend on the decisions made by the legal person's responsible natural persons. Trust may be limited to one or more specific functions, and may depend on the fulfillment of one or more requirements.

3.3.2. Enforcement and Accountability

The use of policies is a very important aspect in enforcement and accountability. A person can only be held accountable if there is some way to specify what he/she is allowed to do within a system. Therefore the policies have to be defined. Each policy should clearly define which actions are prohibited and what are the consequences of misuses. Policies should also include the rules to state what is allowed by law, where applicable.

Next to discuss which actions are allowed, it should also be possible to define the functionality of the services. That way a service provider has to deliver the promised functionality.

If he fails to do this, he can be held accountable. There can be different levels of policies defined for to be used in the system. It can be classified as follows; International policies, governmental policies and internal system policy. The International policies are defined by international organizations according to the international norms. The governmental organizations define the governmental policies and every particular system can have its own internal system policy. Some policies can be defined in the very low level of this hierarchy and some can be used in the high level according to their properties.

It is not possible to hold users or service providers accountable by only using some policies. From a legal point of view accountability has no meaning unless the party in question can be forced to assume liability for his actions. The aim of enforcement is thus to ensure that accountability is translated into liability where appropriate. The following properties are required to ensure the enforcement possible.

Persons should be able to act anonymously in the system. However when they abuse the system somehow, they should be identifiable. To ensure the privacy of the users, only trusted third parties can identify people. Policies should describe the conditions under which a user may be identified. To ensure anonymous operations, different actions of a user should not be linkable. But in some cases, it may be useful to link some of the actions. This way, it can be possible to find out information about how the abuse was performed.

In case a controversy arises, the parties involved will need reliable evidence in order to enforce their rights. Every protocol must be engineered securely to ensure that every party can gather enough evidence. Only the necessary evidence should be kept to limit the amount of disk space required. Policies must clearly state how long evidence must be saved. When some party cannot deliver certain evidence his chances to win a dispute are very small.

3.3.3. Anonymity and Unlinkability

To enable anonymity of a subject, there always has to be an appropriate set of subjects with potentially the same attributes. Anonymity is thus defined as the state of being not identifiable within a set of subjects, the anonymity set. The anonymity set is the set of all possible subjects. With respect to acting entities, the anonymity set consists of the subjects who might cause an action. With respect to addressees, the anonymity set consists of the subjects who might be addressed. Both anonymity sets may be disjoint, be the same, or they may overlap. The anonymity sets may vary over time. Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together. This requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system.

The use of identity data by default in electronic transactions enables serious risks for the privacy of eID holders. In most cases, identity data is not necessary to carry on secure transactions, where all parties are ensured that their requirements are met. The identity data is stored along with transactions that may reveal sensitive personal information. The data gathered by databases in different domains contain common identifiers (such as the national ID number), the possibilities of aggregating huge amounts of data on all users of the eID card grow dramatically. The possession of such extensive information on large amounts of people would enable very sophisticated profiles that could be used for criminal purposes such as identity theft, or for unfair commercial practices, such as price discrimination. In scenarios where human rights and legal guarantees are not respected, this information could also be abused for undermining civil liberties or exercising discrimination on minorities. These risks can be greatly reduced by implementing security mechanisms that rely on anonymous or pseudonymous authentication, unlinkability on the archival data and access control technologies.

3.3.4. Other requirements

Although it should be possible to identify persons who abuse the system, it should not be possible to systematically monitor normal users. The system must maintain the anonymity as much as possible, while maintaining the possibility to hold users accountable for their actions.

When agreeing on privacy policies, every party commits himself to act according to this policy. Service providers can only perform actions on data if this is allowed by the policy. Especially when providing identifiable information, users should be ensured transactions are performed the way they should. This way it is possible to have more trust in an application. Furthermore, when an organization has put much effort in techniques to handle information correctly, it is more difficult to be held accountable in case of mistakes.

There are two ways to ensure the correctness of transactions. A service can go through a procedure to get accredited. When actions of an accredited service are not performed correctly the accreditation organization can be held accountable. A more technical solution is the use of policy enforcement mechanisms.

3.4. Electronic Signature

Electronic Signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. Electronic signatures are much more difficult to impersonate or forge because the technology authenticates the identity of the sender or signer of an electronic document. Electronic signatures also add assurances that the content of an electronically delivered message or document hasn’t been altered since its creation.

The basic characteristic of electronic signatures is that electronic data can be signed by using a secret cryptographic key. The idea behind this authentication is the confirmation of the signatory’s identity by proving the ownership of a secret key. With eID and Electronic signature solutions, it is much more difficult to complete a fraudulent transaction without the eID card holder's knowledge because both the physical card and the card’s protective PIN are required for each transaction.

The long-term storage of documents in trusted archives often relies on electronic signatures in order to protect the integrity of the document. e-government and electronic commerce operations require electronic signatures in order to build the necessary trust to carry on financial transactions. eID stand to be scrutinized from an evidence law point of view. This is fairly obvious where the eID is used to sign contracts, administrative forms and other legal documents. The legal framework must take into account the various technological and organizational aspects of preservation.

3.5. Diverse Data Usage

3.5.1. Data extraction

Interactions with the administration often imply filling forms with personal data: name, birthdate, address, etc. These data are kept in the eID chip, and they are electronically readable.

Capturing the data directly from the card reduces the time needed to complete the transaction, and eliminates the risks of transcription mistakes.

3.5.2. Electronic signatures

The development of e-business requires a common understanding of what constitutes an electronic signature amongst the parties involved. In practice a wide variety of technologies is in use, from very simple to highly sophisticated. The eID card provides secure electronic signature functionalities, being the public key certificate backed by the national administration. The generation of an electronic signature on a document requires the eID holder to introduce a PIN.

3.5.3. E-government services

Traditionally, users were required to physically go to government offices in order to perform transactions (request of travel documents, tax declaration, request for social benefits, etc.). There is an increasing interest in offering the possibility of online EGovernment services. This would increase the convenience for citizens as well as reduce the costs of operation for the pubic administration.

3.6. Multilanguage Support

Multilanguage support is one of the main expected requirements which would be more desirable in a multiethnic county like Sri Lanka. It could be done using transliteration methods. This makes the services very much usable for all citizens of the country in their own languages. For example the central database could hold the data in one specific language, but a service user who prefers his own language can enjoy the service features without any language bars.

3.7. Trusted Archiving

There is a variety of information to be stored in the eID system. They all need to be stored in a reliable, performing, secure, forward compatible and reasonable trusted archive. The archive must offer a high service level. Also, there should be very strict policies on how data will be inserted and updated to archive and also, removed from the archive. The archive shall not lose data. The physical durability of the information carrier is critical. Storage is the practical activity of keeping data in an unchanged status for a period of time.

The design of system must take into consideration the appropriate way to record the identity of the digital records. Data that is written to the archive must be protected immediately. The throughput performance of writing data to an archival system is critical. Care should be taken to ensure that the system's performance doesn't degrade, as more objects are stored on the archive. The archive data needs to be encrypted on the disk. The management of the decryption keys is a huge challenge, especially at the scale of millions of users and billions of documents.

Disaster recovery is the ability of a system to survive large-scale disasters like earthquakes,fires and etc. The first way to implement disaster recovery is through Backup and Restore. This way, the system can be restored to a previously known valid state. Also Backup data carriers should be stored on a different location from the primary site. If data is encrypted, one should make sure that the decryption keys are not destroyed.

4. External Interface Requirements

4.1. User Interfaces

The users of eID system will have different interfaces to interact with the system. The end users such as the holders of eID would have web based or other application based interfaces to interact and get services. Also the system administrators will have various interfaces to access the system and administrator the processes.

4.2. Hardware Interfaces

4.2.1. Physical Requirements for eID Cards

The card should be in plastic including memory chip and an USB interface. The physical interface of the card format is based on the ISO/IEC 7816 standard. That is the card format and physical characteristics correspond to the standard bank card in nowadays wallets. In addition to that it can effectively make a physical contact (electric contact) with the chip memory which is inside the card and the reader through the USB interface. But for the speed accesses of this card, it is better to use the 2D-barcodes and/or Magnetic Stripe with the USB technology. So it is better to maintain hybrid technologies with embedded USB memory card technology, 2D-barcodes and/or Magnetic Stripe for the physical interface of the card.

In the 2D Barcodes data storage is important for secure data storage and fast assess of the data. Main aspect in 2D Barcodes is relatively high storage capacity (up to 5k). And another aspect is a 2D barcode is easy to produce, it can also be seen as an extra security check to ensure the data inside is correct. It is better to having some basic data in that barcode. In the memory chip which is inside the card have to have the personal data and PKI. For this case of the memory requirement, it is better to have an EEPROM.

4.3. Software Interfaces

The various service providers will have different software interfaces to access the authentication services provided by the system. They can perform their services independently, as long as they adhere with the polices and stranded agreed upon. The eID system will use scalable stable operating system and databases at the back end infrastructure. For this software infrastructure many existing FOSS solutions will be used. The software that will be created will also be FOSS based.

5. Other Nonfunctional Requirements

5.1. Performance Requirements

In the aspect of performance of the eID system, latency is one of the main technical aspects. The number of round trips between terminal and card(s) is important and the number of interactions between client and server or archive must be minimized. The network latency must be minimized. Another important aspect is throughput which is the performance measured from the centralized server. It represents how many transactions per second can be accepted or can be processed with the centralized server.

5.2. Software Quality Attributes

5.2.1. Usability

Using an eID card should become trivial and intuitive. All layers of the population must be able to use the eID card without fear. It should not be difficult to deploy the eID card or its applications. The people should trust the eID card and its intuitive applications. Usability at server side is less of an issue. We will assume the availability of technically skilled people.

5.2.2. Availability

The eID system will have to have zero downtime as it will be a critical for other services that might need to use eIDs. This has to be achieved using load balanced application and database servers that in live sync with back up servers. Also other service critical availability measures should be taken into consideration in the eID system.

5.2.3. Manageability

The system administrators must be able to manage and monitor the eID and TAS system. The challenge is to have few administrators with low technical knowledge being able to manage millions of eID cards and certificates, and multiple petabytes of storage.