Contributions to governmental eID platforms: The Portuguese and the European Citizen Cards

Master's Thesis

UNIVERSIDADE DA BEIRA INTERIOR
Covilhã | Portugal

Manuel Fernando V. Preliteiro

Contributions to governmental eID platforms: The Portuguese and the European Citizen Cards

THESIS

regarding the research leading to the attainment
of the degree of

MASTER

in

Computer Science Engineering - Computation and Intelligent Systems

by

Manuel Fernando V. Preliteiro

RELiablE And SEcure Computation Group
Departamento de Informática
Universidade da Beira Interior
Covilhã, Portugal
www.di.ubi.pt

MULTICERT
Rua Sidónio Pais
Porto, Portugal
www.multicert.com

Cover image: Universidade da Beira Interior Heraldry.

Contributions to governmental eID platforms: The Portuguese and the European Citizen Cards

Author: Manuel Fernando V. Preliteiro
Student Id: m1244
Email: manuel.preliteiro@multicert.com

Abstract

This thesis presents two main levels contributions.

The first contribution lies in the context of the STORK project. As a first step to the design of an integrated, uniform and secure European eID platform, a feasibility study was conducted and a small demonstrator was developed as a proof of concept. As a result of such task, several STORK deliverables were submitted along a contribution for the Porvoo Group regarding the current state of eID across Europe. This work also benefits the second contribution.

Second, it is introduced a new middleware solution for the Portuguese Electronic Citizen Card. This middleware should subsume the actual and official version. Its novelty lies in its ability to process foreign (European) eID cards and adapts its provided support and services (including the User Interface) in conformity. The validity of the proposed platform was ensured and proved by several successful case studies that MULTICERT can use and develop.

Supervisors:

Supervisor: Simão Melo de Sousa
Co-Supervisor: Pedro Borges

Dedication

The Author would like to dedicate this work to several people and entities:

- Prof Simão Melo de Sousa - Without whom this opportunity (and many others not related to this thesis) wouldn't have presented itself
- Universidade da Beira Interior - All the Authors knowledge as a Computer Science Engineer started in this great institution
- MULTICERT - For the offer of the scholarship and unique conditions (access to hardware from several different countries and brands) for the production of this work
- MULTICERT Team - As a thanks for the amazing work environment, high moral and spirits
- Family and Friends - There is nothing better than after a good hard day of work go back to the people you love

Declaration

The work of this thesis was possible thanks to a scholarship provided to the author by MULTICERT and with the support of the RELEASE (RELiable And SEcure Computation Group) research group from Universidade da Beira Interior, both from Portugal. Although parts of this thesis are researches of works already done and published (being those parts properly referenced by the bibliography), no part of this thesis has been submitted elsewhere for any other degree or qualification and it is all the authors work, unless referenced to the contrary in the text. There are parts of this thesis that are based on joint research by the author and Austrian partners. The parts and partners are properly identified in the proper sections.

Acknowledgements

Benefiting from the fact of writing this thesis while working in a company such as MULTICERT it was possible to also benefit from the know-how of many of the work colleagues. So, a big thanks is also due to the MULTICERT team, in particular Gonçalo Hermenegildo and Pedro Borges for their availability and guidance. Also, another huge thanks goes to the authors Austrian partners on the STORK projects (Mario Ivkovic, Thomas Zefferer), that also contributed with valuable knowledge, experience and advices.

Manuel Fernando V. Preliteiro
Covilhã, Portugal
June 12, 2009

Contents

List of Figures

List of Tables

Acronyms

ACD Application Capabilities Descriptor 35

AID Applet Identifier 122

AODF Authentication Object Directory File 42

APDU Application Protocol Data Unit 28

API Application Interface 7

ASN.1 Abstract Syntax Notation One 18

AT Authentication Template 21

ATR Answer to Reset 30

bps Bits Per Second 43

CA Certificate Authority 13

CC Citizen Card 1

CCD Card Capabilities Descriptor 35

eID Electronic Identity 1

eServices Electronic Services 1

eGovernment Electronic Government Services 5

EU European Union 3

FID File Identifier 42

GCAL Generic Card Access Layer 35

GSM Global System for Mobile communications 29

GUI Graphical User Interface 6

IAS Identification, Authentication and digital Signature 13

ICAO International Civil Aviation Organization 3

ICC Integrated Circuits Card 26

IEC International Electrotechnical Commission 33

ISO International Organization for Standardization 22

JRE Java Runtime Environment 64

JVM Java Virtual Machine 38

KBps Kilo Bytes Per Second 43

KAT Key Agreement Template 21

Chapter 1

Introduction

Portugal is one of the European countries in the vanguard of electronic identification. The Portuguese Citizen Card (CC) is a reality since a couple of years ago. This card replaced the older plastic and only capable of providing visual ID card and besides providing this same functionality i.e. being a visual identity card, it is also a valid identity card in the World Wide Web or other electronics and virtual means.

CC on the Web: A Portuguese citizen using his CC can securely authenticate himself within websites and perform digital signatures on any type of documents. These signatures, are legally recognized by law enforcement entities.

Middleware: Another advantage is the existence of a software architecture denominated *Middleware* that is capable of communicating with the card (through smart card reader) and in a fast way the citizen can visualize on his computer all the relevant information contained in the card. This Middleware can also be used for other developers to create applications and Electronic Services (eServices) to fit their particular needs.

Complexity: However, several countries in Europe (and of course in the rest of the world) also deployed their National Electronic IDs and even more have implemented other types of valid Electronic Identity methods.

The need: It is known, that communication between peoples of different countries is hard (language barriers for example). However, it is even harder making different computer systems from different parts of the world communicate and inter operate. To achieve this, there is the need to agree in the exact secure protocol the machines are going to communicate in order to obtain such inter-operability.

Different Electronic Identity (eID) schemas: This task is even more difficult when cultural differences come to scene. Identification is treated differently around the world. In Portugal for example, the citizen is identified by a different number

depending on the type of service he requires (Social Security, Health Care, etc), where in England, the citizens are not required to carry any type of identification (except when driving), and, many more different methods of identification exist throughout Europe.

Questions: This gives rise to several issues. But considering the European case, it is possible to ask the following: How does one creates a card that fits everyone needs? However, even thinking that it is truly possible to come up with such a solution, another question arises: How does one integrates and recognizes all the already existing Electronic Identification Cards deployed by the several countries (i.e. how can a English citizen be electronically identified in Portugal?), since it is not logic for an airport attendant need to install in his terminal all existing middleware solutions of all countries who deployed Electronic Identification?

Looking for answers: These questions are not new, and to study them and try to come up with answers, several work groups were created throughout the world. In Europe, the two main groups are the Porvoo Group and Secure idenTity acrOss boRders linKed (STORK). They are introduced in the following sections.

This thesis proposes to follow (and participate when possible) the work of these two groups and at the same time trying to find an answer for the second question stated above, i.e. how can in Portugal be implemented a new middleware solution capable of integrating and recognizing the several different European Electronic Identities and at the same time provide to the user the relevant citizen data that can vary from country to country.

1.1 The Porvoo Group

Electronic Identity (eID) is a fundamental topic in this thesis context. This section will review and summarise the steps and the organization group involved in the definition of eID as it should be implemented in Europe. At the same time, keeping in mind that security is a central issue in relation to the eID card. This is so, because, when the card used, electronic identification and authentication of the owner of the card is required for public and private online services. The organization group responsible for this task is the Porvoo Group.

Introduction: Porvoo is a town in south of Finland. In a conference held in this city in April 2002 it was decided to establish an informal international cooperative network called the "Porvoo EID Group". The Porvoo Group goal is to analyze, study and spread the adoption of eID in Europe by continually sharing information and support for trans-national interoperable electronic public identities using Public Key Infrastructure (PKI) and smart cards. Therefore, the members will provide input and the set of features the eID should support in order to achieve European

Figure 1.1: Porvoo Group Logo

standardization. It also investigates the major barriers in the adoption of a standardized solution that could fit everyone's needs and also of what is being done in countries outside the European Union (EU). The Group meets twice a year. Of this thesis is already in the 14th meeting. The Porvoo Group only sets and studies rules, it is not in the scope of the Group to implement any solution, apart from some test pilots.

Pan-European eID: In the first meeting it was unanimous the agreement that the need for a Pan European digital identity[1] will be essential for secure public and private sector eTransactions. At the time, a summary table of the current national status of eID legislation, policy planning and implementation was compiled and several areas were identified for detailed focus. These included:

- Effective national and trans-national coordination mechanisms for high end identification, authentication and electronic signature services
- Improved cooperation with private sector business areas such as consumer banking community, and provision of mobile phone based public ID services
- National roll-out business plans including manageable certificate costs
- Common European wide focus on low end entry systems such as replacement systems for national Driver Licenses
- Collaboration with International Civil Aviation Organization (ICAO) regarding use and introduction of eID travel documents
- Status and role of relevant standardization efforts and requirements; including interoperable biometrics, Certification authorities recognitions, security conformance criteria, etc
- Services which play an important role
- Data protection
- Comprehensive information for citizens

[1]Pan-European identity refers to the sense of personal identification with Europe

- Services with easy to access websites, since the card is only a key for identification
- Bridge CA, for being able to accept, read and verify else's certificates - the insurance of the interoperability is extremely important

Contents: This concludes the Porvoo Group introduction. Chapter 7 will include the survey regarding the Group several conferences so that an assessment can be made on the work done so far and in order to better understand the current heading of eID and what is left to be made. Also making part of the survey, the involvement and progression of each country regarding the implementation of their own eID solutions will be analyzed.

1.2 The STORK Project

Taking a quick peek forward, in section 3.1 introduction (Smart Cards) it is referred that smart cards can be used for eID. The smart card is then, with no surprise, the basis for the future European eID which, in turn, is a major European project involving several countries and partners. Regarding this factor, it was required the creation of a development and orientation group, so an harmonizing and convergent solution can be found. This solution has to safely keep and fit as best as possible all the interest from the parts implicated. For the research of this solution was created the multi European task force group denominated STORK (Secure idenTity acrOss boRders linKed). STORK follows the Porvoo Group eID concept and starts its implementation and testing on the European scale.

What is STORK: STORK is the acronym for Secure idenTity acrOss boRders linKed. It is composed by a total of 29 consortium partners (one of which is Multicert) including 14 governments[49].

Figure 1.2: STORK Logo

STORK's aim: STORK's goal is to implement an EU wide interoperable system of eID recognition and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State[50].

The conection to STORK: The Author developed/studied several items for STORK, that work is described in the next sections and a small resume is made in section 1.5. This work is framed in the STORK global platform solution for European eID.

The architecture: Under the previous paragraph goal, the STORK interoperable solution for eID is based on a distributed architecture that will pave the way towards a full integration of EU eServices while taking into account specifications and infrastructures currently existing in EU Member States[50], i.e. the current implementations of eID over Europe like, for instance, the Portuguese eID.

Project Advantages: The main highlight of the STORK project are[49]:

- People will be able to authenticate themselves securely and to easily access online Government services across Europe, using their national eID system
- The resulting simplification of administrative formalities will make it easier and cheaper to live and work in different EU countries, and to set up and operate businesses across the EU
- People will be able to use cross-border services over the Internet without the need to visit the country in advance
- The security of on-line transactions will be strengthened through increased use of eID services to authenticate users
- Secure interoperable eID authentication will encourage the growth of online services
- Common specifications at EU level will reduce the costs of implementing eID services
- Interoperable eID authentication is a key enabler for the EU Services Directive, helping Member States to set up single points of contact for Government services access

Pilots and tests: The proposed architecture is tested by implementing several pilots with services that have significant potential impact (like digitally sign some document) and are adequately secure, by making use of open standards when possible and by respecting data protection regulations, i.e. the pilots test the common specification on eID for several applications that have a substantial impact on Electronic Government Services (eGovernment) across Europe[50].

Final results: Upon completion, STORK intents to be as technology-transparent as possible and ensure that interoperability solutions can operate with existing national eID systems[49]. STORK will rely as much as possible on open standards, so the obtained solution is intended to be robust, transparent, safe to use and scalable, and should be implemented in such a way that it is sustainable beyond the life of the pilot[50].

1.3 Middleware

The Middleware is one of the central themes of this thesis. But what is in fact the Middleware? What are its components and what they do in specific? For an introduction to what is a Middleware and mainly what is going to be the Middleware on the context of this thesis, a very small explanation is given in this section.

Definition: Although it does not exists a final definition of Middleware to quote, a piece o Middleware software can be seen as the part that stands between the desired resources (i.e. different smart cards) and several applications or users that want to access those resources. The Middleware is then responsible to provide one homogeneous interface to those applications or users while being capable of access the several different types of resources. A scheme can be seen in the image 1.3.

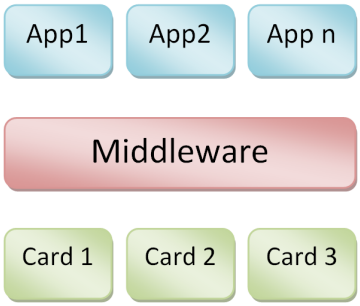

Figure 1.3: Multi Card Middleware for Several Application

Note: Looking at figure 1.3 and instead of "app1", "app2" and "app n" we have for instance "user 1 to n" then this is a middleware between cards and users. In order for the user to manipulate or access the cards, it is underlying that some kind of user interface needs to be present. It can be for instance, a Graphical User Interface (GUI). This is also a valid definition for Middleware.

In this context: In the context of this thesis, the term "Middleware" definition to use is the one also used in the Portuguese Middleware approach.

The Portuguese Middleware: The Portuguese middleware architecture is composed by three different modules: the module responsible to communicate with smart cards that is built over the Personal Computer/Smart Card (PC/SC) standard[2], a Software Development Kit (SDK) module built over the first module which provides to developers an Application Interface (API). This API provides basic functions of the Portuguese CC. Finally, a GUI module also built over the first module (parallel to the SDK modulle) and is responsible to graphically show the user, all the relevant information contained in the chip of some Portuguese CC inserted in the users terminal (figure 1.4).

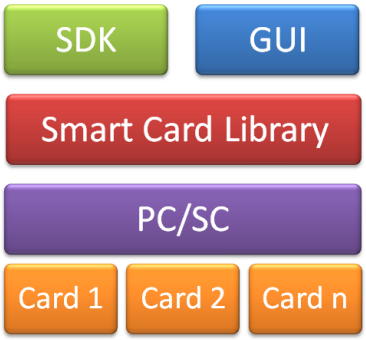

Figure 1.4: Portuguese Middleware Architecture

The Middleware is then from now on (and for convenience of the final solution) some piece of software composed by a set of software modules that can be independent or not. This software is in some way capable of using PC/SC and allow a user to access and manipulate, for instance, the information contained in a smart card and also, benefit from the smart card extended capabilities[3].

1.4 Objectives

Several objectives are proposed in this thesis.

1. **Multi Platform Adaptive Middleware:** As stated previously, different approaches are used throughout Europe when it comes to eID. This creates interoperability problems when a European citizen travels to another country and for some reason intends to use his eID card for identification with for instance, the police. This leads to two possibilities. The first possibility is that the citizen simply cannot use his eID because the police department might not be equipped with the required interoperability tools. The second possibility is that in fact the police is well equipped and allows a correct identification of

[2]Studied in section 3.3.1
[3]Discussed in 3.1

the citizen. However, this means, that the police department needs to have all pieces of middleware software produced by all European countries. This is a cumbersome task for all public (and private) entities. The first objective of this thesis is then to propose solutions and present case studies to allow the creation of a Middleware capable of recognizing the different types of eID cards, and that middleware should present a dynamic and adaptive GUI that transforms itself in order to fit any kind of presented eID.

2. **STORK project:** The global problem addressed in this thesis is eID manipulation and integration. Therefore, aiding the STORK project is another of the main objectives proposed. If objective 1 intents to resolve or at least mitigate the problem of eID harmonization in Portugal in the near future, the STORK project might be capable of completely resolving this problem for all European countries. Although, this picture will only happen in a somewhat far future. But, with this bigger goal on mind, the aid of this most important group is also one of this thesis objectives.

3. **Understanding eID implications:** In order to better understand the "why" behind objectives 1 and 2, a comprehensive survey of international deployment of eID is required. So, the final objective of this thesis is the analysis of scattered information in order to provide a small and simple overview of the eID problem. And, at the same time, the current status of eID throughout Europe in particular and, in a more general view, of the World.

1.5 Contributions

This section provides a small resume of the Author contributed work. The referenced work in this section is better described in the following chapters.

1.5.1 A Survey of eID in Europe

The Porvoo Group conferences are a very important repository of information regarding the evolution of eID across Europe (but not limited to). Therefore, this thesis also contributes to the Porvoo Group, by providing a complete non technical guide and report on the evolution in time of the participating countries in the Porvoo Group conferences, regarding their eID support status (chapter 7).

1.5.2 STORK Contributions

With the last paragraph from section 1.2 in mind, the Author contributed in several key points to the STORK goal.

- Analysis of the European Citizen Card (ECC) specification - Section 3.2

- Study of several possible technologies solutions for the Minimal Footprint Middleware - Section 3.3. As a side note, there were several studied technologies, but not all under the wing of the Author. This work only describes the ones the Author has committed himself
- Implementation of the minimal footprint middleware demonstrator module capable of recognizing the Portuguese eID card and create a digital signature - Chapter 5

1.5.3 Multicert Contributions

Several independent case studies regarding smart card access/manipulation (section 4.2) and dynamic GUI interfaces were performed. These culminated with a simple but complete final solution that can be modularized (and improved in functionality) and then fully implemented by MULTICERT (section 6) as the main part of the future Portuguese Middleware for European eIDs.

1.6 Organization and Parts Overview

This thesis is organized as follows:

- Part I: Brief description on the reasons that led to the writing of this thesis. Presentation of the involved parts and the structural organization of the thesis.
  - Chapter 1: Introduction
- Part II: Preliminary notions and initial research that permitted the execution of this thesis goals.
  - Chapter 2: Key Concepts[4]
  - Chapter 3: Related Technologies
  - Chapter 4: Case Studies
- Parte III: Final implementations regarding the case studies, STORK contributions and research results.
  - Chapter 5: Minimal Footprint Middleware
  - Chapter 6: Common and Adaptive Middleware
  - Chapter 7: Porvoo Conferences
- Parte IV: Results, conclusions and observations.
  - Chapter 8: Results and Conclusions

[4]The key concepts in chapter 2 contains trivial but necessary information in order to understand some of the thesis topics.

Chapter 2

Key Concepts

It is required to the reader not completely familiarized with the topics described in this chapter, the study of the same. These topics will be essential to understand the work described in the rest of the document.

2.1 eID

The use of PKI on eID and other decisions that are described in (for example) the ECC specifications, are based on the eID White Paper (WP) produced by the Electronic Europe Smart Card (eESC). The eID WP is supported by the Porvoo Group resolution on achieving interoperability of eID card schemes across Europe. In this section the need for eID and what the White Paper identifies as relevant, in order to guarantee secure eID across open platforms in Europe is addressed.

Note: The contents of this section were studied from the eID White Paper. The main goal is to give a general idea on what issues the eID implementation brings forth, in terms of challenges and, new problems on a multi cultural environment (like European Union), where different laws and rules exist in order to oversee what is intended to be the same subject, i.e. personal identification and authentication.

Multicultural view: This section also presents a view over one of the main problems concerning cross borders identity, i.e., the cultural barriers. Different countries have different methods of identification and, in accordance, also the methods to protect your privacy vary.

2.1.1 The need for eID

Nowadays citizens want to access electronic services provided by governments (or other official entities) or even perform secure transactions online. For these operations, the standard and widespread paper/plastic documents, where only visual identity verification could be performed are of little or no value. The answer

comes in the form of an Electronic Identity (eID) smart card token as referred in section 3.2.1 (due to the many smart card advantages also referred in that section). The solution is based on the mature technology of PKI by, issuing certificates to some citizen and using them to identify the citizen with the services he pretends to access. This, however, complicates the identification process, because, before the eID White Paper (2003) several countries had already lunched pilots or had in fact worked eID card schemes. This lead to a fragmentation of practices.

2.1.2 The eID White Paper

To avoid fragmentation, the eID White Paper presents a set of minimum requirements and other issues that are considered vital when starting to plan and implement eID smart card systems based on PKI. By implementing this minimum set of requirements, some country should make its eID card compatible with the eServices of some other country that also implements that set of requirements (namely establishing identity) and, at the same time being able to add any other national specific requirements on its eID card.

Development: The eID White Paper was developed by a broad range of interested parties and charters. It found a common way through the complexity of international standards and individual national legislative practices.

Target: The White Paper is targeted at people and organizations responsible for public eID related matters e.g. Certification authorities (CA), Software vendors, Policy makers, Governments, and other eID service providers especially the public officials or, other Member State organizations with legal authorization to issue electronic identity cards/certificates for natural persons.

Structure: The eID White Paper is structured in 3 parts:

- Minimum Requirements for European eID Card
- Current practices in establishing identity. As a side note, the section "*The present PKI-based eID status in Europe*" is outdated in the White Paper (since it dates from 2003). The reader will find in chapter 7 study using has basis the Porvoo Group conferences, where can be seen the international evolution of eID since 2003
- E-ID evolution and implementation

Minimum Requirements for European eID Card

Part 1 is itself divided in 4 subparts:

1. **The smart card as an electronic identity token:** Here, PKI on smart cards is identified as the natural choice, i.e. an eID token should contain at least 2 private keys and, the corresponding certificates that are the electronic counterpart for visual identification of the Citizen. Access to these should be protected by Personal Identification Number (PIN) or biometrics. Therefore, the card should provide Identification, Authentication and digital Signature (IAS) services and included non-repudiation. Also, in this part, the definition of an eID card is presented as "*a smart card based token, containing private keys and the corresponding public key certificates. Optionally, the card may also incorporate a visual identity document*". Having an eID card the citizen should be able to:

   - Perform electronic identification and authentication with public and private online services
   - Perform qualified electronic signatures conforming the EU directive
   - Optionally, access confidentially services, enabling data encryption transmission over a network
   - Optionally, as an official travel document within EU

2. **Requirements for eID cards issuance:**

   In this section are discussed the relevant points regarding card issuance, like for instance, the role of card issuer, the information contained in the certificates, the existence of a Registration Authority (RA) to manage the identification of the card holder before the issuing of certificates, the liability of the CA, assign responsibility to the card holder for protection of the eID card, guarantee the card renewal and, prevent the use of the eID card and it's certificates (by revocation of the certificates prior to the end of their validity in case the card is lost for example).

3. **The requirements on the supporting PKI:**

   Since eID is based on PKI, it is required to have a complete infrastructure to support it, i.e.

   - Obtain and read the certificate

     Applications using the card must therefore be able to read the certificate from the eID card and submit it to the relying party (the entity that relies on the certificate for authentication)
   - Obtaining and protecting the Certificate Authority (CA) certificate

     The CA must provide a secure channel for distributing its CA and Root certificates to relying parties so they can verify the eID certificate
   - Obtaining certificate status information

     The CA needs to provide a Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) service with updated certificate status so the relying party to validate (or invalidate) the eID certificate

4. **The data contents of the certificates**

   Finally, a minimal set of mandatory certificate fields was established. The idea is to ensure the interoperability between the different issuers of eID cards and their relying parties. This small specification needs to be followed by all complying issuers and must be supported by all complying applications. Apart from the mandatory fields that must be present, the certificates can be customized to better fit some particular issuer purposes. The mandatory certificate fields can be consulted in [13] section 1.4.

Current practices in establishing identity

This part of the eID White Paper performs a resumed survey of the practices used by several countries of Europe (Israel is included the survey) to register their citizens and, the steps they take to emit their national citizen ID cards. The countries involved in the survey are: Austria, Belgium, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Ireland, Israel, Italy, Latvia, Luxembourg, Netherlands, Norway, Portugal, Spain, Slovenia, Sweden and United Kingdom. The points identified (and discriminated with small references) are:

- Establishing Identity (i.e. registration of a new born child)

  Across Europe several methods are used, where in some countries the registration is performed by the hospital staff in a report to the pertinent authority (like in Norway) and, in others the parents have a limited amount of days after birth to register the child (like Portugal).

- Documents used for identification

  Some approaches across Europe (harmonization of these approaches must be taken into account by a European eID) are, for instance, the paper birth certificate in Austria is used for governmental usage and the passport for common usage, while in Denmark the identity card is obsolete and no longer used, being replaced by the passport and driving license issued by the police. In Portugal there is the citizen identity number but depending on the services, there are also the health insurance number and the social security number.

- Identification when applying for an ID document

  Some of the different approaches include included are, for instance, the French, where the presentation of some other ID document is required, plus, the birth certificate and the "weeding book" of the parents. In Italy it is required the presence of witnesses.

- Identification when the ID document is delivered

  In this point there are not big differences, practically all countries require physical presence for visual identification.

- National legislation on ID documents

  This point identifies the main national laws and legislation on establishing identity and issuing ID documents. To apply the eID, even countries with modern legislation will have to update them or even make new legislations concerning the eID

- National data protection legislation

  Similarly to the last point, here are identified the legislation documents regarding personal data protection that applies when issuing ID documents

The present PKI-based eID status in Europe: Again, the point 2 of the eID White Paper presents the PKI eID status in Europe as it was in 2003. Being so, the updated situation and completion of this section is performed in chapter 7.

E-ID evolution and implementation

Finally in point 3 of the eID White Paper is performed a study on the relevant aspects of evolution and implementation of eID. These need to be taken into account by countries, organizations (and of course by STORK when implementing ECC) and, magnify the need to assure that the processing of personal data and the protection of privacy is taken into account and, are according to the related European Union regulations.

EU data protection regulations: The European Union has an advanced regulatory framework that regards protection of personal data and, has also directives for the support of eID related frameworks.

The relevant documents are: The directive 95/46/European Counsel (EC) regarding processing of personal data and the free movement of that data, the Decision 01/497/EC regarding the safeguards for personal data transferred from the EU to countries outside the Union, the directive 99/93/EC regarding Community Frameworks for Electronic Signatures and the Directive 00/31/EC regarding a Legal Framework for Electronic Commerce. A complete study of these documents is performed in [14].

Conclusions

Although the European directives aim for harmonization (in terms of data handling and protection), the differences in the various national laws and methods of ID lead to complex legal assessment. This is even more complex if other geographical areas (outside the EU, like Japan or the US) need to be included.

2.1.3 Code of Conduct

The first agreed step in the eID White Paper is the establishment of a Code of Conduct [12] for eID related data protection. This Code of Conduct would be matched against all implementations of the EU Member States. But, only acting as "soft law", meaning, it does not replace any existing legislation. However, it supports the creation of such a legislation (based on the Code of Conduct) in any Member State. In this section the Rules of Conduct will not be explained because they can be consulted in the relevant document, i.e. [12], instead, this section will be focused the need for this Code.

Conscious sharing of personal data: For a successful eID acceptance and adoption by the European Citizen (i.e. the end user), the Citizen needs to feel comfortable and aware on how his personal data is being used and accessed. This is an even more a sensible matter when accessing services online. Even in this case, the Citizen has to have complete control and information on how his personal data is going to be used. If this is not the case and some kind of restriction (like obfuscation on why some part of the data is needed) is presented to the Citizen, it might provoke use resistance. For instance, a data subject may not accept to use some service if he is of the opinion that, an unwarranted restriction has been made or, that he has not been informed sufficiently about the specific reasons for the restriction.

First prerequisite: The way to guarantee the maximum possible acceptance of eID by the Citizen, is to offer the maximum possible protection to his privacy. Being so, the first prerequisite for the rules of the Code of Conduct is to abide the *principle of openness*. This principle covers:

- Data collection or observation:

  From the point of view of the Citizen, it is important to know that data may only be collected when obtained lawfully and for which the Citizen has given permission or at least knows that these data are being collected and for which purpose this collection takes place.

- Data storage

  Two problems may occur in the data storage. The first is related to data pollution: sometimes incorrect, incomplete, inaccurate or irrelevant the personal data are stored. The second problem is the unauthorized access to the data that have been stored i.e. inadequate protection against hacking, managing data carelessly so that anybody can consult or alter them. In order to prevent these two problems, a *carefulness principle* is necessary. This principle consists of three aspects which imply:

  – that the data should be checked for correctness, completeness, relevance and topicality

  - that the Citizen has the right to consult his own data and, if necessary, to correct them
  - that technical and organizational measures should be taken against unauthorized forms of use, disclosure, alteration or destruction of the data

- Data use

  The main issue for "data use" is the risk that data are used for purposes other than the one for which they were originally and validly collected. In order to prevent this danger, the *use limitation principle* is to be maintained. This principle has four aspects:

  - the purpose for which the data are collected and further processed should be laid down and be (made) known to the Citizen since the beginning
  - use and disclosure of data should take place in a way compatible with the purposes for which they are collected, unless it concerns a legal obligation to disclosure or else disclosure or use with explicit consent of the data subject
  - only adequate, relevant and not excessive data should be stored
  - data should not be kept longer than necessary for the purposes for which they are collected or for which they are further processed

Conclusion: The respect of these principles are important to the citizen in order to let him understand why his personal data is needed in certain situations, why his privacy cannot remain 100% preserved and what freedom of choice he himself has. So, the code abides with the points described above and discriminates and explains how some member state should implement this code and, guarantee a high degree of acceptance from the citizens.

2.2 TLV

TLV is a very simple way to identify the correct data among a set of bytes, i.e. in byte arrays. Typically, the first byte (T) is some hexadecimal tag identifying some command or function, while the second byte (L) identifies the length of the data value (V). So, in a single byte array there may be several TLV sets and all can be easily identified and split from each other. Also, in the Value field of some TLV structures may be other TLV structures. With this technique, complex data structures can be represented in a simple way.

Encoding needs: For small vendor specific commands (i.e. like in section 2.3 for passing small byte arrays to a smart card) there is not the need to follow any specific standards, but for big chunks of data coded in TLV format (i.e. like the entire files encoded in PKCS#15 standard) where for example one byte (in the Length field)

might not be enough to represent the length of the Value field (because one byte can represent a max length of 256 bytes). Being so, a complete standard was developed with the required rules to encode large amounts of TLV data and, provide that data with meaning in order to increase performance when parsing a TLV file.

2.2.1 Abstract Syntax Notation One (ASN.1)

NOTE: The value of all eight bits of an octet can be easily and conveniently represented using a pair of hexadecimal digits, for example, $1E = 00011110$. In this case there is no need to use any tag to differentiate the two numeric bases. But this might not always be the case, and in this chapter it will also be used normal decimal notation. So, in order to unambiguously identify the proper numeric base, the tags $_{16}$, $_{10}$ and $_{2}$ will be used for the hexadecimal, decimal and binary bases respectively.

Definition: ASN.1 is a standard that specifies a set of basic encoding rules that may be used to derive the specification of a transfer syntax for values and types, and referred as Abstract Syntax Notation One or ASN.1[47].

Rules: This standard specifies rules capable of unambiguously encode/decode any piece of data. Formally, defines that the encoding of a data value shall consist of four components which shall appear in the following order:

1. Identifier octets
2. Length octets
3. Contents octets
4. End-of-contents octets[1]

Each bit in the identifier and length octets may have different interpretations. Next, is presented a small description on how the encode of this fields is made so it can encode any piece of data.

NOTE: The assumption made over the bit description (most/least significant bit, etc) is described in anex B.

Identifier octets

The identifier octets will encode the ASN.1 tag (class and number) of the type of the data value. A discrimination of this bits and their meaning can be seen in figure 2.1. The value of bits 8 and 7 identifies the class of the identifier octet (figure 2.1). For PKCS#15 data for instance, the class of the encoded data will be context-specific

[1] The end of contents octets shall not be present unless the value of the length octets requires them to be present. In this context, PKCS#15 does not require this octets.

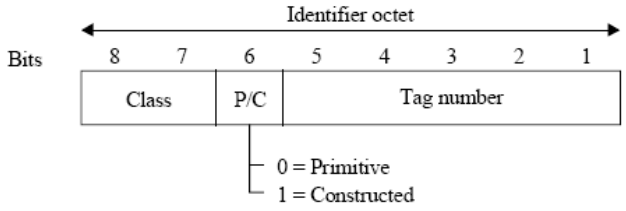

Figure 2.1: Identifier octet

(i.e. to interpret following PKCS#15 ASN.1 rules described in annex A of [33]). Bit 6 identifies if the Value field will contain primitive data (0 = Primitive) or more sets of TLV values for further interpretation (1 = Constructed). The final five bits identify the number of the tag.

Class	Bit 8	Bit 7
Universal	0	0
Application	0	1
Context-specific	1	0
Private	1	1

Table 2.1: Encoding of class tag

NOTE: With five bits, the max value of some tag is 31_{10}. If higher or equal then 31_{10} tag numbers are required, ASN.1 also specifies coding rules for this case which is by using two octets for the tag identification instead of one. But PKCS#15, which is why the study of TLV was required, does not specify any tag grater then 30_{10}.

Length octets

Like in the identifier octet (in case of the tag number is greater than 30_{10}), if a single octet would be used to represent the length of the Value field, its max length value would be 256_{10} octets long. Being so, there are two forms of specify octets, the short form and the long form.

Short form: If the length of the Value field is less or equal to 127_{10} (i.e. 01111111_2) then the short form is used, and one length octet is used to represent the length of the value field.

Long form: If the length of the Value field is greater than 127_{10}, then the first Length octet will not represent the length of the Value field, but instead will represent how

many Length octets are required to represent the length of the Value field. After identifying this number, it is possible then to interpret those remaining Length octets and calculate the length of the value field. This is managed by giving the value 1 to bit eight. The remaining seven bits will identify how many Length octets are required to express the length of the Value field. For instance, the encode of Length $L = 201_{10}$ is "10000001_2 11001001_2".

Value octets

Value octets represent the coded data. These octets can represent human readable data[2] or any other kind of data (for example, ciphered data) or as referred before, other sets of TLV values.

2.2.2 Conclusion

It was described in this section the basics for understanding sets of TLV values. In the context of the produced work, what is explained here is enough to understand how the PKCS#15 files are encoded in the smart cards. But for a full understand of the ASN.1 standard, it is required the reading of the bibliography [47].

2.3 Security Environments

A signature card may contain more than one utility key or signature key and more than one set of user reference data. The mechanisms used by cryptographic cards to manage which keys and data are to be used in some specific situation are, the entities referred as Secure Environment (SE).

Note: The main reference for this section is the manual for the Portuguese eID[18].

References: An SE defines the references to be used for secure mechanisms such as:

- Cryptographic algorithms
- PINs
- Keys (symmetric, public, private)
- Diffie-Hellman (DH) key exchange parameters
- Role IDs
- Mode of Operations

[2] If they are the ASCII code for some human alphabet characters

Use: The SEs are used in two main situations:

- To control access to a file or data object. In this case the SE specifies, both the condition necessary to access the file (one condition can be, for instance, the PIN) and, the identification of the reference of the secure mechanism (such as the reference to the PIN)
- To provide a context for signature creation, decryption and the verification of certificates. In this case the current SE specifies the keys and algorithms to use.

Several SEs: For different secure operations, SEs can be seen as the context references for specific operations. This means, that a cryptographic smart card needs to have several SEs, one for each type of operation. But at any given time, loaded in the Random Access Memory (RAM) there can only be one active SE. When the card is first connected to the reader the default SE is loaded into memory and it can be empty of contents, meaning, there are no access restrictions to the operations associated with that SE.

Structure: A SE structure is composed by tree components each of them encoded in TLV format (section 2.2) using vendor specific tags. The components are:

- The Secure Environment Identifier (SEID)
  - Number of the SE
- Life Cycle Status (LCS)
  - Created or Initialized or Operational (Activated) or Operational (Deactivated)
- One or more control reference templates

2.3.1 Control Reference Template (CRT)

CRTs define the usage of the SE. These can be:

- Authentication Template (AT) - Protects data objects by one of the following:
  - Card holder verification (PIN reference)
  - Symmetric key mutual authentication
  - Asymmetric key mutual authentication
  - Certificate verification used in asymmetric key mutual authentication
- Key Agreement Template (KAT) - Defines CA public key prior to certificate verification

- Cryptographic Checksum Template (CCT) - Protect data objects by specifying Secure Messaging (SM) with Message Authentication Code (MAC) is necessary for the command, the response or both

- Digital Signature Template (DST) - Defines the Algorithm for Public-Key Cryptography (RSA) private key and algorithm to be used when creating a digital signature

- Confidentiality Template (CT) - Protect data objects by specifying SM with MAC is necessary for the command, the response or both. Defines the RSA private key and algorithm to be used when decrypting data

Relevance: In the context of the produced work, of these templates only the Digital Signature Template is relevant. It was one of the key steps to successfully implement the section 4.2.5 algorithm and the Minimal Footprint Middleware Demonstrator (chapter 5) by, configuring the SE with the correct template containing the signature algorithm and the reference to the signing private key.

2.4 XML

In this section introduces XML. Since XML is a widely used and very developed specification, only the pertinent parts of XML (in the context of this thesis) are going to be covered and in a superficial manner. The reader interested in XML should consult the bibliography.

XML: XML is a simple, very flexible text format derived from SGML, the standard International Organization for Standardization (ISO) 8879. Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an always increasingly important role in the exchange of a wide variety of data on the Web and elsewhere[7]. It is recommended by the World Wide Web Consortium (W3C) and is a fee-free open standard[9]. The recommendation specifies lexical grammar and parsing requirements.

Usefulness: XML's set of tools helps developers in creating web pages, but, its usefulness goes far beyond that. XML, in combination with other standards, makes it possible to define the content of a document separately from its formatting. This important characteristic, makes it easy to reuse that content in other applications or for other presentation environments. Most importantly, XML provides a basic syntax that can be used to share information between different kinds of computers, different applications, and different organizations without needing to pass through many layers of conversion.

2.4.1 XML Schema

Since XML has an open format, it is very easy to write a XML string that only needs to obey the XML syntax. However, if one wants to create a XML document that needs to be worked on by several people/computers without errors, it is needed to create the "manual" for that special format. The manual used in the rest of this thesis is denominated XML Schema, and provides a means for defining the structure, content and semantics of XML documents[8].

Example: By creating the XML Schema in appendix C.1.1, it is defined the structure, content and semantics for the XML string represented in appendix C.1.2:

2.4.2 XSL Transformations

Simply put, XSLT is a language for transforming XML documents into other XML (or other type of markup language) documents by using XSLT style sheets[10].

Example: The following example is a very simple and immediate. It starts with the XML to transform in appendix C.1.3. Then it is used some XSLT style sheet (in appendix C.1.4) that obeys the original file semantics. These two strings/files are presented to some tool capable of correctly parsing the two documents and accordingly transform the first document, resulting in appendix C.1.5.

Chapter 3

Related Technologies

In this chapter, related/required technologies for the achievement of these thesis goals are investigated and analyzed.

Note: Also, present in this chapter, are other possible technologies that were studied but are not used in the final solutions or case studies. If this is the case, a comparison between the different technologies is presented, along the reasons that lead to the choice.

3.1 Smart Cards

Although not directly present in the topic of this thesis, smart cards are nonetheless one of the most important resources/technologies to study and investigate in the context of this thesis. Smart cards are the current Ex Libris when it comes to a secure computation, storage and data conveyance. Being so, it is not surprising that they are the main hardware devices used for personal secure IAS (Identification, authentication and digital signature) services and, as result they are the support for the top of the line eID solutions (as explained in section 2.1.2 point 1) across the most vanguard European countries in this field. In this section it is shown why.

3.1.1 Introduction

Some history: Security is one of the main concerns since the beginning of our societies. Starting with the early locks, these methods revealed to be ineffective, and on top of this, current every day needs are more logical/virtual then physical. Under this context, magnetic cards that are of easy and cheap production were one of the first solutions for the computer dependent world. But magnetic cards are no longer an answer to the current market needs, since any one with the appropriate (and very easy to acquire) equipment can read and write in a magnetic card, causing severe issues of fraud[20].

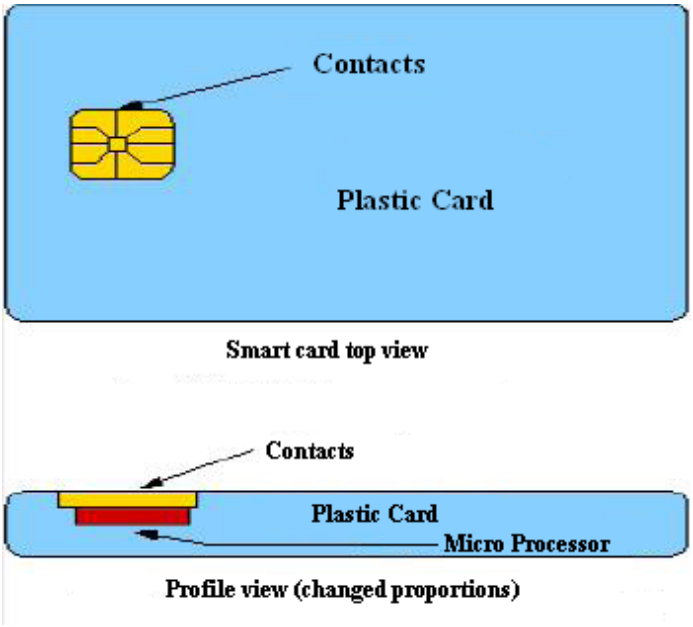

Figure 3.1: Smart card example

Combating Fraud: The current answer to this problem emerged in the end of the sixties with the introduction of a new technology, an Integrated Circuits Card (ICC) or as it became better known, the Smart Card. It has the property of being safe because its information is only visible to those who possess the correct access key[1] and remaining blocked to everyone else. Nowadays, smart cards are capable of running commands, programs and cipher/decipher information, conferring them the ability of, for instance, storing electronic money, act as credit card, storing classified medical information, stop unauthorized access to broadcast transmission by satellite or cable and increase the security of mobile phone communications[20][6].

3.1.2 Smart card description

Advantages: The interest in using smart cards derives from the several advantages they provide. One of these advantages is, undoubtedly their ubiquitous computational power. In practice, a smart card is a portable computer that fits in a wallet. Security and ease of use are other key advantages of smart cards.

Ideal of security: The processor, memory and I/O devices are arranged in an integrated circuits chip. This chip is normally embedded in a plastic casing with a

[1] This key can assume a lot of shapes, like for example, a simple PIN code to biometrics

credit card format. It is physically designed to be tampering resistant[2]/apparent[3][32] and can even benefit from a cryptographic co-processor, hence it can be used as an extremely safe storage environment for all kind of classified information, like for example, passwords, digital money, etc. As mentioned before, another important characteristic of smart cards is that their information cannot be copied without prior consent of the card owner (by providing the card pin for example). This is opposite to magnetic cards where, their information can be easily copied and used in illegitimate ways.

Achieved Security and uses: Currently, smart cards can be so evolved that they can handle authentication information such as digital certificates. Therefore (and since smart cards are tamper proof), they are a secure storage, and also an isolated processing facility, capable of using the contained information without exposing it to the host environment (i.e. a smart card is built in a way that a private key can never be read, that is, all operations that require the private key are performed by the smart card) where there may be dangerous code. This is always extremely desirable, but it takes even major proportions because, when needed, by using cryptographic means, it can correctly share its information with the pretended and authenticated target[4].

Practical example: For a practical example off smart cards flexibility, it can imagined, for instance, the everyday life of some company worker that uses his smart card to open a door, then login to his computer and later in the day use it to pay his expense in the company bar, always respecting the most strict security rules of authentication and non-repudiation.

3.1.3 Technical summary

Software security: Smart card software security is based on cryptography. Keys, certificates and even biometric information are stored as files in the card. Additionally, in cryptographic smart cards, are implemented cryptographic algorithms and protocols allowing the manipulation of those files in secure ways. These algorithms include symmetric (Data Encryption Standard (DES), 3DES, etc.), asymmetric (RSA) and elliptic curves, with the purpose of secure authentication, communication or performing digital signatures[21].

Operating System: The first smart cards operating systems cannot be compared to what we think of a classic operating system. They were more like collections of

[2]That is, given physical possesion of a smart card, it is a nontrivial task to get to the chip and even more nontrivial to extract information from the chip

[3]Or tamper evident. I.e., any attempt to compromise the card will typically leave an obvious trail that the card has been tampered with

[4]It can identify the other peer via PKI and certificate authentication and negotiate symmetric session keys for information exchange (see also point 3.1.3)

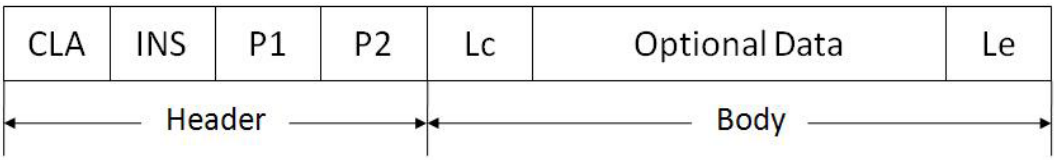

Figure 3.2: Command APDU

on-card commands to which the smart card responds. But the most recent cards are more evolved and can dynamically manipulate file sizes, or better, accept programs that were built off-card like for example the Java Card in section 3.1.5.

File system: The file system is composed by a Master File (MF) and several Directory File (DF) and Elementary File (EF) that in practice are stored as a contiguous block of memory. It is based on the ISO 7816[24] standard, so it is a single rooted (the MF) directory based (DFs that can contain EFs and other DFs) hierarchical file system in which files (DFs and EFs) can be identified by long alphanumeric names and numeric names.

Architecture: Because smart cards do not have internal power nor clock, all smart cards have to be integrated into larger systems which typically contain additional computers and data storages. Therefore and due to their mobility, the type of architecture where smart cards traits would shine the most (among many others like, for instance, storing electronic money), is in large, distributed and multi party systems where secure identity is one of the main requisites, for example, access to public ATMs, or in this thesis context, eID.

3.1.4 Communicating with smart cards

This section, provides a small explanation on how host machines can in fact communicate with a smart card.

Application Protocol Data Unit (APDU)

What are APDUs: Direct low level communication between host and card is done via APDUs. In terms of programming language code they can be translated has byte arrays that comply with rules defined in the ISO 7816-4[26] standard. There are two kinds of APDUs: Command APDUs (figure 3.2) which are sent from the host to the card, and Response APDUs (figure 3.3) which are the card mandatory response to the commands[5].

[5]The host plays has master, by sending commands, and the card as slave, by returning answers

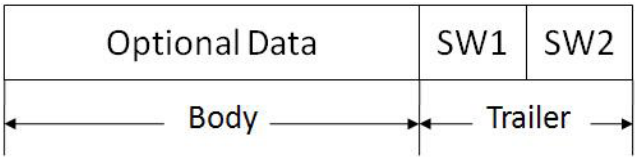

Figure 3.3: Response APDU

Command APDU: A command APDU is composed by the following:

- One class (CLA) byte. Identifies the instruction class, like for instance, if it is an ISO or proprietary instruction, or even if it's using any security conditions
- One instruction (INS) byte. Along with the CLA byte, the INS byte identifies the pretended command
- Two parameters bytes (P1 and P2). They are used to pass specific parameters to the command
- One length (Lc) byte. It states how long is the optional Data field. I is set to 0_{16} if the command does not require a Data field
- A set of bytes with length determined by Lc representing the information passed to the card by the command, for example, the hash required to perform a digital signature
- One response length (Le) byte. It specifies the length of the expected answer (Response APDU) from the card CLA, INS, P1 and P2 are the command APDU header and they are always present, the remaining bytes are the body

CLA, INS, P1 and P2 compose the command APDU header and they are always present, the remaining bytes are the body.

Response APDU: A response APDU is composed by the following:

- An optional set of bytes with length specified in the Command APDU Le byte. Contains, for example, signed data
- Two status bytes. Together they identify the result of the command (success or some error code) as stated in ISO 7816-4[26]

Communication protocols T=0 and T=1

T=0: T=0 is a byte oriented protocol (i.e. a byte is the minimum unit of information transferred across a channel and the error handling is done one byte at a time). It is used in smart cards since their creation. The Global System for Mobile

communications (GSM) card is probably the best known application of this protocol. It has a simple implementation but subsequently, it can not be completely separate between the transport layer and the application layer. As shown previously in this section, to a command APDU always follows a response APDU (even if it only caries the success of the the command APDU). So, when issuing a command APDU there is always the need to also call the GETRESPONSE command. This is the result of an attempt to make the protocol as responsive as possible, in order to make the communication between the card and the reader as efficient as possible. Consequently, in the T=0 protocol, the error handling and the application protocol support are optimized to minimize the amount of information that flows across the reader-to-card interface and, thereby to minimize the transaction times.

T=1: With protocol T=1, after receiving a command APDU, the card automatically sends the response APDU. So it efficiently separates the transport layer from the application layer and it is suitable for safe transaction between host and card. Nontheless, it increases the complexity in asynchronous transfers when it comes to error handling and also might increase the application waiting time, since the card might require more processing time than usual for some operation (for example, complex cryptographic operations). This waiting time may also happen because T=1 on the contrary to T=0 is a block-oriented protocol. This means that blocks of information of variable size are moved between the card and the reader as a single unit of information. Moving information in a block, however, requires the block to be error free causing the error handling to be more complex with this protocol[6].

Higher level communication: Higher level software exists (normally provided by the smart card vendors) in the form of libraries that encapsulate several APDU commands in order to hide this low level layer from developers and provide easier use of the smart card functionalities[7].

Answer to Reset (ATR)

What is an ATR: Nowadays, smart cards use one communication protocol or the other or even both (in this case, giving the choice to the developer of which protocol he intends to use). But being able to use one protocol does not mean it can recognize or use the other. So, to unambiguously identify a card and its communication protocol the first thing a card does when it powers up (when inserted into the reader) is transmit to the host its Answer to Reset (ATR). The ATR is a special APDU and, besides identifying the communication protocol, it is also the card fingerprint, which means, that every card model from some vendor has a unique ATR. The ATR is specified in ISO 7816-3[25].

[6]Most used techniques, such Longitudinal Redundancy Check (LRC), and Cyclic Redundancy Check (CRC), are for error handling, being more complex than using simple parity check (i.e. in the protocol T=0)

[7]For example a PKCS#11 standard (section 3.3.4) implementation

3.1.5 Java Cards

Java Cards in particular, are not the main scope of this project, but with an eID applet they can also be used has a regular eID smart cards. Therefore, this section provides a very superficial insight to Java Cards.

What is a Java Card: A Java Card is a smart card that on top of the operating system has a running Java Virtual Machine with the respective Java Runtime Environment. The Java Card was a major advancement to smart cards. It brings the Java language perks to the smart card world. Among other things, it allows a card to:

- Contain and run several Java Applets (Java Card programs)
- Exception handling
- Object creation/manipulation/deletion
- And finally, the multi platform philosophy from Java was imported to the cards, that is, the Java Card is a public specification which means vendors can implement their own Java Cards following that specification. So, any developer who creates a Java Card Applet knows it is going to work on any Java Card from any vendor (restricted only to the correct Java Card Specification version)

Restrictions: The Java Card (and any other smart card for that fact) scarcest resource is memory. As result, only a very small subset of the java language is available (for example, integers are present but strings are not). This has to be taken into account by the developer.

3.2 ECC

This section will introduce the ECC (European Citizen Card). It will provide some background on the National Identity Cards (ID), how they can be embedded in smart cards (eID) and finally what is the standard defined by the Comité Européen de Normalisation (CEN) so the several and different countries eIDs can integrate with each other (ECC).

Note: The contents described in this section were studied by the Author for STORK (section 1.2) in the context of this project. They are also present in the deliverable 3.2.3 [38] of the STORK project.

3.2.1 ID and eID

National ID Card: A National ID card is issued by a government or some agency to a citizen of the respective country. This document confirms the identity of a

citizen and proves his legitimate nationality and residence. All the information regarding the citizen is physically visible in the card, so the focus of an ID card is visual identification.

National eID Card: In the context of National Identification, an eID is a card with visible and invisible security features and a secured microprocessor, i.e. a smart card chip and is supposed to act (but not mandatory) as an inter-European travel document and facilitate logical access to e-government or local administrative services.

Advantages of the eID smart card: By embed a smart card chip on a National ID card all the advantages of smart cards seen in section 3.1 are now available, being the most important the security gains, since a smart card processor is virtually impossible to be counterfeited[8]. For this reason, the card can now, for instance, carry the biometric data of the citizen in a secure and invisible way. Other important advantages of mixing smart cards and National ID are[15]:

- eID smart chip technology protects the individual's privacy while securely assuring their identity by using PIN codes or biometrics
- eID's proven security increases confidence in a national credentialing system
- Using eIDs does not require on-line access to central databases as citizen verification and identity authentication is performed off-line
- Virtually impossible to counterfeit, the eID provides a strong countermeasure against Identity theft
- eID's digital signatures contribute to the accountability of government officials and employees
- eID's enable citizen's authentication and accountability
- An eID reduces government expenses by eliminating multi-claim benefit fraud

3.2.2 The ECC standard

As mentioned in this section introduction, some countries have developed their eID projects following different approaches[9], emerging the need for interoperability between the solutions already implemented (or in final stages of development). And in a next phase create common grounds for every European parts involved in eID. And so the adoption of the ECC standard (which addresses this kind of issues) is being taken into account by STORK (section 1.2).

[8] As discussed in section 3.1.2

[9] For example the future German eID card[11] and the Latvian eID card[57]

The ECC: As defined in [2], the ECC is a smart card issued under the authority of a government institution or an entitled private organization, either national or local, and carries credentials in order to provide all or parts of the following services:

- Verify the identity
- Act as an Inter-European Union travel document
- Facilitate logical access to e-government or local administrative services

Besides the mandatory standard definitions, it also allows and defines how to implement extra and context specific information relevant to some country or authority. This information will only be available to those authorities without interfering with the normal ECC eID procedures.

Technical Specification

The technical specifications for the European Citizen Card (ECC) are described in a set of four documents partly based on the ISO/International Electrotechnical Commission (IEC) 24727 specifications. These documents are denominated "Identification card systems - Europe Citizen Card - Parts 1 to 4"[2][3][4][5].

Description of Part 1[2]: Part 1 specifications describe the physical and electrical characteristics of the ECC, defining identity justification with emphasis on remote civil service procedures and remote public services. The last ones requiring the generation and/or verification by the ECC card of electronic signatures and electronic certificates.

The requirements described in this part of the ECC specification are used to:

- Define a plastic body card with associated physical and logical securities
- Specify the electrical interface and data transport protocols for the ECC
- Support the basic set of identification and authentication elements visible at the card surface

Description of Part 2[3]: Part 2 specifications describe the logical characteristics and security features at the card/system interface for the European Citizen Card. It has the objective of ensuring the interoperability at he card/system interface in the usage phase and is also compliant with ICAO 9303 specification (Machine Readable Travel Documents).

The ECC is a smart card with Identification, Authentication and electronic Signature (IAS), therefore in this part of the specification:

- The supported services are specified
- The supported data structures as well as the access to these structures are specified

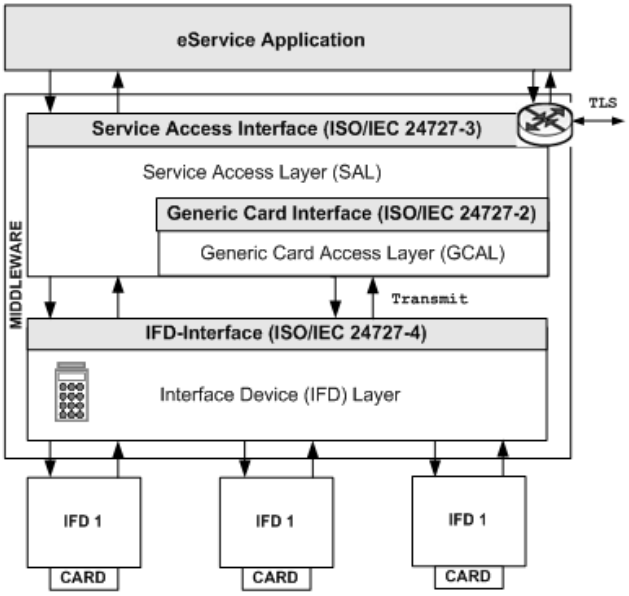

Figure 3.4: Middleware Architecture

- The command set is defined

Always having in mind the interoperability objectives described above, the services supported by the ECC include:

- IAS services compliant to prEN 14890 part 1[22] and part 2[23]
- Biometric on card matching
- Command chaining
- Role authentication

Summarising: This part of the specification has the goal of ensuring the interoperability at the card/system interface in the usage phase[3], i.e. the directory file structure and the services supported by the ECC (the set of mandatory and optional extensions) are defined as well the APDUs required to access them.

Description of part 3[4] - The middleware: Part 3 of the ECC specification provides an Interoperability Model (i.e. the middleware architecture, image 3.4). This model enables a Personal Computer (PC) client application compliant with the technical requirements to interoperate with different implementations of the European Citizen Card.

The Interoperability Model is developed as follows:

- Picking up where part 2 left, part 3 of the ECC provides additional technical specifications for a middleware architecture. This middleware, in its turn, provides an API (the Service Access Layer (SAL) API based on ISO/IEC 24727-3[30]) for some PC client application access the ECC IAS services
- A standard mechanism for the validation of the eID credential stored in the ECC and retrieved by the eService

In order to support the IAS services, this part of the standard also specifies the following:

- A set of mandatory and optional requests to be supported by the middleware implementation
- Data set content for interoperability to be personalized in the ECC

The Service Access Layer (SAL) API: As mentioned in previous sections, the ECC SAL API is directly based on the ISO/IEC 24727-3. ECC part 3 strictly follows ISO/IEC 24727-3[10]. To better understand the role of the SAL API, it will be provided a simple overview of the Service Access Interface that can be seen in Figure 3.4. The Service Access Interface is composed by the Generic Card Access Layer (GCAL) and the SAL:

- The SAL is in charge of interpreting the requests addressed by the client application to the card via a high level API. The SAL translates the requests in terms of sequences of APDUs that are sent out to the underlying abstraction layer (the GCAL). This translation is performed according to the rules defined by a set of interoperability data reflecting the rules governing the card-applications.

  The SAL generates on the fly these interoperability data out of the ISO/IEC 7816-15[27] information available in the card. This ISO/IEC 7816-15[27] information is either provided within the CardApplicationServiceDescription data, or within the DF.CIA[11] file, or both.

  Upon invocation of some method of the SAL API from the PC client application, the SAL may surface the return data to the PC client application.

- The Generic Card Access Layer (GCAL) is in charge of translating the APDU handed on by the SAL in terms of APDU understandable to the smart card.

  This translation is applied according to the rules defined in the Application Capabilities Descriptor (ACD) and/or in the Card Capabilities Descriptor (CCD) templates[12].

[10] And also ISO/IEC 24727-2[4][29] for the GCAL

[11] For example, the DF.CIACS#15 is the directory where certain system EFs must be stored for PKCS#15 profiles. See section 3.4 for PKCS#15

[12] Describes how to format the information in a way the card is capable to read

These templates are read out of the card by the GCAL. The GCAL performs a bootstrap mechanism upon card detection in order to retrieve the ACD and CCD containers from the card. The bootstrap operation is the first step of the discovery mechanism[13].

It maximizes the interchangeable capabilities of several independent implementations of its prescriptions. This property of this part of ISO/IEC 24727 is realized by positing a minimally sufficient subset of the base standards which realizes their core functionality through the minimization of the number of options provided.

The GCAL functionality is specified in part 2 of ISO/IEC 24727 series[29].

Description of part 4[5][15]: A card used as ECC can have different primary applications[14]. Being so, part 4 specifications have recommendations for ECC issuance, operations and use for the different applications intended for the card.

Profiles: Along with each use case, it also identifies a subset of the technical requirements for that specification from ECC part 1 (the interface and transport protocol) and part 2 (services) and considers the operation of the ECC in its particular environment. Each profile thereby is linked to a distinct Object Identifier (OID)[44] to be used as interoperable reference, e.g. to ease the discovery of the card's and/or application's capabilities.

Adding profiles: More profiles can be included or existing ones can be updated, so it is also specified a profile template so any country can have the option to define its own profiles in a comparable and compatible way to the existing ones.

3.3 STORK project studied technologies

Note: The technologies researched in this section were intended for the STORK project. It will also be included in each technology in particular, a critical analysis having in mind the goals for the Minimal Footprint Middleware Demonstrator which it is described in section 5.4.

3.3.1 PC/SC

Note: Belongs to layer 2 of the Minimal Footprint Middleware Architecture (Refer to chapter 5).

[13] I.e. the mechanism (set of steps performed) that is going to identify a card
[14] For example, ID card or health card

PC/SC[60] is a well disseminated standard. It was created by the PC/SC Workgroup in order to provide the necessary interoperability that enables the effective use of smart card technology in computer-based applications. This motivation arose because the use of smart cards on computers was hampered due to the lack of interoperability at various levels/layers, like for instance[58]:

- The solution to fix the interoperability problems of interfacing different cards from different vendors at the application level led to increased costs for both the level of development and the maintenance of the software
- The lack of a high-level API that enables the encapsulation of the basic features of the cards.
- Lack of implemented mechanisms that allow resource sharing of a smart card by several applications. These mechanisms are impossible to develop without the existence of an accepted standard

Due to these requirements, the PC/SC standard for smart cards was developed by several cooperating companies in order to create a standard for communication/manipulation of smart cards. Later, several others IT and smart card leading companies joined the PC/SC Workgroup.

Analysis

Due to the significant global presence of the companies (Microsoft, current Gemalto, Toshiba, etc.) involved in the development of this standard, it has rapidly become the most used standard for communication with smart cards.

Its most important layer, the Resource Manager[59] is native to most modern Operating Systems (Windows, Mac OS, and UNIX/Linux) so it is also platform independent.

At this model layer level, it is the most widely spread and mature solution.

3.3.2 ActiveX

Note: Belongs to layer 4 of the Minimal Footprint Middleware Architecture (Refer to chapter 5).

ActiveX[43][41] (formerly known as Object Linking an Embedding (OLE) controls) from Microsoft, is a technology developed for resource sharing between applications. It can be used, for instance, to share a Microsoft (MS) Excel graphs with MS Word.

ActiveX, or better, ActiveX Control uses several programmatic elements to interact efficiently with a control OLE container and with the user[40].

The technology is Microsoft's answer to Java Applets (section 3.3.3) in a way that it can be automatically downloaded and executed by the Internet Explorer Web browser[41].

Unlike Java Applets, however, ActiveX controls have full access to Windows. This gives them much more power than Java Applets, but with this power comes a certain risk that the ActiveX control may damage software or data on the machine. To control this risk, Microsoft developed a registration system so that the IE Web browser can identify and authenticate an ActiveX control before downloading it[42].

Another concern with ActiveX is the fact that it's only compatible to Microsoft systems/solutions by default (Windows, IE), and for Mac OS with IE for Macintosh. Microsoft is planning on support UNIX based systems also[16][37].

Analysis

ActiveX is a very powerful technology. The unlimited access to the computer resources makes it extremely flexible but also dangerous.

It is not browser independent (supported by IE and a few others through plug-ins only), which causes severe limitations when it comes to a multiplatform/multi-browser solution.

There is support for Mac OS but that support is intrusive as users might not be willing to install IE or other browsers in their systems. For UNIX/Linux the support is in a planning stage at the moment and not readily available yet.

3.3.3 Java Applets

Note: Belongs to layer 4 of the Minimal Footprint Middleware Architecture (Refer to chapter 5).

A Java Applet[52] is a program written in the programming language Java that can be included in an HTML page in the very same way as, for instance, an image can be included. If the used Internet browser has the necessary plug-in to execute the Applet embedded in some Web page, the Applet code (i.e. a .jar file) is downloaded and executed by the Java Virtual Machine (JVM) integrated in the browser.

They are used to provide interactive possibilities/characteristics to Web applications that could not be accomplished by HTML alone.

Since Java Applets are available in byte code[51] (in the .jar file), they are also platform independent. But since the required plug-in[54] to run the Applets needs to be installed in the browser, they become instead browser dependent. Although the plug-in is readily available and can be easily installed in most of the current browsers (IE, Firefox, Opera, Safari, etc.) it is not a default characteristic of them.

Like other technologies that run in a browser (Microsoft Silverlight, Adobe Flash)[15], Java Applets are executed in a sandbox[56]. With the user permission it can run outside that sandbox and access system resources, like for example smart cards.

[15]These technologies were also researched and analyzed, but not by the Author

Analysis

Due to the possible integration in most of the commonly used browsers (after the installation of the plug-in), a Java Applet is platform independent. It can also be executed (with the user permission) outside the context of the sandbox.

Being embedded in HTML, Java Applets are very easy to be manipulated and configured, and passing parameters and options through the HTML is very simple.

The main disadvantages of a Java Applet comes from the performance side. The first time an Applet is accessed it has to be downloaded and the VM has to be started. This is not required in subsequent accesses to the Applet, because the Applet stays cached in the system and the VM is already started.

Further, the required download and installation of a plug-in in the browsers is a disadvantage regarding the minimal-footprint constraints.

3.3.4 PKCS#11

Note: Belongs to layer 3 of the Minimal Footprint Middleware Architecture (Refer to chapter 5).

The Public Key Cryptography Standards (PKCS) are a set of specifications produced by the RSA labs in cooperation with developers of secure systems of the entire world. The purpose was to speed up the implementation of public key cryptography[36].

These documents are so important that many of the specifications defined in them became in fact real standards like for example S/MIME and SSL.

One of these specifications is PKCS#11 - the Cryptographic Token Interface Standard. It specifies a platform independent API denominated Cryptoki for devices capable of processing and storing cryptographic information (e.g. cryptographic smart cards)[34].

This API follows a simple object based approach (i.e. the information stored inside the device is treated, for example, like a normal Java Object). The API was developed always having in mind the technology independency, resource sharing and presenting to applications a logic and common perception of smart cards.

PKCS#11 defines the most commonly used cryptographic objects to be stored in a smart card (RSA keys, X509 certificates, DES/Triple DES Keys) as well as all necessary functions to create, alter, and delete those objects.

With PKCS#11 any developer can create and manage his cryptographic objects in any arbitrary way. This creates portability problems for applications. To avoid this problem, the PKCS#15 standard[35] (chapter 3.4), basically representing a standard for file structures, was developed by RSA. Due to this standard, applications that are PKCS#15 aware can communicate with any card that is implemented following PKCS#11 and PKCS#15 standards.

Analysis

At the moment, PKCS#11 is the *de facto* standard in use for any cryptographic token. It was thought to be platform independent and although Cryptoki is a C implementation, PKCS#11 is so well disseminated and accepted that wrappers exist in most currently used languages (e.g. Java, Python, etc.).

This acceptance and almost total platform (and programming language) independency are huge advantages of PKCS#11.

The need to implement PKCS#15 in order to achieve application independency is one of the disadvantages of this standard. Another disadvantage is the fact that for several card vendors the developer will need the dynamic link libraries implementations of PKCS#11 for each particular vendor. In case the developer has access to those libraries and can correctly identify the card in question, this is no longer a problem although is still problematic when it comes to a Minimal Footprint Middleware.

3.3.5 OpenSC

Note: Belongs to layer 3 of the Minimal Footprint Middleware Architecture (Refer to chapter 5).

OpenSC[45][46] offers a set of libraries and utilities for smart card access. Its main focus is on cards that support cryptographic operations and ease their use in security applications like e-mail ciphering, digital authentication, and digital signature.

It implements the PKCS#11 API so it's available to any application that supports this standard and has the particularity of also implementing the PKCS#15 standard (refer to Section3.4). Thus, it aims to be compatible to any application that is PKCS#15 aware.

Since OpenSC follows the PKCS#11 standard, all considerations about PKCS#11 apply to OpenSC as well. Additionally, the characteristics of PKCS#15 also applies to OpenSC.

This technology is available as a C++ implementation on all main platforms (Windows, Mac OS, and UNIX/Linux) and already supports a high number of different cards from different manufacturers. This means that there is no need to load different DLL files during runtime for the supported cards.

One extra that comes with OpenSC is the fact that its API allows low level communication with PC/SC in a simplified manner. It supports APDU communication in a higher level of abstraction than the PC/SC technology, especially if we think that C++ is considered by some persons to be close to a low level programming language.

Analysis

OpenSC is already used in smart card middleware architectures of several countries, like Belgium (eID), Germany (German ID Cards), etc. This is because it counters the disadvantages of PKCS#11 by implementing PKCS#15 and has native support for several cards.

It encapsulates simple APDU communication, which increases the development level if we think in C++.

The main disadvantage comes from the fact that it is not programming language independent, it's implemented in C++ (current version is 0.11.6) and there are not any good wrappers for it. OpenSC is also available for Java but its underdeveloped comparing to the C++ version (current OpenSC for Java version is 0.2.2).

3.4 PKCS#15

Some of the cards the Author used during his work were PKCS#15 compliant and formatted. Being so, an extensive study of this standard was required for the intended manipulation/access to this cards.

Note: Only the cryptographic data defined in PKCS#11 can be stored in PKCS#15 format on the card. There is no standard for normal data files (for example, the citizen public data like name or birth date). These must be accessed via APDUS whose format can be consulted in documents provided by the card vendor and by the issuer.

What is PKCS#15: PKCS#15 is another standard from the RSA Labs[33]. In the context of secure identity tokens, e.g. smart cards, their use was hampered by the lack of industry standards for storing a common format of digital credentials (keys, certificates, etc) in them.

The need for PKCS#15: Solving this kind of interoperability problems at application level leads as usual to increased costs in both the development and maintenance, not to mention for the end user that get's tied to some particular application. For applications this is also a problem, since without a standard they are not able to share the required digital credentials. So, without an agreed-upon standard for credential sharing, acceptance and use of them (both by application developers and by consumers) would be limited. Therefore, it was developed in a manner that supports a variety of operating environments, application programming interfaces and broad base applications[16].

Features: PKCS#15 was developed with the above considerations in mind, so its main features are:

[16] the same case as PC/SC (chapter 3.3.1)

- Platform independency
- Vendor independency
- Application independency

Example: An initialized card in PKCS#15 format and containing a digital certificate should be able to be read by any application in any host.

Specified characteristics: To achieve this kind of goals, PKCS#15 specifies a file and directory format for storing security-related information on cryptographic tokens with the following characteristics[33]:

- dynamic structure that enables implementations on a wide variety of media, including stored value cards[17]
- allows multiple applications to reside on the card (even multiple eID applications)
- supports storage of any type of objects (keys, certificates and data)
- support for multiple PINs whenever the token supports it

3.4.1 How it works

The mandatory PKCS#15 information is read from the token/smart card when it is presented to the system. This information is used by the PKCS#15 interpreter (which is part of the software environment) to identify the PKCS#11 objects and data. The PKCS#15 information is stored under the DF(PKCS#15) with File Identifier (FID) 5015 under the token's MF. It contains the following files:

- Authentication Object Directory File (AODF)
  - Optional EF with information about authentication objects known in the token
  - FID - Decided by application issuer
- Certificate Directory File (CDF)
  - Optional EF with information about certificates known in the token
  - FID - Decided by application issuer
- Data Object Directory File (DODF)
  - Optional EF with information about data objects known in the token
  - FID - Decided by application issuer

[17] Uses the ASN.1 standard for basic encoding rules of data (section 2.2)

- Private Key Directory File (PrKDF)
  - Optional EF with information about private keys known in the token
  - FID - Decided by application issuer
- Public Key Directory File (PuKDF)
  - Optional EF with information about public keys known in the token
  - FID - Decided by application issuer
- Secret Key Directory File (SKDF)
  - Optional EF with information about secret keys known in the token
  - FID - Decided by application issuer
- TokenInfo
  - Mandatory EF with generic information about the card
  - FID - 5032
- UnusedSpace
  - Optional EF used to keep track of unused space in already created EFs
  - FID - 5033
- Object Directory file (ODF)
  - Mandatory EF with information about all the other DF's known in the token and described in the previous points
  - FID - 5031

Browsing files: Knowing this info, the PKCS#15 aware applications can easily and automatically navigate in the card and interact with the desired data objects. The format of this files are all described in the PKCS#15 standard[33].

3.4.2 Performance issues

In practice, regular communication speeds between the host and the card are on the order of 9600 Bits Per Second (bps) or a little more than 1 Kilo Bytes Per Second (KBps). So, communicating with a smart card is generally a slow process. The added read/write operations required by the PKCS#15 protocol make it more cumbersome than the normal and direct access to card files. Also, and as a practical example, the certificates in a PKCS#15 formatted card are all in the same file. Instead of reading just the pretended certificate, the host needs to read all the certificates and then interpret the information in order to access the required certificate data.

3.4.3 Conclusion

With PKCS#15 is provided a comprehensive set of rules and data format to store information and navigate on the card having access to just a couple of mandatory files to start with, mainly the PKCS#15 DF and the ODF file. But unlike regular binary files, PKCS#15 files can't be just read and translate their bytes to the corresponding letter. They have to be interpreted according ASN.1 rules[18] and following the PKCS#15 structure format defined in annex A of [33].

3.5 Graphical Interface Technologies

One of the requirements for the new middleware proposed in this thesis is a dynamic GUI that adapts itself depending on the presented eID. A study of several GUI tools was then performed in order to identify the most suitable one. The methods used were the ones used in a common way nowadays, i.e. search engines and specialty forums[19]. Several prerequisites were drafted, mainly:

1. Total Operating System independency (or at least in the 3 main platforms - Windows, Linux and Mac OS)
2. GUI building interface
3. Automatically adapt to the look & feel of the running Operating System (OS). This may cause some problems in some tools. The most significant are:
   - System tray on the different OSs
   - Application menu (mainly in Mac OS X)
4. High Level (more design, less code)
5. XML plays the main part in terms of configuration for the eIDs recognition. So, a peculiar goal is that the tool can build its GUIs from a XML file
6. Preferably, the solution must support the Java programming language[20]
7. Known applications

Candidates: The research came up with too many tools to list. However, with the help of several forum communities, a filtering was done to select the most mature and promising ones. These are:

- FLTK (pronounced Fulltik)

[18] I.e. a set of TLV values. Refer to section 2.2

[19] The research was exhaustive, and definitely no major solution should have escaped the Author investigation

[20] This point it is not mandatory, but it is to be taken into account since in MULTICERT Java is the main programming tool.

- wxWidgets
- QT (pronouced Cute)
- Swing/AWT/SWT

analysis: Each one of these tools is going to be analyzed and confronted with the prerequisites stated above.

3.5.1 FLTK

The Fast Light Toolkit (FLTK) is a cross-platform C++ GUI toolkit for UNIX/Linux (X11), Microsoft Windows, and MacOS X. FLTK promises modern GUI functionality in a light way and supports 3D graphics via OpenGL and its built-in GLUT emulation. FLTK is designed to be small and modular enough to be statically linked, but also works fine as a shared library. FLTK also includes a GUI builder called FLUID[17].

Prerequisites evaluation:

1. FLTK is independent of the operating system
2. FLTK has a UI builder called FLUID
3. Version 2.0 of FLTK will have native look & feel. However, current stable version is 1.1.9
   - References to system tray icon with FLTK only refer to platform specific solutions
   - Not tested
4. The FLUID tool provides some high level GUI building capabilities.
5. GUIs are built from C++ files
6. There are no known wrappers for Java
7. Some applications
   - ITK-SNAP - Which is an open-source software application for medical image segmentation (`http://www.itksnap.org/pmwiki/pmwiki.php`)
   - Nuke - A piece of high-end digital compositing software[21]
   - EDE - The Equinox Desktop Environment (`http://equinox-project.org/`)

[21] `http://www.thefoundry.co.uk/pkg_overview.aspx?ui=CBC2593A-2C9F-4EF9-84BE-C198B0171453`

Extra features: FLTK is intended to be lightweight, with low memory usage while providing advanced GUI building. From this, it is possible to statically link the developer code with the graphical library of FLTK without a significant increase on the application deployment size. This allows for the easy distribution of the software without the requirement of installing graphic libraries on the target machines.

Conclusion: FLTK is a promising solution. However, it still has some drawbacks (not accepting XML, there are no wrappers for Java, etc.). Nonetheless, it remains still as a possibility that is going to be counter analyzed with other solutions.

3.5.2 wxWidgets

wxWidgets lets developers create applications for the intended platforms. It can be used from languages such as C++, Python, Perl, and C#.NET. wxWidgets applications have native look and feel because it uses the platform own native controls rather than emulating them. It is also extensive, free, open-source, and mature[61].

Prerequisites evaluation:

1. wxWidgets is independent of the operating system
2. wxWidgets has several GUI builders, however, none is deployed together with the wxWidgets packages
3. wxWidgets supports native look & feel
   - Supports system tray icons
   - Correctly adapts the application menu to the Mac OS environment
4. Several possible GUI builders might hinder the easy learning of the tool (because the is not a standard one)
5. No references found about creating a wxWidgets interface through a XML file
6. There are no known wrappers for Java, although they exist for other languages
7. Some applications
   - BitTorrent - Famous peer-to-peer file sharing application (`http://www.bittorrent.com/`)
   - FileZilla - FTP client (`http://filezilla-project.org/`)
   - TortoiseCVS - Famous CVS client (`http://tortoisecvs.sourceforge.net/`)

Conclusions: wxWidgets is another promising solution. Main drawbacks are the lack of wrappers in Java and does not accept XML as a GUI building option. It is going to be counter analyzed with the other solutions.

3.5.3 QT

QT is present for over 14 years and is in constant development. It is a cross-platform application and UI framework. It includes a cross-platform class library, integrated development tools and a cross-platform IDE. Using Qt, it is possible to write applications once and deploy them across many desktop and embedded operating systems without rewriting the source code[48].

Prerequisites evaluation:

1. QT is independent of the operating system
2. QT provides a multi-platform stand alone GUI builder that can be integrated with Eclipse in any platform and particularly in Windows with .NET
3. QT supports native look & feel
   - Supports system tray icons
   - Correctly adapts the application menu to the Mac OS environment
4. QT is very easy to understand, further, QT has excellent support for developers, via its active community and huge set of online examples and tutorials
5. QT graphic object files are in fact XML files. The GUI builder translates all object visually represented on the screen to a XML hierarchy representing what is being displayed
6. QT was fully "wrapped" to Java. The name of the tool is QT Jambi.
7. Some applications
   - Google Earth - 3D mapping, satellite imagery integrated with Google search (`http://earth.google.com/`)
   - Lucas Film Ltd - Lucas Film is using Qt to develop their cross-platform digital entertainment software (`http://www.lucasfilm.com/`)
   - KDE - a popular desktop environment for Unix-like operating systems (`http://www.kde.org/`)

Conclusion: Given its development/evolution time, QT is one of the most complete multiplatform GUI development tools in the market. If fits almost perfectly the prerequisites list.

3.5.4 Swing/AWT

If one thinks about GUI designing in Java, it is easy to think in the classic Java solutions. AWT[53] and Swing[55]. Each of these solutions has it pros & cons, but with some degree of effort (less after Java 6.12) they can be used together. Therefore, and in order to include all Java GUI capabilities. After these solutions are presented they will be analyzed like if they were only one.

AWT: The Abstract Window Toolkit features the core foundation of the Java SE desktop libraries, i.e. it comes standard with every version of Java technology. It includes only GUI components defined for all Java host environments. Using only AWT it is guaranteed full multiplatform compatibility.

Swing: Swing is built on top o AWT, providing more graphic components, usability, native and custom look & feel. However, also the complexity of the technology is increased when compared to AWT and cross platform development. Nevertheless, Swing is highly efficient when programming in multiplatform. However, it requires extra care in multiplatform tests.

1. AWT/Swing are Operating System independent
2. Several important third party GUI builders exist
3. AWT/Swing support native look & feel
    - Supports system tray icons
    - Correctly adapts the application menu to the Mac OS environment
4. For someone who understands Java, AWT/Swing is easy to learn. The support community is the Java community, making it one of the biggest development support communities
5. Usage of XML as a GUI builder might be possible using third party software. This is not however an immediate step
6. AWT/Swing are Java language native technologies

Conclusion: AWT/Swing is a very complete solution. The only point it misses is the fact it does not natively supports XML files as a way to build the UI.

3.5.5 Assessment

Looking at this section conclusions, only QT fulfills all the required points (AWT/SWING come close). All GUI case studies and final proof of concept application (chapter 6) were developed using QT, Java, and XML.

3.5.6 QT Revised

Since QT was the elected tool, a closer analysis on its architecture and how it works in practice is made in the following points. It is also analyzed, how by passing a XML file to the QT Java Loader class, this file can be instantiate at run time a QT GUI object, allowing the generation a dynamic GUI interfaces.

QT Objects

The best way to learn the QT objects is by designing some simple interfaces that use those objects. This is where the GUI designer comes handy. One can draw the objects and then analyze the generated XML output.

The QT XML Schema is available online from the QT web site[48]. After analyzing the generated XML files and by looking at the XML schema, a developer can then manually (and later automatically) create his own XML file that represents a QT GUI.

QT events

One problem that arises when generating a GUI is how to handle events. For instance, if one has several separation tabs, how can they be differentiated and consecutively create different events over them? Using the tabs example, imagine there is defined in the GUI XML[22] a container for tabs named "*tabWidget*" i.e.:

$$< widgetclass = \text{“}QTabWidget\text{”} \ \textbf{name} = \text{“}tabWidget\text{”} > ... < /widget >$$

With this information and by parsing and navigating through the XML file it is possible to make the following Java call:

$$QTabWidgettabWidget =$$

$$(QTabWidget)window.findChild(QTabWidget.class, \ \textbf{name}^{23});$$

Now, one has access to the object representing the container for the tabs and can create an event over it that is triggered when selecting the contained tabs, i.e.:

$$tabWidget.currentChanged.connect(this, \text{“}isProtectedEvent()\text{”});$$

Where "*this*" represents the local class and "*isProtectedEvent()*" is a method implemented in the local class. Using this technique, any time a tab is selected under "*tabWidget*" the method "*isProtectedEvent()*" will be executed.

[22] For now, the origin of this XML file is unimportant

[23] Notice in the previous XML line that "name" is also in bold. This is how a specific object name is identified. In this case is "*tabWidget*"

Conclusion

The functionality described above is exactly what is intended for the final solution. Being so, QT is the selected GUI development tool.

3.6 Java

Java is the preferred programming language for any solution proposed in this thesis. This programming language is chosen not because there aren't other programming languages that also would produce desirable solutions but because Java is part of MULTICERT culture. Being so, Java is directly accepted as a technology for the final solution without a study of pros & cons.

Chapter 4

Case Studies

This chapter will describe the intermediate work produced in the context of the proposed objectives. The work topics described here are not final solutions, but each one of them is part of it or somehow contributed to it. They can be for example be seen has integrable software modules, that, when put together would form a complete system.

4.1 Connecting to a smart card

This section will give a quick overview on how to connect to a smart card. The steps required are trivial, but any application requesting smart card access has to perform them.

1. PC/SC deamon must be running in the OS
2. Connect to the PC/SC Resource Manager [59] and get its handle
3. List the available readers using the Resource Manager handle
4. Select one of the readers and get it's handle
    - Here several automatic enhancements can be made, for example, create threads for each of the available readers and block the threads waiting a card insertion
5. Connect to a card in the reader and get its handle
    a) The card handle is used to communicate with the card itself
    b) Using the card handle, identify the card (using the card ATR for example)
    c) If its the pretended card, do the intended operations until the end or the card is removed and move to the next step. If it is not the pretended card, move directly to the next step.

6. Use the card handle to disconnect the card

    - Even if the card is removed, the Resource Manager will send error codes that can be used to close the broken connection. This is a good practice, because even if this step was not made, the Resource Manager will accept new connections to that card on the same reader

4.2 Portuguese eID

The Portuguese eID smart card contains all the relevant information of the citizen to who it was issued to. Some of this information can be visually seen in the card plastic body, while other is stored in the smart card chip and can only be addressed with the properly formatted APDU commands. Some of this information is public information, like for example, the name. But other types of information might be private, like for example the citizen address to which a PIN has to be presented. This section discriminates what kind of operations were successfully implemented and explain their particular issues. It will be exposed in a structured algorithm fashion, describing the required steps with the relevant notes to each point.

Pertinence: In order to create a GUI that displays the data contained in some eID, it is necessary to access that data. Also, to create a middleware that is independent from the vendor[1] of the smart cards, it is required to know how to access the data and communicate with the cards. This is the topic addressed and solved in this section.

Note: All operations are performed via low level APDU commands. These commands were studied from the smart card Operating System manual. It was a relevant effort to understand how to apply them and in which context they can be used, i.e. with secure or without secure messaging, with or without PIN, or even with or without Secure Environments configuration. The specific APDUs are not discriminated in the algorithms.

Note: The communication between host and card is correspondingly of master and slave, i.e. the host sends a command APDU and the card answers with a response APDU, which will be labeled respectively "C:" for command APDU and "R:" for response APDU. Host software operations are labeled "H" for Host.

Note: In this algorithms descriptions, it will always be assumed a command was performed with success. So the mandatory response APDU that the card returns to the host will be omitted. The response APDU will only be discriminated if it carries relevant information on its body (refer section 3.1.4). It will also be assumed, that

[1] Who normally provides proprietary tools to access the intended data

the card connection steps described in 4.1 were successfully made and the host has the correct card handle.

4.2.1 Public Data

This is the most basic algorithm that is smart card aware and capable of communicating with the Portuguese (PT) eID.

```
Entidade Emissora = República Portuguesa
Pais = PRT
Tipo de Documento = Cartão de Cidadão
Numero do Cartao = 11586403 2 YO1
PAN = 6046320000487772
Versao Cartao = 001.001.11
Data Emissao = 07 08 2007
Local Pedido = PAC Cedros
Data Validade = 08 01 2012
Apelido = da Conceição Ávila
Nome Proprio = Paula Andreia
```

Figure 4.1: Public Data

1. C: Select the public information file through its FID
2. C: Command to read the file
3. R: Content of the file
    - The single file read contains all the public information (name, gender, photograph, etc), which needs to be accessed on the right positions inside that file (next point)
4. H: Read the information from the correct file positions
5. H: Print the information (example with some data: figure 4.1)

4.2.2 Address Data Reading

This algorithm is very similar to the last one, but with the added step requiring from the user the address PIN.

1. C: Select the address file through its FID
2. H: Read the address pin from some input device
3. C: Select the PIN file
4. C: Pass to the card the PIN for validation

```
Pais de Residencia = PT
Distrito de Residencia = 11
Descricao do Distrito de Residencia = Lisboa
Concelho de Residencia = 1106
Descricao do Concelho de Residencia = Lisboa
Freguesia de Residencia = 110639
Descricao da Freguesia de Residencia = São Domingos de Benfica
```

Figure 4.2: Adress Data (test card)

- If the validation was a success the host can now read the address file. Else the address file is still blocked for reading

5. C: Command to read the address file
6. R: Content of the file
   - The single file read contains all the address information (street, number, zip code, etc), which needs to be accessed on the right positions inside that file (next point)
7. H: Read the information from the correct file positions
8. H: Print the information (example with some data: image 4.2)

4.2.3 Notebook Writing

The notebook writing is similar to the address reading, in the sense that the notebook file is also protected by a PIN. But instead of a read operation on the file, it will be performed an update operation

1. C: Select the notebook file through its FID
2. H: Read the authentication pin from some input device
3. H: Read the data to write on the notebook from some input device
4. C: Select the PIN file
5. C: Pass to the card the PIN for validation
   - If the validation was a success the host can now update the notebook file. Else the address file is still blocked for reading
   - The file could be directly updated, leading to the loss of all the previous saved data. Else it can be read first and then append the current content with the new content and finally update the notebook. Other approaches can be used
6. C: Update the notebook file

4.2.4 Certificate Reading

Since a certificate is also a public object, the necessary steps to read it are quite straightforward like the public citizen data (section 4.2.1). The only changes is the processing of the read bytes. In this case they can be used to instantiate for example, a Java Object representation of a PKI certificate.

4.2.5 Digital Signature

Performing a digital signature on a smart card can be more or less complicated depending on the implemented security features and requirements. In the PT eID several preparation steps are required besides executing the actual signing command. It is required to prepare and configure the signing Secure Environment (refer to section 2.3), insert the signature PIN and also get the hash value of the data that is going to be signed.

1. H: Read the signing PIN from some input device
2. C: Pass to the card the PIN for validation
3. If it's the correct PIN proceed
4. C: Load/restore the signing SE
5. H: Create a TLV byte array with the SE configuration
    - Reference of the hash algorithm
    - Reference of the signing private key
        - Although we know the reference of the private key, the card never allows it to be accessed by the host[2]. The reference is just an indication of the key that is going to sign the data, since a smart card can hold several private keys
6. C: Update the SE
7. H: Digest the data to be signed in order to get the hash
    - The digest algorithm must be the same as the one indicated in the updated SE
8. C: Send the hash to the card
9. C: Perform the digital signature
10. R: Read the signed data from the card

[2]It is built this way, there are no software workarounds to access the private keys

4.2.6 Conclusion

Since these small software modules are intended to be vendor software free (i.e. without using vendor proprietary libraries) there is the need to implement these modules via low level APDU control. Being so, it is required an intensive study and knowledge of the card and operating system capabilities and file organization.

4.3 PKCS#15 Compliant Smart Cards

With a PKCS#15 card the process of exploration and access to the card files is no longer dependent of some manual provided by the card vendor. But to benefit from it is required a greater understanding of the protocol in order to create automatic mechanisms of navigation/manipulation of the card.

NOTE: To fully understand this section, it is required the reading of sections 3.4 and 2.2. Also, the automatic piece of software responsible for decomposing and interpreting the TLV values of the PKCS#15 files it is not implemented, but through visual and manual decomposition following the ASN.1[47] and PKCS#15[33] specifications, the required values are easily identifiable.

NOTE: The acronyms used in this section are all described in the acronyms list and explained in section 3.4

Steps: In a simplified manner, here are the required steps to read a certificate from a card:

1. Select the mandatory PKCS#15 DF with FID 5015
2. Select the mandatory PKCS#15 EF ODF with FID 5031
3. Read the ODF from the card
4. Interpret the ODF and get the FID for the PKCS#15 EF CDF
5. Read the CDF from the card
6. Interpret the CDF and get the FID for the certificate EF
    - All the certificates will be inside the certificate EF. The developer needs to know which certificate he wants to get. So, there is always the need to at least know some of the context on how the card is going to be used to access the correct certificate
    - Security issues are also solved because, for instance, the certificates to which the CDF EF points can be associated with some PIN object that needs to be validated

7. Read the certificates EF
8. Interpret the read data and access to the pretended certificate
9. The read certificate is also in ANS.1 notation, so it also needs to be interpreted in order to extract the required bytes and instantiate the (for example) corresponding Java Object that represents a certificate

Chapter 5

Minimal Footprint Middleware

The Minimal Footprint Middleware was one of the author tasks (in concrete, the Portuguese eID integration on the demonstrator). Its main goal is to be an eID recognition software that should be capable of running in any Operating System with minimal requirements when it comes to other software's/libraries dependencies.

Note: This chapter is based in the deliverable 3.2.5 [39] of the STORK project co-authored by the Author of this thesis. All the technologies referred in this chapter are described and discussed in that deliverable. Being so, some of those technologies are discussed and mentioned in this chapter without the proper discussion or introduction to them. If this is the case, those technologies were investigated by one of the Author partners in the STORK project.

Why: Nowadays, most of the commonly used middleware solutions are implemented in the form of ordinary software that has to be installed on the user's local computer. Although this approach is working satisfactorily, this kind of middleware implementation is far from being ideal. The fact that additional software needs to be installed and maintained in order to be able to use smart card enabled applications is a handicap that reduces the usability of these applications significantly.

Goal: The goal of this study is to investigate different approaches that could be able to remove this barrier and to make future middleware approaches more usable. Ideally, the resulting middleware approach should fulfill the minimal-footprint criterion, i.e. it should be applicable without requiring the user to install any additional components. Furthermore, in order to provide a solution for as many users as possible, the final middleware approach should also be platform and browser independent.

Smart card aware applications architecture: Typically, smart card aware software architecture is composed by four layers. These four layers can relate to the Open

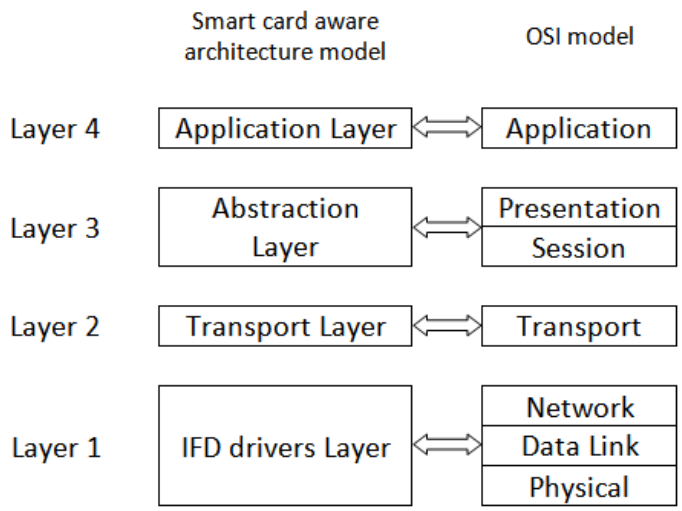

Figure 5.1: Smart card aware application model and OSI model

Systems Interconnection (OSI) model seven layers model[1] (figure 5.1). In terms of meaning, the bottom layer represents the vendor specific drivers of the card reader normally provided by the card reader vendor (or even by the Operating System). Next, is the transport layer, where the data from the top layers is sent to the card in a specific low level format (i.e. APDUs. Refer to section 3.1.4). The next layer is a higher level abstraction of the transport layer, where the required commands from the top and last layer (the application layer) are processed and converted into Transport layer data. Finally the top layer is some application that is intended to be smart card aware.

Considerations: Having in mind this model and the multi platform minimal footprint middleware demonstrator objectives, some layer context dependent considerations can be made:

- Layer 1: There will always be the need to install a driver for the card reader, this can be manually by downloading from the vendor or automatically installed by the OS
- Layer 2: Analyze solutions for layer 2
  - Refer to section 3.3
- Layer 3: Analyze solutions for layer 3
  - Refer to section 3.3

[1] much in the same way we compare TCP/IP and OSI model in the networks area

  - Being an abstraction layer this level can be suppressed, leaving to the application layer the handling of the low level card commands. This option as the advantage of requiring less components but adds to the development and maintenance costs

- Layer 4: The only application present in all current OS's that comes ready to use and can provide high quality visual interfaces are Web Browsers
  - New consideration. Browser dependency
  - Analyze multi-browser software solutions
    * Refer to section 3.3

5.1 Smart Card Abstraction Technologies Review

This section will provide a critical analysis between concurring (i.e. at the same model layer) of the analyzed technologies. It tries to scrutinize which technology has advantages over the other. This section refers to the smart card technologies, which were investigated by the Author. The web browser related technologies scrutiny was investigated by another member of the STORK project.

PC/SC: We start by looking to PC/SC before all the other technologies. This is because PC/SC is not in any way a competing technology of the remaining studied smart card abstraction technologies. It is in fact a lower layer (compared to the other technologies) of the complete architecture (and practically the unique option on that level). The other studied technologies all depend on PC/SC to access the smart cards placed on the readers. They can be seen as an encapsulation and automation of PC/SC API calls and they make the use of PC/SC transparent to the developer when it comes to cryptographic object manipulation.

Concurring technologies: Moving to the other technologies, which are in fact competing with each other, they can be classified in three kinds: the Proprietary solution, the Standard and the Open Source Implementation of the Standard.

The proprietary solution (CSP/CNG from Microsoft) is the less capable technology in terms of fitting the described middleware requirements. Not because it's not a good technology but because it does meet the established requirements of platform/browser independency.

Thus, the solution has to be based on a standard that is widely accepted and freely implemented in all platforms. According to the analysis of the section 3.3, it turns out that PKCS#11 or some technology that implements it, seems to be the most appropriate solution. Together with OpenSC, PKCS#11 may be combined with other layers technologies in order to benefit from diverse synergies.

OpenSC is a PKCS#11 open source implementation with additional low level controls that allow the direct transmission of APDU commands to the cards. Since

not all objects contained in smart cards are necessarily cryptographic objects defined in PKCS#11, the simplified C++ API of OpenSC allows a direct communication with the PC/SC layer allowing the direct manipulation of DFs (directory files) and EFs (Elementary Files, used to store for example public data in a smart card). It also has the big advantage of supporting PKCS#15, automatically storing the cryptographic objects in the cards according to that standard. The limitation of OpenSC comes from the fact that it is programming language dependent, since there are no known wrappers for it in other programming languages. Contrary, for the PKCS#11 C API named Cryptoki there are a lot of good tools to interact with it in a lot of programming languages.

5.2 Possible MFM Architecture

The different technologies that have been analyzed (in sections 3.3.1, 3.3.2, 3.3.3, 3.3.4, and 3.3.5) and compared to each other (in Section 5.1) can be combined in order to obtain synergies that may be used for the development of minimal-footprint middleware architectures. The most promising synergies that were studied by the Author are described and analyzed in this section in order to reveal their pros and cons.

5.2.1 Java Applets and OPenSC

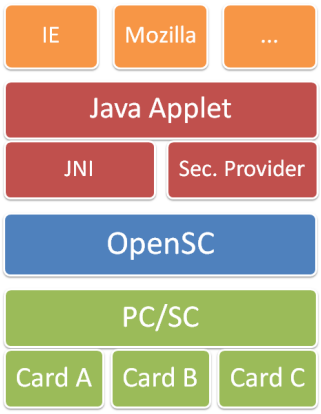

Figure 5.2: Java Applet over OpenSC architecture

This architecture (figure 5.2) is ideally platform/technological independent. To be precise, it is compatible to all platforms that are able to provide support for Java and PKCS#11 (via OpenSC API) and also provides PKCS#15 which further improves technological independency, comparing to a PKCS#11 only approach. But, besides requiring the installation of the Java Runtime Environment, there is no wrapper for OpenSC in Java, which would lead to a greater development effort plus the

installation of the OpenSC libraries which starts to become somewhat cumbersome for a minimal footprint middleware.

5.2.2 ActiveX and Javascript

By combining a mixed approach of ActiveX and JavaScript, two of the nowadays most used browsers (IE and Mozilla based browsers) can be included in this architecture. But other browsers would not be capable of smart card access as the already mentioned ones, and even the Mozilla based ones would have serious access limitations due to JavaScript very strict sandbox environment[2]. Introducing OpenSC instead of PKCS#11 in the third layer allows benefiting from advantages provided by PKCS#15 as well as low level control of APDU commands. However, OPenSC cannot solve the main problems of this approach which is located in the top layer.

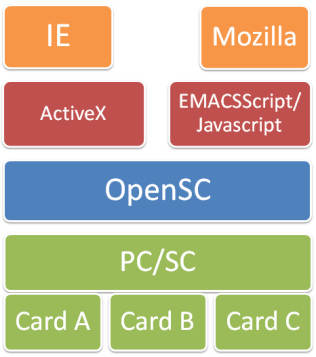

Figure 5.3: Java Applet and ActiveX architecture

5.3 Conclusion

The success of an eID middleware depends on several criteria. One of the most important is the degree of acceptance that is shown to the provided solution by the users. The acceptance itself depends mainly on a relation between functionality and cost. In this case, cost can be seen as the number of steps required for a user to install and run the middleware on his machine. Being so, these steps shouldn't depend on the browser or operating system that is being used by someone, and although Microsoft Windows based operating systems are widely spread throughout the entire world, there are a number of alternative platforms that have to be supported in order not to discriminate a certain group of citizens. So, besides Microsoft based systems, support for at least the most significant competitors must be present (i.e. for MacOS and UNIX based systems). Also, for the different Operating Systems there are a variety of browsers, which usually differ in the features they actually

[2]Conclusion reached by the Author partner

support. Thus, offering a browser based solution of an eID middleware that is compliant to all browsers is as important as providing a multi platform solution. Finally, the usability of some software product begins at installation time. So, this is why the solution being elaborated is denominated minimal footprint middleware, i.e. as less components as possible should be installed in the target system.

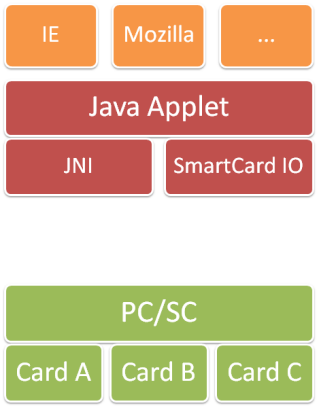

Figure 5.4: Java Applet Solution

The solution: Having in mind this points, and after the analysis conducted throughout this section, it can be seen that there is no solution that is able to completely satisfy all the requirements. All proposed technologies/architectures show some benefits but also drawbacks. So a minimal loss commitment has to be made. So the final proposed architecture can be seen in figure 5.4. This architecture relies on the use of the Java Applet technology in order to guarantee browser independency. Additionally, it has no abstraction layer, i.e., the applet communicates directly with the card via PC/SC interface. This decision increases development time since low level coding is required, but no additional components need to be installed (no need for vendor specific PKCS#11 libraries or even OPenSC). For the end user, the only drawback comes from the fact of requiring the installation of the Java Runtime Environment (JRE) (but this step is already a common for many users worldwide).

5.4 Demonstrator description

As a proof of concept, it was implemented a Minimal Footprint Middleware Demonstrator based on the previous section architecture description (section 5.3).

Goal: The demonstrator will collect some data passed by the user and perform a digital signature on it. For this, it uses the algorithms defined in sections 4.2.4 and 4.2.5.

Description: The final version demonstrator is available on line[3]. It presents a home page (figure A.1) where the user can input some string and digitally sign it. For this, the user needs to give the browser Authorization to download and run the Java Applet, since this requires access to the Operating System Resources (refer to section 3.3.3) as can be seen in figure A.2. Next, the demonstrator will be downloaded into the system cache and execute. So, the next step must be insertion of the card by the user. At this stage, the applet blocks waiting for a smart card insertion as seen in figure A.3. If the card is not supported the corresponding page is presented (figure A.4). If the card is supported and identified, the flag of the country whose eID corresponds is shown. The required signing PIN is also requested (figure A.5). Finally, if the PIN is correctly introduced a page is shown with some relevant data regarding the digital signature (figure A.6).

[3] `https://apps.egiz.gv.at/middleware-demo/`

Chapter 6

Multiplatform Common and Adaptive Middleware

In this chapter, the first point of the proposed objectives (section 1.4) of this thesis is addressed. A small proof of concept application was developed using the technologies studied in the previous sections. These include XML (section 2.4), XML Schemas (section 2.4.1), XML Transformations (section 2.4.2), QT (sections 3.5.3 and 3.5.6), Java (section 3.6) and the case studies for the Portuguese CC (section 4.2). The next points in this chapter explain the synergies of these technologies and, how they allow the creation of a Multiplatform Common and Adaptive Middleware solution, that might be used to interact with different eIDs from different countries.

Note: In chapter 5, the middleware approach used in this chapter is described only has "satisfactory". However, the STORK solution (described in chapter 5) will only be available on the long run and is intended to be a common solution for all European members. The proposed solution in this chapter is a Portuguese specific solution with the Portuguese specific interests (whatever they may be) in mind. In this case, the classic middleware approach (used in this chapter) is still the best solution.

Contributions of the chapter: As described in the beginning of this chapter, this is one of the proposed objectives of this thesis. It is an important part of the Author/MULTICERT joint collaboration in order to find a replacement solution for the currently existing Portuguese Middleware solution. The current solution is working fine for the Portuguese eID. However, it has some disadvantages. The main ones, arise from the fact that only supports the Portuguese National eID. Also, it is not easily expansible in order to accept new eIDs. The solution for the new Portuguese Middleware proposed in this chapter, intents then, to be as reliable and robust as the current solution, while addressing and fixing its main drawbacks.

Relevance inside the thesis: It is important to remember that this chapter is one of the key points of this thesis. As explained before, many of the addressed concepts and technologies described in the past chapters, are used together here. This specific work is therefore the culmination of many previous chapters and sections of the body of this thesis.

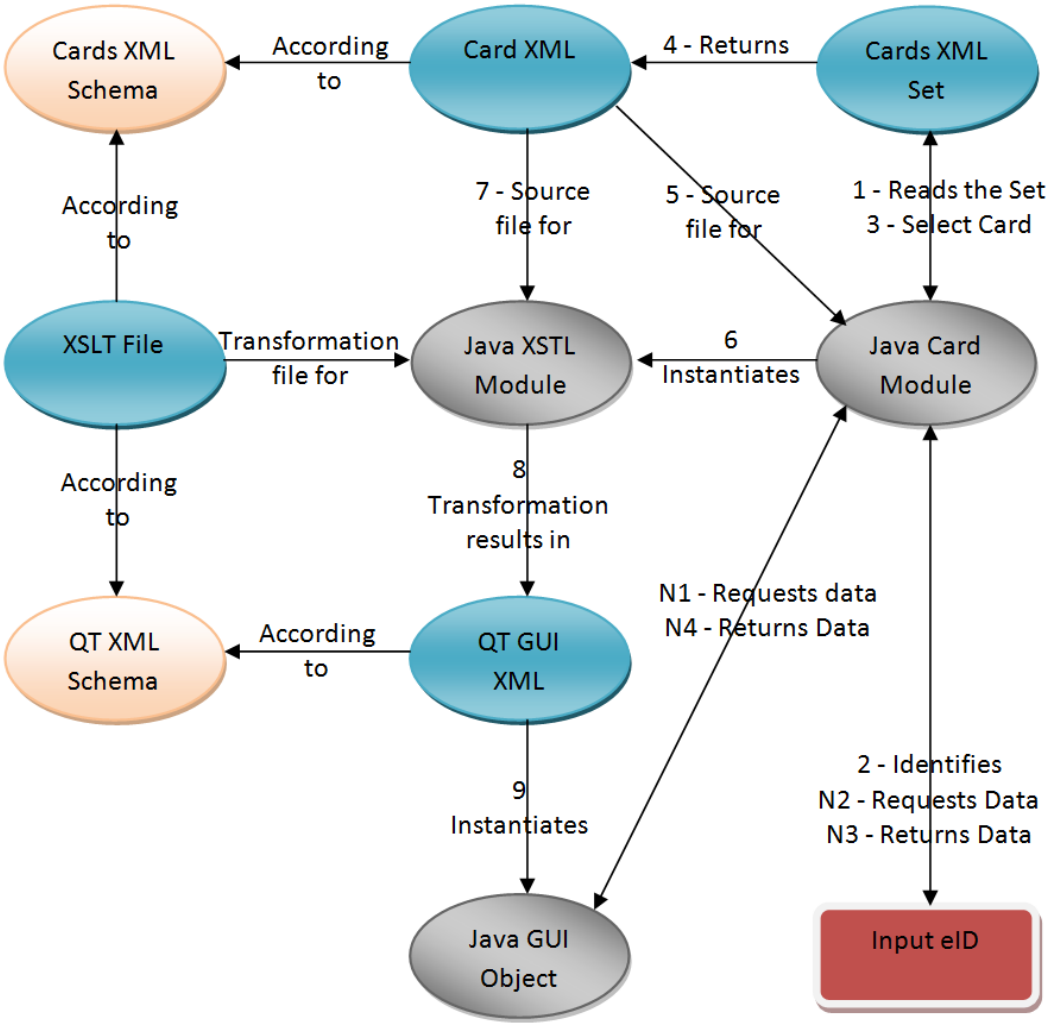

Figure 6.1: Architecture

6.1 Planning

The planning and concept of this solution was drafted in meetings with the MULTICERT responsible parts and with the presence of the Author. It followed a brainstorm format where ideas were noted (like for example, using XML to create

dynamic GUIs) and then investigated on their feasibility, being this part left for the Author. The Author investigated these ideas and completed some small proof of concepts applications. The final result was a final proof of concept application and the design of the architecture depicted in figure 6.1 and described in section 6.2.

6.2 Architecture

Figure 6.1 shows the different components/modules composing the complete middleware software solution (including the XML components). The easiest way to explain the architecture workings is by first explain the part each module takes in order for the whole to work. Finally will be explained how each of these parts communicates with the others in order to allow the dynamic adaptation of the GUI and the flow of data between the eIDs and the GUI.

Multiplatform: Notice that the planned architecture in figure 6.1 is built on multiplatform technologies and tools. This fulfills the multiplatform requirement.

6.2.1 Software Components

In this section, each architecture component is described:

- **Cards XML Schema:** The XML file containing the schemas that allow the creation of eIDs profiles. To come up with a final file that encompasses all the possible eID configurations is probably the hardest task to implement in this architecture. At some point, a commitment between the total data contained in an eID and the most relevant data will have to be made (stick to general data, avoid specific data that might not be present in any other eIDs).
- **QT XML Schema:** The QT Schema is the only component of the architecture that was not designed by the Author. It is designed by QT Software [48] and describes all GUI objects the QT technology is capable to graphically represent.
- **Cards XML Set:** For each eID there is a XML file that acts as that particular eID profile. When new eIDs are introduced, a new XML eID profile file needs to be created and added to this set.
- **Card XML:** Represents one eID XML profile. This profile is built according to the Cards XML Schema. It specifically contains instructions on data location (in the eID), how to access it and how to graphically display that data.
- **XSLT File:** The XML Transformation file is another sensitive part of this architecture. It has to obey the rules of two XML schemas. The Cards XML Schema and the QT schema. More precisely, it must be capable of transforming a XML file obeying the Cards XML Schema into a XML file obeying the QT XML Schema for a correct graphic display of the desired data.

- **Java XSLT Module:** This Java software module takes two inputs, the CARD XML representing the eID and the XSLT FILE. It outputs the QT GUI XML file representing a QT GUI.
- **Java Card Module:** This Java module is automatically built to support the data types described in CARDS XML SCHEMA and reads the selected CARD XML profile. It first identifies the eID using the profiles in the CARDS XML SET and selects the proper profile[1]. Using the selected profile information it can communicate with the eID. The profile also "teaches" the JAVA CARD MODULE how to communicate with the JAVA GUI OBJECT.
- **QT GUI XML:** XML file representing a QT GUI generated by JAVA XSLT MODULE according to QT XML SCHEMA. It is used by the JAVA XSLT MODULE to instantiate the JAVA GUI OBJECT.
- **Java GUI Object:** The graphic GUI itself that is presented to the user of the middleware. By user commands it requests eID data to the JAVA CARD MODULE and when in its possession graphically displays it for the user.
- **Input eID:** The eID present in the system that is going to be handled by the middleware.

6.2.2 Software Components Communication

In figure 6.1 besides the software/XML modules it is also described the communication sequence (via numeric characters) inside the architecture that allows for the "all" to work. This sequence is explained presently:

1. JAVA CARD MODULE gets the complete set of the several XML eIDs profiles from the CARDS XML SET.
2. The JAVA CARD MODULE searches in that set the profile corresponding to the Input eID and identifies it.
3. After the identification of the eID the correct XML profile is selected.
4. This step is symbolic, it represents the return of the selected profile
5. The selected profile will be the source of meta information for the data contained in the eID.
6. The JAVA CARD MODULE instantiates the JAVA XSLT MODULE
7. Next, the JAVA XSLT MODULE using the selected eID profile and the XSTL File, the JAVA XSTL MODULE performs the transformation of the profile file.
8. The profile file is now a QT GUI XML file

[1]The most immediate way to identify an eID (if we think in smart cards) is through its ATR.

9. The JAVA XSLT MODULE, using the generated file instantiates a new JAVA GUI OBJECT.

Communication: Client - Java GUI Object - Java Card Module - eID: The process of interaction between the client and the eID is performed after the client requests some function (display of data for example) from the middleware via the Java GUI Object. Then:

- **N1** - Via some event, a method requesting eID data on the JAVA CARD MODULE is triggered.
- **N2** - The JAVA CARD MODULE requests the data from the eID.
- **N3** - The eID returns the data.
- **N4** - The JAVA CARD MODULE fills the GUI with the returned data from the eID.

6.3 Conclusion

This proof of concept strongly indicates the path for a final and official version of the middleware. The Cards XML Schema part of the architecture of the middleware requires however, some more study and considerations. At the writing of this thesis, the Author is performing a new technical study on the STORK partner's eIDs solutions. This study although not in the wing of this thesis will encompass information like, cards capabilities and contained information and how to access it. When ready, should prove to be a valuable tool for helping the construction of a complete and extendable CARDS XML SCHEMA. Also, several tweaks can be made on the existing architecture, mainly the JAVA CARD MODULE should be split in more modules in order to increase the modularity independence of the proposed architecture.

Results: Although this solution it is not a final one, it definitely proves the concept and demonstrates the steps required for achieving the final and desirable solution. Screen shots and a XML profile can be found in appendix D.

Chapter 7

Porvoo Conferences

In the Porvoo Group conferences several countries (mostly from Europe) presented their situation and evolution regarding the status of their National eID plans or, implementations or, any other kind of eID supporting infrastructure. As referred in previous sections, the Porvoo Group started its conferences in April 2002, being the last conference (until the date of writing) in October 2008. Between the third (May 2003) and fourth (September 2003) conferences, it was published the eID White Paper [13] which (as explained in section 2.1.2), aggregates the current situation regarding several countries eID implementations and, their respective support infrastructures. In this chapter, the Porvoo Group conferences after the release of the eID WP (from the fourth until the fourteenth, considering that it was not updated since its release in June 2003) are going to be analyzed and, their results and countries evolutions are going to be discriminated. The Porvoo Group Home Page [19] points to all the different conferences web pages regarding the specific conferences where all pertinent documents studied and bibliography for this section can be found.

Pertinence: When implementing/analyzing a solution for some kind of problem, it is of the utmost importance to gather as much information as possible about that problem. In the context of this thesis, the idea is to identify the problems and status of the current situation of eID in Europe. However, the eID WP survey is outdated and no other survey of the same kind exists. The Porvoo Group has in its web pages important presentations from the several European country official representatives regarding eID. Therefore, it becomes automatically the source for the survey presented in this chapter which, intends to update the eID WP and provide other kind of conclusions discussed in the end of the present chapter.

7.1 Notes

This set of notes is important for the reader to understand the approach used on the study of the Porvoo Group conferences.

	Country	City	Date
1	Finland	Porvoo	April 2002
2	Ireland	Dublin	November 2002
3	Norway	Oslo	May 2003
4	Paris	France	September 2003
5	Estonia	Tallinn	May 2004
6	Italy	Rome	November 2004
7	Iceland	Reykjavik	May 2005
8	Belgium	Brussels	October 2005
9	Slovenia	Ljubljana	May 2006
10	Finland	Porvoo	November 2006
11	Portugal	Coimbra	May 2007
12	Italy	Grosseto	October 2007
13	Norway	Hurtigruten	April 2008
14	United Kingdom	Cardiff	October 2008

Table 7.1: Porvoo Group Conferences

Note 1 - Contexts: There are two contexts regarding eID cards described in this chapter. First, the "National eID" refers to a National Identification Document regarding some country and which the Citizen uses to prove his identity inside and outside the relevant country. Since the document is an eID, the National eID also allows the identification and authentication of the Citizen in order to grant him access eGovernment and eServices. Second, "eID" refers to some Electronic Identification Document that might allow access to some eServices and eGovernment but does not act as a full Identification Card inside or outside the issuer country. Some times and to have a cleaner text the "National eID" will be referred only as "eID", but depending on the context it should be easy identify the type eID which was referred.

Note 2 - Continuity: Again and reminding that the eID White Paper already presented the updated status until the fourth Porvoo Group conference, the introduction to each studied country (i.e. any country that presented at some time an update on the Porvoo Group Conferences) starts with the summarized eID WP conclusions regarding that country. These conclusions relate to the PKI infrastructures that supports some kind of eID.

Note 3 - Approach: For a better idea on how the several countries evolution regarding eID developed, each update from some particular country will be individually analyzed and posted under the respective conference point, under the respective country point. The date of that conference can then be seen in Table 7.1.

Note 4 - Time line: When using terms like "current" under some conference point, the term "current" refers to the current time of that particular conference point. For example, if some conference took place in the second semester of 2007 and the following expression is stated: "currently there are no cards issued", this expression refers to the situation in the second semester of 2007 and might not be already valid, for example, for the first semester of 2008.

Note 5 - Participants: The participants are all the countries that at some time presented their updates on the Porvoo Group conferences or are referenced in the eID White Paper [13].

Note 6 - Future work: The work conducted in this chapter is based on the eID White Paper and in the Porvoo Group conferences. It only covers the countries that are committed with these initiatives. It would be useful to identify other countries with any kind of eID approach and do some analysis on their situation. That however is reserved for future work.

7.2 Country updates

In this section, the eID study on the several Porvoo Group conferences is made. A quick list discriminating the level of participation of each country can be seen in Table 7.2.

7.2.1 AICF - Asia IC Card Forum

The Asia IC Forum is a body similar to the Porvoo Group established in 09 June 2004. The focus of the AICF is on the Asian countries. The forum expresses its vision as "*One Card, One Asia*" and consists of China, Japan, Korea, Singapore and Thailand. The group seeks to promote the interoperability of electronic identity and, the so-called Tourist Card.

Note: Japan is individually present in the Porvoo Group conferences, so its situation will not be discussed in this section, but instead, in its own section.

Eighth Conference

Having in mind the Group motto "One Card, One Asia" a pilot is being prepared for Jeju Island located in South Korea. It will be a multipurpose card for transports and payment using eID.

China: The Golden Cards project started in 1993 from bankcards and. expanded to telecom, social welfare & security, urban public transport, ID cards, etc. Currently, China is still deploying its Citizen ID Card. In 2008 the deployment should be complete with 900 million cards issued.

Country	First Conference	Number of Presences
Austria	1	6
Belgium	1	11
Estonia	1	12
Finland	1	8
France	1	4
Germany	8	3
Greece	1	1
Iceland	4	2
Ireland	1	3
Israel	1	2
Italy	5	4
Japan/Asia	7	6
Latvia	1	2
Netherlands	1	2
Norway	2	6
Poland	13	1
Portugal	8	3
Slovenia	2	3
Spain	2	4
Sweden	1	6
Turkey	14	1
United Kingdom	2	7
United States	7	6

Table 7.2: Countries Present at the Porvoo Group Conferences

Korea: Korea issued its National ID in 1968. In 1995 the New Residents Card Project intended to launch a smart card based ID. This ID should also integrate the: Driver License, Health Insurance Card and National Pension Card. This project failed due to the public opposition. A new National eID is currently under study, aiming to be interoperable with AICF and ISO standards.

Singapore: Currently, there is work on specifications and standards for a passport with Biometric and ePassport/ID functionalities.

Thailand: A smart card ID project is underway with PIN, finger print biometrics and certificates.

Ninth Conference

The continuing works of AICF include the assembly of a Task Force Team to establish a new Committee for eID Studys and ePassaport interoperability. The Tourist Card Project is launched. Main goals is interoperability. Possible use cases are planned in sectors like transportation, ePayment, insurance, etc.

China: The issuance of the National ID continues. The new ePassaport project is in a technical feasibility study phase and its issuance should start in June 2008.

Korea: The new National ID project in Korea is titled National Identification Card Project. It will allow identification both offline and online, easier access to public services and introduction of highly secure technology.

Singapore: The Singapore Standard for ID (SS-ID - Version 0.95) will be based on ePassaport Standard.

Thailand: The Thai smart card ID project is capable of: certification (offline), biometric authentication (offline), eServices without PKI (online), provide access to healthcare services, act as ePassaport and eBorder pass.

Tenth Conference

An agreement was reached regarding a rough direction for the eID Work Group. The first plans are to:

- Understand other areas trend (eg. other Asia, EU, USA,)
- Discussion for rough scheme of eID
- Cooperation with Asian governments for the expansion of eID activity (Conversation and Promotion) through the meetings and conferences.
- To promote the eID in Asian area for "One (eID with) Card, One Asia".

China: No relevant updates.

Korea: No relevant updates.

Singapore: No relevant updates.

Thailand: No relevant updates.

7.2.2 Austria

Austria is from the start a very active country in the Porvoo Group Conferences. Has presented its national updates in six occasions.

eID WP

Austria started the Citizen Card project in November of 2002 under the name Bürgerkarte under a voluntary basis. At this time, the Bürgerkarte defines the minimum requirements from an eGovernment perspective and, is based on open standards and interfaces in order to allow free expansion and adaptation to new emerging technologies. Full IAS is supported and the certificates for the signatures are issued by private sector certification service providers. The identity link (data structure linking the citizen unique ID in the Central Residents Register to the citizens certificates) is signed by the Ministry of the Interior during issuance of the certificates.

Fifth Conference

The Austrian government put into force eGovernment laws (March 2004) and by-laws (April 2004) regarding the National eID. At this time, Austria already had started mobile signatures and had issued 60.000 student cards. Several interoperability tests were performed with success with the Finish and Italian cards. Austria guarantees high quality in privacy and data protection in cross application and, in cross border use of its National eID. With the eID, Austria offers electronic service of documents, instant ePayment, Rapid eGovernment and back office functionalities.

Sixth Conference

Austria divided this update in two. First presented an overview of the Citizen Card initiatives and its status. Second, the response to the Porvoo Group questionnaire issued for this conference.

Overview of Citizen Card initiatives and status: Austria identified and described the several smart cards that work as "citizen Card". The National eID (which is under discussion because Austrian citizens are not obligated to possess/carry any ID document[1].), the health insurance card and the bank account cards, along some use cases, description of the security layer and technology neutrality. Austria concludes, that all citizens will have more than one eID by the end of 2005 and, citizens can chose whether to activate the eID functions.

Porvoo Group Questionnaire: Due to the implementation of several Citizen Cards for different purposes in Austria, it was hard for the country to answer the questionnaire. Even so, Austria describes its current situation and plans, where describes

[1] Therefore, in this conference, this document will be referred as the future National eID

the eID cards[2] as mandatory and intends to issue a total of 13 million cards (between the future National eID, health insurance and civil servants cards) until the end of 2005. All the cards support IAS (including the future National eID) and a range of 80 to 100 eServices are available. Austria expects that by the end of 2007, 90% of all public/government/private services will be accessible to card holders. Depending on the type of card in question, this can be multi application or not, but in either case, the Austrian card does not follow ICAO recommendations nor supports biometrics. Finally, Austria recognizes that the technological neutrality is an advantage since it allows for various private sector issuers to follow the concept and, at same time, allows easy integration of emerging technologies.

Seventh Conference

Austria made the same presentation as to sixth conference. No relevant updates were identified, taking out the fact that Austria recognizes the need for greater pan-European cooperation (especially on recognition of digitally signed and authenticated Austrian documents abroad).

Ninth Conference

In this update, Austria stated once again that smart card based and non smart card based Citizen Cards are available, all allowing eGovernment use. The most relevant facts come from the usage of mobile phones as eID devices and the issuance of 10 million eID cards until this date. Austria identifies the goal of issuing 15 million cards until the end of 2007 (the sum of all kinds of eID cards available in Austria). Another relevant fact comes from the integration of the Belgian, Estonian, Finish and Italian cards on the Austrian Citizen Card software.

Twelfth Conference

Austria is currently amending its eGovernment laws issued in 2004. Any signature performed by an Austrian Citizen Card now must be a qualified signature. Also making part of the amendment, company-specific unique identifiers for private sector applications will be enrolled, improving the usage of eID by private companies.

7.2.3 Belgium

Belgium has made eleven updates in the Porvoo Group conferences.

[2]Health and bank eID cards are mandatory, but the National eID is under discussion as stated above

eID WP

By this time, Belgium has already planed its project strategy. Several initiatives were lunched, like the FedPKI (the Belgian PKI initiative for supporting IAS), the BelPIC (aims at creating the infrastructure required for linking the municipalities and the National Register) and finally the EIC (Electronic Identity Card) for which a pilot will be launched.

Fifth Conference

There are no direct documents pointing to a Belgian update in the Porvoo Group conferences. But other documents present in the Fifth conference web page refer to the Belgian evolution in this field. The pilot for the EIC was launched in March 2003. The program was considered a success and the next step is the end of the pilot and mass distribution of the National eID. The intention is to replace all the current paper cards (around 10 million) with electronic ones in 5 years (which is the validity date of the ID document and also the eID), turning the electronic ID card in the principal method for personal identification and authentication. For the electronic administrative services, plans are being drawn for the creation of a nationwide ePortal.

Sixth Conference

In the questionnaire presented for the Porvoo Group sixth conference, Belgium explains that eID legislation is already in place and, the eID card is mandatory for all citizens over twelve years old. By this date, there are 85000 (170000 certificates) card holders from a total of 10.3 million citizens. The Belgian eID is the official ID document and also serves as a European travel document. Sensitive data is protected by PINs and, biometrics are under study. Regarding digital signatures, their value is the same as a handwritten signature. At this time, an inventory on how many services are available that depend on that kind of functionality (or other) is being made. Finally, Belgium states also, the importance of open communication with the citizen, cooperation with banks and, the need for good availability of the card readers.

Seventh Conference

Belgium made the same presentation as the sixth conference. The most relevant update comes from the fact that in six month, Belgium issued half a million new National eID cards. The number is now 584.573 (1.169.146 certificates) eID cards. Also, Belgian expressed the need to follow-up the technical evolution and consolidation of the current know how.

Eighth Conference

Belgium made a general overview of the National eID card features. With focus on both, physical and logical security. It has also explained what kind of data the eID card contains, what applications are available (along with small tutorials) and stated that for future applications "the sky is the limit". Taking out some minor tweaks and functionalities there was no significant new updates on the Belgian eID.

Ninth Conference

In the ninth Porvoo Group conference, Belgium followed the model of the sixth conference and presented the country updates since the last conference it attended (the eighth conference). Relevant updates come from the fact that as of May 1 of 2006, Belgium issued more 2.7 millions eID cards in a growth rate of 20% per year. Also, Belgium is planning to add social security and health insurance information on the card.

Tenth Conference

Belgian made two important updates. The first comes from the number of distributed eID cards since the last Group meeting. Between the ninth and tenth conferences, Belgium issued over 1 million new eID cards, bringing the number to just over 4 millions. The second is the lunching of the pilot for the Kids ID (December 2006) and the pilot for the Foreigners eID (January 2007).

Twelfth Conference

Currently, Belgium delivered over 6 millions National eIDs offering to its citizen's access to 130 eServices. It is now planning specific eID for Belgian living outside the country. The Kid's ID project (that is a secure electronic identity document for citizens under 12 years old) contains a unique phone number that can be linked to other numbers by the parents. When dialing the unique Kid's ID number, all the linked numbers will be called one at a time and if none can be reached, the call is directly linked to the police. The Kids ID pilot has issued 6421 cards and the roll out phase will happen in the near future. Other Belgian eID project is the Foreigner Project, which is a secure electronic identity document for Foreigner authorized to live in Belgium. It will replace the corresponding paper documents and conforms with the EU Resident permit card. Pilot as already started and, the roll out phase will start in the near future.

Thirteenth Conference

By this date, Belgium delivered over 7 million National eID cards along with over 14 million Qualified Certificates. Using the Belgian eID, the Belgian citizen can now

login and authenticate himself in the popular auctions website eBay[3] where, the capability of unambiguously identify its users and the guarantee of nonrepudiation is probably the most important feature the web site requires. Since the web site can use the full PKI features of the Belgian National eID, this becomes a very important example of the eID capabilities and possibilities. Also, Belgium is still in the planning phase for an eID for Belgian citizens living outside the country.

Fourteenth Conference

Belgium is still steadily deploying its National eID. Currently, over 8.1 million cards were delivered which means, over 16 million active qualified certificates. Also under deployment, is the electronic foreigner card, with 700 000 units already deployed. In this field, another future Belgian project is the Electronic Card for Foreign Children (< 12 years), along with the creation of new and better eServices.

7.2.4 Denmark

Denmark has never presented plans or updates in the Porvoo Group Conferences.

eID WP

The eID WP states that Denmark has no concrete plans to introduce National eID cards. Instead, Denmark uses a software based digital signature which does not require people to show up in person to prove their identity. This is performed by installation of a decentralized certificate on the Citizens personal computer. This is of voluntary use for Citizens to use for eGovernment. Since Denmark does not have any presence in the Porvoo Group conferences, there will not be further analysis to the Denmark situation.

7.2.5 Estonia

Estonia is one of the pioneers in the field of National eID. The Estonian example provided invaluable information on eID implementation and acceptance. It was present in twelve conferences updating its eID situation.

eID WP

In 2003 Estonia already had fully implemented its National eID. Cards are mandatory to citizens over 15 years old and are valid for 10 years. The eID provides access to a wide variety of online government (greatest part of the eGovernment services were already available on the web), private services and digital signature capabilities. The interoperability issues were solved by adoption of the Digital Document Exchange Format and development of Open Source Software. At this time it was already possible to notice the positive reactions of government agencies

[3] http://www.ebay.be/

and companies and, also, that people trust the system. Considering it even more efficient and secure then traditional paper based operations. Still the public reaction was hostile due to the fact of the underestimated need for serious PR work and, therefore, the card usage possibilities were not correctly transmitted to the Citizens from the beginning of the project.

Fourth Conference

30% of Estonian Citizens already possess the National eID. The first court ruling regarding the validity on an electronic signature issued a positive sentence concerning the evolution and acceptance of of the same (i.e., it confirmed the same legal status of ES and regular paper signature). All the required software for eID interaction is now complete and freely available. It was signed a contract for the implementation of virtual ticketing systems for public transports relying on the eID, which for example, facilitates the checking if the user is entitled to get a special tariff, such as a lower price for residents.

Fifth Conference

There are no direct documents pointing to a Estonian update in the Porvoo Group conferences. But other documents present in the Fifth conference web page refer to the Estonian evolution in this field. By this date, Estonia issued a total of 500.000 (with a population of 1.3 million) National eID. It is the country with most progress in this field. There are projects under way in Estonia aimed at establishing eEstonia, where information is accessed using centralized communication tools on the Internet. To increase service transparency, new services are being developed and entitled eCitizen. The new services intended for citizens include, online access to the citizen personal data and online information on whom and for what purposes has accessed the data. At EU level, the intention is to support eEurope programmes and projects aimed at enhancing administration.

Sixth Conference

In the follow up of the Porvoo Group questionnaire for the sixth conference, Estonia presented its status, explaining that by this date, 50% of the population (total number of inhabitants is 1.3 millions) is already in possession of the mandatory National eID card. National legislation on the eID exists since 1999. The eID card acts as the official ID document and as a European travel document. Data security is guaranteed by the use of PINs, plus, the use of biometrics is on a piloting stage. The card supports PKI and there are available, hundreds of services that benefit from the eID card. Even so, the goal is a complete adherence of all public services to the eID model.

Seventh Conference

Estonia made a similar presentation as for the sixth conference. The main differences come from the fact that now 70% (a total of 750000 cards) of the population already has the National eID card. Also, Estonia is going to add a second chip to the card containing biometrics (facial image and fingerprints) according to ICAO standards.

Eighth Conference

Apart from the Estonian presentation in the eighth Porvoo Group conference, by October 2005 Estonia had the first local elections where, citizens could vote over the Internet using the electronic identity card, being the first country in the world to do so. Regarding the conference, Estonia made a quick overview over its National eID card capabilities but did not add any significant remarks over what was already presented in previous conferences.

Ninth Conference

As one of the pioneers in eID deployment, the biggest updates from Estonia were presented in the past conferences. However, Estonia did not stop its development in this field and still aims to be compliant with every standard in power except the ones concerning biometric information.

eVoting: The event that most marked the Estonian update in the Porvoo Group ninth conference was the fact that the first world eVoting (for National Elections in October 2005) act took place in Estonia. However, only 2% of the voters choose to use this option. Estonia does not consider this an eID failure and stated that eVoting is just one of the many eID faces and, also because peoples attitude and behavior (in this case voting) change in decades and generations, not in a day.

Tenth Conference

Estonia issued more eIDs between the last and the tenth conference it participated bringing the number to just over 1 million, from a total of 1.4 million inhabitants. At this stage and regarding interoperability, Estonia is planning integration with CEN/TS 15480 (ECC[2]), ISO 24727 (ICC Programming Interfaces[28]) and ISO 19794 Part 2 (referring to Finger Minutiae Data biometrics) standards.

Twelfth Conference

Estonia keeps advancing its eID technologies and infrastructures. At this date, Estonia presented some of its updates, like, the changing of the original card chip for a newer version with faster processor and more memory, although, the main reason of the change was that the old chip was no longer manufactured. Other projects include the m-ID where one can use a mobile phone to act as card reader and pin-pad allowing for authentication and digital signature. Also presented, was

the Quick eID, where in case of, for instance, loss of the eID card, broken chip, or any other reason that might prevent the electronic part to work, the citizen should be able to in a fast way have access to a new eID. For this purpose, a card is under study that has no visually personalization, but containing the same certificates as the original and allowing the same electronic functionalities as the ID card.

Fourteenth Conference

Estonia main advancements are the tweaking of its already strong eID with PKI, along with the deployment of the previously planned projects. The eID base software is now supported by all three main platforms (Windows, Linux and Mac OS X). The project intended to quickly replace a broken eID is named "Supplementary ID" and citizens can already benefit from it along with the m-ID project. Finally, Estonia is starting to acknowledge foreign certificates. The starting chosen are the Portuguese, Belgian and Finnish certificates.

7.2.6 Finland

Finland is another European pioneer in the implementation of the its National eID. It was present in eight conferences presenting its eID updates.

eID WP

The voluntary National eID card distribution has started in 1999. Around 50 services are available with the eID card at this time and, more projects and services were underway. The eID is provided by the police and, the Finish Population Registry Centre supplies the onboard certificates required for IAS. Unfortunately, the deployment of the eID card dropped behind expectations. It was then realized that public/private coordination and cooperation is essential together with efficient communication to all key target groups (this is also stated from the Estonian case). So a working group (PRO-FINEID) was established in 2001 in order to develop proposals on the promotion of the Finland National eID. At the same time, the Population Register Centre changed its strategy to accept wider options of platforms and uses. Also, Finland altered its eID legislation in order to eliminate some of the bureaucracy that surrounded the eID.

Fourth Conference

Until recently 16 000 chip-cards were issued in Finland. The number is increasing at a rate of 1000 cards per week thanks to the facilitation of the process of acquiring a National eID card. Also, the Social Security card and the eID card can be combined, decreasing the number of cards a citizen has to use. A Mobile Communication Project which coordinates the Sonera[4] mobile system and the Finish Population

[4]Sonera is the dominant telephone company and mobile network operator in Finland

Register Centre citizen certificate infrastructure has started and, at the same time, Finland also has several ongoing projects which are showing progress:

- Production launch for bank card with citizen certificate (1 October 2003)
- Phone with citizen certificate
- E-mail in citizen certificate
- Free-to-load software package for authentication of the citizen certificate and digital signature

Fifth Conference

Finland is already with approximately 40,000 issued electronic ID cards. The Population Register Centre is also developing a mobile certificate, a mobile telephony service allowing the electronic identification of users, in co-operation with three operators. The goal is to have the services available for consumers during 2004. The mobile citizen certificate is part of the national basic solution based on the reliable identification of persons anywhere, at any time and, without physical documents.

Sixth Conference

In the questionnaire presented for the Porvoo Group sixth conference, Finland explains that eID specific regulations are already enacted and in place. Although the card is not mandatory Finland already issued a total of 60.000 cards and, they can be used as the official National ID document and also act as travel document within the EU. All software is available free of charge. Besides PKI the eID supports PINs for data protection and the use of biometrics is under survey. A total of 50 eID based services are available and by the end of 2007 are expected a total of 200. Finally, Finland states that: usability, the adding of social and health services functionalities, broad, cross-administrative cooperation and private sector cooperation are important prerequisites for success.

Seventh Conference

Finland made a similar presentation as the sixth conference. It has updated its numbers, and, in six months Finland issued 18000 new National eID cards[5]. The cooperation with the telecommunication operators is consolidated and there is now the possibility to put a Citizen certificate on SIM-Cards in mobile phones and use eServices requiring IAS. Finally was announced a technological update, i.e. the adoption of 64k Java chips for the cards.

[5]Remember that although the Finland eID is an official ID card it is not mandatory

Tenth Conference

Since the previous Porvoo Group conference that Finland attended, the country politics remain basically the same (the card is not mandatory for example). Relevant updates come from the fact that Finland issued 123 000 eID cards and expects the number to rise to 160 000 by the end of 2007. Concerning standards and interoperability, the Finland eID now supports in full ISO/IEC 24727[28], CEN Workshop Agreement (CWA) 15264 (eAuthentication) and CWA 14890 (eSign). ECC[2] and biometric standards support are still in planning phase.

7.2.7 France

France started the study on several eID possibilities in the early decade. It has reported their eID status by four times in the Porvoo Group conferences.

eID WP

At this time three projects were underway with different degrees of completion.

- The TITRE FONDATEUR focuses on identification of professional groups, namely elected representatives and civil servants. Still at a preliminary phase, it is identified as a key element of the French eGovernment strategy.

- The CSP (Professional Health Card) and the CESAM-Vital (general population health card) work together in the domain of healthcare and social insurance. The CSP supports electronic signature for administrative purpose and protection of sensitive information and, the CESAM-Vital is for identification of insured persons

- Finally, the demonstrator for a Citizen Electronic ID Card (CEC) was already completed in 2003 but waiting for large scale tests. The goal is to increase the productivity and effectiveness of administration and provide IAS. Being so the CEC provides proof of identity with means of control including biometrics. Acts as travel document in the EU and, provides access to eServices by using authentication and electronic signatures where required. The project integrates the European dimension and intends to be operable with the rest of the EU

Seventh Conference

The French update as it is described in the Porvoo Group web page for the seventh conference is in fact the presentation of the ECC standard in its early stages (part 1 was released one day before this update). Since ECC is already covered in this thesis in section 3.2, this update will not be further analized.

Ninth Conference

France made a complete update of its eID situation in the ninth Porvoo Group conference. At this time, France did not have any kind of specific eID legislation in place. However, an eID bill was being studied by the government. Responsible CA for the existing infrastructure is the Ministry of the Interior. France does not expect to start the roll out of the eIDs before the end of 2008, which by then, it will be an official national ID document, European travel document and, will support on-line access to eServices. The card will be valid for 5 years and should be compliant with the current international standards.

7.2.8 Germany

The German eID project although not yet implemented, is considered a good example on eID planning. It was even subject of study by STORK and compared to the ECC (in [38]). Germany presented their updates four times in the Porvoo Group Meetings.

eID WP

At this time, Germany was studying different cases and scenarios of smart card applications. The main pilots were:

- The LAND OF BADEN-WÜRTTEMBERG which uses smart cards for several purposes, like car registration, requests for agricultural funding and, applications in the department of justice. The users being: civil servants, citizens or enterprises. It will provide IA (identification and authentication) services
- The BESCHAFFUNGSAMT (procurement agency) of the Federal Ministry of Home Affairs, aims at implementing qualified electronic signature throughout the whole life cycle of the contractual relationship between administrations and providers

Eighth Conference

The German eID project is called eCard. The eCard strategy focuses on the adoption of joint standards to ensure interoperability. Germany plans to make of the eCard the National German eID. However, the eCard will not replace the existing cards (for example the electronic health card or the digital signature cards) nor will the existing cards be fused together with the eCard. Germany is putting a high effort in following standards in order to achieve maximum interoperability. Qualified electronic signature will be an optional feature, but, ICAO standards and biometrics will be mandatory.

Eleventh Conference

Germany explained that is going to follow the lessons learned from the usage of the ePassport, giving special emphasis to ICAO standards. The immediate plans are not only the introduction of the German National eID card in 2008 targeting the German citizens, but also the eResidence Card for third country nationals in 2009. Both cards will have biometrics, eSignature and eAuthentication, allowing access to online banking, Internet auctions, online shopping, citizens portals, etc.

Twelfth Conference

In the twelfth Porvoo Group conference, Germany officially presented its eCard-Strategy which is heavily focused in achieving harmonization between several (already existing and future) other eCard projects by enabling smart card interoperability (arbitrary cards, arbitrary applications, one interface), making electronic services for eBusiness and eGovernment easy, cheap and secure. Germany developed then the so called eCard-API-Framework (studied by the one of the Author partners in [38]), based only on open standards with emphasis on ISO 24727 [30]. Germany explained that the eCard-APIFramework may provide a good starting point to define a comprehensive eID framework for Europe and be used on the EU eID Large Scale Pilot project by STORK.

7.2.9 Greece

Greece was only present in the first Porvoo Group meeting. The eID White Paper refers to the "*Greece in the Information Society*" White Paper so a small resume is made, but after that, there will not be further analysis to the Greek situation.

eID WP

Along with the White Paper, it was adopted an Operational Programme for the Information Society (OPIS) in, the framework of the EU's 2000-2006 Structural Funds Framework, in order to promote the use of the electronic signature in a coherent and integrated way.

7.2.10 Iceland

Iceland updated its situation twice, in the fourth and seventh Porvoo Group conferences.

eID WP

In 2003, Iceland had still no concrete plans to introduce eID.

Fourth Conference

Iceland has implemented many successful eApplications. As an example, 80% of all tax returns are processed electronically. So far, Pretty Good Privacy (PGP) has been used and considered sufficient. However, in this context, eID uses PKI (as explained in the eID White Paper). Therefore, a digital certificate pilot has been launched in December 2002 and, prior to that, it was established a Workgroup comprising government institutions to study all the benefits, risks, costs, and technical aspects of some potential migration. So far, Iceland does not yet uses eID (with PKI) but recognizes it as necessary for future applications.

Seventh Conference

In the seventh Porvoo Group conference, Iceland identified acts number 28/2001 and, 30/2002 on electronic signature and, electronic commerce and other electronic services respectively. The PKI pilot project issued the first certificate in May 27, 2003. With this pilot, Iceland expects to gather experience to build is future PKI, identifying the urgency in defining a PKI for the government.

7.2.11 Ireland

Ireland participated in the first three Porvoo Group conferences.

eID WP

Although Ireland participated in the first three conferences of the Porvoo Group (which are all previous to the eID White Paper), it had no relevant plans concerning the eID. Since Ireland is not represented in any conference after this date there will be no further analysis to the Irish situation.

7.2.12 Israel

Israel participated in the first two Porvoo Group conferences

eID WP

At this time, the introduction of smart cards as an ID method on the National ID system was already on the way. The actual deployment did not start yet but the decision was made. Also, the Certificate authorities had not yet been chosen, but a tender process was on the way. Since Israel did not updated its situation on further Porvoo Group conferences there will be no further analysis to the Israeli situation. But from this case it is possible to take some lessons that although may seem trivial, are very easy to neglect:

- Stick to the standards
- Quality assurance is of critical importance

- Co-ordinate and synchronize all the efforts (cards, card readers, applications, customer preparation, CAs.)

7.2.13 Italy

Italy first update was in the Porvoo Group fifth conference. Italy presented its updates four times.

eID WP

At this date, Italy did not had any presence in the Porvoo Group conferences. Nonetheless, by this date it already had lunched the pilot. Citizens, during this time, could acquire the National eID (IEIC - Italian Electronic Identity Card) for free. The certificates are issued by a Certificate Service Provider (CSP) accredited in compliance with the directive 99/93/EC (i.e. according to the Community Framework for Electronic Signatures referenced in section 2.1.2). The IEIC provides IAS services to various sectoral administrative applications and network access control.

Fifth Conference

There are no direct documents pointing to an Italian update in the Porvoo Group conferences. But other documents present in the Fifth conference web page refer to the Italian evolution in this field. The first pilot phase of electronic identity has been completed. It involved 83 of the country 8102 municipalities and 100,000 electronic ID cards were issued to citizens. The second phase is currently under way. The electronic ID card can already be used at national level for the following services: identification of persons at the polls and, citizen checking of his/ her fiscal position. The services available locally include: children school enrollment and, school fees payment, as well as city residence and street residence change. Several services are being prepared at both national and local levels.

Sixth Conference

In the follow up of the Porvoo Group questionnaire for the sixth conference, Italy presented its status and plans for the future. At this point, eID specific regulations are in place since the Italian National eID card is mandatory. So far Italy has issued 400.000 cards and certificates but, the plan is to cover the entire 40 million citizens nd, enabling to them, the use of a wide range of eServices and eGovernment using PKI. The Italian eID also serves as travel document inside the EU obeying ICAO recommendations. Data protection is done via PIN and biometrics (fingerprint).

Seventh Conference

At this date, Italy was now in a consolidation and rationalization phase (to finish in 2005) where 2 million cards are in production and 800000 were already issued. The

deployment phase should start in 1 Jan 2006 and finish in 2010 and, by then, all 40 million Italian citizens should have their respective National eID card.

Twelfth Conference

Unfortunately, in the web site referent to this conference[6] there are no references (links) to the pertinent document.

7.2.14 Japan

Although Japan is already included in the AICF, in a winding of frontiers concerning a possible future integration of a National eID on a wider range than Europe, Japan also presented its situation updates regarding eID on the Porvoo Group conferences. The first update was on the seventh meeting in a total of five updates.

eID WP

The eID White Paper as no reference of Japan.

Seventh Conference

Japan for the first time updated its eID strategy. This strategy fits in the midst of the technological plan named e-Japan.

ID documents: In Japan the documents used for ID are: the certificate of resident registration in order to prove the current address of the individual, the certificate of family registration, the driver license and health insurance certificate.

IT infrastructure: In 2001 Japan started the construction of its broad band infrastructure and in 2003 it had a full usable IT backbone. For 2006, Japan plans to promote advanced applications under government initiative i.e. eGovernment.

Resident Registration Card (RRC): For the coming of the IT society, Japan created the Resident Registration Card that intends to replace the certificate of resident registration. For this, the resident registration law was revised in 1999 and became effective in August 2002. All local Japanese governments start issuing the RRC in 2003. The RRC is not mandatory, but is a smart card capable of digital signature and enables the card holder to receive eGovernment services in the cyberspace. The RRC uses only RSA (no PKI) signature for authentication and electronic signature. The keys are stored in the card chip. Japan expresses that the number of issued RRC's is much lesser than expected. Lack of sufficient services, health care and payment capabilities, etc, are pointed as causes for the current situation.

[6]The direct link is on the Porvoo Group home page[19]

Eighth Conference

In this conference, Japan announced the publishing of its next eJapan strategy to occur in January 2006. It will focus on using IT on the health care and eGovernment. In that year all government employees will receive their electronic identity for authentication and login into systems. Currently, Japan issued around 700000 RRCs but found that this number falls under expectations. The project was then re-launched and the main goal was to make all eGovernment services accessible with a single card. Besides allowing electronic signature, the card will act as a passport and include the biometric details required by ICAO.

Ninth Conference

In the ninth Porvoo Group conference, Japan stated that continues the development of its new eID strategy. This strategy was started in January 2006 and the short term goal (up to 2007) is the reduction of the social costs through structural reforms, maintaining a focus on Healthcare and eGovernment where 96% of the applications and declarations should be on-line.

Twelfth Conference

Japan continues the promotion of IT in healthcare by forwarding projects like home healthcare using digital TV and, promises that medical cost settlements will be 100% paperless by 2010. The core of these projects is the Health Insurance Card, but now Japan plans to introduce the Social Security Card, which will have added features. For instance, it will serve as pension booklet, health insurance card, nursing care card, etc. This card allows his owner to check his pension records safely from any location (that offers the proper means i.e. Internet and a card reader), linkage with the resident registration network while ensuring the proper security needs. The roll out should start in 2011. To support this and other eServices, Japan will also introduce the concept of eP.O. (Post Office) box, where, a Japanese citizen can open a personal account in the cyberspace and, access it with a smart card. This will allow access to all the eServices available to the citizen in just one portal and, should be online in 2010.

Thirteenth Conference

Due to the fact that the new Japanese Social Security Card will have at least 3 strands (pension booklet, health insurance and nursing care), Japan explained its card logic architecture. I.e. the card will be a multiple application card where the required program will run when prompted. Current discussion for the Social Security Card involves which identifiers will be used for individual identification, which is going to be the issuers and finely the qualification management system of insurance. Japan also further developed its eP.O. box presentation with, special emphasis on the eP.O. box security features. To conclude, Japan presented what

considers to be the key issues for social acceptance: the service provider must be well trusted by the users, account status can be checked by the user at any time and, the use of the account must always be under the users control.

7.2.15 Latvia

Latvia participated in the first and third Porvoo Group meetings.

eID WP

Law on personal identification documents was effectively adopted in July 2002. In January 2004, Latvia started issuing ID cards. At this time there was no official CA established yet, and since Latvia does not have further updates so there will be no further analysis to the Latvian situation.

7.2.16 Luxembourg

Luxembourg is referred in the eID White Paper. However, Luxembourg never updated its situation in the Porvoo Group Conferences.

eID WP

According to the eID White Paper, in 2003, Luxembourg had no relevant data available regarding Electronic Identification. Since Luxembourg does not have further updates so there will be no further analysis to its situation.

7.2.17 Netherlands

Netherlands was present and updated its situation in the first and in the thirteenth Porvoo Group meetings.

eID WP

Until this date Netherlands expressed great enthusiasm in the implementation of eID, it inclusive had tested several pilots. But unfortunately the practical implementation is not accompanied by the theory. The paper based cards were already replaced by plastic cards (of the size of a smart card) with a reserved spot for a chip but does not contain it yet. Netherlands is however, consolidated its goals regarding eID by, defining its main goal and support documents:

- The goal is to provide high level electronic services and transactions with IAS capabilities that offers at least the same guarantees as what was currently standard in non-automated services
- The specifications requirements for the certificates are expressed in the "programma van eisen PKI Overheid" or Statement of Requirements and can be found at http://www.pkioverheid.nl/

- The PKI should be hierarchically designed and aimed at achieving the maximum interoperability

Thirteenth Conference

Unfortunately, in the web site referent to this conference[7] there are no references (links) to the pertinent document.

7.2.18 Norway

After WWII there has been resistance against compulsory public identification systems in Norway. After 1970 the use of cheques became more and more widespread. The banks felt the need for identification systems to avoid bad cheques. The government refused in 1975 to take action, and the banks established joint systems for bank identification cards. These became, and are, the *de facto* visual identification standard in Norway today. Norway is an active country in the Porvoo Group conferences. It was present in a total of six conferences posting regularly its updates concerning National eID implementation.

eID WP

In this date, Norway already issued eIDs on smart cards to the Doctors in the medical sector for, digital signature of medical reports and, prescriptions, expecting the wide use of digital signatures in the public sector. Also, some municipalities have chosen to deploy eID for use in public service, voting, etc. Norway was well prepared for the reception of eID, with National law regarding certificates based on the EU directives. Also, commercially qualified certificates were already available to the general population.

Fourth Conference

Norway used with high success (50% adhesion rate) eID for public elections. A voting ticket was putted in an ID smart card and an "enablePKI Toolkit" provided the necessary functionalities of signing and encryption of the election tickets, by wrapping votes in signed and encrypted envelopes, verifying signature, and extracting (anonymous) votes from the signed and encrypted envelopes. Another eVoting event is already prepared for next elections. Also, it is under way, a tender for a new contract for the personalization of new electronic passports which use biometrics and PKI.

Fifth Conference

After a market survey in 2004 Norway defined some objectives, where and if possible alternatives to PKI should be found and, defining "authentication" as more

[7] The direct link is on the Porvoo Group home page[19]

important than "signature". New services have been introduced to the social security and health sectors, and students can apply for government grants electronically. Voting using a smart card has also been tried out in local elections, and in the 2005 general elections it should be an alternative to conventional voting. Currently, the Norsk Tipping issued 2,1 million smart cards.

Sixth Conference

As stated in previous sections, Norway does not issues National eID cards. It issues however a smart card with eID capabilities for easy access to eServices requiring IAS. Being so and regarding the questionnaire issued for the sixth conference of the Porvoo Group, Norway explained that does not have eID specific regulations, but its eID card (not mandatory but with PKI) was already issued to 2.1 million citizens, allowing them access to a set of 10 eServices but, in the future, that number should arise to 50. The access is protected by PIN but biometrics (fingerprint match-on-card) is envisioned. Finally, Norway recognized the need for user awareness on PKI but it will not adhere to interoperability measures before critical mass of eID requirements is reached.

Seventh Conference

Norway used the seventh Porvoo Group conference to present its new project for eID, the "Sikkerhetsportal", i.e., the Norwegian "electronic signature act". Piloting is already underway and expected date of issuance is in the beginning of October 2005. The card is intended to be an official ID document and allow access to eServices but, not as a European travel document. For data protection the card uses PIN keys and for the eServices it provides PKI functionalities which include electronic signature.

Ninth Conference

Continuing the work presented in the seventh Porvoo Group conference, Norway is currently implementing the required eID regulations and, a system for qualified certificates has been established. Currently, Norway has issued 1.8 million eID cards but expected a deployment of 5 million by the end of 2007.

Tenth Conference

Currently, Norway eID regulations are part of an act on eSignature only. No other laws define attributes of ID or eID, however, there is ongoing discussion whether national birth numbers should be included or not. At this date, Norway is still going to decide which CA organization is going to issue the certificates. Along with this future decisions, Norway is also deciding if the future eID is going to be an official ID document (no certain answer here), if it will function as European travel

document (probably will) and if there will be deployed eServices supporting the card.

7.2.19 Poland

Poland exposed its progress and propositions only once in the Porvoo Group conferences, being that the thirteenth conference.

eID WP

The eID White Paper as no references regarding Poland.

Thirteenth Conference

This is the first time Poland updated its situation. Currently there is not any kind of eID support infrastructure or legal regulation in Poland. However, several related R&D projects are underway. The most relevant are:

- Semantic web
- Electronic Health Care records
- Biometric, PKI, cryptography, RFID and electronic tickets
- Fraud detection

Considered data on the card is the identity number, names, biometric data (face picture and fingerprints according to ICAO specifications) and address with history. Under consideration is information about children.

7.2.20 Portugal

Portugal first update was in the eighth Porvoo Group conference. So far, it has updated its situation three times.

eID WP

At this date the Portuguese parliament was still discussing the future implementation of the National eID.

Eighth Conference

The eighth Porvoo Group conference was when Portugal first presented its updates and plans for eID implementation. Unfortunately, in the web site referent to this conference[8] there are no references (links) to the pertinent document.

[8]The direct link is on the Porvoo Group home page[19]

Tenth Conference

Since there is no data regarding Portugal's first Porvoo Group conference, this conference is going to be addressed as the actual first conference. At the date of this conference, the Portuguese eID regulations were on the Parliament for discussion and approval. However, the main entities were already decided, for example, the responsible CA organization, the card and certificates issuer and, the number of certificates on the card (2, for authentication and signature). With a total population of 10 million inhabitants, at the date of this conference, Portugal did not issued any card, but expected the issuance of 200 000 cards by the end of 2007. The eID will be mandatory and will replace the current official ID card (and also act and replace the current Tax Card, the Social Security Card, the Health Services User Card and the Voters Card), act as European travel document and offer access to a number of eServices. Also, a wide range of standards were taken into account while developing the Portuguese eID, making it compliant with CWA 15264 and 14890, CEN/TS 15480 1[2] and 2[3], ICAO 9303 and ISO 24727 1[28], 2[29] and 3[30]. The project pilot should start in January 2007.

Eleventh Conference

Unfortunately, in the Porvoo Group eleventh conference page, the hyperlink for the presentation document titled "The Portuguese Citizen Card" it is not available. There are however, other available presentation documents where analysis can be made. For example, "ama - Agência para a Modernização Administrativa" made a presentation explaining the evolution of internet usage in Portugal and referring the Portuguese eID priority number 1, citing, "in 2010 every citizen will be able to use electronic public services through the most suitable channel".

7.2.21 Slovenia

The first update from Slovenia was in the second Porvoo Group conference. Since then it has updated its situation two more times.

eID WP

At this date, in Slovenia, citizens can already authenticate themselves to eServices using an eID card. The eID card can contain two certificates issued by different CAs and for different scopes. One for public administration and other for citizens and for the private sector. In the eID White Paper there is no information regarding if this eID document is mandatory or not or, if it replaces any other type of ID document.

Ninth Conference

Slovenia has presented in the ninth Porvoo Group conference the newly adopted strategy for eComerce and eGovernemnt. This strategy started in April 2006 and

should be complete in 2010. Slovenia states that the goals of the new strategy are better, more efficient and secure public administration services, extending functionalities to the private sector.

7.2.22 Spain

The first update from Spain was in the second Porvoo Group conference. Since then Spain has updated its situation three more times.

eID WP

At this date in Spain, an eID PKI providing IAS is already available for tax declaration and Social Security eServices. This eID is issued by the "*Fabrica Nacional de Moneda y Timbre*" (MINT). In addition, the project for creating a national electronic ID card issued by the police was already started, along the establishment of a single and universal certificate for all administrative transactions.

Seventh Conference

By the time of the seventh Porvoo Group conference, Spain already had eID specific regulations and, concluded its plans of deployment of a national eID card. The DNI - "*Documento Nacional de Identidad*" electrónico issued by the police. The card is mandatory for all citizens over 14 years old and the issuance should start in the first quarter of 2006. By the end of 2007, Spain expects to issue 5 million cards (having a total of 42 million citizens). The DNI electrónico also serves as European travel document but, does not comply with ICAO standards (planed for 2007). It uses biometrics (match on card) for certificate updates and PKI for eServices access.

Eleventh Conference

Spain made a technical update on the eleventh Porvoo Group conference. First, explained the reasons for the replacement of the National ID for a smart card Based eID. For example, since the previous National ID card accounted for 99% of the Public Registries as the main citizen identification number, Spain explained that adding eSignature and eAuthentication capabilities to such a document is a logic step and, as the date of the eleventh conference, Spain offers a set of 361 eGoverment services to its citizens, available by the use of the DNIe. Second, Spain somewhat described its PKI, that allows all the online use of the eID to be safe and reliable, for instance, the certificate verification methods (CRLs, OCSP), validation of different types of eSignatures using XML (DSIG, XAdES), support services, etc. However Spain did not presented its eID evolution regarding for example, how many DNIe were issued so far or, for example the planed steps for the future.

Thirteenth Conference

Regarding eID dissemination, good news come from Spain, where there is no social rejection to the use of the new electronic identity card. Daily figures show 24 000 eID cards issued per day. Spain as already issued 3.2 million eID cards along with 6.4 million certificates. Regarding Spanish objectives, one of the goals was to offer the citizens at least 100 eGovernment services in several different areas. Nowadays, Spain offers over 400 eGovernment services. In response to the increasing complexity and management of all these different services, it was created a centralized Validation Authority (VA) that allows eGovernment applications to verify the status of all the qualified certificates and eSignatures created in the country. The idea is to harmonize among all public administrations, the use of the same digital signature formats and other technical issues related to X509 certificates, assuring interoperability between the different services.

7.2.23 Sweden

Sweden was present in the first Porvoo Group conference and updated its status six times.

eID WP

In 2003, Sweden had already issued multi-function ID cards for three basic services: identification, signing and coding. It included 2 certificates stored in a Swedish standard that in its turn is based on PKCS#15.

Seventh Conference

Sweden has national eID legislation in place. Banks can issue eIDs (not mandatory) with PKI (although, these are not the official ID document), but, only allowing access to eServices. Sweden is planning a national eID which will be the official ID document and also will serve as European travel document.

Tenth Conference

Sweden has since 2000 (the date of the law on qualified electronic signatures) eID specific regulations in place, although there are no CAs who issue the qualified certificates, due to the lack of current business demand for them. By this time, and although the card is not mandatory, Sweden had issued 2 million eID Bank cards, to over 20% of the population. However, only 25 000 National eID card (launched one year ago) were deployed. The card follows the main standards currently in use (ECC, ICC, CWA and ICAO) on the eID context but lacks its proper PKI and CA.

Thirteenth Conference

Sweden presented its BankID solution. Its purpose is electronic identification and signing and is used by the government, authorities, private companies and banks. It was developed to meet the requirements from the Swedish authorities, to enable eGovernment and also, meet security requirements for Internet banking. Nearly all Swedish banks are connected to BankID (in production for 5 years). This type of ID is generally accepted by the citizens where 60% of them are Internet bank users. Current interaction solutions are by means of a file (to store on the PC), a smart card and, mobile phones (this solution is still under development). The service is in expansion as more banks will be capable of issuing BankID and, more eServices will be made available.

7.2.24 Turkey

Turkey presented its eID status only once, in the fourteenth Porvoo Group conference. It was however, a very complete presentation of a very complete infrastructure, identifying all the relevant services and laws involved in eID uses. In Turkey, there is one main entity responsible for the implementation of the eID infrastructure, the UEKAE (Research Institute of Electronics and Cryptology) that, for instance, also implemented the country National Operating System (PARDUS - Based on Linux).

eID WP

The eID White Paper as no references regarding Turkey.

Fourteenth Conference

In 2000, it was introduced in Turkey the Central Civil Registration System (MERNIS), where citizen civil status is stored electronically and updated in real time over a secure network. With this supporting background, Turkey established its eGovernment steps, i.e., the eTransformation (convert the traditional government business processes into electronic environment), the eCitizen (taking the benefits of the citizen to the center of eGovernment business processes), the eApplications (development of the portals for the eGovernment applications) and the eSignature (encourage the use of digital certificates in public services). Also, the Turkish Prime Minister Circular published on the 4th of July 2007 decrees a single eID card for citizens that cover all authentication functionality, the use of biometrics, the first application areas (Health and Social Security) and the pilot deployment. The eID card will then contain identity information, finger prints and electronic certificates. For this reason, a Smart Card Operating System is under development making the card compliant with CEN/TS 15480[2], ISO/IEC 7810 (physical format of the card), ISO/IEC 7816[24], ISO/IEC 10373 (test methods for smart cards) and ICAO standards. Finally, Turkey to fulfill the following project milestones:

- MI: Issuing 10.000 eID cards by the end of 2008, in one district of Bolu.
- MII: Issuing 300.000 eID cards by the end of 2009, in Bolu covering the whole of the province.
- MIII: All the hospitals, family doctors and pharmacies will be involved in the pilot till the end of 2009.
- MIV: All the covered eGovernment applications will be tested in the pilot regions.
- MV: The pilot application will be finish by 1 May 2010.

7.2.25 United Kingdom

United Kingdom has presented its updates in the Porvoo Group conferences since the second conference and, has done so for a total of seven times. Even so, United Kingdom poses a sensitive case due to the lack of legislation regarding any kind of ID document as perceived in the context of this thesis.

eID WP

By 2003, in the UK, identity cards issued by the authorities do not exist and their possible introduction was a politically sensitive matter. Even though, tries and debates were being made concerning the issue. Talks ranged from how the card should be (smart card or not), and, if it was a smart card, then should the certificates be issued by the government or not, etc. A single card with driving license, passport card, and entitlement card ("gold standard") is envisioned but seems improbable because of contradictory standards and regulations.

Fourth Conference

In the Porvoo Group web page, the UK did not present any update, but there are other documents that refer to survey that takes in to account the constitutional issues regarding an ID document in UK. A public consultation on entitlement cards has ended and the majority voted "yes" to ID card. But the strong disagreement from the minority made the government hesitate. Nonetheless, future perspectives are positive.

Sixth Conference

The UK eID card is in the process of legal specification. The UK government and 80% of the population support the concepts. First ID-card roll-out is scheduled for 2008. UK plans to store biometrics (face, iris and fingerprints) in a central database.

Seventh Conference

In this conference, UK stated that ID cards will be reintroduced under the Home Office ID cards Programme. With this goal in mind, UK is replacing the existing card technology with smart cards and PKI. Issuance is expected to start in 2006. However this card will not be the official ID document nor will it perform as a European travel document.

Eighth Conference

Another step for the implementation of a PKI infrastructure for eID in the UK passes through the electronic driving license. Until this date, the second EC Directive on Driving License precludes the inclusion of electronic devices. But the draft on the third Directive now removes that restriction, allowing the advance of electronic driving license in the UK. Regarding Identity Cards, by January 2006 it is expected that they become law and, the first cards should be introduced in 2008.

Ninth Conference

In the ninth Porvoo Group meeting, the UK started to announce that the Identity Cards Act was in place since 30 March 2006. Quoting, this Identity Cards Act is *"An Act to make provision for a national scheme of registration of individuals and for the issue of cards capable of being used for identifying registered individuals; to make it an offence for a person to be in possession or control of an identity document to which he is not entitled, or of apparatus, articles or materials for making false identity documents; to amend the Consular Fees Act 1980; to make provision facilitating the verification of information provided with an application for a passport; and for connected purposes."*[1]. This act also defines the National Identity Register (NIR), which is a data base where are defined fifty items for citizen information (personal, biometric, etc.). In parallel, the development of the electronic Driving License continues. The chip is ready but waiting EU agreement on standards.

Tenth Conference

The UK did not advance much its previous situation. Chip information and standards to follow are currently under discussion in the EU Commission. The DVLA (Driver and Vehicle) launched a pilot regarding eID for more than 6500 employers.

7.2.26 United States

Again, like in the Japan/Asian case, in a winding of frontiers concerning a possible future integration of eID on a wider range than Europe, the United States also presented its situation updates regarding National eID on the Porvoo Group conferences. The first update was on the seventh meeting in a total of six updates.

eID WP

The eID White Paper as no references regarding the United States.

Seventh Conference

The Government Smart Card Program began in the United States in 2002. The achieved progress was gradual and slow up until 27 August 2004, when the President signed the "Homeland Security Presidential Directive 12" where is stated that "Federal agencies are directed to deploy secure and reliable forms of authentication for employees and contractors that can be rapidly authenticated electronically". After, several initiatives went forward being the most important the "technical framework for Personal Identity Verification (VIP)". In April 2005 was released a publication with the technical specifications for: the PIV card interface, client API and, data model. These specification intend to be technological neutral and compliant with ISO standards (i.e. ISO/IEC 24727[28][29][30][31]).

Eighth Conference

In this conference US made a presentation on the current status and development of the ISO/IEC 24727 standard. After, it explained that between employees and contractors of the federal agencies, the US should issue around 40 million PIV cards. The main focus is on services and on standardization related to their interfaces.

Ninth Conference

In the ninth Porvoo Group conferences, the US described some technical options adopted for the PIV. An update was made to one of the PIV publications (the special publication 800-73 re-nominated to 800-73-1), where the main changes come from biometrics consideration and, the removing of PIN protection on the certificates. However, no major architectural changes were made. The deployment is expected to start in October 2006.

Tenth Conference

By the time of the tenth Porvoo Group conference, the PIV program started as expected in 01 October 2006. For future considerations, the US recognizes an increase in contactless operations, and intents to implement more complex card operations.

Eleventh Conference

In the eleventh Porvoo Group conference, the US made a very small resume on its major eID efforts and Collaborations (but without develop them). These include: the Homeland Security Presidential Directive 12 (PIV card), the Western Hemisphere Travel Initiative (PASSCard), RealID, and United Nations OECD WPISP. Several

identity management issues were found, mainly, technical interoperability issues, Logical (semantic) interoperability, "pure" identity vs. sector-specific, from where, the US recognizes the need for common models between the involved parts of different projects. With all this aspects and experiences in mind, the US goal is to produce some card so that a citizen can use it anywhere in the world to access transit, health care, ICT and any other type of eServices in a secure way. Therefore, the US states that is important to understand the cultural, legal and political aspects of global eID.

Fourteenth Conference

A Task Force on Identity Management was assembled in the US and completed its work in January 2008. The report is available online at `http://www.ostp.gov/cs/nstc/documents_reports`[9]. Also, regarding the PIV cards, the "Extra-Federal Trust" (the Governance Working Group of the Federal Identity Credentialing Committee) is drafting a document entitled "Interoperability Parameters for Trusting PIV Compatible Cards" that will describe how, parties outside the US can produce ID cards that are semantically and, functionality interoperable with the federal PIV card reader, middleware and application infrastructure.

7.3 Conclusions

The intention of this study was to understand the situation of the several European countries regarding eID at a non technical level. However, thanks to the international dimension the Porvoo Group acquired (outside Europe) it was also possible to somewhat analyze the current situation in Asia and in the United States of America. As expected, one of the conclusions of the study is the high number of different implemented solutions (many times due to different cultural principles) for eID and National eIDs. However, a very encouraging conclusion is the fact that even countries that do not have National IDs or others that do not yet want to migrate their infrastructures are all studding solutions. These solutions are all generally based in the same open standards which might reveal to be an important measure, considering a mid to long term harmonization of the several eIDs from the several countries.

Connection to the Multiplatform Common and Adaptive Middleware: With the conclusion of this study in mind, and taking special consideration on the desirable fact that most of the countries are embracing international standards (most relevant ones are the ICC Programming Interface[28] and ECC[2]), a main point stands out: Although requiring a thorough study, achieving a universal (almost) and relatively

[9]Because this document was not presented in the Porvoo Group conferences (the target of this study), its results will not be present anywhere in this thesis.

simple XML CARDS SCHEMA module for the Multiplatform Common and Adaptive Middleware is definitely possible.

Connection to STORK: This chapter will serve has basis for a STORK technical study on its members eID status.

For the Porvoo Group: This study and survey of information will be made available for the Porvoo Group.

Chapter 8

Results and Conclusions

In this chapter, the obtained results derived from the thesis studies are analyzed. Then, the final conclusion is presented.

8.1 Results

In section 1.4 the proposed goals for this thesis were described. Discriminating once again these goals and, looking at the body of this document, the following results were obtained:

1. **Multi Platform Middleware:** The combination of the various technologies referred and presented in this thesis, allowed for the implementation of a particularly effective and flexible solution. As stated in chapter 6 further investigation is required in some points. Nonetheless, the feasible of the proposed solution is clearly demonstrated.

2. **STORK project:** Two STORK deliverables were written with collaboration of the Author. Along these studies, the Author also implemented the Portuguese part of the Minimal Footprint Middleware, providing thus, a STORK proof of concepts.

3. **Understanding eID implications:** This multi-purpose study provides valuable information. Not only for the analysis on the eID White Paper but also because of the analysis on the Porvoo Group conferences. This analysis allows for the new reader (to eID) to quickly understand the implications derived from eID implementations and how these implications are being addressed by the different involved countries. This study will also be the starting basis of a new STORK contribution.

8.2 Conclusion

Although the three main parts of this thesis seem unrelated, they are in fact contributing as a whole in different fields. In the most immediate way, the eID study provided in this thesis is a starting point to a new STORK study with a more technical strand. Although this is a STORK study, when complete, will be an important source of information for MULTICERT, allowing the creation of a new, improved and reliable XML Cards Schema for the Multiplatform Common and Adaptive Middleware. Being so, all major goals of this thesis have been achieved and are valid grounds and basis for continuing work. This work will culminate with the new STORK contribution and a new Middleware solution for Portugal. Finally, the eID study will also be available to the Porvoo Group, who in fact as already admitted interest in it.

Bibliography

[1] Identity cards act 2006. Web, March 2006.

[2] CEN. Identity card systems - european citizen card - part 1: Physical, electrical and transport protocol characteristics, January 2007.

[3] CEN. Identity card systems - european citizen card - part 2: Logical data structures and card services, January 2007.

[4] CEN. Identity card systems - european citizen card - part 3: European citizen card interoperability using an application interface, 2008. Draft.

[5] CEN. Identity card systems - european citizen card - part 4: Recommendations for european citizen card issuance, operation and use, 2008. Draft.

[6] Zhiqun Chen. *Java Card Technology for Smart Cards - Architecture and Programmer's Guide*. Addison Wesley, 2000.

[7] World Wid Web Consortium. Extensible markup language (xml). Web, 2009.

[8] World Wid Web Consortium. W3c xml schema. Web, 2009.

[9] World Wide Web Consortium. Extensible markup language (xml) 1.0 (fifth edition). Web, 2009.

[10] World Wide Web Consortium. Xsl transformation (xslt). Web, 2009.

[11] Technical directive of the BSI number TR-03112-1. ecard-api-framework - part 1 - overview and generic definitions. Technical report, BSI, 2007.

[12] eESC. General model for a privacy code of conduct for interoperable smart card systems. Technical report, eEurope SmartCards, March 2003.

[13] eEurope Smart Card. Electronic identity white papper. Technical report, EESC, 2003.

[14] Stefan Engel-Flechsig. Study on legal issues in relation to the use of public id (electronic identity). Technical report, Radicchio Ltd., October 2002.

[15] EUROSMART. Position paper - european citizen card: One pillar interoperable eid success. Technical report, The voice of the Smart Card Security Industry, October 2008.

[16] Mozilla Firefox. Activex. Web, January 2009.

[17] FLTK. Fast light toolkit (fltk). WEB, 2009.

[18] Gemplus. *GemSafe v2 Applet - Reference Manual*. Gemplus, June 2006.

[19] Porvoo Group. Porvoo group. Web, 2009. Porvoo Group Web Page.

[20] Uwe Hansmann. *Smart Card Application Development Using Java, second edition edition*. Springer, 2002.

[21] Vesna Hassler. *Java Card for E-Payment Applications*. Artech House, 2002.

[22] British Standards Institution. Application interface for smart cards used as secure signature creation devices part 1: Basic requirements, 2004.

[23] British Standards Institution. Application interface for smart cards used as secure signature creation devices part 2: Additional services, 2004.

[24] ISO/IEC. Identification cards, 1987.

[25] ISO/IEC. Cards with contacts - electrical interface and transmission protocols, 1989.

[26] ISO/IEC. Organization, security and commands for interchange, 1995.

[27] ISO/IEC. 7816-15: Cryptographic information application, 2004.

[28] ISO/IEC. Identification cards - integrated circuit cards programming interfaces - part 1: Architecture, September 2005.

[29] ISO/IEC. Identification cards - integrated circuit cards programming interfaces - part 2: Generic card interface, December 2007.

[30] ISO/IEC. Identification cards - integrated circuit cards programming interfaces - part 3: Application interface, July 2008.

[31] ISO/IEC. Identification cards - integrated circuit cards programming interfaces - part 4: Application programming interface (api) administration, October 2008.

[32] Timothy M. Jurgensen and Scott B. Guthery. *SMART CARDS - The Developer's Toolkit*. PH PTR, 2002.

[33] RSA Labs. Pkcs#15 v1.1: Cryptographic token information syntax standard, June 2000.

[34] RSA Labs. Rsa laboratories - pkcs#11: Cryptographic token interface standard. Web, May 2009.

[35] RSA Labs. Rsa laboratories - pkcs#15: Cryptographic token information format standard. Web, May 2009.

[36] RSA Labs. Rsa laboratories - public-key cryptography standards (pkcs). Web, May 2009.

[37] MacTech. Activex controls for macintosh. Web, January 2009.

[38] Mario Ivkovic Manuel Preliteiro. D3.2.3 list and assessment of priority technologies - european citizen card. Technical report, STORK, January 2009.

[39] Thomas Zefferer Manuel Preliteiro. D3.2.5 list and assessment of priority technologies - eid oss middleware. Technical report, STORK, January 2009.

[40] Microsoft MSDN. Activex controls. Web, May 2009.

[41] Microsoft MSDN. Activex controls: Overview. Web, May 2009.

[42] Microsoft MSDN. Activex security: Improvements and best practices. Web, May 2009.

[43] Microsoft MSDN. Overview: Creating an mfc activex control program. Web, May 2009.

[44] Oid. Oid repository. Web, May 2009.

[45] OPenSC. Opensc. Web, May 2009.

[46] OPenSC. Opensc faq. Web, May 2009.

[47] International Telecommunication Union Telecomunication Standardization Sector. Information technology - asn.1 encoding rules: Specification of basic encoding rules (ber), canonical encoding rules (cer) and distinguished encoding rules (der), July 2002.

[48] Qt Software. Qt - a cross-platform application and ui framework. web, 2009.

[49] STORK. Stork - what is it? Web, May 2009. What is STORK.

[50] STORK. Stork eid. Web, May 2009. STORK Home Page.

[51] Sun. 1.2 the java virtual machine. Web, May 2009.

[52] Sun. Applets. Web, May 2009.

[53] Sun. The awt in 1.0 and 1.1. web, 2009.

[54] Sun. Java downloads for all operating systems. Web, May 2009.

[55] Sun. Java se desktop overview. web, 2009.

[56] Sun. Java security architecture. Web, May 2009.

[57] Miroslaw TOCICKI. Latvian post pki id card - technical specifications. Technical report, Latvia, March 2006.

[58] PC/SC Workgroup. Interoperability specifications for iccs and personal computer systems - part 1: Introduction and architectural overview, 2005.

[59] PC/SC Workgroup. Interoperability specifications for iccs and personal computer systems - part 5: Icc resource manager definition, 2005.

[60] PC/SC Workgroup. Pc/sc workgroup specifications. Web, May 2009.

[61] wxWidgets. wxwidgets. web, 2009.

Appendix A

Demonstrator Print Screens

In this appendix, the Minimal Footprint Middleware demonstrator screenshots are shown, i.e. the user graphical interface for performing a digital signature using the PT eID card.

Figure A.1: Demonstrator Home Page

Figure A.2: Requesting permission to run the Java Applet

Figure A.3: Waiting for some smart card insertion

Figure A.4: The inserted card is not a supported eID

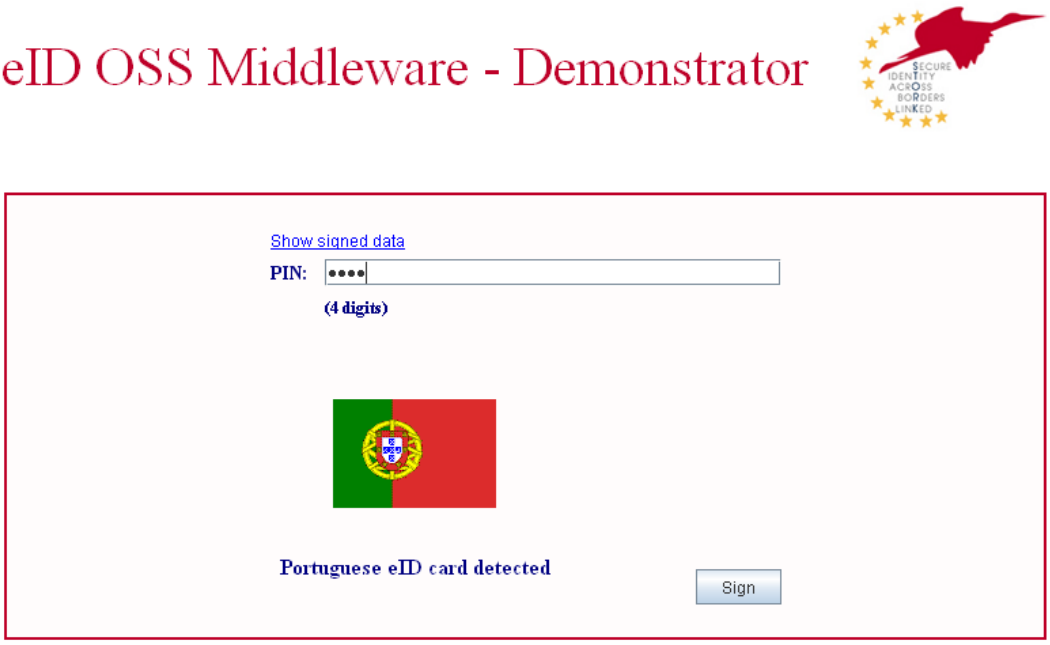

Figure A.5: Demonstrator recognizing the PT eID

Figure A.6: Demonstrator success page

Appendix B

Bits and octets convention

B.1

In this document it is specified the value of each octet in an encoding by use of the terms "most significant bit" and "least significant bit".

B.2

In this document it is specified that the bits of an octet are numbered from 8 to 1, where bit 8 is the "most significant bit", and bit 1 the "least significant bit".

Appendix C

Multi Purpose Code

C.1 XML

C.1.1 XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="Author">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="FirstName" type="xs:string" />
        <xs:element name="LastName" type="xs:string" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

C.1.2 Resulting XML

```
<?xml version="1.0"?>
<Author xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:noNamespaceSchemaLocation="Author.xsd">

  <FirstName>Mark</FirstName>
  <LastName>Twain</LastName>
</Author>
```

C.1.3 XML to Transform

```
<card type="simple">
  <name>John Doe</name>
  <title>CEO, Widget Inc.</title>
  <email>john.doe@widget.com</email>
  <phone>(202) 456-1414</phone>
</card>
```

C.1.4 XSLT Style Sheet

```
<?xml version="1.0" encoding="UTF-8"?>

<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0"
  xmlns="http://www.w3.org/1999/xhtml">

  <xsl:template match="card[@type='simple']">
    <html xmlns="http://www.w3.org/1999/xhtml">
      <title>business card</title>
      <body>
        <xsl:apply-templates select="name"/>
        <xsl:apply-templates select="title"/>
        <xsl:apply-templates select="email"/>
        <xsl:apply-templates select="phone"/>
      </body>
    </html>
  </xsl:template>

  <xsl:template match="card/name">
    <h1><xsl:value-of select="text()"/></h1>
  </xsl:template>

  <xsl:template match="email">
    <p>email: <a href="mailto:{text()}"><tt>
      <xsl:value-of select="text()"/>
    </tt></a></p>
  </xsl:template>
  ...
</xsl:stylesheet>
```

C.1.5 Resulting XML

```
<html xmlns="http://www.w3.org/1999/xhtml">
  <title>business card</title>
  <body><h1>John Doe</h1><h3><i>CEO, Widget Inc.</i></h3>
    <p>email: <a href="mailto:john.doe@widget.com">
      <tt>john.doe@widget.com</tt></a>
    </p>
    <p>phone: (202) 456-1414</p>
  </body>
</html>
```

Appendix D

Multiplatform Common and Adaptive Middleware: Working

This appendix is a small demonstration of the current implemented solution for the Multiplatform Common and Adaptive Middleware in chapteradapgui. Using the Portuguese CC as a demonstration basis, a XML profile is displayed, representing the access to different information on the card with different ways of handling. On print screens is displayed the graphical output.

D.1 Profile

D.1.1 XML Profile

```
1
2  <?xml version="1.0" encoding="UTF-8"?>
3  <xs:citizen xmlns:xs="http://www.example.org/schema2"
4          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
5          xsi:schemaLocation="http://www.example.org/schema2 src/xmlSchemas/schema2.xsd ">
6
7    <xs:applet aid="0x60:0x46:0x32:0xFF:0x00:0x00:0x02" isApplet="true"/>
8
9    <xs:tab value="Identification">
10     <xs:singleFile isSingleFile="true" path="0x5F:0x00:0xEF:0x02"/>
11     <xs:protected isProtected="false" pinEtcInfo=""/>
12
13     <xs:label target="labelName" targetText="Nome Completo:" targetX="50" targetY="50"
14         targetW="90" targetH="17" target2="labelName2" targetText2="" targetX2="160"
15         targetY2="50" targetW2="150" targetH2="17" offset="450" maxLength="120"/>
16
17     <xs:label target="labelBirthDay" targetText="Birth Day:" targetX="50" targetY="100"
18         targetW="50" targetH="17" target2="labelBirthDay2" targetText2="" targetX2="120"
19         targetY2="100" targetW2="50" targetH2="17" offset="578" maxLength="20"/>
20
21     <xs:label target="labelIdNumber" targetText="Id Number:" targetX="50" targetY="150"
22         targetW="50" targetH="17" target2="labelIdNumber2" targetText2="" targetX2="120"
23         targetY2="150" targetW2="50" targetH2="17" offset="606" maxLength="18"/>
24   </xs:tab>
25
26   <xs:tab value="Address">
27     <xs:singleFile isSingleFile="true" path="0x5F:0x00:0xEF:0x05"/>
28     <xs:protected isProtected="true" pinEtcInfo=""/>
29
30     <xs:label target="labelConcelho" targetText="Concelho:" targetX="50" targetY="50"
31         targetW="50" targetH="17" target2="labelConcelho2" targetText2="" targetX2="120"
```

```
32          targetY2="50" targetW2="50" targetH2="17" offset="118" maxLength="100"/>
33
34      <xs:label target="labelFreguesia" targetText="Freguesia:" targetX="50" targetY="150"
35          targetW="50" targetH="17" target2="labelFreguesia2" targetText2="" targetX2="120"
36          targetY2="150" targetW2="50" targetH2="17" offset="230" maxLength="100"/>
37    </xs:tab>
38  </xs:citizen>
```

D.2 XML Description

Looking at line 7 of the XML it can be seen that the Portuguese CC is a multiplication card (Java card) and the eID Applet Identifier (AID) is also described in this line. With this info it is possible to select that particular applet and access its eID functionalities. Line 9 to 24 identifies the first tab that shows in the application and, under its wing all the labels that will contain the requested data and, their location in the GUI (figure D.1). Finally, the second tab ("Address") contains a special parameter in line 27 stating that this is protected information and the use of a PIN is required to access it (figure D.2). Finally, after PIN insertion the data can be accessed (figure D.3).

Figure D.1: Public Personal Data

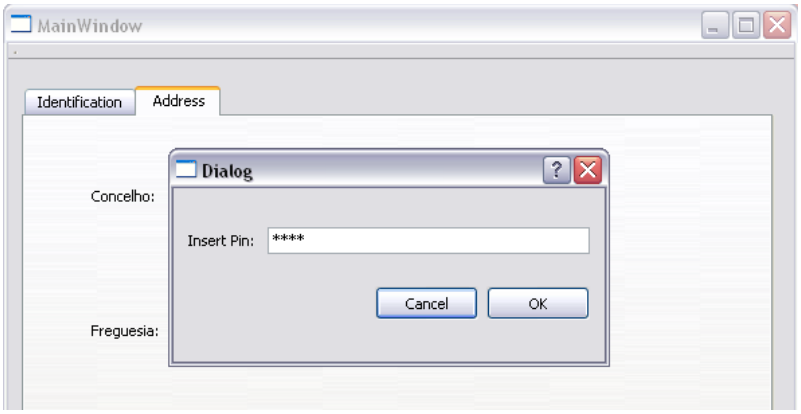

Figure D.2: Request PIN

Figure D.3: Protected Personal Data