FIDIS

Future of Identity in the Information Society

Title:	"D3.6 Study on ID Documents"
Author:	WP3
Editors:	Dr. Martin Meints (ICPP, Germany)
	Marit Hansen (ICPP, Germany)
Reviewers:	Jozef Vyskoc (VAF, Slovakia)
	Ronald Leenes (Tilburg University)
	Mark Gasson (Reading University)
Identifier:	D3.6
Type:	[Deliverable]
Version:	1.10
Date:	Wednesday, 20 December 2006
Status:	[Final]
Class:	[Public]
File:	fidis-wp3-del3.6.study_on_id_documents.doc

Summary

This document gives an overview of concepts, prototypes and implementations of European ID documents including machine readable travel documents (MRTDs). Although not totally comprehensive, it summarises basic technologies that are used for ID documents such as PKI, RFID, biometrics and chip card technologies. Legal grounds for European MRTDs are described and analysed. In addition to a short overview on implementations, five good practice examples are described and discussed. Security and privacy aspects of ID documents are analysed basing on current state-of-the-art in the described basic technologies and existing implementations of ID documents. Further, critical elements of cost projections for ID documents are presented and analysed from a social perspective.

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	20.09.05	• Initial structure of the draft, draft version of chapter 2 (Martin Meints, ICPP)
0.2	12.01.06	• Structure revised, abstracts and first contributions (chapters 3.1, 3.3, 3.4, 3.5, 3.6, 5.1, 5.7, 6.2 and 6.3) included (Martin Meints, ICPP)
0.3	27.02.06	• Contributions with three exceptions integrated, chapter introductions and conclusions added, integrative editing (executive summary and general conclusions still missing) (Martin Meints, ICPP)
0.4	06.03.06	• Additional input for the chapters 2.1, 3.3, 3.7, 3.8, 5.3, 5.5, 5.8.2, 6.2 and 6.4, integrated. Summaries and conclusions written, glossary integrated. (Marit Hansen, Martin Meints, ICPP)
0.5	13.03.06	• Additional input for chapter 3.2, 3.7, 3.8, 4.1, 5.8 and 7 integrated, summaries adjusted, references integrated (Martin Meints, ICPP)
0.6	17.03.06	• Chapter 4.1 integrated, summary finished, executive summary added (Martin Meints, ICPP)
1.0	30.03.06	• Remarks of the internal reviewer and replies of the corresponding authors integrated (Marit Hansen, Martin Meints, ICPP)
1.1	18.12.06	• Editorial changes throughout the document (Marit Hansen, Martin Meints, ICPP) • Recent and additional information on security of MRTDs integrated and analysed (chapters 1, 3.3, 5.3, 6.3, 6.7 and 8) (Martin Meints, ICPP)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Executive Summary)	Martin Meints (ICPP), all
2 (Introduction)	Stephan Alexander Freh (chapter 2.1, LSE), Martin Meints (chapter 2.2 and 2.3, ICPP)
3 (Basic Technologies for ID Documents)	Marcel Jacomet (chapter 3.2, AXSionics), Mark Gasson (chapter 3.3, Reading University), Günter Karjoth (chapter 3.3, IBM ZRL), Stephan Alexander Freh (chapter 3.7, LSE), Martin Meints (chapter 3.1, 3.4, 3.5, 3.6 and 3.8 ICPP)
4 (Legal Grounds for ID Documents in Europe)	Paul De Hert, Wim Schreurs (chapter 4.1.1 to 4.1.5, VUB) Eleni Kosta (chapter 4.1.6, KU Leuven), Xavier Huysmans (chapter 4.2, KU Leuven)
5 (Leading Concepts, Prototypes and Implementations)	Claudia Diaz (chapter 5.2, KU Leuven), Marit Hansen (chapter 5.2 and 5.8, ICPP), Danny De Cock, Christopher Wolf and Bart Preneel (chapter 5.6, KU Leuven), Eleni Kosta (chapter 5.5, KU Leuven), Reshma Thomas (chapter 5.4 KU Leuven), Martin Meints (chapters 5.1, 5.2, 5.3, 5.5, 5.7, 5.8 and 5.9, ICPP)
6 (Security and Privacy Aspects)	Els Kindt (chapter 6.3.1, KU Leuven), Andreas Pfitzmann, Sandra Steinbrecher (chapter 6.3.2, TU Dresden), Eleni Kosta (chapter 6.4.1, KU Leuven), Günter Karjoth (chapter 6.4.2, IBM ZRL) Marcel Jacomet (chapter 6.5.1, AXSionics), Marit Hansen (chapter 6.5.2, ICPP), Reshma Thomas (chapter 6.6, KU Leuven), Martin Meints (chapter 6.1, 6.2 and 6.7, ICPP)
7 (Economic Aspects)	Ian O. Angell, Dionysios S. Demetis (LSE)
8 (Summary, Conclusion and Outlook)	Martin Meints (ICPP), all

Table of Contents

1 Executive Summary 8

2 Introduction 12

2.1 Identity, Identity Management, and eID 12
2.2 Scope and Structure of the Document 12
2.3 Categorisation of ID Documents 14

3 Basic Technologies for ID Documents 15

3.1 Introduction 15
3.2 Chip Card Technologies (Smart Cards) 15
3.2.1 History 15
3.2.2 Smart Card Technology 16
3.2.3 International Standards 17
3.3 RFID for Machine Readable Travel Documents 18
3.3.1 Contactless Automatic Identification 19
3.3.2 Use of Contactless Technology in MRTDs 20
3.3.3 MRTD Data 21
3.4 Electronic Signatures 22
3.5 Biometrics 23
3.6 Back-Office Systems 25
3.6.1 PKI 25
3.6.2 Databases for Biometric Reference Data 27
3.6.3 Other Back-Office Systems 28
3.7 Interoperability Aspects 28
3.7.1 Interoperability 28
3.7.2 Value and Use of Privacy Enhancement Technologies in eIDs 31
3.7.3 Mergence of eID, Interoperability and Privacy 32
3.7.4 eID Interoperability Analysis 33
3.8 Summary and Conclusions 37

4 Legal Grounds for ID Documents in Europe 40

4.1 Machine-Readable Identity Documents with Biometrical Data in the EU Legal Framework. 40
4.1.1 Introduction 40
4.1.2 Overview of Legal Instruments 41
4.1.3 European Data Protection and Human Rights Framework 52
4.1.4 Critical Observations 56
4.1.5 Conclusion 69
4.1.6 Legal Sources with Respect to RFID 70
4.2 A Regulatory Framework for Entity Authentication and Pan-European eIDs? 71
4.2.1 Introduction 71
4.2.2 Context of the Study 71
4.2.3 Using the Existing Regulation as far as Possible 72
4.2.4 Key Issues When Drafting a Directive on Authentication 74
4.2.5 Porvoo / Myhr's Suggestions 78
4.2.6 Conclusion 79

5 Leading Concepts, Prototypes and Implementations 81
5.1 Introduction 81
5.2 Overview on ID Documents in Europe 82
5.3 European Passport 85
5.4 FINEID Card 86
5.5 Austrian "Bürgerkarte" 90
5.6 Belgian ID Card 94
5.7 German E-Health Card 99
5.8 Alternate Implementations and Ongoing Research 101
5.8.1 Laser Band Technology in the Italian eID Card 101
5.8.2 Principles for eIDs and Suggestions for Advanced eID Concepts 101
5.8.3 Server Derived IDs 102
5.9 Summary and Conclusions 102
6 Security and Privacy Aspects 104
6.1 Introduction 104
6.2 General Threats 104
6.3 Biometrics 105
6.3.1 The Legal and Procedural Perspective 105
6.3.2 The Technical Perspective 111
6.4 RFID 115
6.4.1 The Legal and Procedural Perspective 115
6.4.2 The Technological State-of-the-Art 118
6.5 Chip Card Technologies (Smart Cards) 123
6.5.1 Security Aspects 123
6.5.2 Privacy Aspects 126
6.6 Electronic Signatures and PKI 127
6.6.1 Risks of Using PKI 127
6.6.2 Conclusion 128
6.7 Summary and Conclusions 129
6.7.1 Technology related conclusions 129
6.7.2 Conclusions with respect to MRTDs 130
7 Economic Aspects 133
7.1 Complexity Factoring into the Economics of eIDs 133
7.2 Cost Projection Elements (of Systemic Economic Complexity) 134
7.3 Cost Projection Elements (of Environmental Complexity) 139
7.4 Conclusions 141
8 Summary, Conclusions and Outlook 143
9 References 147
10 Glossary and Abbreviations 156
11 Appendices 159
11.1 List of Figures 159
11.2 List of Tables 160

1 Executive Summary

This document concentrates on the technical perspective of ID documents and focuses on the use of new technologies. It non-exhaustively covers existing and planned electronic ID documents, also called eID documents, within the EU which use technologies for identification of citizen for various purposes. In addition on a European level the corresponding legislation is described and analysed with respect to the European data protection and privacy framework. A special emphasis is put on the European passport as the European implementation of international Machine Readable Travel Documents (MRTDs).

The study starts with the description of five highly relevant technologies including the corresponding standards for current concepts and implementations of ID documents. These include:

- Chip card technology (smart cards)
- RFID
- Electronic signatures and PKI
- Biometrics
- Back-office systems such as biometrics databases.

Relevant aspects of interoperability of European eIDs are described and analysed. It can be concluded that by looking on a global and EU level common law based countries seem to have an extremely low adoption rate of national eID strategies. In contrast the civil law based European nations seem to be among the group of early adopters of national eID solutions. Despite that perhaps surprisingly clear and evident finding, by far the more challenging and pressing problem appears on a pan-European eID interoperability level, as the national individual legislation has to be harmonised in order to allow EU Member States to share, interconnect and use national versatile identities. Issues like data protection, privacy, information liability, access authority and the quality of authentication are heavily disputed issues.

In chapter 4 current European initiatives regarding machine-readable documents with biometrics are described: Eurodac (the EU central fingerprint database in connection with asylum seekers), the Visa Information System (VIS – the EU central database set up to create a common visa policy) and the European Passport (requiring fingerprints and facial images as biometrical identifiers). These initiatives are analysed with respect to the European data protection and privacy framework resulting in the following conclusions:

- The European data protection and privacy frameworks apply to the Regulations but in no case this means that the Regulations are *a priori* compliant with the Data Protection Directive nor with the European Charta of Human Rights (ECHR). In addition machine-readability of people and of their documents may turn out to be excessive, hereby surpassing the necessity and proportionality criteria set out by the European Court of Human Rights.

- The legal basis itself of the VIS and EU passport Regulations is questioned. While the VIS is in fact a 'first pillar' database, the proposal for the EU passport Regulations provides for access possibilities by 'third pillar authorities' – for which normally other legal grounds than Articles 62 and 66 of the Treaty establishing the European Communion (TEC) must be invoked. While the EU regulates its passport on the basis of standards established by non-democratic standardisation bodies (ICAO), Article 18 (3) of the TEC even excludes the adoption of provisions by the EC on passports, identity cards, residence permits or any other such document.
- Eurodac, the EU passport and the VIS are subject to possible change in purposes for which stored data could be used (so-called function creep) that is not foreseeable. The impact of this deployment and the future of identity can – regrettably – not be entirely assessed at this moment. A step-by-step approach seems the essential requirement to safeguard the fundamental rights and freedoms.

In addition a study written by Thomas Myhr[165] with respect to a European legal framework for ID documents is compared with the results of a similar discussion in the Porvoo group[34]. The chapter concludes that in this area still basic research is necessary.

In chapter 5 a non-exhaustive overview on current concepts and implementations of European ID documents is given. Five implementations or concepts in advance phases of the project are described and analysed. This includes (1) the European passport, (2) the FINEID, (3) the Belgian citizen card, (4) the Austrian Citizen card ("Bürgerkarte") and (5) the German e-health card. From the analysis with respect to the implementation of the projects the following factors of success could be concluded:

- Careful planning especially concerning the purpose of the eID and the appropriate technical solution (keep it small and smart); this should include technical, formal and informal aspects of interoperability
- Intensive laboratory and field testing of prototypes
- Refinement of the concepts using the results of the testing phase
- Open communication within the project including all stakeholders of the eID and external experts
- Appropriate education and qualification of the personal involved in the project

In addition alternate implementations and ongoing research in the area of ID documents are summarised.

The main already introduced basic technologies for ID documents are analysed with respect to security and privacy. Chip card technology has been discussed, used and further developed for many years now. As a result this technology is accepted as mature by technicians and privacy commissions in Europe. Of course, the combination of chip card technology with other technologies such as biometrics can result in new questions concerning security and privacy. PKI also has been used for ID document systems in some European countries for nine years now, though the number of issued certificates still seems to be limited. No major

security problems were published. PKI currently does not implement privacy in an optimised way because of the existing linkability of transactions performed via the information in the certificates. Current technical approaches to improve the privacy compliance for authentication purposes using eIDs are presented and analysed in this document.

In difference to these established technologies the use of biometrics and RFID in ID documents is relatively new. The first European ID document using both of these technologies is the **European passport**. RFID and biometrics raise a number of obvious privacy and security issues.

In addition to well documented security aspects of biometrics, for example with respect to (1) the quality of biometric identification, (2) identity theft and (3) devaluation of classic forensic techniques, a number of privacy aspects still needs to be addressed. This includes (1) minimisation of linkability, (2) enforcement of the purpose binding principle and (3) avoidance of additional, in many cases health concerning, information in biometric raw data. Advanced technical approaches for authentication using biometrics have not been tested for or implemented in ID documents so far.

RFID originally has been designed for unrestricted remote access to the information stored on RFID tags. For the use of RFID in the European passport basic security measures, for example Basic Access Control (BAC), have been applied to restrict the unauthorised access. BAC seems to be cryptographically weak and uses information stored in the Machine Readable Zone (MRZ) on the document itself; this is like storing the key of a cash box directly under it. Together with well documented projects of non-European countries aiming at the storage of biometric data of foreign visitors in large databases[301], this creates a significant risk of identity theft via biometrics in cases the document is (even properly!) used or gets lost. Extended Access Control though cryptographically improved significantly will not solve the described access control issues. In addition meanwhile cloning of an RFID chip in a German passport was demonstrated.

From the technological perspective biometrics and RFID as implemented in the European passport do not seem mature. For the use of the European passport as issued currently we suggest:

- The European passport should be used and carried around only when necessary.
- In case the European passport is not used, it should be kept in a Faraday cage (for example aluminium foil) to hamper unauthorised and unrecognised access.
- In case the European passport is not used, it should especially be locked carefully to avoid loss or theft of the document because of additional risks compared to traditional paper documents.

In addition organisational implementation and enforcement of the finality principle is required, especially for biometrics used in European passports, where the defined purpose is identification of international travellers. Passports should not be used for authentication purposes, e.g., in the private sector. Citizens need to be informed of the risks inherent in owning, carrying and using their passports and the corresponding security measures which can be undertaken by them (see above). Security measures such as Faraday cages, which are

available but not widely implemented, should be integrated into newly issued Passports immediately. In addition organisational and technical procedures are required to prevent abuse of personal data from Passports, including tracking and identity theft.

For the next generation of the European passport, a new convincing and integrated security framework covering MRTDs and related systems needs to be developed. It should be investigated how the implementation of technologies utilised can be improved, e.g., on-card matching and on-card sensors for biometrics and it should be considered whether inherently more secure and privacy-preserving technologies such as contact instead of contactless mechanisms should in fact be used.

Finally economic factors that are relevant for eIDs were analysed. A number of elements that are critical for the cost projection have been elaborated and described. In addition the post implementation costs have to be calculated carefully to get a view on the Total Costs of Ownership (TCO) for an eID solution. Relevant factors in this context are:

- Security aspects
- Privacy aspects
- Renewal of identity documents and register updates
- Handling of complaints and false negatives
- Internal audits
- Costs of management of the register
- Infrastructural costs and integration

The analysis performed in this Deliverable shows that there is need for enhancement of eID concepts and implementations. In the future this topic should be further monitored within the FIDIS network. We hope that the findings from eID research will be considered in future (and perhaps even current) plans in the field of eIDs and related systems.

2 Introduction

2.1 Identity, Identity Management, and eID

Identity is understood as being any subset of attributes of an individual which uniquely characterise this individual within any set of individuals. Put this way, there is no such thing as "the identity" (Hansen et al. 2003). Identity is therefore explained as an exclusive perception of life, integration into a social group and continuity, which is bound to a body and shaped by society. Other models distinguish between *ipse*-identity (the inner identity of a person) and *idem*-identity (its external projection) (Nabeth, Hildebrandt 2005). One must therefore recognise a difference between what constitutes an individual and what is used to identify him or her (the subset of attributes).

Once the totality or part of the subset of attributes become digitised then we have a transcendence and transformation of a person's identity to what we can call an *electronic identity* (*eID* hereinafter). The concept of an eID denotes all personal data that can be stored and automatically interconnected by a computer-based application. On a technical level, these attributes are data (Hansen et al. 2003).

The objective of any identity management solution is the identification, authentication and confirmation of an identity. In order to ensure trust among the communicating parties involved, further issues like non-repudiation, confidentiality, availability, and security have to be addressed (Backhouse et al. 2003). Technical solutions like Public Key Infrastructure (PKI), Digital Certificates (DC) and Trusted Third Party Services (TTPS) provide the basis for electronic or virtual identity and ID management. Academic scholars and professionals have been intensively involved with underlying issues such as policy making, liability, risk evaluation, legal frameworks, trustworthiness, data protection, privacy, and revocation (Backhouse 2000, CEN/ISSS 2004, Cowcher 2005, Dhillon and Backhouse 2001).

2.2 Scope and Structure of the Document

This "Study on ID Documents" which has been elaborated in the FIDIS workpackage "High-Tech IDs", concentrates on the technical perspective of ID documents and focuses on the use of new technologies. Thus, the study covers existing and planned electronic ID documents, also called eID[1] documents, within the EU using technologies for identification of citizen for various purposes. It bases in part on the results of FIDIS Deliverable 4.1 "Structured account and approaches on interoperability" (Backhouse, 2005), especially chapter 9 "case study: eID projects, from capability to use" and Deliverable 3.2 "Study on PKI and Biometrics" (Gasson, Meints, Warwick 2005)[2]. Further important aspects being discussed in this chapter are technical standards that are relevant for ID documents.

[1] As in Deliverable 4.1 "Structured account and approaches on interoperability" we adopt the following definition of Electronic Identity (eID) systems given in (CEN/ISSS 2004: p. 68): "*Electronic identity solutions have the aim to guarantee the identity of a person (or a legal entity, e.g. a company) during the access to e-services and in order to provide the trust to the parties involved in the electronic transaction."* In this sense eID documents are central parts of a system aimed to identify a person using technologies such as biometrics, electronic signatures, etc.

[2] Both reports are available from http://www.fidis.net/.

A special emphasis will be put on the European passport as the European implementation of international Machine Readable Travel Documents (MRTDs). The reasons are:

1. Within an international context European standards for security and data protection are now a generally accepted base for the use of MRTDs. The implementations of these fundamental aspects have to be ensured by international standards, treaties and corresponding technical and procedural implementations of MRTDs. Very sensitive aspects in this context are the issuing process and the implementation of a procedural and technical access control that ensures the use of personal data on MRTDs by authorised authorities for international agreed purposes only. As monitoring and enforcement of the purpose binding principle especially in an international context is very difficult, the implementation of the data minimisation principle becomes very important.
2. The European passport uses technologies and standards that have not been used in this way for international MRTDs to date.
3. The international issuing of new MTRDs is a very large project as the concept for MRTDs potentially has to be applicable for the whole global population.

The European passport uses a number of highly relevant technical standards that have been issued by the International Civil Aviation Organisation (ICAO)[3]. They will be analysed from a technical and procedural (chapter 3) and legal perspective (chapter 4) followed by an analysis of security and privacy aspects (chapter 6).

Basic technologies used for eID documents will be introduced and summarised based on other FIDIS studies in chapter 3. This study does not cover well established basic technologies of machine readability such as bar codes or optical character recognition (OCR) which have been utilised for more than 25 years (Garfinkel, Rosenberg 2005) and are still used for the machine readable zone (MRZ) on ID documents. Magnetic stripes which are not going to be used future eID documents are also omitted here.

In chapter 4 legal grounds for ID documents throughout Europe are summarised and analysed with respect to the European data protection and privacy framework. In addition current developments concerning a future European legal framework on ID documents are summarised. Chapter 5 starts with an overview on known ID documents in Europe. It continues with the introduction and discussion of five leading and typical concepts of ID documents.

In chapter 6 security and privacy issues of the introduced implementations are presented and examined. This chapter is followed by an overview on economic aspects which are relevant for most of the introduced eID documents. This study concludes with a summary and conclusions in chapter 8.

[3] See http://www.icao.int/

2.3 Categorisation of ID Documents

Looking into current and planned implementations, two general concepts for eID documents in Europe can be distinguished:

- Solutions bound to a specific implementation on a certain card; these implementations require a specific card, in some cases specific reader technologies and linkage to a specific back office technology. Examples are the Belgian ID card or the German e-health card.
- Solutions basing on certificates and procedures which are not bound to a specific card; these implementations do not require a specific card because a standardised back office technology such as PKI or PKI in combination with additional procedures is used. To carry the necessary certificates or other information needed for procedural purposes, a variety of commercially available card solutions can be used; this includes in some cases even SIM cards of mobile phones. Examples of this type are the Austrian "Bürgerkarte", the FineID Card and the German JobCard procedure.

Current implementations, prototypes and concepts cover a large range of purposes. Currently the most important four among them are[4]:

Abbreviation	Purpose for / sector of use
Ident	Official identification of a citizen of a state by passports or official identity cards
Sign	Identification of an individual/company and electronic signing for e-government and / or e-commerce applications; remark: PKI integration needed
e-health	Identification of an individual and transfer of or access to sensitive data in the e-health sector (e-health cards)
SocIn	Identification of an individual and transfer of or access to sensitive data for social insurance purposes

Table 1: Purposes of ID documents

Existing solutions, concepts and prototypes cover one or more of these purposes.

[4] See also FIDIS Deliverable 4.1 "Structured account of approaches on interoperability" chapter 9 and references cited therein.

3 Basic Technologies for ID Documents

3.1 Introduction

In this chapter basic technologies which are going to be used for eID document-implementations are introduced. The selection of these technologies here is based on various presentations and demonstrations at the conferences Net-ID 2005[5], World eID 2005 and e-Smart 2005[6], Digital World ID 2005[7] and Net-ID 2006[8]. Currently the following technologies are mainly being discussed:

Abbreviation	Description
SmCh	Smart Chips
Laser	Laser-optical Zones for storage of mass data (up to 1.8 MByte)
RFID	Radio Frequency Identification
Cert	Digital Certificates
ElSig	Electronic Signatures
PKI	Public Key Infrastructure
Bio	Biometrics
Face	Face Recognition
Finger	Fingerprint Recognition
Iris	Iris Scan

Table 2: Overview on technologies used for eID documents

3.2 Chip Card Technologies (Smart Cards)

3.2.1 History

The name *smart card* is ambiguous and thus stimulates the imagination. The term *integrated circuit card* (ICC) is often used to encompass all those devices where an integrated circuit is contained within an identification card piece of plastic. These plastic cards have a well defined size 85.6mm x 53.98mm x 0.76mm. The first plastic cards had very limited technical functionality as they used an embossed card number for counterdrawing or magnetic stripe technology for machine reading. The first magnetic stripe cards were used in the early 1970s

[5] Net-ID 2005, 21-22 February, 2005 in Cologne, Germany. Proceedings / CD-ROM ISBN 3-923171-93-5. See also http://www.computas.de/html/netid-archiv1.html.
[6] World e-ID and e-Smart Conference 2005, 21-23 September, 2005 in Sophia Antipolis, France. Presentations are documented on CD-ROM. See also http://www.strategiestm.com/conferences/we-id/05/ and http://www.strategiestm.com/conferences/esmart/05/.
[7] Digital ID World 2005, 4-6 October, 2005 in Offenbach, Germany. Presentations are documented in the proceedings and on CD-ROM. See also http://www.digitalidworld.de/.
[8] Net-ID 2006, 30-31 February, 2005 in Berlin, Germany.

on transit tickets and in the 1970s for bank cards. Credit cards were first issued in 1951, but it was not until the establishment of standards in 1970 that the magnetic stripe technology continuously grew and became a factor in the use of plastic cards. Today with an infrastructure that encompasses every store in the high street giving them the ability to read the information on the magnetic stripe, the technology is everywhere. Although some limitations exist in the amount of information that can be stored on the stripe and the limitations in the security of the data, the magnetic stripe card will still be used in the foreseeable future. With the advent of new technologies many people have predicted the demise of the magnetic stripe. However with the investment in the current infrastructure the magnetic stripe card will still co-exist with newer technologies for at least another decade.

3.2.2 Smart Card Technology

Smart cards are not new either. The idea to put an integrated circuit into a plastic card is nearly as old the first commercial integrated circuits itself. The first patent for a smart card technology was filed in 1971 and the first cards were used more than two decades before. The technology was rapidly accepted in Europe because the high cost of telecommunications made on-line verification of transactions very expensive. The smart card provided the mechanism to move that verification off-line, thus reducing the cost without sacrificing any of the security. Smart cards can be as small as SIM cards (25.1mm x 15.1mm x 0.76mm) or as large as the well known plastic cards described above. Smart cards contain relatively large amount of information in an embedded micro-chip. There are several terms used to identify cards with integrated circuits embedded in them. The terms *chip card*, *integrated circuit card*, and *smart card* really all refer to the same thing.

There are two types of smart cards. The first is really a “dumb” card in that it only contains memory. These cards are used to store information. Examples of this might include stored value cards where the memory stores a Euro value which the user can spend in a variety of transactions. Examples might be pay phone, retail, or vending machines. The second type of card is a true “smart” card where a microprocessor is embedded in the card along with memory. Now the card actually has the ability to make decisions about the data stored on the card. The card is not dependent on the unit to which it is attached to make the application work. A smart purse or multi-use card is possible with this technology. As there is a microprocessor on the card, various methods can now be used to prevent access to the information on the card to provide a secure environment. This security has been touted as the main reason that smart cards will replace other card technologies.

The microprocessor type smart card comes in two flavours – the contact version and the contactless version. Both types of cards have the microprocessor embedded in the card however the contactless version does not have the gold plated contacts visible on the card. The contactless card uses radio communication to pass data between the card and the reader without any physical contact being made. The advantage of this contactless system is that there are no contacts to wear out, no chance of an electric shock coming through the contacts and destroying the integrated circuit, and the knowledge that the components are completely embedded in the plastic with no external connections. The disadvantage to this is that the card and reader are slightly more sophisticated and hence are more expensive. The biggest disadvantage today with smart cards is the cost to create a smart card system. Individual card prices have fallen over the past few years but they are still high when compared with a magnetic stripe card. The biggest advantage is of course the amount of data that can be stored

and last but not least, the security that can be built into the card. Standards for the smart card technologies exist for both contact and contactless versions of the technology.

3.2.3 International Standards

The prerequisite for the worldwide penetration of smart cards into everyday life, such as their current use in Europe in the form of telephone cards, health insurance cards and bank cards, has been the creation of national and international standards. A smart card is normally one component of a complex system. This means that the interfaces between the card and the rest of the system must precisely be specified and matched to each other. This could be done on a case-by-case basis, without regard to other systems. However this would mean that a different type of smart card would be needed for each system. Users would thus have to carry a separate card for each application as it is still common today. In order to avoid such situations in the future, an attempt has been made to generate application-independent standards that allow multi-functional cards to be developed. A good example is telephone cards. In technical terms, they are very simple objects. Their true function, which is to allow public telephones to be used without coins, can be realised only after umpteen thousand card phones have been installed throughout a region and connected to a network. The large investment required for this can only be justified if the long-term viability of the system is ensured by appropriate standards and specifications. Standards are an indispensable prerequisite for the emerging multi-functional smart cards for several applications, such as telephony, electronic purses, electronic tickets etc.

The ISO/IEC (International Organization for Standardization / International Electrotechnical Commission) standards are especially significant for smart cards, since they define the basic properties of smart cards. The purpose of these worldwide associations of around 100 national standards agencies is to promote the development of standards throughout the world, with the objective to simplifying the international exchange of goods and services, and developing cooperation in the fields of science, technology and economy. Both, globally operating large enterprises down to small start-up companies profit from standardisations. For the global players international standards may act as a protection for large investments, for small companies standards may be the entry ticket in large markets which otherwise might have been closed to them.

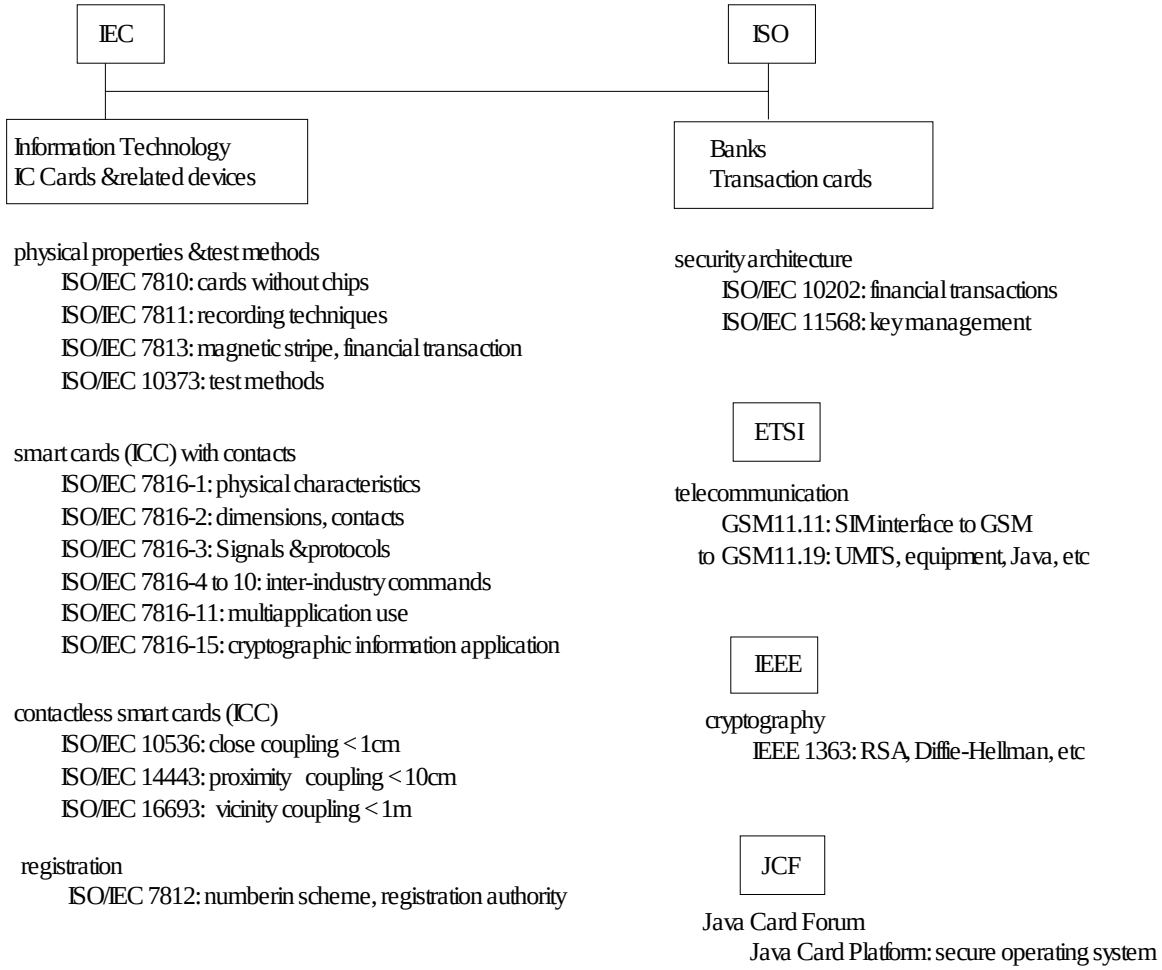

Figure 1: Overview of important international standards for smart cards.

The list shown in Figure 1 is by far not complete as there exist numerous additional national and international standards and specification organisations who made contributions related to identification cards (EN, FIPS, DIN, Java Card Forum, etc).

3.3 RFID for Machine Readable Travel Documents

The European Union sees the introduction of the epassport as a step towards rendering passports more secure against forgery while facilitating more reliable border controls. This is further driven by the USA's insistence that countries wishing to use its visa waiver programme must have in place a programme to put 'biometric chips' in their passports.

The epassport is a specific type of Machine Readable Travel Document (MRTD). Many existing passports are already MRTDs which use a Machine Readable Zone (MRZ) at the bottom of the passport with two lines of forty-four characters each which encode all of the passports key information. These characters are printed in the monospace font OCR-B at "Size 1", as required by the ISO Standard 1073-2:1976. The location of the MRZ, the type of paper, reflectivity and so on are specified in ISO 1831:1980. However, these documents have to be swiped through a reader, i.e. they are not contactless. The new epassports will not only

be contactless, but will also contain other biometric[9] details from the owner which can be used for identification in addition to the standard printed data, see Figure 2.

Figure 2: A transparent sample epassport showing the normally visible MRZ at the bottom and the normally hidden RFID loop antenna with the small RFID tag in the antenna top left which holds the biometric data

Globally, the International Civil Aviation Organization[10] (ICAO)'s Document 9303 has been adopted as the standard for these new epassports. By adopting a global standard, all passports should be interoperable between regions and countries. Differing from the traditional passport, the standard specifies the use of a microchip embedded in an a plastic card in the paper passport and a contactless mechanism for data communication.

3.3.1 Contactless Automatic Identification

Methods of automatic identification have become increasingly popular over the last few decades, perhaps being traced back to the now ubiquitous barcode and more recently the smart card.

However, it was found that a more flexible method of auto-ID would allow for reprogramming of the data the item carried, use a contactless method of transferring this data, and it would have power supplied to it by the reading device, i.e. it would not need its own power supply such as a battery. Implementations of such a device have become known by the generic term Radio Frequency Identification (RFID) due to the method of data transfer and power, i.e. by radio frequencies[11] which exist at the lower end of the electromagnetic spectrum, see Figure 3. RFID is a specific means of automatically identifying an item and is part of a class of technologies known as Dedicated Short Range Communication (DSRC) technologies.

[9] More detail on biometrics can be found in FIDIS deliverable D6.1 at http://www.fidis.net/
[10] http://www.icao.int/
[11] Radio Frequencies (RF) are the portion of the electromagnetic spectrum in which electromagnetic waves can be generated by alternating current fed to an antenna.

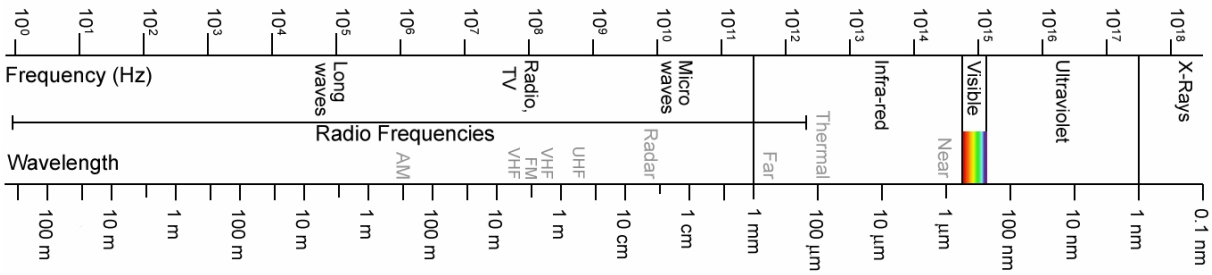

Figure 3: Electromagnetic spectrum showing the broad range of the radio wave frequency component

The RFID system consists of two main components (see Figure 4), the small transponder, more commonly known as a tag, which is attached to the item needing identification and the interrogator, or reader, which is used to power the tag and read its data without contact. The tag is known as a passive transponder since it is unable to function without the reader since the reader supplies the power it requires to function. Note that 'reader' is somewhat of a misnomer as the device can in some cases actually be used to write to the tag as well to change its data.

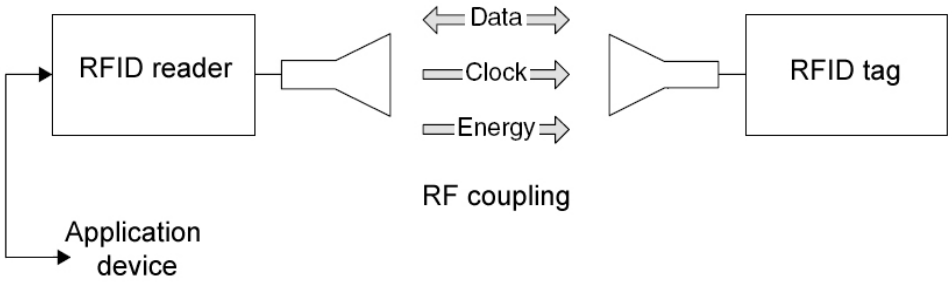

Figure 4: The two main components of the RFID system

The range of RFID implementations available are broad, and are covered in more depth in other FIDIS deliverables[12]. As such, here we shall only be concerned with the implementation utilised in the proposal for the new European epassport.

3.3.2 Use of Contactless Technology in MRTDs

For MRTDs, the ICAO specifies the use of the ISO 14443 standard for proximity coupling transmission between the epassport and the reader. It should be noted that this standard relates to contactless *smart cards* and not specifically to RFID tags. However contactless smart card and RFID technologies are related, and as the range of RFID technologies grows, the distinction between the two will continue to blur. However, essentially the contactless smart card is a 'high-end' RFID device, with the 'low-end' consisting of devices which have a simple, fixed data set, usually a serial number.

[12] This will be part of Deliverable D3.7 – A structured collection on information and literature on technological and usability aspects of Radio Frequency Identification (RFID)

The ICAO specification details the range over which the epassport should be readable, i.e. the distance from the reader in which the tag will be activated, and the operating frequency of radio waves which the reader should use and the tag should respond to. The different RFID transmission frequencies are classified into the three ranges, LF (low frequency, 30-300 kHz), HF (high frequency)/RF radio frequency (3-30 MHz) and UHF (ultra high frequency, 300 MHz-3 GHz)/microwave (>3 GHz). RFID systems are also classified by range into close-coupling (0-1 cm), remote-coupling (0-1 m), and long-range (>1 m) systems.

The MRTD standard specifies an operating frequency of 13.56 MHz and a read/write range of up to 10 cm. This frequency was chosen for various technical reasons such as suitability for efficient proximity inductive coupling (power transfer), compliance with EMC regulation (already allocated as ISM band) and low absorption by human tissues.

3.3.3 MRTD Data

The new epassport is to contain additional biometric information, stored within the embedded microcontroller and memory. The ICAO recommends a minimum memory size of 32 kBytes to store the data, although it indicates 512 kBytes as a target memory size. The MRTD storage mechanism has to operate in a write-once/read-many fashion, i.e. after the document is issued, it is impossible to change any data.

Data on the epassport is organised in the ISO 7816-4 standard logical data structure (LDS) which specifies a number of Data Groups, as well as the encoding of the data:

- DG1 is mandatory and contains the same data as printed on the passport, such as name, date of birth, expiration date, document number, nationality, etc.
- DG2 is mandatory and contains a ~15 kBytes JPEG2000 encoded facial image and corresponding biometric data
- DG3 is optional and is designated for biometric fingerprint data
- DG4 is optional and is designated for biometric iris data

The ICAO standard specifies that the data in DG1 and DG2 are stored unencrypted, since the same data is human-readable on the printed pages of the passport. However, it is up to the issuing country's discretion as to whether optional biometric data are encrypted – although this has wider interoperability issues. In any case, all biometric data are stored in the Common Biometric Exchange File Format (CBEFF) NISTIR 6529-A.

3.3.3.1 Basic Access Control

On the simplest level, the transmission between tag and reader incorporates basic error checking and correcting coding to ensure data integrity. However, this is only in place to protect against data corruption through outside interference during the data transfer. In order to protect against unauthorised disclosure of the digital data, Basic Access Control (BAC) is used to deny access to the MRTD data until the inspection system has proven that it is authorised to access it. The standard specifies that any communication leading-up to BAC has to be encrypted via ISO 7816-7/8 secure messaging.

The reader first acquires the standard MRZ information from the data page of the passport, generally via an OCR scanner. This MRZ information is used for computing the encryption and message authentication keys used for the "secure" exchange of the session keys. Using information that is available on the actual travel document is intended to limit access to only those people who have physical access to the passport.

3.3.3.2 Authenticity of the RFID

It is a further mandatory requirement that the data stored on the epassport is digitally signed by the issuing country. These digital signatures are stored on the epassport and are checked during validation of the document to ensure that the data has not been altered in anyway. This however does not alone protect against cloned MRTDs or the unauthorised disclosure of the digital data.

Active authentication is employed to verify that the chip has not been substituted. It is based on a challenge response protocol, using the Public Key Infrastructure (PKI) mechanism[13]. The keys required for this process that are stored in the epassport are located within secure memory, and cannot be accessed until the BAC stage has been successfully completed.

3.3.3.3 Extended Access Control

In August 2006 the draft version 1.0 of Extended Access Control (EAC) was published.[14] EAC aims at a more secure access control mechanisms and at stronger encryption of data transferred from the RFID chip to the reader. For this purpose (1) authentication of the reader using a public key infrastructure (PKI), (2) negotiation of session keys and (3) improved entropy and length of the session keys are core elements of EAC.

But EAC is only partially effective as only selected elements of the personal data (notably those categorised as privacy-sensitive such as biometric fingerprint data) are protected using the described enhanced mechanisms. Basic authenticating data such as the digital face picture and other personal data such as name, date of birth etc. are not covered. Furthermore, because EAC is not an international standard accepted by the ICAO, it cannot be enforced internationally, and thus non-European countries will only support BAC.

3.4 Electronic Signatures

A basic introduction of the European Directive 99/93/EU on electronic signatures, the technology and cryptography behind electronic signatures and possible privacy and security problems are given in the FIDIS Deliverable 3.2 "Study on PKI and Biometrics" (Gasson, Meints, Warwick 2005) in chapter 3.

[13] For more information on PKI see FIDIS deliverable D3.2: Study on PKI and Biometrics
[14] Issued by the German Federal Office for Information Security (BSI) and announced at http://www.bsi.bund.de/fachthem/epass/eac.htm

An important aspect is that although based on the European Directive 99/93/EU[15] the implementation of electronic signatures in Europe shows a large variety. So far no consensus has been reached as to which technological implementation can be used to reach one of four levels of electronic signatures (simple, advanced, qualified and accredited signatures) as defined in the European Electronic Signature Directive. In addition there is no consensus, for which kind of administrative procedures what kind of signature is needed.

Many European Countries have introduced signature schemes that do not necessarily need a smart card and a type III card reader (for example Lithuania, Austria, Finland). In these cases alternatively the signing procedure can be carried out using a mobile phone or even a USB stick (for example in Austria). In these cases we speak of a *procedural signature solution*. These signature solutions are not restricted to ID documents. Other countries such as Belgium and Germany tend to use signature cards and type III card readers for electronic signing in most e-government processes. In these cases we speak of a *card-bound signature solution*.

3.5 Biometrics

This chapter mainly describes biometrics relevant for ID documents, their planned use and technical limitations that will have influence on authentication procedures when using ID documents with biometric data and biometric authentication procedures.

Biometrics as an additional security element for international MRTDs such as passports have been discussed in the ICAO. This resulted in two resolutions[16] that biometric face data on passports are necessary for new passports issued and fingerprint and/or iris recognition may be used as additional biometric data. In addition the ICAO issued a technical report how biometrics in machine readable documents should be deployed (ICAO 2004). The EC Regulation 2252/2004[17] "on standards for security features and biometrics in passports and travel documents issued by the Member States" states, that biometric face data has to be implemented for new passports issued after mid of 2006. As additional biometric data fingerprints in interoperable formats are recommended for European countries. As a result most European countries currently prefer fingerprints as additional biometrics for the use in passports.

A basic introduction on biometrics including face geometry, fingerprinting and iris scan can be found in the FIDIS Deliverable 3.2 "Study on PKI and Biometrics" (Gasson, Meints, Warwick 2005) in chapter 4.

The ICAO issued standards on how biometric data is to be stored on passports (ICAO 2004, p. 59). These standards foresee biometric raw data using digital photos of the face, the fingertips and the iris. To store those photos the JPEG or JPEG-2000 format are to be used. Resolution and colour schemes are standardised in the following ISO norms:

- Face: ISO/IEC CD 19794-5

[15] European Parliament. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, January 2000.
[16] ICAO TAG-NRTG/NTWG Resolution N001 – Berlin, 28 June 2002; documented in (ICAO 2004, p. 17) and New Orleans Resolution, 21 March 2003, documented in ICAO 2004, p. 19).
[17] See http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf

- Fingerprints: ISO/IEC CD 19794-4
- Iris: ISO/IEC CD 19794-6

For example the resolution for a face image is according to ISO/EIC CD 19794-5 defined as 413x531 pixels (corresponding to 35x45 mm at 300 dpi) with an inner region of at least 240x320 pixels where compression should be lower than in the outer region. As colour schemes 24 bit RGB, 8 bit monochrome and YUV422 colour spaces are defined. This standard includes a number of rules and examples how pictures should be taken and prepared. The resulting image size should be 8 to 15 kBytes. The complete CBEFF file includes additional data in the facial record header such as the gender, eye and hair colour, a CBEFF header and a CBEFF signature.

The privacy implications of these standards will be discussed in chapter 6.3.

For fingerprints additional ICAO-standards can be used:

- Fingerprint minutiae format: ISO/IEC CD 19794-2
- Fingerprint pattern format: ISO/IEC CD 19794-3

On a European level currently the fingerprint picture according to ISO/IEC CD 19794-4 seems to be preferred[18].

Most biometric systems are optimised to be used with biometric templates. The German Federal Office for Information Security tested in 2003 to 2004 four pre-selected biometric systems (one for face geometry, two for fingerprinting, one for iris scan) with 2000 participants at Frankfurt airport. There is an ongoing discussion in Germany whether the conditions of these tests were optimistic compared to realistic conditions of future border controls ([19] and Krissler, Kurz 2005). But even if we do not take this into account this study shows a number of problems the planned use of biometrics in passports might encounter.

The quality of the authentication using templates and ICAO-compatible digital photos (BSI 2005) was compared. In general false rejection rates (FRR) were higher when ICAO-compatible digital photos were used as reference data.

An additional result of the BSI-study (BSI 2005) was that fingerprinting systems had the best recognition rates followed by face recognition and iris scan. Configuring the systems towards a False Acceptance Rate (FAR) of 0.1 % resulted in average FRR between 1.8% and 5 % (ibid, p.14). All investigated systems showed differences in the FRR between experienced users using the biometric systems every two weeks and a user using the system rarely (less than ten times within the testing period). Especially for iris scan FRR for users using the system rarely went up to 22%, for face recognition the FRR went up to 5.5% (ibid, p. 13).

Another study concerning the implementation of biometrics in MRTDs was published in 2005 by the Ministry of Interior of The Netherlands (BZK 2005). For this study 14504 test

[18] See http://www.interoptest-berlin.de/pdf/Carter_Munde_-_Brussels_Interoperability_Group.pdf
[19] For example: http://www.heise.de/newsticker/meldung/63024, http://www.ccc.de/updates/2005/pm20050906, http://www.heise.de/newsticker/meldung/64565

documents were issued and tested at Schiphol airport in Amsterdam. In general the test documents contained digital face data generated from a photo in accordance to the ICAO and ISO standards and digital data of two fingers according to the classes 1, 2 and 3 defined by the (U.S.) National Standards Institute and Technology (NIST) in 2004. Observed FRR for face recognition were ca. 4% (ibid p. 19). For fingerprinting in 7.8% of the initial tests after issuing of the test documents the verification of one or both fingers failed (ibid p. 21).

In addition the enrolment of biometrics to children was investigated. The study concludes that enrolment for fingerprinting up to the age of 6 is nearly impossible. Up to an age of 6 face recognition shows partially significant error to enrol rates (EER) in the range between 8% and 25% (ibid p. 27).

Another result of the tests in this study is that fingerprinting can not be enrolled to all people. The study concludes that rule on a European level are needed how to proceed in these cases (ibid p. 29).

Two procedural conclusions can be drawn from these results:

- It can be expected, that these FRR will in addition to the time needed to read out RFID and to perform biometric authentication increase the time needed for authentication when using biometric authentication.
- To deal with citizen not successfully authenticated when using biometrics (due to the ERR and FRR) internationally standardised and accepted back-up procedures are needed. This will especially be an issue at airports where most of the passengers are tourists that do not authenticate very often using biometrics.

The storage of biometric reference data in databases will be discussed in chapter 3.6.2.

3.6 Back-Office Systems

In addition to the infrastructure that is obvious for the user such as the ID document, reader technology, software to use the ID document or biometric sensors in many cases a remote infrastructure is used. This infrastructure provides reference data of different type depending on the technical method that is used and / or allows for logging of transaction data or the use of ID documents in general. These remote infrastructures are also called back-office systems. In this chapter we are introducing back-office systems that are highly relevant for ID documents.

3.6.1 PKI

Public key infrastructure (PKI) in general has been introduced in the FIDIS Deliverable 3.2 (Gasson, Meints, Warwick 2005). In this document we will focus on current developments to reach interoperability on a technical level in Europe with respect to ID document, as this was not covered in the FIDIS Deliverable 3.2.

Especially relevant for ID documents are differences that can be observed among European countries in the way the PKI is operated. While the registration and certification for example in Austria and Belgium is done by the public administration (supported by enterprises), registration and certification is done by private enterprises for example in Germany and Sweden. In addition to the differences there is no European Root-CA. As a result electronic signatures today are on a technical level not interoperable in Europe.

Currently we observe two approaches to address the technical aspects of interoperability of authentication procedures including the use of electronic signatures: The GUIDE project[20] and bridge-CAs.

GUIDE uses a federated network identity management approach (Guide 2005). General scenarios taken into account in the GUIDE project are principals logging onto a pan-European Governmental Service (PEGS) in a foreign country. In these cases the PEGS has no possibility to authenticate the foreign user (principal). To do this an Identity Provider (IP) in the home country of the principal is needed. This IP provides in general two basic services:

- Authentication Service (AS) and
- Attribute Provider Service (APS)

In cases where principal, PEGS and IP use standardised interfaces such as the GUIDE Interface communication would be quite simple as shown in the following figure[21]:

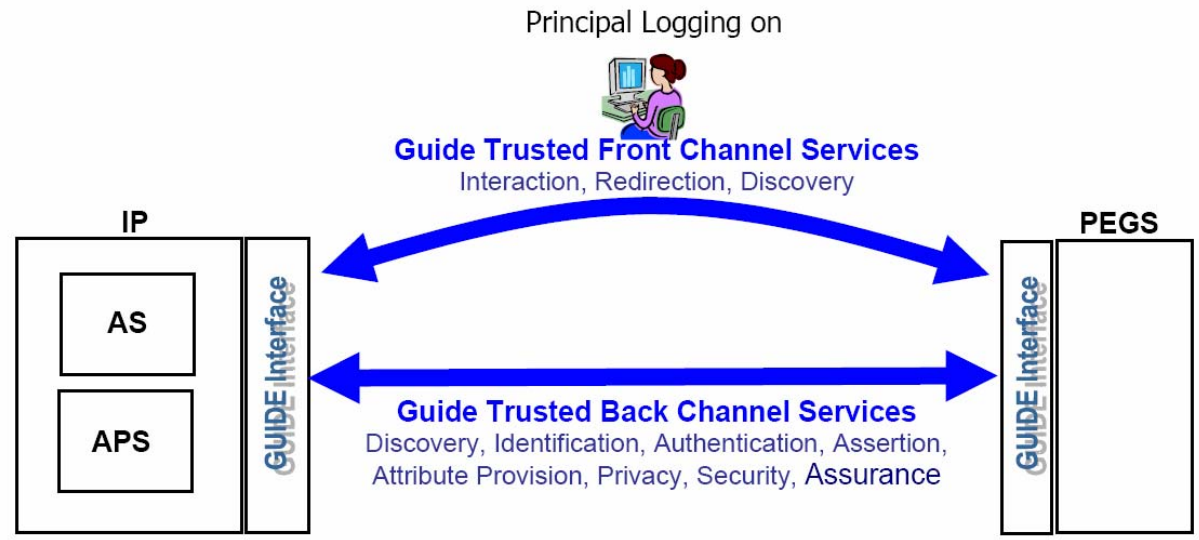

Figure 5: International authentication and authorisation using GUIDE interfaces and services

[20] See http://istrg.som.surrey.ac.uk/projects/guide/
[21] Figure taken from (Guide 2005), p. 19

Such an interface is not introduced so far; existing interfaces normally support national IPs only. In addition different communicational standards such as Liberty, SAML, Shibboleth and WS-* are supported and different document formats are used.

To overcome this situation GUIDE proposes the introduction of Gateways equipped with the GUIDE Software Agent (GSA). This agent transforms data formats and standards used by PEGS and IPs (in this example a remote procedure call (RPC) able web service application programming interface (WS API)) into an intermediary GUIDE profile as shown in the following figure[22]:

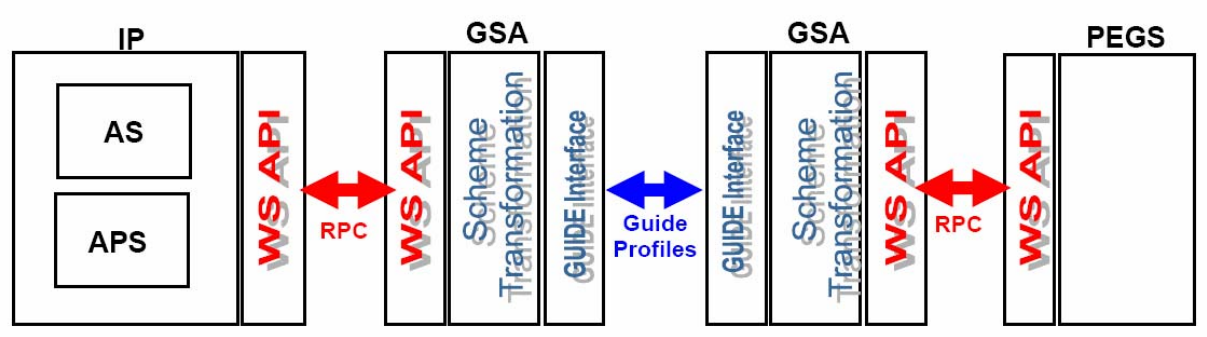

Figure 6: Gateways transforming nationally used data formats and standards for authentication

An alternate concept compared to the GUIDE-approach is the use of a so-called bridge-CA. Mainly driven by German and Austrian Certificate Authorities (CAs) the European Bridge CA (EB-CA)[23] offers interoperability of PKI and electronic signatures to her members (private and public organisations) in Europe, the US and Asia.

3.6.2 Databases for Biometric Reference Data

From a legal and technical perspective, where in addition to the MRTD the biometric data will be stored is an interesting question. On the European level a central database for biometric data has been discussed[24]. The resulting Council Regulation (EC) No. 2252/2004[17] ultimately does not include a central European database and leaves this topic up to national legislation in the member states (see Recital 4).

The European member states follow different strategies concerning central databases for biometrics, so that no general line can be observed. Central databases are planned in the UK[25], The Netherlands and Sweden (storage planned at the police), in Italy and Germany for example the data needed for the passports including biometric data will be stored decentralised in accordance with the issuing process at the municipalities. In France currently

[22] Figure taken from (GUIDE 2005), p. 20
[23] See http://www.bridge-ca.org/eb-ca2/index.php?option=com_content&task=view&id=19&Itemid=74
[24] For example see Proposal of the European Commission for the Council Regulation on standards for security features and biometrics in EU citizens' passport; download: http://register.consilium.eu.int/pdf/en/04/st06/st06406-re01.en04.pdf and the open letter to the European Parliament see http://www.edri.org/campaigns/biometrics
[25] See http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-168059

two different proposals are being discussed outlined in the INES project (proposed by the Ministry of Interior) and the strategic e-government plan. While the strategic e-government plan foresees a decentralised storage of biometric data, the INES project prefers a centralised database for all citizens.

In addition to databases set up by the issuing countries of ID documents some non-European countries plan to implement databases on biometrics of foreign visitors[301]. In this case the issuing countries and the users of the ID document have no control any more over their personal data. This is especially problematic in countries where data protection, fair information practices and similar principles are not applied.

3.6.3 Other Back-Office Systems

Depending on the purposes for which additional ID documents are going to be used additional back-office systems may be used. They are dependent on the underlying procedures and different, mainly national implementations. Mainly those back-office systems play a role in the social insurance and health sector. Planned implementations show a big variety. Examples are:

- Centralised database approaches for permanent data storage and workflow-systems basing on that data (such as planned for social security data in the German JobCard),
- Combined approaches for long term, database like storage of certain data and post-box like, short term storage of other data (such as implemented in prototypes of the German e-health card)

In these different back-office systems the ID document has different functions. Mainly it is used to identify and authenticate citizen and officer processing the data. In rare cases such as the German e-health card the central storage is a back-up and the enabler for additional functions for the e-health card.

3.7 Interoperability Aspects

This section starts by examining interoperability and its relation to identity and privacy from a rather theoretical perspective before it focuses on the current situation of eID interoperability in Europe and other countries world-wide. A theoretical perspective at this stage facilitates an in-depth understanding of the issues around interoperability.

3.7.1 Interoperability

Even though some define interoperability in order to describe the capability of different programs to read and write the same file formats and utilise the same protocols, such a definition is considerably skewed and prejudiced; the term *interoperability* itself lacks a dictionary definition (Payette et al. 1999).

Early academic publications on interoperability investigate the domain from a strong technical point of view (Miller et al. 2001). They typically explore interoperability within a defined scope, such as within a particular community (e.g., scientific communities, government agencies, commercial bodies), or within a specific organisation of information (e.g., software, electronic reports, technical records), or even within a particular information technology area (e.g., digital imaging, data visualisation, relational databases). Technical interoperability is concerned with the connection and compatibility of *computer systems over networks* and hence the right choice of IT artefacts grants a successful interconnection but still, the technical aspect of interoperability might be comparatively easy to achieve.

Studies on interoperability in government information systems address the challenges of generating a general structure for information access and integration across many of the different domains. A common goal of these efforts is to facilitate different government agencies, with different types of knowledge and solutions, to achieve an agreed level of information sharing and, through the process of computation and aggregation, to create new and more powerful types of information (Payette *et al.* 1999).

Interoperability within the context of pan-European information systems does not only mean that there is the potential for increased collaboration between national government offices to simplify transactions with citizens, but also the potential for improving relationships with business, adapt to a globalised and mobile world, and support entrepreneurship. It also requires the willingness to create more efficient cross-country processes to lower administrative costs, to consolidate the alliance between the EU Member States and to avoid the time-consuming redundancies of data between administrative agencies. *Interoperability is more than a simple connection between different computers on a wired or wireless network to transport digital data*. It is also the ability to share data, information and knowledge between different administrations, involving machine to machine[26], man to machine and human interactions. It also means a reorganisation of working processes, semantic compatibility and sharing of information in order to enable the seamless delivery of eServices (European Commission 2004b, Kinder 2003).

[26] Which is what we refer to as technical interoperability

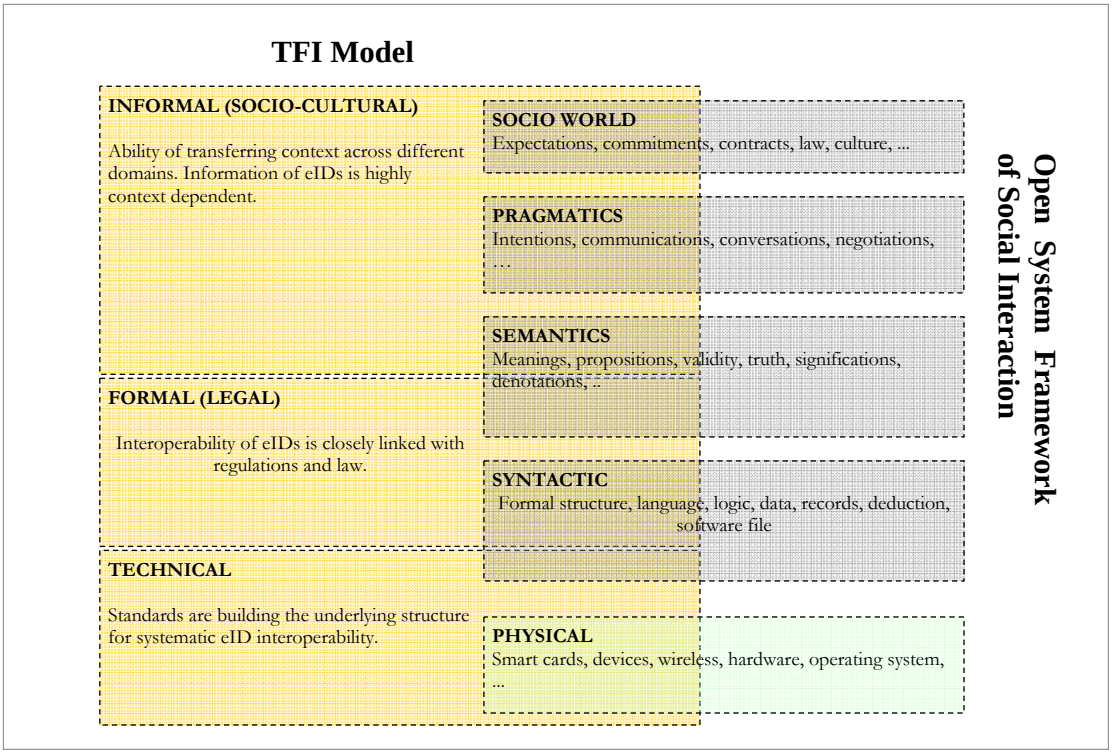

Figure 7: Modified TFI model, influenced by the Open Systems Framework of Social Interaction

Despite the fact that the last definition incorporates a strong human element in relation to interoperability, it is still lacking the socio-cultural attributes such as the meaning of data or differences of information related to diverse cultures. With his Open System Framework of Social Interaction (illustrated in Figure 7), Ouksel calls for a strong *semantic approach to interoperability* in information systems (Ouksel 1999). It is argued that current theories are insufficient to account for a realistic view of social environments. They are specifically inadequate for supporting heterogeneous information in terms of internal semantic, pragmatic, syntactic and the complexity of the social world.

Semantic interoperability is a topic of extreme complexity by itself and consequently many different approaches towards tackling such complexity can be found. In the following section two approaches will be discussed: an approach from a technical and one from a social network point of view.

The approach to semantic interoperability from a technical point of view ensures that agents and other system components can make “sense” of the resources encountered. Its objective is comprehensible to all applications, including those that were created separately, or not developed for this purpose (Klischewski 2000). The semantic compatibility between different systems facilitates the automation of information. It requires agreement on the format in which information is transmitted. To enable the translation of information between the systems, a single language to describe the structure and the underlying data must be defined. As it currently stands, the most plausible universal language to be used is XML (European Commission 2004a).

The semantic interoperability approached from a social network point of view ensures that the systems can effectively relate to the world view of the local actors in charge (Stamper et al. 2000). Ouksel and Sheth (1999) propose to research real-world semantics with the framework

of "context". By doing so, the authors believe in capturing critical components of semantic like differences in human interpretation, the dissimilar use of information and the role or use of ontologies.

Organisational compatibility allows the sharing of information stored in different data storages and the ability to understand the meaning of the information contained (Ouksel 1999). Realini proposes analysing pan-European G2G interoperability with a three layer framework: technical interoperability, semantic interoperability and organisational interoperability (Realini 2004). This described methodology is very similar to the TFI model, which is the underlying scientific approach of this chapter. The TFI model looks on interoperability from a technical, formal and informal perspective (Backhouse 2000). Figure 7 shows the merger of these three methodologies just described. It highlights the common emphasis on the socio-cultural domain of interoperability, particularly in connection with the complexity of the government sector. Backhouse (Backhouse 2005) came to a similar conclusion after reviewing more than 100 interoperability and eID related papers and conclude semantic being virtually a melting pot for issues from the three layers of the TFI model.

3.7.2 Value and Use of Privacy Enhancement Technologies in eIDs

Privacy Enhancing Technologies (PETs) offer the possibility to ensure trust between users, increase security aspects and ultimately make an eID solution lawful in the first place. Pfitzmann and Hansen (2006) describe PETs as being able to limit as much as possible the release of personal data, whereas for that released, ensure as much unlinkability as possible. Though, several Information Systems researchers point out that any technological construct can be compromised (Brooks 1997) or might result in a failure (Markus and Robey 1988). Bearing in mind these limitations it will never be possible to achieve total unlinkability. Pfitzmann and Hansen (2006) suggest that the user should be empowered to decide on the release of data and on the degree of linkage of one's personal data within the boundaries of legal regulations, i.e., in an advanced setting the privacy enhancing application design should also consider the support of "user-controlled linkage" as well as "user-controlled release". An application is designed in a privacy enhancing identity management enabling way if neither the pattern of sending/receiving messages nor the attributes given to entities (e.g., organisations, computers, humans) entail more linkability than is firmly necessary to attain the purposes of the application. Generally speaking, there are two concepts of privacy enhancement technologies (1) centralised eID database solutions and (2) decentralised or federated eID database solutions (Leitold 2005).

Technically supported identity management has to empower the user to recognise different kinds of communication or social situations and to assess them with regards to their functionality, relevance, and their security/privacy risk in order to take adequate action (Engberg 2005). Generally, the identity management solutions (IMS) should assist the user in managing one's partial identities, meaning that different pseudonyms with associated data sets can be used according to different roles in which the user is acting and pursuant to different communication partners (Pfitzmann, Hansen 2004). A privacy enhancing IMS makes the flow of personal data explicit and gives its user a larger degree of control. The guiding principle is

"notice and choice", based on a high level of data minimisation, and can be summarised as "user-controlled linkage" of personal data[27] (Engberg 2005, Pfitzmann, Hansen 2006).

3.7.3 Mergence of eID, Interoperability and Privacy

Scholars and professionals are more or less unified in the belief that pan-European eID interoperability from a pure technical point of view would be relatively easily achieved if wanted by the stakeholders (Cowcher 2005, Backhouse 2005, Leitold 2005, Martin 2005, Otter 2005b, Posch, Holzbach 2005). Basic legal/technical artefacts examining privacy issues are no concern either as basic agreement on human rights, data protection and privacy protection is enforced and guaranteed in all EU Member States (Bennett 1992, Bennett, Raab 1997).

In contrast to the technical level the formal notion of pan-European eID interoperability consists mainly of a legal perspective (cf. Figure 7). This is because any integration of government systems, sharing of information and collaborative approaches have to be based on and supported by a valid legal framework. In general, government agencies should only have access to information if (1) the specific information is needed in order to complete the public assignment, (2) the gained access to the information is lawful and (3) a misuse of the access to information is highly unlikely or virtually impossible (Etzioni 1999). In the case of eID interoperability projects the formal level is represented by the legal framework in which the country is working. These legal frameworks aim to restrict the power for the purpose of protecting the citizen from government arbitrariness and ensuring their privacy (Stalder, Lyon 2002). All laws and regulations of a country are based on the country's legal framework. This analysis is focused on six world legal systems being Civil law[28], Common law[29], Customary law[30], Muslim law[31], Talmudic law[32], and Mixed law[33] systems, the latter referring not to a single system but to a combination of systems (University of Ottawa 2005).

---

[27] And by default unlinkability of different user actions so that communication partners involved in different actions by the same user cannot combine the personal data disseminated during these actions.

[28] Generally speaking, the countries found in this category have drawn mainly on their Roman legal heritage in addition to other sources, and while giving precedence to written law, have resolutely opted for a systematic codification of their ordinary law (University of Ottawa 2005).

[29] Like that of civil law, the common law system has taken on a variety of cultural forms throughout the world. Notwithstanding the significant nuances that such diversity can sometimes create, and which political circumstances further accentuate, this category includes political entities whose law, for the most part, is technically based on English common law concepts and legal organizational methods which assign a pre-eminent position to case-law, as opposed to legislation, as the ordinary means of expression of general law (University of Ottawa 2005).

[30] Hardly any countries or political entities in the world today operate under a legal system which could be said to be typically and wholly customary. Custom can take on many guises, depending on whether it is rooted in wisdom born of concrete daily experience or more intellectually based on great spiritual or philosophical traditions. Be that as it may, customary law (as a system, not merely as an accessory to positive law) still plays a sometimes significant role, namely in matters of personal conduct, in a relatively high number of countries or political entities with mixed legal systems (University of Ottawa 2005).

[31] The Muslim legal system is an autonomous legal system which is actually religious in nature and predominantly based on the Koran. In a number of countries of Muslim persuasion it tends to be limited to personal status, although personal status can be rather broadly defined (University of Ottawa 2005)

[32] According to the survey there is only one country in the world based on a Talmudic law system. However the country is not mentioned. For the purpose of further analysis in this paper Talmudic law system based countries are neglected.

On an informal level, the TFI model addresses socio-cultural aspects like culturally dependent differences such as meaning, intention, commitment, interpretation of law, and expectation of communication processes. In a nutshell, the model includes the "human factor" to the equation of collaborative data systems.

3.7.4 eID Interoperability Analysis

In this section we aim to provide a high-level overview of the current status of international and European eID projects regarding interoperability. The research data of this chapter is primarily based on a working paper of the European Commission (CEN/ISSS 2004), a white paper of the Information Society Technologies (Ringwald 2003), a survey of a government advisory agency (Hayat et al. 2004), a global survey of legal systems of countries (University of Ottawa 2005), and complimented by extensive online research.

3.7.4.1 Technical Perspective

Trying to expand the scope of analysis, we identified an additional number of countries outside the European Union and based on data readily available concerning the implementation (or not) of an eID scheme along with the conditions underpinning that. A total of 67 countries (including the EU 25) were analysed with the purpose of getting a broader picture on eID implementation throughout several geographically dispersed countries (instead of solely focusing on one region). At this point, it should be noted that the level of information on eID projects in these surveys varied considerably from country to country. However, the information on the countries in these surveys quite often showed significant similarities in content, structure and length. In other words, it is anticipated that large amounts of information from previously published surveys was reproduced in later surveys with little additional research being carried out.

Using a bottom-up approach, the following paragraph takes a closer look at the technical level of global eID projects. Figure 8 shows 46 investigated countries supporting various eID functionalities, as far as data was available for them. Two thirds of 42 countries (excluding the EU 25) have made the decision to introduce an eID, and an even higher percentage of countries (80%) are planning one but have not yet reached a formal decision. This for instance is the case in the United Kingdom. Several countries including Australia, New Zealand and the US, have made the decision not to introduce a national-wide eID in the near future.

[33] The term "mixed", which we have arbitrarily chosen over other terms such as "hybrid" or "composite",, should not be construed restrictively, as certain authors have done. Thus this category includes political entities where two or more systems apply cumulatively or interactively, but also entities where there is a juxtaposition of systems as a result of more or less clearly defined fields of application (University of Ottawa 2005).

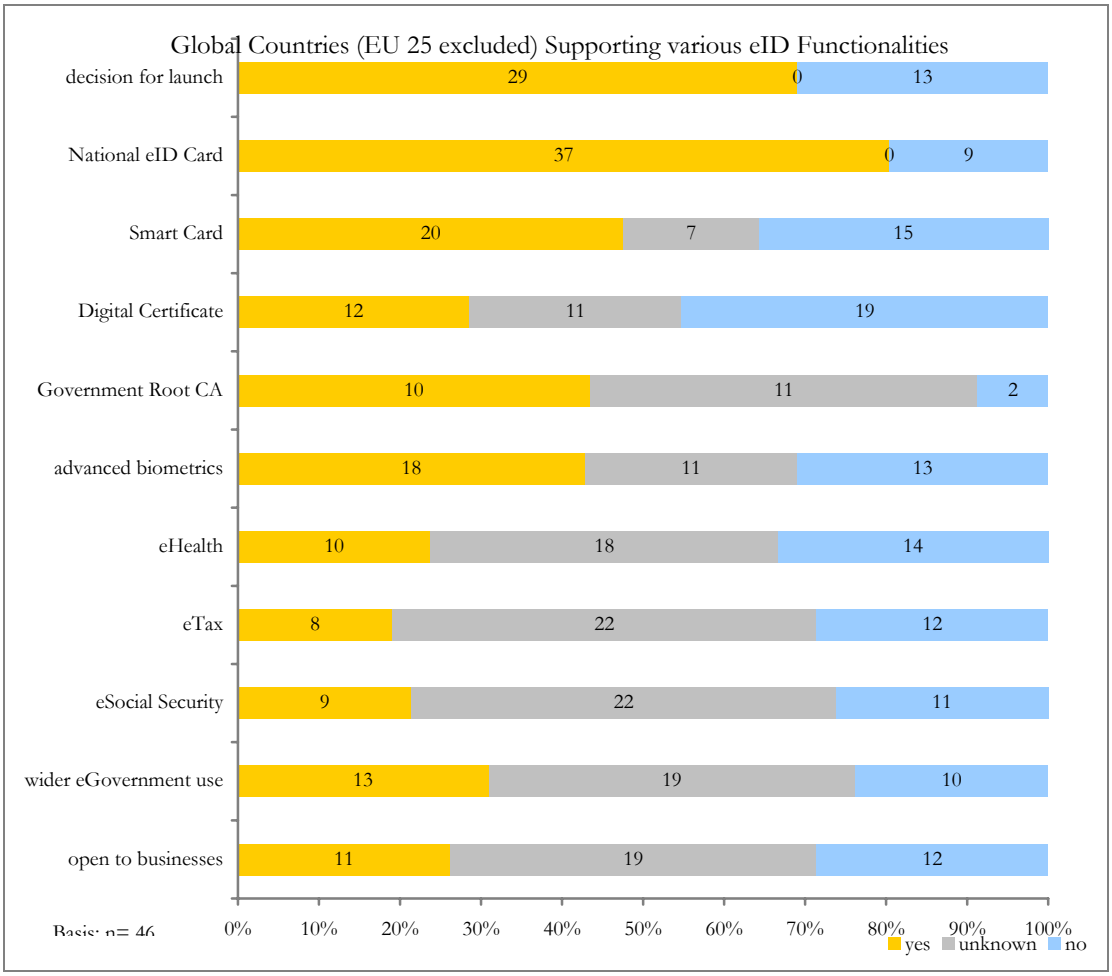

Figure 8: Number of Global Countries (EU 25 excluded) Supporting Various eID Functionalities

For the latter discussion on the informal level of eID interoperability, it is assumed that the multifunctional eID solutions, identities which can be used in a great number of different domains, require an even more complex interconnection and are therefore of special interest to eID researcher. Multifunctional eIDs are not necessarily but almost certainly supported by Smart Card and Digital Certificate technology. Although, less than a third of the countries support or plan to support these features. In any case when Digital Certificates are used, the argument arises as to, who will be the Root CA. This is closely linked to liability, privacy and most importantly to power issues. Apart from Norway and Singapore, all countries surveyed operate with a government agency controlled Root CA.

Advanced biometric solutions are usually linked with data and identity security. Technologies like digital finger prints, DNA codes, iris scans or facial recognitions are classified as advanced in comparison to technologies like photos, signatures or physical descriptions of individuals. Advanced technologies are primarily used for all types of fraud prevention. However, less than 50% of the countries which either have or plan to have eIDs are supporting some kind of advanced biometric technologies.

In Europe, the current situation with regard to national eID interoperability appears different. While only a little more than half of the EU 25 countries have either already launched or are planning to issue a national eID, the projects seem to be quite ambitious in terms of

interconnection complexity and use of advanced technology. Whereas 14 countries (56%) plan an eID solution, Figure 9 shows a greater number than 14 countries that are working on or are already supporting various forms of eID functionality. The reason is that some countries such as France and Italy have more than one national-wide eID project running.

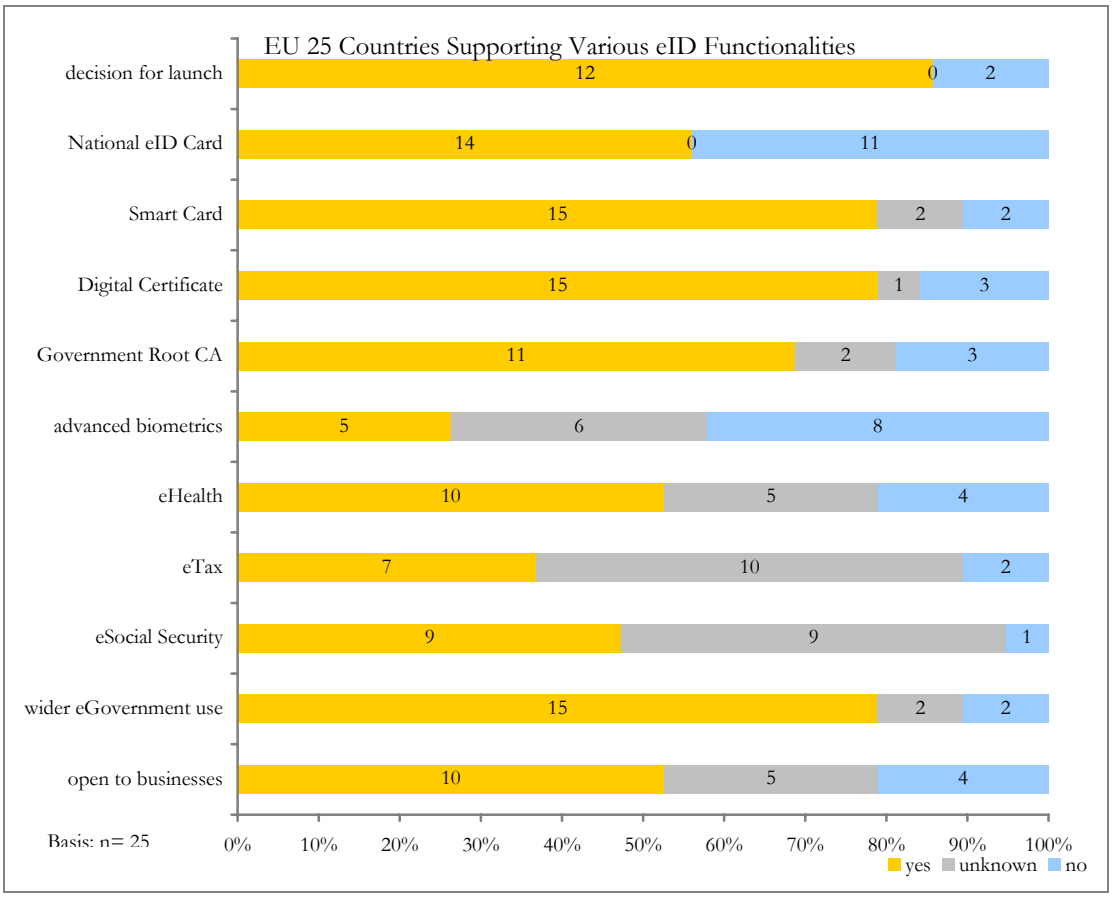

Figure 9: Number of EU 25 Countries Supporting Various eID Functionalities

Almost 80% of the EU 25 will offer a Digital Certificate service to its citizens and businesses by 2008 out of which Estonia, Luxemburg and Sweden do not have a government managed Root CA. While a relatively high proportion of EU 25 countries are in favour of Digital Certificates, their willingness to work with advanced biometrics is rather low in comparison to the rest of the world. Whereas 5 countries plan to use digital fingerprints, facial recognition and other similar advanced technologies, 8 countries have concluded that they do not believe that such high security measurements are needed. Another significant difference is the collaborative approach of a majority of the European eID interoperability projects. While a high proportion of tax, health, social security and other government agencies will be able to use the national eIDs for identification and authentication purposes, more than half of the countries plan to open its eID solution to commercial organisations.

3.7.4.2 Formal Perspective

On the formal level, interoperability of eIDs is primarily seen through the lens of legal frameworks. In order to issue a national eID systematically, the government has to gain access to all necessary information concerning its citizens and businesses required for the registration process. While most former Eastern European countries have a central registry for all citizens, most countries based on a common law system do not have similar databases. As a result, nation-wide eID solutions in common law countries require a greater number of interconnection, are of greater complexity and involve a higher level of interoperability. However, this also means that a common law country would need to change its laws and regulations considerably in order to allow for the implementation of such national eIDs in its government agencies (CIA 2003, University of Ottawa 2005). This is most probably one of the key reasons, why countries like the USA, Canada or Australia do not have a national eID nor do they plan to issue one.

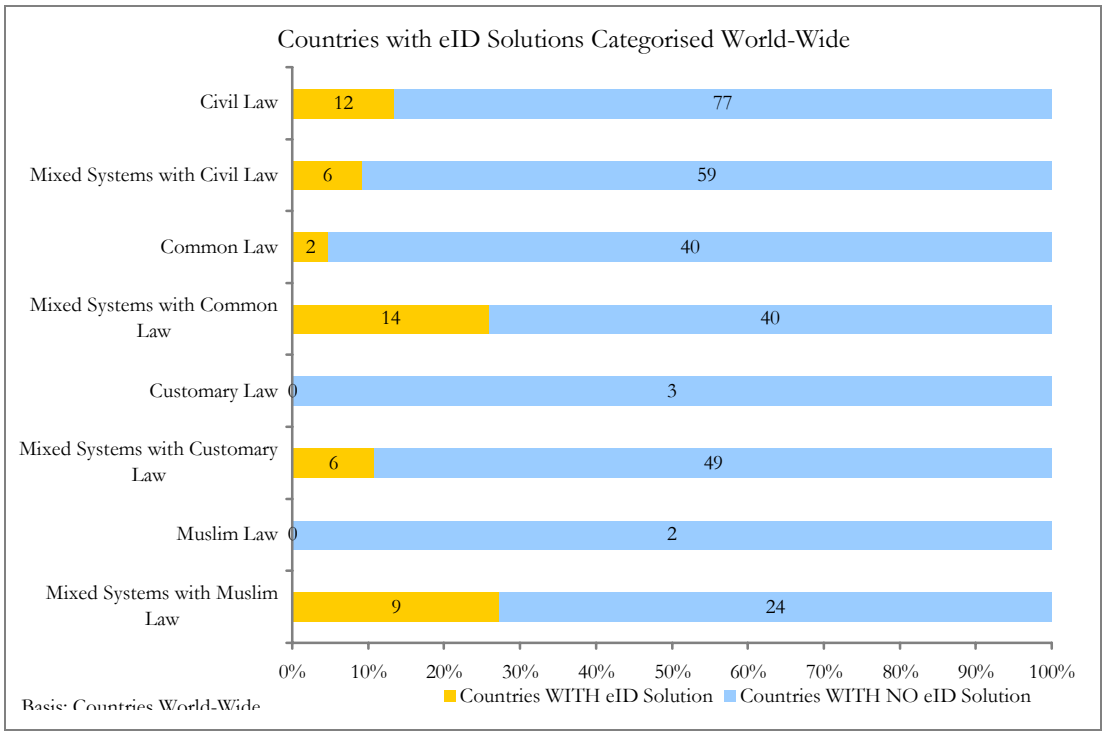

Figure 10: eID Solutions in Countries Categorised by Legal Systems World-Wide

In fact, worldwide only 2 common law countries (5%) in comparison to 12 civil law based countries (16%) have a national eID solution in place or in preparation. By far the greatest proportion of countries having launched a national eID solution is found in the segment of countries with mixed legal systems of common law and of Muslim law. 14 countries (35%) with a mix involving common law legislation and 9 countries (38%) with a mix involving Muslim law already have decided or at least plan to launch a national eID. However, the real element of significance in Figure 10 is the fact that countries with pure common law legislation seem to have considerable less often a national eID solutions in place.

The analysis of differences on the formal level among countries in Europe (EU 25 countries have either a common law or a civil law based system) shows a considerably different trend

than the developments on a global scale. By comparing Figure 10 and Figure 11, it is easily noted that the percentage of 64% civil law based countries with a national eID solution in Europe compared with 16% on a global scale is noticeably higher. In contrast the common law based countries follow the international trend not (yet) having a national eID solution in place. Despite heavy discussion about the possible launch of a national eID in the UK and Ireland no formal definitive decision has yet been made by these two countries.

It can be concluded that by looking on a global and EU level common law based countries seem to have an extremely low adoption rate of national eID strategies. In contrast the civil law based European nations seem to be among the group of early adopters of national eID solutions. Despite that maybe surprisingly clear and evident finding, by far the more challenging and pressing problem appears on a pan-European eID interoperability level, as the national individual legislation has to be harmonised in order to allow EU Member States to share, interconnect and use national versatile identities. Issues like data protection, privacy, information liability, access authority and the quality of authentication are heavily disputed issues (Hollosi 2005, Leitold 2005, Martin 2004, Otter 2005a).

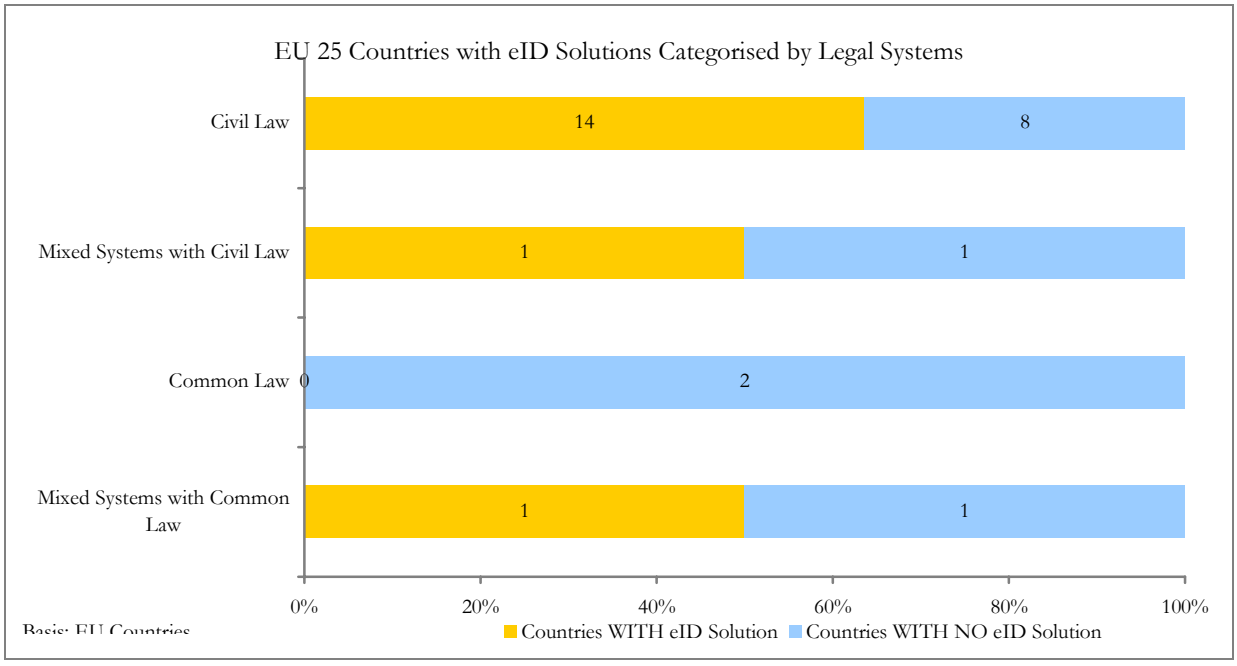

Figure 11: eID Solutions in Countries Categorised by Legal Systems in the EU

3.8 Summary and Conclusions

In this chapter basic technologies currently used for ID documents have been introduced. This includes:

- Chip card technology
- RFID

- Biometrics
- Electronic signatures
- Various back-office technologies such as PKI and databases for biometrics.

Chip card technology has been used successfully in the context of ID documents for almost 10 years now.

RFID has been used for access control in the past, but the use in the context of ID document is relatively new and started with the European passport in November 2005. To adopt RFID to the needs of ID documents a number of additional security functions have been developed recently. This includes (1) Basic Access Control (BAC) and passive and active authentication of the RFID chip. BAC will be further investigated in the chapters 5.3 and 6.4.

Biometrics in the context of ID documents has been investigated in two studies recently. The results show that biometrics still faces a number of quality problems (FAR, FRR, EER) that limit the application of this technology at least to certain groups of citizen. Technical and procedural back-up solutions have to be implemented.

Electronic signatures and PKI have been used in various European countries together with chip card technology for almost 10 years now though the diffusion and the use do not seem large until today. The technology seems to be mature. Remaining privacy and security issues will be analysed in chapter 6.6.

Back-office technologies, especially databases on biometric (raw) data, can be problematic. When data is stored in such data bases in general the purpose binding principles can not be enforced easily. This is especially true in cases these databases are run and controlled by foreign countries for foreign visitors. This especially raises the need for data minimisation. Concepts should be investigated, that allow control of the user of the ID document over his personal data. In any case additional information in authentication information should not be included. Concerning biometrics this means that biometric raw data such as photos of faces and fingerprints should not be used. But biometric raw data are due to the need of technical compatibility an integral part of the technical concept of the European passport, especially pictures of the face. This is a weak point of current concepts and implementations of MRTDs. Concerning fingerprints the NIST standards for minutiae and papillary pattern can and should be used.

In addition to basic technologies aspects of interoperability of ID documents are investigated and described using a modified TFI model. Technical compatibility, homogenisation of formal procedures and privacy aspects (for example Privacy enhancing Technologies, PET) to achieve a broad social (informal) acceptance are highly relevant aspects for successful interoperability. This chapter has given an overview on the implementation of ID documents in various European and non-European countries with respect to these factors.

It can be concluded that by looking on a global and EU level common law based countries seem to have an extremely low adoption rate of national eID strategies. In contrast the civil law based European nations seem to be among the group of early adopters of national eID solutions. Despite that maybe surprisingly clear and evident finding, by far the more challenging and pressing problem appears on a pan-European eID interoperability level, as the national individual legislation has to be harmonised in order to allow EU Member States

to share, interconnect and use national versatile identities. Issues like data protection, privacy, information liability, access authority and the quality of authentication are heavily disputed issues.

4 Legal Grounds for ID Documents in Europe

This chapter analyses legal grounds for ID documents in Europe and summarises a discussion in the Porvoo group[34] with respect to a future legal framework for ID documents in Europe.

4.1 *Machine-Readable Identity Documents with Biometrical Data in the EU Legal Framework.*

4.1.1 Introduction

With computers being able to recognise faces, fingerprints, irises, DNA sequences, human language and other body-related aspects, society has gained a powerful tool to verify an individual's identity and thus to ensure the maintenance of a certain required level of security.[35] Development of biometric technology is no longer in an embryonic stage, but has become the core of national and international security and immigration policies and is gaining importance as a market product for the private sector.

The use of biometrics is not without risk. Biometric technology incorporated in machine-readable documents allows for enhanced surveillance; theft of biometrical data, unique by nature, might be far more detrimental for the person concerned then loss of other personal data (Prins 1998, 159). It is therefore important that the legal consequences of the development and deployment of biometric identification and authentication methods and deployment of machine-readable travel documents be considered.

In chapter 4.1.2 we will give an overview of current European initiatives regarding machine-readable documents with biometrics: Eurodac (the EU central fingerprint database in connection with asylum seekers), the Visa Information System (VIS – the EU central database set up to create a common visa policy) and the European Passport (requiring fingerprints and facial images as biometrical identifiers). The scope of each (draft) Regulation will be described with a focus on the privacy, security and data protection requirements laid down in the Regulations.

The chapter 4.1.3 will contain an overview of European data protection (Directive 95/46) and the European human rights framework. The scope of these frameworks will be shortly explained and further linked with the provisions in the Regulations.

In the chapter 4.1.4 we will critically analyse the Regulations for Eurodac, for VIS and for the European Passport; Regulations that all rely on the body as a 'document' or a 'tool' for identification. Hereto, we will discuss i) the choice for biometrics as such as a tool for identification and verification, ii) the underlying legal framework for the laws establishing Eurodac, the VIS and the European Passports and travel documents; iii) the validity of the

[34] The Porvoo group is an international cooperation network of stakeholders in the area of electronic signature and PKI from the public and private sector. See http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/20710B02C6C5B894C2256D1A0048E290/

[35] This chapter focuses mainly on the biometric-related aspects of machine-readable passports and travel documents processed by public authorities. For a clear overview of RFID-related aspects of passports and travel documents, we refer to chapter 6.3.1.

Eurodac, VIS and European Passport in light of the principles of proportionality, finality and individual participation, and, iv) the issue of a central biometrical database.

4.1.2 Overview of Legal Instruments

4.1.2.1 Eurodac

What

Eurodac is a computerised, **central database** set up to assist in determining which EU Member State is to be responsible for examining an application for asylum lodged in a Member State.

Eurodac has been established by *Council Regulation (EC) 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention*.[36]

The **Dublin Convention**[37] aims at avoiding 'orbiting' asylum seekers and preventing asylum applications in different Member States. Principally, someone seeking asylum is required to apply in the Member State first entered. In principal, personal data in Eurodac may be processed only for the purpose set out in Article 15 (1) of the Dublin Convention: *'Each Member State shall communicate to any Member State that so requests such information on individual cases as is necessary for: - determining the Member State which is responsible for examining the application for asylum, - examining the application for asylum, - implementing any obligation arising under this Convention.*

The Eurodac system consists of a Central Unit – established within the Commission – that operates the central database and means of transmission between the Member States and the central database.

There are **three categories of people** (or data subjects), whose data are processed in Eurodac: (i) applicants for asylum, (ii) aliens apprehended in connection with the irregular crossing of an external border, and (iii) aliens found illegally in a Member State. The biometrical data processed are **fingerprints**.[38]Given the specific purpose of the Dublin Convention, the purpose of processing and data retention periods are separately regulated for each of these categories.

---

[36] *Official Journal* L 316, 15 December 2000. Hereafter called: the Eurodac Regulation. Provisions for the transmission and comparison of fingerprints and on the tasks of the Central Unit responsible for the central database and the comparison of fingerprints (see *further*) are further laid down in Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, *Official Journal* L 62 of 5 March 2002.

[37] Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities – Dublin Convention, *Official Journal* C 254, 19 August 1997, 1-12.

[38] Although Eurodac is not considered as a travel document (there is no travel document or passport or visa issued) and although Eurodac does not contain other data than the fingerprints and the sex of the fingerprint owners, the fingerprints of these people are used for identification and verification purposes (see further).

Applicants for asylum[39]

Each Member State shall promptly take fingerprints of all fingers of every applicant for asylum of at least 14 years and shall then promptly transmit the fingerprint data to the Central Unit together with gender and other data regarding the application.[40] The Central Unit will record the data in the central database.[41]

When the Central Unit records the transmitted fingerprint data in the central database, the fingerprints of the applicant for asylum will be compared with fingerprints already transmitted by the Member States and stored in the central database.[42] The comparison covers only previously recorded fingerprints of applicants for asylum and of aliens apprehended in connection with irregular crossing of an external border: fingerprints taken from aliens found illegally in a Member State, are not recorded in Eurodac (see further).

The comparison will result in a hit or in a negative result. Only when there is a hit, all data[43] corresponding to the hit will be transmitted to the Member State that transmitted the data for comparison.[44] That Member State will check the comparison immediately and then a final identification will be made in cooperation with the Member States.[45]

Aliens apprehended in connection with irregular crossing of external borders

Each Member State promptly takes the fingerprints of all fingers of every alien of at least 14 years who is apprehended by the competent control authorities in connection with the irregular crossing of a border of that Member State having come from a third country and who is not turned back.[46] The Member State shall then promptly transmit the fingerprint data to the Central Unit together with gender and other data that relate to the fingerprint.[47] The Central Unit will record the data in the central database.

---

[39] An 'applicant for asylum' is defined as 'an alien who has made an application for asylum or on whose behalf such an application has been made' (Article 2.1.a of the Eurodac Regulation).

[40] Besides fingerprint data and sex, the following data are transmitted to the Central Unit and recorded in the central database: *Member State of origin, place and date of the application for asylum; reference number used by the Member State of origin; date on which the fingerprints were taken and on which they were transmitted to the Central Unit*. The Central Unit adds the date on which the data were entered in the central database and details in respect of recipient(s) of data transmitted and the date(s) of transmission(s) (*see* Article 5).

[41] Article 4 of the Eurodac Regulation. The Central Unit can use these data for statistical purposes (see Article 3 of the Regulation).

[42] Article 4 of the Eurodac Regulation describes the procedure.

[43] *See* footnote 40..

[44] Article 4.5: '… *although in the case of [fingerprint data], only insofar as they were the basis for the hit*'. This extension makes it unclear whether only fingerprints or also other data are used to compare.

[45] Article 4.6 of the Eurodac Regulation.

[46] Article 8 of the Eurodac Regulation. Article 1 of the Dublin Convention defines an alien as 'any person other than a national of a Member State'.

[47] Besides fingerprint data and sex, the following data are transmitted to the Central Unit and recorded in the central database: *Member State of origin, place and date of apprehension; reference number used by the Member State of origin; date on which the fingerprints were taken and on which they were transmitted to the Central Unit*. The Central Unit adds the date on which the data were entered in the central database (*See* Article 8(2) and 9.1).

The personal data of aliens apprehended in connection with irregular crossing of an external border, will be recorded for the sole purpose of comparison with data on applicants for *asylum* transmitted *subsequently* to the Central Unit. This means that the biometrics of apprehended aliens will – at the moment of transmittal – not be compared with any previously stored data. Their fingerprints will be used later, as a tool to identify future asylum seekers.

Aliens found illegally present in the territory of a Member State

Contrary to the imposed and promptly taking of fingerprints of applicants for asylum and of aliens apprehended in connection with the irregular crossing of an external border, the fingerprints of aliens illegally present, must not be promptly taken by the competent authorities: Member States *may* transmit to the Central Unit any fingerprint data relating to fingerprints which it *may* have taken of any such alien of at least 14 years.[48]

Also contrary to the recording in the central database of fingerprint data of applicants for asylum and aliens apprehended in connection with the irregular crossing of an external border, fingerprint data of aliens found illegally may *not be recorded* in the central database. These fingerprint data may solely be transmitted to the Central Unit with a view to checking whether the alien found illegally has previously lodged an application for asylum in another Member State. Therefore, the fingerprint of the alien found illegally may only be compared with fingerprint data of applicants for asylum already recorded in the central database. They may not be compared with previously recorded fingerprint data of aliens apprehended in connection with irregular crossing of an external border.

Purpose of the database and access rights

The Member States' access rights to the data in the central database are limited: The Central Unit carries out the comparison. Member States can only transmit the data for specific purposes (see above) and *only have access* to the data when the Central Unit communicates there is a hit that occurred after a 'lawful' comparison. Member States *always have access* to all the data in the central database that they have transmitted by themselves to the Central Unit. They may never conduct searches in data transmitted by other Member States.[49]

Data retention periods for the central database

Data relating to *applicants for asylum* are stored for a period of ten years from the date on which the fingerprints were taken. They will be *deleted* earlier when the applicant acquired citizenship of a Member State.[50] Data relating to persons that are recognised and admitted as a refugee in a Member State, will be *blocked* until another regulation amends the Eurodac Regulation.[51] Until then, the Central Unit will return hits concerning recognised and admitted refugees as negative results.

---

[48] Article 11 of the Eurodac Regulation.
[49] Article 15 of the Eurodac Regulation.
[50] Article 6 and 7 of the Eurodac Regulation.
[51] The amendment can take place after a period of five years after the Eurodac implementation. This amendment will provide whether data concerning recognised and admitted refugees will be stored for 10 years from the date when the fingerprint has been taken, or be erased in advance (Article 12.2).

Data relating to *aliens apprehended in connection with the irregular crossing* of an external border will be stored in the central database for two years from the date on which the fingerprints were taken and will be deleted earlier when the alien obtained a residence permit, left the territory of the Member States or acquired citizenship of any Member State.[52] Data relating to *aliens found illegally* are not stored: they will only be used for comparison purposes and will be erased immediately once the results of comparison have been transmitted

Data controllers and responsibilities[53]

The *Member States* are responsible data controllers as regards to the lawful taking of fingerprints, the lawful transmission of accurate and up-to-date personal data to the Central Unit, the lawful use of the results of the fingerprint comparison and the final identification of the data subject upon the results of the fingerprint comparison. They are responsible for the confidentiality and security of the national installations and of the data before and during transmission and after receipt of the data.

The *Commission* (the Central Unit) is responsible for the lawful recording, storage, correction and erasure of the data in the central database. It is also responsible for the confidentiality and security of the Central Unit and the central database.

The rights of the data subjects

The data subjects' rights, elaborated in the European Data Protection Directive 95/46 (see further), are applicable: the data subjects must be informed of the identity of the controller and of his representative, the purpose of processing within Eurodac, the recipients of the data from Eurodac, the obligation to have the fingerprints taken (except for aliens found illegally present in a Member State – see above) and the existence of the right to access and rectify data concerning him or her.[54] The data subjects' rights include the right to obtain from the controller knowledge of the logic of the processing involved, at least in the case of 'automated decision taking'[55] takes places and the right to request that 'factually' inaccurate or unlawfully recorded data be corrected, respectively erased by the Member State that transmitted the data[56].

---

[52] Article 10 of the Eurodac Regulation.
[53] Article 13 and 14 of the Eurodac Regulation.
[54] This information shall be given to asylum seekers and aliens apprehended in connection with the irregular crossing of external borders 'when the fingerprints are taken' Aliens found illegally will receive this information 'no later than the time when the data relating to the person are transmitted to the Central Unit', unless 'the provision of such information proves impossible or would involve a disproportionate effort'.
[55] Article 15 of the Data Protection Directive: "**1.** Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. **2.** (…) a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision: (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.
[56] Article 18 of the Eurodac Regulation.

The future of Eurodac

On 24 November 2005, the Commission sent a Communication to the Council and the European Parliament on improved effectiveness and enhanced interoperability among European databases.[57] As regards Eurodac, the Commission concluded that the Eurodac database has been under-exploited because the quantity of the data to be transmitted to Eurodac is a 'surprisingly low fraction of the total migratory flow'[58]; that too many data in [Eurodac] increase the probability of incorrect results and wrong identification; that many apprehended illegal immigrants have no valid id document so that the identification process is time-consuming and expensive. On the other hand, however, the Commission concludes that the Member States have no means to check whether an asylum applicant has had a (valid) visa issued and that the absence of access by internal security authorities to Eurodac data is 'considered by the law enforcement community to be a serious gap in the identification of suspected perpetrators of a serious crime'.

Consequently, the Commission defines ' further possible developments' for Eurodac and lists amongst others more comprehensive access to Eurodac by authorities responsible for internal security in well-defined cases 'when there is a substantiated suspicion that the perpetrator of a serious crime has applied for asylum'

4.1.2.2 The European Visa Information System (VIS)

What

On 28 December 2004, the Commission proposed for a **Regulation**[59] constituting the establishment and the legal framework of the VIS for the exchange of data between Member States on short stay-visas. The establishment of the VIS has been introduced as a key factor for the European Union to achieve a **common policy on the exchange of visa data** between Member States, to guarantee the free movement of persons and to abolish checks at internal borders (Article 29 Data Protection Working Party 2005b, 3, 6). This would prevent people from filing several visa applications in different Member States and would allow visa authorities to check the visa history of the person concerned. But also other finalities can be found in the VIS Proposal that allows indeed different authorities to access the system for different purposes than visa policies only.[60]

---

[57] Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of justice and home affairs**,** Brussels, 24.11.2005**,** COM(2005) 597 final, 11 p.
[58] Idem, 5.
[59] Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final). Hereafter called: 'VIS Proposal'.
[60] See also further. Article 1.2 of the VIS Proposal summarizes the different purposes, namely to: (a) prevent threats to internal security of any of the Member States; (b) prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application; (c) facilitate the fight against fraud; (d) facilitate checks at external borders and within the territory of Member States; (e) assist in identification and return of illegal immigrants; (f) facilitate application of EU Regulation 343/2003.

The VIS consists of a central database under the responsibility of the Commission (CS-VIS) that connects through a communication infrastructure with the different national interfaces of and under the responsibility of the Member States (NI-VIS).

Photographs and fingerprints in a central database

The people or data subjects concerned are **third country nationals** filing applications for a visa. Citizens from 134 countries in the world require a visa to enter the EU.[61] All these application data will be processed in the central database of VIS.

The categories of personal data processed are alphanumerical data on the applicant together with his **photograph and fingerprint** as biometrical data.[62] The personal data are collected upon lodging the application for a visa and are linked to other visa applications (to applications by members of the same travelling group or to former applications of the same applicant).

The application file in the VIS database will contain other personal information such as the grounds for refusal, annulment, revocation or extension of the visa.

The **storage medium** for the biometrical data will be a **centralised database** (VIS). At the moment, the biometrical data will not be stored on the visa sticker ('uniform format for visas') accompanying the valid travel document because this may lead to possible technical conflicts of 'collision' between too many biometrical identifiers in one document,[63] for example a travel document containing a passport identifier together with identifiers of visa issued by other countries.[64] Consequently the visa holders do not have the biometrics on their documents.

[61] See Council Regulation (EC) 539/2001 of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement, *Official Journal* L 81 of 21 March 2001 (modified by Regulation n 2414/2001 and Regulation n 453/2003). See *also* Euractiv, *Central EU visa system will hold biometric data*, 7 January 2005, http://www.euractiv.com/Article?tcmuri=tcm:29-133939-16&type=News.

[62] Article 3.1. Article 6 lists the alphanumerical data that are entered in the application file. Some of the alphanumerical data are surname, first names, sex, date, place and country of birth, nationality, type of travel document, place and date of application, application number and the visa status information.

[63] On the technological 'collision' problems of the biometric identifiers in the Uniform visa document, *see* the technical reports of the Visa Working Party available through Statewatch, "*EU: Biometric visa policy unworkable"*, http://www.statewatch.org/news/2005/jan/02update-visas-biometrics.htm.

[64] The visas for travel and transit within the EU must have a uniform format of which the specifications can be found in Council Regulation (EC) No 1683/95 of 29 May 1995 laying down a uniform format for visas, *Official Journal* L 164 of 14 July 1995 and – for the standardised integration of a highly secured photograph (according to ICAO Document 9303) – in Council Regulation (EC) No 334/2002 of 18 February 2002 amending Regulation (EC) No 1683/95 laying down a uniform format for visas, *Official Journal L 053 of 23 February 2002.*

Purpose of the database and access rights

The access right for entering, amending or deleting data in the VIS is reserved to duly authorised staff of the *visa authorities*.[65]

The access rights for consulting data in the VIS are in the first place reserved to duly authorised staff of *visa authorities* for the purpose of examining applications, of consultation and request for documents and of reporting and statistics.[66] The access rights for consulting data in the VIS are also reserved to duly authorised staff of *other authorities* that are competent for activities beyond a common visa policy. Inherently, they access the VIS for different purposes. This means that the following authorities can have access to at least the alphanumerical data provided for in Article 6(4)(a)[67] and to the biometrics (photograph and fingerprints) of the applicant:

1. Competent authorities for carrying out checks on visas at external borders and within the territory of the Member State for the sole purpose of verifying[68] the identity of the person and/or the authenticity of the visa (Article 16).
2. Competent immigration authorities for the sole purpose of identification[69] and return of illegal immigrants (Article 17).
3. Competent asylum authorities for the sole purpose of determining the Member State responsible for examining an asylum application and for the purpose of examining an application for asylum (Article 18 & 19).

In other words: VIS will not only be accessed for examining applications but also for improving administration of the common visa policy and consular cooperation in order to prevent threats to internal security and 'visa' shopping; facilitate the fight against fraud; assist in the identification and return of illegal immigrants and facilitate application of the Dublin II Regulation. The Commission will table a proposal allowing Europol and internal security authorities to access VIS for clearly defined purposes. [70]

Data retention periods for the central database

The data retention period for each application file is established at maximum five years starting at the last expiry date of the visa or on the date of the creation of the application file in the VIS if the visa is not issued. The application file will be deleted earlier when the data

---

[65] visa authorities are defined as *authorities of each Member State which are responsible for examining applications and for decisions taken hereto of for decisions whether to annul, revoke or extend visas* (Article 2 (3)).
[66] Article 13, 14 and 15 of the VIS Proposal.
[67] Surname, surname at birth (earlier surname(s)); first names, sex, date, place and country of birth.
[68] Article 2 (10) of the VIS Proposal defines verification as *"the process of comparison of sets of data to establish the validity of a claimed identity (one-to-one check)"*.
[69] Article 2 (11) of the VIS Proposal defines identification as *"the process of determining a person's identity through a database search against mulitiple sets of data (one-to-many check)"*.
[70] Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of justice and home affairs**,** Brussels, 24.11.2005**,** COM(2005) 597 final, 4.

appear to be inaccurate or processed in the VIS contrary to this Regulation or if the applicant acquired the nationality of a Member State.[71]

Data controllers and responsibilities

The Member States are data controllers responsible for the lawful processing of the data, for the lawful collection and transmission of the data to the VIS in accurate and up-to-date form, for the confidentiality and the security of the data before and during the transmission to NI-VIS and after receiving data from the VIS. The Commission is responsible for the confidentiality and security of the CE-VIS and the communication infrastructure between CE-VIS and NI-VIS.[72]

The rights of the data subjects

The visa applicants[73] have the right to be informed by the responsible data controller of the controller's identity, the purpose of processing within the VIS, the recipients of the data, the mandatory character of collecting the data, the existence of the right to access and correct. They have the right to access, correct and delete the data.[74]

The future of the Visa Information System

In the aforementioned Communication of the Commission, the absence of access to VIS by internal security authorities has been considered as a serious gap in the identification of suspected perpetrators of a serious crime. Intelligence communities have also considered as a 'shortcoming', the fact that VIS only deals with third country nationals, under visa obligation: '*The control of the identity or the legality of the entry of other categories of third-country nationals (…) e.g. holders of a long-stay visa or a residence permit (…) could also be more efficient.* Finally, the fact that VIS cannot identify persons that remain illegally in the EU, has been considered as 'incomplete monitoring of entry and exit of third country nationals'.[75]

As regards VIS, the Communication described as 'further development of existing systems and planned systems': i) more comprehensive access by asylum and immigration authorities; ii) extending access to authorities responsible for internal security for the purposes of the prevention, detection and investigation of terrorist offences, and iii) access to the systems for contributing to the identification of disaster victims and unidentified bodies.[76]

Finally, the Commission stated that 'the development of a service-oriented architecture of European IT systems would help maximise synergies' and 'is a way of sharing functions in a flexible and cost-efficient way without merging existing systems. The Commission even gives

[71] Article 21 and 22.
[72] Article 25 & 26.
[73] Also name and address of the person(s) (or companie(s)) who issued an invitation or who are liable to pay the costs of living of the visa applicant during his stay, are entered into the application file upon lodging (Article 6). Consequently, these persons (or companies) also enjoy the right to information and to access, correct or delete the data (see Article 30 e.q.).
[74] Article 30 e.q.
[75] COM(2005) 597 final, 6.
[76] Idem, 7-8.

an example that we integrally quote here: "In concrete terms, one example would be to use the highly performing future Automated Fingerprinting Identification Systems (AFIS) part of the VIS to deliver AFIS–related services (i.e. a biometric search for other applications, such as EURODAC or, possibly, a biometric passport register). Data storage and data flow could still be strictly separated".[77]

4.1.2.3 The European Passport

What

Although Member States already issue passports with biometrics, the EU is currently heading for a far-reaching development of biometrical passports and travel documents for the EU citizen.

After having introduced minimum-security requirements for travel documents and for passports of Member States in 2000[78], the European Union upgraded, standardised and harmonised the minimum-security features and included biometrical requirements for passports and travel documents by **Council Regulation 2252/2004**.[79]

The minimum level of security for Member States' passports and travel documents is laid down in the Annex of the Regulation and relates to the specific materials used, the machine-readable biographical data page, printing techniques, protection against copying, issuing techniques. With regard to the standards for the biometrical features, Regulation 2252/2004 states that these must comply with the standards laid down by the International Civil Aviation Organization (ICAO) **in ICAO Document 9303**[80].

The biometrics for passports and travel documents were introduced by this Regulation 'in order to render the travel document more secure and to establish a more reliable link between the holder and the passport and the travel document'.[81] So, at first sight, the use of biometrics aims at verifying the validity of a claimed identity instead of establishing a person's identity.[82] The main provisions of Council Regulation 2252/2004 are the following:

---

[77] Idem, 10.

[78] Resolution of the representatives of the governments of the Member States, meeting within the Council of 17 October 2000 supplementing the resolutions of 23 June 1981, 30 June 1982, 14 July 1986 and 10 July 1995 as regards the security characteristics of passports and other travel documents (2000/C 310/01), *Official Journal* C 310, 28 October 2000. The minimum-security requirements for EU travel documents laid down in this resolution relate to the materials, printing techniques, protection against photocopying and issuing techniques. As stated in Annex II of this Resolution, the minimum-security standards also apply to ordinary passports, official passports and short-term passports with more than six months' validity.

[79] Council Regulation (EC) No 2252/2004 of 13 December 2004 for security features and biometrics in passports and travel documents issued by Member States, *Official Journal* L 385, 29 December 2004. Hereafter called: 'Council Regulation 2252/2004'.

[80] Document 9303 is available at http://www.icao.int/mrtd/Home/Index.cfm.

[81] Recital 2 and 3 of Council Regulation 2252/2004.

[82] For a legal definition of 'verification' and 'identification', see Article 2 (10) and 2 (11) of the VIS Proposal

Facial image and fingerprints stored on an RFID chip

Passports and travel documents issued by the Member States must include a storage medium that contains a **facial image**. Member States shall also include **fingerprints** in interoperable formats.[83]

The Regulation states expressly that no information in machine-readable form shall be included in the passport or travel document unless this is foreseen in the Regulation or mentioned in the passport or travel document by the issuing Member State.[84]

The storage medium, which must have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data, is a **RFID chip**. This was decided by the Commission in February 2005.[85]

The important issue whether the biometrical data – taken upon the application for a passport or travel document and stored in the passport or travel document – are also stored in a **central database**, is not handled in Regulation 2252/2004. Consequently, the option to import the biometrics in a central database has been left to the Member States. In other words: there is no special provision imposing or forbidding the storage of the biometrics in a central database.

Purpose of the biometric features

The biometric features in passports and travel documents shall, *for the purpose of the Council Regulation*, only be used for verifying the authenticity of the document and the identity of the holder by means of directly available comparable features when the passport or travel document is required to be produced by law.[86]

The rights of the data subjects

Persons to whom a passport or travel document is issued will – without prejudice to data protection rules – have the right to verify the personal data contained in the passport or travel document and, where appropriate, to ask for rectification or erasure.[87]

Limited scope and implementation

Council Regulation 2252/2004 applies not to national identity cards or to temporary passports and temporary travel documents having validity of 12 months or less.[88] The scope of harmonisation is also limited to the security features including biometric identifiers: the

[83] Article 1.2.
[84] Article 4.2.
[85] Commission Decision K (2005) 409 of 28 February 2005, of which the French text is available at http://europa.eu.int/comm/justice_home/doc_centre/freetravel/documents/doc/c_2005_409_fr.pdf. No official English is text available because the United Kingdom and Ireland have not taken part in the adoption of this measure. See also chapter 6.3.1.
[86] Article 4.3
[87] Article 4.1
[88] Article 1.3

designation of the authorities and bodies that will be allowed access to the data in the storage medium of the issued document, remains a matter of national legislation.[89]

Member States must implement the digitalised facial image into the passports before 28 August 2006 and the fingerprints before 28 February 2008.[90]

Comparison with Eurodac and VIS

Contrary to Eurodac and VIS at the moment, biometrical passports and travel documents are physical documents assigned to people. People with the biometrical passport carry the biometrics with them. Eurodac and VIS are databases and do not require a document for verification or identification. They simply use the human body as a tool for identification.

The fact that EU Regulation 2252/2004 does not deal with the issue of a central database (this has been left to the Member States) can have important consequences in the sense of privacy and data protection. The (disputable) safeguards that are laid down in connection with VIS and Eurodac (defined access rights, responsibilities, confidentiality and security and data subjects' rights) are consequently not present for the EU passports.

Future of the Passport

There are some signals on EU level that encourage the creation of a central database on the national level for EU passports and travel documents. In the Communication of the Commission it is remarked that 'there is no comprehensive database which would allow for the identification of disaster victims and unidentified bodies': this sounds like a (quite far-fetched) argument to open doors for interconnected and interoperable EU passport databases.[91] Also, the intention to interlink national *DNA* databases shows that authorities that combat crime and terrorism have indeed a real desire for an umbrella network of interlinked databases.[92]

Finally, the Commission's Communication already reveals that 'most Member States will have a central repository of issued documents and biometric identifiers linked to a certain identity' but seems to regret that '*a query of that central repository only allows a check as to whether in that same Member State a document has been previously issued to the same person under another name. In addition, it is currently not possible to launch a query on a person who is, say, wanted for a terrorist crime on the basis of whether this person has ever been issued with a travel or ID document*. [93] The Commission even concludes that this 'gap in the fight against identity theft (…) substantially damages the European economy'.[94]

[89] Recital 4
[90] Article 6
[91] COM(2005) 597 final, 7
[92] COM(2005) 597 final, 6: "Lack of biometric identification tools".
[93] COM(2005) 597 final, 6-7.
[94] COM(2005) 597 final, 7.

4.1.3 European Data Protection and Human Rights Framework

4.1.3.1 Data Protection Directive 95/46

General overview

Data Protection Directive 95/46 regulates the processing of personal data.[95] Personal data are 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.[96]

Biometrical data (fingerprints, photos) and alphanumerical data on persons (age, sex, name, address etc.) are personal data (Hes et al. 1999, 39).[97] Directive 95/46 applies to Eurodac, VIS and the European Passport: this is expressly recognised in all Regulations.[98] Moreover, these Regulations are in fact further elaborations and clarifications of the principles of data protection as laid down in Directive 95/46.

The basic principles of the Data Protection Directive are the following: Processing of personal data must be lawful and fair to the individuals concerned; personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (finality/purpose specification principle)[99]; the data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (proportionality principle); data processed must be accurate and where necessary, kept up to date: every reasonable step must be taken to ensure that inaccurate or incomplete data are erased or rectified. [100]

Processing of so-called sensitive data[101] is principally forbidden although exceptions to this principal prohibition are foreseen, such as the existence of explicit consent by the data subject; the necessity to protect the vital interests of the data subject or another person where

---

[95] Data Protection Directive: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, *Official Journal* L 281, 23 November 1995, pp. 31-50.
[96] Article 2(a) of the Data Protection Directive.
[97] "*There is no reason to think that what applies to the human characteristic itself, would not apply to the digital representation of that characteristic, the templates which are composed on the basis of these representations, and to any subsequent transformation. As the process continues, the amount of detail will change, but the unique link with the person concerned is kept. It is reasonable therefore to conclude that the data involved will remain personal data in most, if not all stages of their processing.*"
[98] Recital 15 Eurodac Regulation; Recital 14 VIS Proposal; Recital 8 Regulation 2252/2004.
[99] It should be mentioned that article 6.1.b. continues as follows: "further processing of the data for historical, statistical or scientific purposes is not considered as incompatible provided that appropriate safeguards are provided by the Member States whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual."
[100] Article 6 of the Data Protection Directive.
[101] "Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life."

the data subject is physically or legally incapable of giving his consent; processing of data which are manifestly made public by the data subject.[102]

An important obligation is that the data controller[103] provides the data subject with at least the following information: the identity of the controller and of his representative and the purpose of the processing for which the data are intended.[104]

A substantial safeguard relates to the confidentiality and security of the processing. Data controllers must implement appropriate technical and organisational measures to protect personal data against destruction, loss, alteration or unauthorised disclosure and access. Such measures shall "ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected".[105]

Data Protection law applied to machine-readable documents and identities

Many provisions in the Regulations concerning Eurodac, VIS and the European Passport and travel documents are in fact no more than further elaborations and clarifications of the general principles laid down in Data Protection Directive 95/46.

A first clarification regards the finality/purpose specification principle: The finality of *Eurodac* is to assist in the determination of the State responsible for examination of an application for asylum. Eurodac's central database may as a result only be accessed to compare fingerprints in particular situations and depending on whether it concerns an applicant for asylum, an alien apprehended at an external border or found illegally within the Territory. The finality of *VIS* goes further than only achieving a common visa policy: different authorities (even 'third pillar' authorities) can access VIS for other purposes than related with visa (e.g. check on visa in the territory, identification of illegal immigrants and assistance in applying the Dublin Convention). The finality of the *European Passport* is limited to 'verifying the authenticity of the document and the identity of the holder when the passport or travel document is required to be produced by law.[106]

The clarifications relate also to the data retention period when the data are centrally stored in a database (see Eurodac, VIS). The Regulations indicate also who the responsible data controllers are (the Commission and the Member States) and points out some specific security and confidentiality requirements.

However, the actual content and scope of some of the provisions in the Regulations are sometimes difficult to reconcile with the principles of data protection – especially with the principle of proportionality and the purpose specification/ finality principle. We will indicate further how these Regulations may infringe data protection law.

[102] Article 8 of the Data Protection Directive.
[103] "The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of processing of personal data (...)" (Article 2.d Data Protection Directive)
[104] Article 10.a and 10.b of the Data Protection Directive.
[105] Article 16 and 17 of the Data Protection Directive.
[106] See further.

4.1.3.2 Human Rights in the European Union

What

Human rights and in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms[107] apply to Eurodac, the VIS and the European passport. The VIS Proposal recognises explicitly the application of human rights.[108] The Eurodac Regulation states that '… the procedure for taking fingerprints shall be determined in accordance with the safeguards laid down in the European Convention on Human Rights and in the United Nations Convention on the Rights of the Child'.[109]

We will discuss four fundamental rights: freedom of movement of persons, the human right to data protection, the human right to a fair trail and the human right to privacy.

Freedom of movement

The use of the databases that we discussed above can lead to illegitimate grounds for stopping people (at border controls). It is not unimaginable that people's applications for visa or travel documents are refused without being informed of the reasons why; that people are not informed of the reason why they are stopped at a border, or; that people are stopped solely on the grounds of personal data such as criminal convictions that are available to the access authorities. It is also not unimaginable that agents often merely follow the results of a database query. In these cases, people cannot freely move.

In a recent case relating to the use of the SIS (the Schengen Information System), the European Court of Justice declared that Spain infringed the right of free movement of people, by refusing entry to a person into the Schengen area and by refusing to issue a visa for the purpose of entry into that territory to this person and his wife, nationals of a third country who are the spouses of Member State nationals, *on the sole ground that they were persons for whom alerts were entered in the Schengen Information System for the purposes of refusing them entry, without first verifying whether the presence of those persons constituted a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society*.[110] The applicable Council Directive 64/221 (Article 3) – which Spain infringed – stated that "measures taken on grounds of public policy or of public security shall be based exclusively on the personal conduct of the individual concerned" and that "Previous criminal convictions shall not in themselves constitute grounds for the taking of such measures."

[107] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950 (Rome), text available at http://conventions.coe.int. Hereafter called: ECHR.
[108] Recital 20 of the VIS Proposal: "This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union."
[109] Articles 4 and 8 of the Eurodac Regulation.
[110] European Court of Justice, Case C-503/03 (Commission v Spain), Judgement of 31 January 2006, available through http://curia.eu.int/.

The human right to data protection

The human right to data protection is explicitly recognised in Article 8 of the Charter of Fundamental Rights of the European Union[111]. The right to data protection as a human right has been included in a separate Article 8, besides the right to privacy in Article 7. This highlights the difference between privacy and data protection and underlines the need for co-existence of both human rights: there are indeed circumstances where the right to privacy applies and the right to data protection does not, and vice versa (De Hert, Gutwirth 2003, De Hert, Gutwirth 2005).

The human right to a fair trial

Article 6 European Charta of Human Rights guarantees the right to a fair trial. The right to a fair trial constitutes a basic element of a democratic society governed by the rule of law (De Hert 2005). Specific guarantees exist under Article 6, second paragraph: '*Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law*'.[112]

The human right to privacy

Article 8 of the European Convention on Human Rights (ECHR) provides for the fundamental right of privacy. [113]

The European Court of Justice (ECJ) has confirmed that the criteria and limitations set forward by Article 8 apply when assessing whether processing of personal data conforms to Community law.[114]

Article 8 imposes strict limitations on interference with an individual's private sphere by public authorities: If there is a law that provides for an interference with private life, such interference must be further justified. An important limitation on the interference by a public authority with an individual's private life is the 'necessity criterion': the interference must be 'necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.[115]

This necessity criterion imposed by privacy law relates to the proportionality principle of data protection law: 'personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. Non-compliance with the

---

[111] *Official Journal* C 364 of 18 December 2000.
[112] This right is included also in Article 48 of the EU Charter of Fundamental Rights.
[113] Article 8 ECHR states: '1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.' In Article 7 of the Charter of Fundamental Rights of the EU, it is stated: 'Everybody has the right to respect for his or her family life, home and communications'.
[114] Judgment on the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (E.C.J. 20 May 2003 Österreichischer Rundfunk and others, joint cases, C-138-01, C-139/01 and C-465/00, http://curia.eu.int/; see also Article 29 Data Protection Working Party 2005b, 8).
[115] Article 8 ECHR.

proportionality requirement of data protection law (namely when inadequate, irrelevant or excessive data are processed) implies at the same time that the necessity requirement imposed by privacy law may be infringed (in situations of course when the right to privacy of Article 8 ECHR applies). The European Court of Human Rights confirms this: 'the notion of necessity implies a 'pressing social need'; in particular, the measure employed must be *proportionate to the legitimate aim pursued*".[116] If too many or irrelevant data are processed in relation to the purpose of the processing, the processing can be considered as illegitimate.

We will further indicate how the different Regulations might infringe these principles.

4.1.4 Critical Observations

This part contains some critical observations. These relate in the first place to the choice – as such – for biometrics as a unique identification and verification tool. Further, we will discuss the underlying legal framework in which the Regulations (including the ICAO standards) came into existence. We will then apply the principles of proportionality, purpose specification/finality and individual participation to some provisions of the Regulations. We will finally say some words on the issue of central storage of the biometrical data.

4.1.4.1 The Choice for Biometrics

Concerns about the body as a passport

Storing digital photos and fingerprints for visa applications relates to the data subjects of more than 130 countries in the world. The mandatory taking and storing of fingerprints of asylum seekers and aliens concerns hundreds of people, every day. The fundamental issue in Regulation 2252/2004 concerns the duty to sample fingerprints of over 450 million people and the possibility of central storage (that is not excluded) of these fingerprints, together with digital photographs and other data.

Article 29 Data Protection Working Party – Europe's data protection observatory – has published a critical opinion on EU Regulation 2252/2004 (Article 29 Data Protection Working Party 2005c). It had already issued an opinion on the use of biometrics and an opinion on the inclusion of biometrics in residence permits and visas (VIS) (Article 29 Data Protection Working Party 2003 and 2004).

The expectations in connection with biometrics are probably overestimated. Indeed, biometrics could 'cause us to place too much trust in the effectiveness of electronic solutions'.[117] Biometrics is based on probabilities: false positives and negatives are unavoidable. Pincodes are not based on probabilities (Van Kralingen et al. 1997, 14). If only one percent of a targeted group of 100,000 people a day suffers from a false negative, this would cause every day 1,000 people to be 'automatically' (but wrongfully) stopped. That

[116] ECHR Judgment of 24 November 1986 (Gillow vs. The United Kingdom), http://www.echr.coe.int/echr.
[117] However, a contra argument has been given also by "the introduction of a new chip-enabled bank card in France [which] did not result in lower fraud rates until the fallback scenario had been abandoned". X., "KJD&I Symposium resounding success. A brief overview of the forum discussions" *Keesing Journal of Documents & Identity*, Issue 16, 2006, 7.

biometrical data, even fingerprints, change throughout time, confirms this risk (Wayman 2006, 14).

Furthermore, most of the information we know about the reliability, accuracy and efficiency of biometrics, is provided by the vendors of biometrics (OECD 2004, 32). The 'Biometric summary table' in the OECD Report of 2004 (see next page) shows that the biometric technology – as is – is not perfect. Moreover, no biometric technology seems to be in line with all data protection principles and user acceptance at the same time (data quality principle, transparency principle, data security principle). Whereas fingerprint scanning is only 'possibly' very high, the user acceptance is medium to low. Whereas the accuracy of facial recognition is medium to high, the stability and the transparency are low.

Biometric	Accuracy	Ease of use	User acceptance	Stability	Cost	Trans-parency[1]	Typical applications	Suitability for	
								1:1	1:N
Finger-scanning	High, possibly Very High	High	Medium Low	High	* to ***	Overt	Traveller clearance, driver's license, welfare	Yes	Yes
Hand geometry	High	High	Medium High	Medium High	***	Overt	Access control, traveller clearance, day care	Yes	No
Facial recognition	Medium High[2]	Medium High	High	Medium Low	***	Covert	Casino, traveller clearance	Yes	Poten tially[3]
Iris scanning	Very High	Medium Low	Medium High	High	*****	Covert	Prisons, access control, traveller clearance	Yes	Yes
Retinal scanning	Very High	Low	Low	High	****	Overt	Access control, traveller clearance	Yes	Yes
Finger geometry	Medium	High	Medium High	Medium High	***	Overt	Access control, amusement park ticket holder	Yes	No
Voice recognition	Medium	High	High	Medium Low	*	Covert	Low security applications, telephone authentication	Yes	No
Signature verification	Medium	High	Medium High	Medium Low	**	Overt	Low security applications, applications with existing 'signature'	Yes	No

Table 3: Biometrics summary table

Table 4 from the same Report confirms this.

	Facial recognition	Fingerprint	Iris scan
Advantages	Public acceptability Ease of use Use of passport photo Useful for watch list	Mature technology High accuracy Stable over time Large extant database	High accuracy Stable over time
Disadvantages	Accuracy controversial Questions as to effects of aging over time	Low public acceptability	Very new technology Single vendor issues Not yet user friendly

Table 4: Candidates and preferred technologies

Biometrics does not exclude identity theft or forgery. Although biometrics prevent so-called 'identity substitution' to a certain degree, the fraudulent issuance of a genuine passport cannot be prevented. In addition, the best fakes seem to be still intercepted by inspectors on the basis of the holder's behaviour, among other variables.[118]

These conclusions can make that the 'necessity' criterion – indispensable to interfere with an individual's private sphere – can still play a role in a later discussion on the legitimacy of the Regulations. Although we do not expect the European Court of Human Rights to decide that one or more databases (or parts thereof) or biometrics identification systems as such turn out to be unnecessary infringements of the private life of people, the tension is clear and should bring policy-makers in the European Member States to greater care.

Biometrics, privacy and sensitive data

Two questions with legal consequences arise: Are biometrics sensitive data in the sense of data protection law and does the obligation to be subjected to biometrical identification not conflict with feelings of (bodily) dignity of people?

The issue whether biometrical data are sensitive data, remains important. Article 8 of the Data Protection Directive principally prohibits processing of sensitive data.[119] The use of biometrics can involve the processing of sensitive data in the sense of Article 8. Biometrical data of disabled people may relate to their medical condition and correlations could for example be made between papillary patterns and diseases such as leukaemia and breast cancer.[120] Face recognition can reveal racial or ethnic origin (Article 29 Data Protection Working Party 2003, 10). The processing of biometrical data may thus reveal – more or less immediately – sensitive information about an individual. This goes far beyond the purpose for which biometrical identification is supposed to be used.

It seems clear that the *taking* of fingerprints and photos may involve the processing of sensitive data. It is however not clear if the algorithms and machine-readable templates that contain the information, are also to be considered as sensitive personal data (Hes et al. 1999, 42).[121]

---

[118] X., "KJD&I Symposium resounding success. A brief overview of the forum discussions" *Keesing Journal of Documents & Identity*, Issue 16, 2006, 7. However, a counterargument has been given also by "the introduction of a new chip-enabled bank card in France [which] did not result in lower fraud rates until the fallback scenario had been abandoned".

[119] "Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life."

[120] The Article 29 Data Protection Working Party opinion on Council regulation 2252/2004 refers to the FIDIS study on PKI and biometrics (Article 29 Data Protection Working Party 2004, 68) and states: "In the case of storing fingerprints attention will have to be paid in so far as various correlations between certain papillary patterns and corresponding diseases are discussed. As for instance certain papillary patterns are said to depend on the nutrition of the mother (and thus of the foetus) during the 3rd month of the pregnancy. Leukaemia and breast cancer seem to be statistically correlated with certain papillary patterns. Any direct or precise correlations in these cases are not known …".

[121] "Several stages in the processing of biometrical data were identified. The first stage is the capture or measurement of the human characteristic and the creation of a template. In this stage the 'raw' or unprocessed

Possibly, case law (of the European Court of Human Rights) will make a distinction between different biometrics (e.g. non-sensitive fingerprint *vs.* sensitive facial image).

Taking, measuring and processing of biometrical data may also harm a person's personal feeling or experience of dignity. The fact that people feel uncomfortable with close observations (they are obliged to look into a lens, they are obliged to put fingers on holders used by other people etc. …) has already been observed as a possible feeling of intrusion of dignity (Wayman 2006, 15).[122]

That taking facial images is related to this observance, may also be derived from the fact that for example the Quality Assurance (QA) software – used to examine the properties of the applicant's photo for a passport or travel document – can reject a photo thereby *explaining why* (Friedrich, Seidel 2006, 5). Exceptions to the photo requirements are possible for handicapped citizens and for certain religious reasons, but this may at the same time confront people with themselves as being an exception; and force them to reveal their religion.

The use of 'your' body as an identification tool for others might likewise infringe what is called our informational privacy. Anton Alterman states in other words: "*The degree to which the body is objectified by the process, suggest[s] that biometric identification alienates a part of the embodied self. The body becomes an object whose identity is instantly determinable by purely mechanical means, and subject to external controls on that basis; while those means themselves are removed from the control of the subject. The representations are infinitely reproducible by their owner, but are not even accessible to the subject whose body they represent. The embodied person now bears, more or less, a label with a bar code, and is in this respect alienated from her own body as well as from the technology used to recognize it. If having an iris scan on file is not quite like being incarcerated in the world at large, being made known to mechanical systems wherever they may be is still a tangible loss of privacy that is not precisely paralleled by any other kind of information technology."* (Alterman 2003, 146) [Emphasis added]

The use of two biometric identifiers

The introduction of two biometric identifiers in EU passports and travel documents raises lot of concern. The impact of these choices is great. Whereas the Council is calling for the use of two biometrical identifiers, the U.S. and the ICAO only require one, and this only involves a digital photograph. Nowhere in the Regulation have we found the need for two biometrics argued as a proportional measure.

The inclusion of a fingerprint biometric is unprecedented. Moreover, the U.S. has no intentions of implementing fingerprints in their passports. In the Regulation it is said that these choices are 'in accordance with the principle of proportionality' and do 'not go beyond what is necessary in order to achieve the objectives pursued, in accordance with the third paragraph of Article 5 of the Treaty'.[123] This Article of the EC Treaty contains the

---

template sometimes contains information which can directly be interpreted in terms of e.g. race or state of health. Examples are facial images showing skin colour or certain signs of illnesses. These initial templates can in those cases be classified as sensitive data. Subsequent steps often follow in the processing, in which the original data are being manipulated. Whether these processed data still classify as sensitive data is questionable.

[122] "Some people feel uncomfortable with the close observation of bodily traits required for biometric recognition, often citing privacy considerations".

[123] Council Regulation 2252/2004 of 10 December 2004, Recital 9.

proportionality principle of the EC law.[124] It should be noted with regard to the vagueness of data protection that some members of the Parliament proposed to limit the passports to only one identifier with exactly the same reference to the principle of proportionality.[125] Steve Peers reaches a similar conclusion (Peers 2004, 3).[126]

When Article 4.1 of the Council Regulation states that no information in machine-readable form shall be included in a passport or travel document unless foreseen in the Regulation or unless it is mentioned in the passport or travel document by the issuing Member State, the latter possibility raises concern: The possibility for Member States to include other machine-readable information than the information described in the Regulation itself and the fact that this must merely be mentioned on the passport or travel document, opens doors for different interpretations of the principle of proportionality.

4.1.4.2 The Underlying Legal Framework (Reconsidered)

EU Regulations enter – contrary to directives – immediately and integrally into force in the Member States on the date indicated in the Regulation. EU Regulations achieve the highest harmonisation level, since no deviation can be made by a Member State.

The legitimacy of EU Regulation 2252/2004

The procedure followed by the Council – to vote the Regulations – has met strong criticism. It is said to have exploited the democratic deficit of the European Union to an unheard extreme.[127]

---

[124] EU legislation must conform to the principle of proportionality (Article 5 EC, third paragraph) to be valid. Article 5 of the EC Treaty provides that "action by the Community shall not go beyond what is necessary to achieve the objectives of this Treaty". The form taken by Community action must be *the simplest form* allowing the proposal *to attain its objective* and to be implemented as efficiently as possible.

[125] "The respect of the principle of proportionality requires proof that there are no other means to achieve the objective of increasing document security. The Commission has not provided yet the Parliament with the requested information on: - the scope and the seriousness of the problem of false documents; - the results of the former improvements (integration of a photograph on visas and residence permits; - the cost of biometrics, the error rate of the various biometric options, the risk of misuse; the principle of proportionality, the confidential requirement ... Only a detailed knowledge of the above mentioned questions will allow the Parliament to give a balanced opinion on the introduction of any other biometric data in visas, residence permits and passports" (Justification to Amendment 18 proposed by Tatjana Ždanoka in Committee on Civil Liberties, Justice and Home Affairs, 14 October 2004, Doc PE 349.798v01-00/15-30).

[126] "It might be argued that the Commission's initial proposal conformed to the proportionality principle, but there are far greater doubts that the latest version of the legislation (Council document 15139/04) conforms to the principle. The key change is the decision to fingerprint all EU citizens who need a passport. This will entail considerable costs for citizens and Member States' administrations and considerably alter the process of obtaining a passport in most Member States. The doubts about the proportionality principle are particularly cogent in light of the position of the US government and the ICAO standards related to document security, which do not require fingerprinting for the purposes of travel document security. The Commission's initial proposal expressly accepted that the security and identity checking objectives and objectives of meeting US and ICAO standards could be achieved without making fingerprint data mandatory. In light of this position it is difficult to justify the validity of mandatory fingerprinting in light of the proportionality principle." (Peers 2004)

[127] Cf. 'Rush vote European Parliament on biometrics', *EDRI-gram* (Biweekly newsletter about digital civil rights in Europe), 2 December 2004, Number 2.23, sub 1.

Firstly, more than seventy civil society organisations from the EU and abroad, nine national or regional Data Protection Commissioners and more than two hundred concerned citizens signed an open letter by Privacy International, Statewatch and European Digital Rights opposing this proposal and the procedural 'black-mail' of the Parliament by the Council, to vote on the amended Regulation that was only send to the Parliament at the latest minute.[128]

A second critique concerns the legal basis for the European Union to act. The idea of common standards for ID cards set out in EU measures is new. Commentators hold that new and separate legislation is required, since the EU does not have the power to adopt measures on ID cards at present, although it would gain such powers if the Constitution is ratified (Peers 2004).[129]

This non-competence of the EU could be found in Article 18(3) of the Treaty Establishing the European Community. Article 18 (amended by the Treaty of Nice) states:

1. Every citizen of the Union shall have the right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in this Treaty and by the measures adopted to give it effect.
2. If action by the Community should prove necessary to attain this objective and this Treaty has not provided the necessary powers, the Council may adopt provisions with a view to facilitating the exercise of the rights referred to in paragraph 1. The Council shall act in accordance with the procedure referred to in Article 251.
3. Paragraph 2 shall <u>not apply to provisions on passports, identity cards, residence permits or any other such document</u> or to provisions on social security or social protection. (emphasis added)

A third critique concerns the speed and the impact of the proposals. Sensitive information may be transferred to other countries when verification is required at border controls. With the traditional passports, personal data in the passports were shown to the border authorities, but not as such *processed*. Hence, the Directive did not apply. With automated verifications the Directive applies. Whenever the EU tolerates that the new passports are scanned in countries without adequate data protection, it knowingly permits violations of its own principles.

This risky attitude seems to be of a more general nature. Immediately after the parliamentary vote, doubts were expressed about the willingness of the Council, to take any of the

[128] See Privacy International, Statewatch and EDRI, *An Open Letter to the European Parliament on Biometric Registration of All EU Citizens and Residents*, November 30, 2004, 14 p. via http://www.edri.org/campaigns/biometrics/0411 or http://www.privacyinternational.org/. See also: '*EU governments blackmail European Parliament into quick adoption of its report on biometric passports*' 27 November 2004, http://www.statewatch.org/news/2004/nov/12biometric-passports-blackmail.htm.

[129] The starting point for this analysis is Article 18(3) EC, which provides expressly that the EC's powers to adopt legislation to facilitate the free movement rights of EU citizens: *'shall not apply to provisions on passports, identity cards, residence permits or any other such document…'.* The Council legal service's Opinion on the legality of the passport proposal (Council doc. 6963/04, 3 March 2004) also recognizes that Article 18(3) is the starting point for the analysis. There is no other provision of the EC Treaty which gives express powers for the EC to adopt measures concerning such matters, and no precedent for the adoption of EC legislation harmonising any aspect of Member States' passports.

amendments voted by the Parliament into consideration.[130] The amendment to make Recital 7 more stringent, for instance, was not followed.[131] A proposed amendment of the Parliament to prohibit the establishment of a 'central database of European Union passports and travel documents containing all EU passport holders' biometric and other data' was again not upheld. Also not upheld were amendments to involve the data protection experts of the Article 29 Working Party in the follow-up of the Regulation and the more precise choice of standards.

The legitimacy of the ICAO standards

As we have seen (see above), ICAO has a major impact on the technical aspects of the biometrics deployed for passports and travel documents. Document 9303 is the guideline legally implemented by EU legislation. The ICAO however does not oblige encryption of the data on the RFID chip (storage medium).

The reference in Regulation 2252/2004 to Document 9303 and the mandatory use of the RFID-chip has met criticism: The ICAO[132] is not a legislative body representing all members of the society (including citizens) and the standards established by ICAO might be considered as the result of a non-transparent procedure. Although this is the case for many standardisation bodies, this observation must be made because the implications of the ICAO standards will probably have huge impacts – good or 'bad' – on the long term.

The (non-binding) Report of the Parliament concludes the same where it states that '*Document No 9303 should not be referred to in an EU regulation, since it is constantly being amended by means of a process which lacks transparency and democratic legitimacy.*'[133]

4.1.4.3 Compliance with Quality Principles Taken from Privacy Law and Data Protection Law

Although all the (draft) Regulations expressly recognise the application of the Data Protection Directive and although these (draft) Regulations contain provisions that elaborate the principles of data protection law, it can be argued that some of the Articles of the (draft) Regulations infringe the qualitative principles such as the principle regarding proportionality contained in the Data Protection Directive 95/46 and the privacy case law. We will give some examples that relate to the principle of confidentiality, proportionality, finality/purpose specification and individual participation.

---

[130] Under the European Union's consultation procedure the Council can globally reject all of the Parliament's amendments.

[131] Council Regulation of 10 December 2004, Recital 8 (formerly 7) states: "With regard to the personal data to be processed in the context of passports and travel documents, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data applies. It should be ensured that no further information shall be stored in the passport unless provided for in this Regulation, its annex or unless it is mentioned in the relevant travel document." The Parliament proposed to suppress the last phrase 'to make very clear what information is to be stored in the passport'.

[132] The ICAO has been founded in 1944. It is an agency of the United Nations linked to the Economic and Social Council. See OECD, *l.c.*, 16.

[133] Report of the Parliament on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS), 7.

The proportionality principle

Some provisions of the Proposal for the VIS Regulation show that the personal data processed are inadequate, irrelevant and excessive in relation to the purpose for which they are collected (Article 29 Data Protection Working Party 2005b). For example: The requirement to hand over surname at birth (Article 6.4.a) can infringe the right to a private life. The obligation to provide the nationality at birth (Article 6.4.b) is of no relevance and may lead to discrimination. The possibility to link individuals with a group (Article 5.4) opens the door to make profiles; the definition of 'group' is unclear and should be precisely defined.[134] The Proposal justifies the inclusion of such data stating merely that 'these data are required for the assessment of the application and for checks on the visa of the applicant. (…).[135]

Article 6.4.f. requires to give the name and address of the person issuing an invitation or liable to pay the costs of living during the stay of the applicant. Why should this (possibly very) sensitive information – for example the issuer or liable person being a hospital, a politician, a priest – be given and stored in the database? Here, the Proposal justifies by stating that 'the inclusion of data on persons and companies issuing invitations will help to identify those persons and companies which make fraudulent invitations. This constitutes important information in the fight against fraud, illegal immigration, human trafficking and the related criminal organisations which often operate in an international scale'.[136]

The retention period for each application file being maximum five years (Article 20) is also subject to critique for specific situations such as in case of visa applications being refused or visas that have been issued for less than three months (Article 29 Data Protection Working Party 2005b, 18).

As already indicated, the inclusion of two biometric identifiers (not encrypted) in the EU passport also candidates for an infringement of the proportionality principle.

The purpose specification and finality principle[137]

According to the purpose specification principle, personal data can be processed as long as the processing meets specified, explicit and legitimate purposes. This principle is the most important touchstone of data protection law because it provides the criteria to decide about the legitimacy of a processing and the use and quality of the personal data processed.

Many purposes foreseen in the *VIS* Regulation may be criticised: they go far beyond the achievement of a common visa policy. For example, the purpose to prevent threats to internal security of any of the Member States is already pursued by means of the SIS and other tools available for police cooperation (Article 29 Data Protection Working Party 2005b, 10).

---

[134] Article 2 (7) defines 'group members' as '*other applicants with whom the applicant is travelling together, including the spouse and the children accompanying the applicant*'. Linking individuals with groups could for example be limited to specifically defined and enumerated lists of events or cases when the link with a group is deemed to be of utmost importance.
[135] Annex "Commentary on the Articles" of the VIS Proposal, 33.
[136] Ibid
[137] Article 6.1.b of the Data Protection Directive.

The purpose of facilitating checks at external border checkpoints and within the territory of the Member States, of assistance in the identification and return of illegal immigrants and of facilitating the application of Regulation (EC) No 343/2003, is excessive when analysing the legal basis of the Proposal, namely Article 62.2.b, ii and Article 66 of the Treaty establishing the European Community (TEC).

There exists currently a Proposal for a Council Decision concerning access to the VIS by Europol for the purpose of prevention, detection and investigation of terrorism and other serious criminal offences. [138] This Proposal reflects a more general trend to allow several law enforcement authorities to access all available databases for their work on terrorism and other serious criminality.[139]

The EDPS stated very clearly in an Opinion on the VIS Proposal: "*One must bear in mind that the VIS is an information system developed in view of the application of the European visa policy and not as a law enforcement tool. Routine access would indeed represent a serious violation of the principle of purpose limitation. It would entail a disproportionate intrusion in the privacy of travellers who agreed to their data being processed in order to obtain a visa, and expect their data to be collected, consulted and transmitted, only for that purpose*".[140] EDPS proposes here that access to VIS by law enforcement authorities should only be granted 'in specific circumstances on a case-by-case basis and must be accompanied by strict safeguards'.[141] For example, the condition in the Proposal's Article 5 that "*the consultation of VIS data will contribute to the prevention, detection or investigation of [a specific] offence,* does not suffice for the EDPS: consultation must "substantially" contribute.[142]

Also other purposes mentioned throughout the Proposal (examination of applications, consultation between authorities, reporting and statistics, identification) derive from the main

---

[138] Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences" – COM (2005) 600 final.

[139] See for example the Commission's Communication of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs (COM (2005) 597 final), point 4.6: "*In relation to the objective of combating terrorism and crime, the Council now identifies the absence of access by internal security authorities to VIS data as a shortcoming. The same could also be said for SIS II immigration and EURODAC data*".

[140] European Data Protection Supervisor, "Opinion of 20 January 2006 on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM (2005) 600 final)", http://www.edps.eu.int, 2. Hereafter called: EDPS Opinion of 20 January 2006.

[141] EDPS Opinion of 20 January 2006, 3.

[142] EDPS Opinion of 20 January 2006, 4. An additional concern is that law enforcement activities in the third pillar do not fall under the application field of Data Protection Directive 95/46. There is currently a Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, COM (2005) 475 Final, adopted by the Commission on 4 October 2005, forwarded to the European Parliament for mandatory consultation. The text is available via http://europa.eu.int/prelex. According to article 3.1, the Framework Decision shall apply to the processing of personal data (*…) by a competent authority for the purpose of the prevention, investigation, detection and prosecution of criminal offences*. The Framework Decision shall however not apply to the processing of personal data by Europol, by Eurojust and by the Custom Information System (see Article 3.2.). Although the scope of the Proposal is not clear, we will not further discuss this here.

purpose of improving the common visa policy. Since VIS seems to become a common search- and research tool for all authorised public authorities within the EU, privacy and data protection safeguards should be indisputably introduced in a clearly defined and accessible way before effectively deploying the VIS.

Also the *European Passport* requirements for biometrics can lead to unexpected and unforeseen purposes. Once biometrical data and corresponding information (for example: a person x is identified in Frankfurt Airport through facial recognition) are available, the risk of their use for other purposes than the ones they were collected for will undeniably remain present.[143] Obviously, enhanced interoperability of systems will contribute to increasing such risk. The possibility that the data subject will never be aware of such illegitimate uses and/or processing of data is realistic as well.

This is not just a scenario. A most intriguing example has already been demonstrated in America. During the American Super Bowl Final in Tampa (Florida) in June 2001, the police deployed intelligent video cameras with facial recognition technology to scan the faces of all the 100,000 spectators present in the stadium. The faces of these spectators were compared with the facial templates of wanted criminals and terrorists, stored in a database.

Personal data collected through machine-readable passports and travel documents could be used for other purposes than legally permitted, such as profiling. It is not clear whether and when profiling falls under the rights and obligations of the Data Protection Directive; privacy and anti-discrimination law may also apply (Hildebrandt, Backhouse 2005, Hildebrandt, Gutwirth 2005, Schreurs et al., 2005). The directive may allow statistical processing or profiling of personal data, once the data are made anonymous.[144]

But the results thereof (the profiles) can be applied afterwards to data subjects without them knowing that the profiles are applied to them: this could for example result in people being individually stopped at a border control or individually checked because they fall under a certain profile[145]. How is it guaranteed that the data subject is informed that such automated individual decisions are applied to him? How can be guaranteed that the data subject can exercise the right to obtain from the controller knowledge of the logic involved in such automatic processing operations? Will all authorised agents acting upon these automated

---

[143] "… the Working Party supports the European Parliament's demands that each Member State shall maintain a register of the competent authorities and authorised bodies referred to in Article 2 par. 1a of Regulation (EC) 2252/2004." (Article 29 Data Protection Working Party 2005c, 9)

[144] Recital 26: "whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable"; Article 6.1.b: "further processing of the data for historical, statistical or scientific purposes is not considered as incompatible provided that appropriate safeguards are provided by the Member States whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual; …"

[145] Article 15 of the Data Protection Directive principally prohibits that a person is subject to automated decisions which produce legal effects concerning him or significantly affects him and which are based solely on automated processing of data intended to evaluate certain personal aspects relating to him. However, this principal prohibition is not applicable if that decision

" (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests" (Article 15.2).

decisions 'know' this logic involved and be able to communicate this logic to the data subject?[146]

Another risk can be that the machine-readable systems (and not only personal data) may be used by other persons and for other purposes than foreseen. In 2005, the 27th International Conference of Data Protection and Privacy Commissioners adopted a Resolution in which it expressed its awareness '*of the fact that the private sector is also increasingly processing biometric data mostly on a voluntary basis*'. The Conference called for *'1. effective safeguards to be implemented at an early stage to limit the risks inherent to the nature of biometrics; 2. the strict distinction between biometric data collected and stored for public purposes (e.g. border control) on the basis of legal obligations and for contractual purposes on the basis of consent; 3. the technical restriction of the use of biometrics in passports and identity cards to verification purposes comparing the data in the document with the data provided by the holder when presenting the document'* (emphases added). [147]

It should be added here that the strict separation between public and private authorities blurs, also in law enforcement practices (such as airport security). This creates the risk that personal data that are primarily processed for identification purposes, may afterwards be used for private purposes such as – for example – the billing of outstanding debts for the use of a service, proof of evidence in a private litigation (divorce, employment) or direct marketing. The latter practice is forbidden without prior consent of the data subject but it is widely spread and hardly sanctioned. The law does not guarantee us that – roughly said – 'these data or databases can and will never be used for any private purpose, whatever later legislation may say'.

The individual participation principle

The individual participation principle is also confronted with problems. While there is no difference with traditional passports (without biometrical identifiers) when a person wants to access or rectify personal data that are visibly written *on* the passport, this may not be the case for his biometrical identifiers *in* the passport. How to check and verify if the biometrical data are still accurate? How an individual for example knows that the biometrical identifiers in his passport are still *working* before or during his travel? What if the storage medium is *destroyed*?[148] What if his physical data do not match the biometrical data any more and access is unexpectedly refused? How to settle these (literally) *unforeseen* problems? Fallback procedures should be available to constitute safeguards for the introduction of biometrics, as they are neither accessible to all nor completely accurate." (Article 29 Data Protection Working Party 2005c, 8). It remains however not clear how these fallback procedures can be worked out.

[146] Article 12 (a) of the Data Protection Directive
[147] 27th International Conference of Data Protection and Privacy Commissioners, "*Resolution on the use of biometrics in passports, identity cards and travel documents*", Montreux 16 September 2005, http://www.edps.eu.int/legislation/05-09-16_resolution_biometrics_EN.pdf.
[148] See further: The data controller must implement appropriate technical and organisational measures to protect personal data against accidental or u lawful destruction (Article 17.1 Data protection Directive)

4.1.4.4 Central Biometrical Database(s)?

What

The issue whether *one central European database or several databases* in the Member State will be deployed, is still open. Council Regulation 2252/2004 does not oblige central storage but leaves this important issue to the Member States open.

The European Parliament, in its Report on the Commission's proposal for the Council Regulation[149], proposed that the creation of a central database of EU passports and travel documents containing the biometric and other data of all EU passport holders should be forbidden. The Council finally did not take into account this proposal of the Parliament.

Article 29 Data Protection Working Party states in its Opinion on Council Regulation 2252/2004 that "there is a risk that the setting up of a centralized database containing personal data and in particular biometric data of all (European) citizens could infringe against the basic principle of proportionality; intensifies the dangers of abuse and function creep; raises possibilities of using biometric identifiers as 'access keys' to various databases, thereby interconnecting data sets."

In the ICAO reports[150], centralised databases are also an important feature. The ICAO calls for central databases that allow for additional security confirmation checks, but does not go so far as to effectively *require* such systems. Hence, there is some flexibility permitted by the ICAO and some states may interpret the ICAO standards to require centralised databases.

Which are some of the possible impacts of databases containing biometrical data?

First of all, a central database allows determining that the *biometrics* of an applicant is enrolled only once (Wayman 2006, 15). If the biometrics are not stored in a central database or the database is not connected with other databases, a fraudulent person might use the same (but stolen) biometrics (of a former bona fida applicant) for the second time. Or the other way around: a bona fida applicant can enrol without knowing his biometrics is already circulating in the system (OECD 2004, 26).[151]

But central database bring along risks.

When biometrics is stored in a database, the database allows for identification. State authorities can determine one's identity independently, without the data subject being aware of it.

---

[149] Report of the Parliament on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116-C5-0101/2004-2004/0039 (CNS), 8.
[150] See generally ICAO, *Biometrics Deployment of Machine Readable Travel Documents ICAO TAG MRTD/NTWG Technical Report: Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents*, Montreal: ICAO, May 12 2003. See also ICAO Press Release PIO 09/2003, *Biometric Identification to Provide Enhanced Security and Speedier Border Clearance for Travelling Public*, Montreal, May 28, 2003, available at http://www.icao.int/icao/en/nr/pio200309.htm.
[151] "Biometrics in travel documents are not sufficient to prove one's identity. They only bind the individual to the travel document he owns. This does not mean that the declared identity is the real one. Therefore, ensuring that an individual does not enroll with more than one identity may require that biometrics be included in a global and internationally interoperable system."

All terrorist attacks in the last years have been committed by people who were already suspect in a way or another. So these people were already in a database. This did not help to prevent the attacks. The question can be asked whether putting everybody in the database would prevent then these kinds of serious crimes? Why would putting millions of innocent people in a database help to prevent crime, whereas having had the possibility to access the data of thousands of suspected people in a much smaller database did even not prevent serious crimes?

Another reason why creating a database of 'innocent' biometrics raises questions, is the simple fact that terrorists are clever enough to be not in the database. Moreover, terrorists come often from third countries and just need to pass the border. It will not be difficult to stay out of the database when you have bad intentions.

Having your biometrics put in a central database gives raise to security problems that are the mere consequence of the compulsory 'being' in the database.

Identities can be stolen without any physical perception of the theft (Hoepman, Jacobs 2006).[152] Whereas in case of a token, one needs to copy the template of the biometrics on the token, a central database just needs to be accessed by authorised or unauthorised persons. Studies prove that often the computer crimes occur from the inside. Another issue concerns profiling (see further).

In addition, databases containing biometrics can offer big business opportunities, even for governments. This would however irrevocably lead to a function creep and infringe the finality and proportionality principle. But the exercise must be made. Biometrics are principally used to verify the link of an individual with the document containing the biometrics (Van Kralingen et al. 1997, 9).[153] When biometrics are stored in a database, biometrics can also be used to *identify* an individual (Jacobs 2006). Even more: the identification can be established without the need for a passport. Once stored in a database for the purpose of issuing passports, these biometrical data can be used to offer services to public and private institutions that want to identify people (customers) with merely a fingerprint reader or face recogniser ('the body as passport'). If access rights to these databases will be granted to private institutions, governments are building a major asset for the future: they could ask 'fees' or 'costs' each time the database is consulted by third parties for identification (Van Kralingen et al. 1997, 4).

For the same reason, a biometrical database can offer huge possibilities for law enforcement agencies. The traditional approach in law enforcement was to look first for suspects and then to search them among citizens. Biometric databases allow law to look for all citizens and than search for suspects. In other words: Every search for a possible perpetrator of a crime can start with a presumption of all persons present in a database, being suspect.

The possibility to allow a combination of at least two verification methods should be encouraged. When biometrical data are measured against the template in a database, a second

---

[152] "Two basic laws for ordinary password use are: change regularly, and avoid multiple use of the same password. Both laws are broken with the use of biometrics: you use the same 'password', say a scan of your finger or iris, everywhere, and you can never change it – after it is compromised. Biometrics may actually lead to an increase of identity fraud via what we like to call 'bio-phishing': fraudulently taking your biometrics in order to be admitted as you somewhere else."

[153] "Verification is not a process that investigates the identity of a person, it only determines if two data belong to the same person".

verification tool such as a password seems *appropriate* to allow individuals to secure their own personal data (Van Kralingen et al. 1997, 20).

4.1.5 Conclusion

Europe is looking for powerful tools to verify the identity of individuals and thus ensure the maintenance of a certain level of security is required. However, in the approach for a standardised use of machine-readable documents, the fundamental rights and freedoms of each person have to be considered carefully. New threats to fundamental rights but also risks for new crimes against citizens (such as identity theft) *as a consequence of the deployment of machine-readable documents* must be carefully taken into account.

The European Union is now developing the legal basis of an information society that will have a major impact on the identity and the personality of EU citizens and third country nationals.

Three categories of data subjects may already be subjected to the processing of their biometrical data. *Applicants for asylum and aliens* apprehended in connection with irregular crossing of an external border must promptly give their fingerprint and the fingerprint will be stored in a central database for a period of respectively ten years and two years from the data on which the fingerprints were taken. *Visa applicants* must also provide a huge database (the VIS) with their fingerprints for a period of five years after expiry of the visa. However, the VIS database – as the proposal is today – can be accessible by almost any public authority for almost any purpose, including the purpose of prevention, detection and prosecution of 'serious criminal offences'. *EU citizens* who want to go abroad can not leave without having their face and fingerprint stored in their passport or travel document, while nor the U.S. neither the I.C.A.O. standards require the use of two biometrics and while the impact and the risks of the deployment of biometrics has not been assessed adequately yet. Moreover, the Member States themselves will decide whether the biometrical passport data will be stored in a central database: the Regulation leaves the option open and ignored hereby the amendments of the Parliament.

The European *data protection and privacy frameworks* apply to the Regulations but in no case this means that the Regulations are a priori compliant neither with the Data Protection Directive nor with the ECHR.

The use of biometrics as such is in the first place questioned. Biometrical identifiers are unique: once stolen, they are difficult to replace. People may not be willing to be scanned all the time, especially when they need to look into a camera or have to put their finger on a reader, as if they were criminal. The accuracy of the data and the security of processing is hardly proven and almost merely promoted by the vendors of biometrics. Biometrical data may appear to be sensitive data, which in principle may not be processed. Machine-readability of people and of their documents may turn out to be excessive, hereby surpassing the necessity and proportionality criteria set out by the European Court of Human Rights.

The legal basis itself of the VIS and EU passport Regulations is questioned. While the *VIS* is in fact a 'first pillar' database, the Proposal provides for access possibilities by 'third pillar authorities' – for which normally other legal grounds than Articles 62 and 66 of the TEC must be invoked. While the EU regulates its *passport* on the basis of standards established by non-democratic standardisation bodies (ICAO), Article 18 (3) of the TEC even excludes the

adoption of provisions by the EC on passports, identity cards, residence permits or any other such document.

Eurodac, the EU passport and the VIS are subject to possible function creep that is not foreseeable. The impact of this deployment and the future of identity can – regrettably – not be entirely assessed at this moment. A step-by-step approach seems the essential requirement to safeguard the fundamental rights and freedoms.

4.1.6 Legal Sources with Respect to RFID

According to the Council Regulation of 13 December 2004[154] and the Commission Decision of 28 February 2005[155] the RFID chip has been chosen as the storage medium for the European Passport (usually called 'electronic' or 'biometric' passport)[156]. Although the aforementioned Council Regulation does not apply to identity cards issued by Member States to their nationals or to temporary passports and travel documents having validity of 12 months or less[157], The Hague Programme[158] requested the development of minimum standards for national identity cards[159]. To this direction the United Kingdom, having at that time[160] the presidency of the Council of the European Union, proposed the incorporation of biometric identifiers inserted in the new identity cards in a radio frequency chip.[161] However the Belgian government has already entered a reservation on the use of fingerprints and RFID chips on the ID cards[162].

---

[154] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, L 385/1-6

[155] Entscheidung der Kommission vom 28.02.2005 über die technischen Spezifikationen zu Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, K (2005) 409 endg. (As the United Kingdom and Ireland did not take part in the adoption of this measure, an authentic English version has not been established).

[156] The ICAO specification for epassports relies on the International Organisation for Standardisation (ISO) 14443 Standard, which specifies a radio frequency of 13.56 MHz. (http://www.icao.int/mrtd/download/documents/Annex%20I%20-%20Contactless%20ICs.pdf). These tags are passive, they have a shorter intended read range and they include other features such as tamper resistance and cryptography. More details at Juels A., Molnar D. & Wagner D, Security and Privacy Issues in E-passports, available online at http://eprint.iacr.org/2005/095.pdf

[157] Art. 1 (3) Council Regulation No 2252/2004

[158] The Netherlands Presidency of the Council of the European Union (July-December 2004) produced a new draft programme for justice and home affairs, called Tthe Hague Programme. This document introduced the idea of common standards for identity cards among the Member States, although the European Union does not have the power to adopt measures on identity cards at present (Art. 18 (3) EC Treaty).

[159] 'The Hague Programme; strengthening freedom, security and justice in the European Union', Council of the European Union, 13302/1/04 LIMITE JAI 370 (15.10.2004), 13993/04 LIMITE JAI 408 (05.11.2004) and 16054/04 JAI 559 (13.12.2004), p. 17

[160] July-December 2005

[161] Draft Conclusions of the Representatives of the Governments of the Member States on common minimum security standards for Member States' national identity cards, Council of the European Union 14351/05 LIMITE ASIM 51, available online at http://www.statewatch.org/news/2005/nov/eu-biometric-ID-Cards-Conclusions.pdf.

[162] Draft Conclusions of the Representatives of the Governments of the Member States on common minimum security standards for Member States' national identity cards, Council of the European Union 14622/05 LIMITE ASIM 54, available online at http://www.statewatch.org/news/2005/nov/eu-ID-Cards-Conlclusions.pdf. The Belgian reservation led to a change in the Council conclusions adopted on the 1st and 2nd December 2005. See

4.2 A Regulatory Framework for Entity Authentication and Pan-European eIDs?

4.2.1 Introduction

The Porvoo Group is an international cooperative network whose primary goal is to promote a trans-national, interoperable electronic identity, based on PKI technology (Public Key Infrastructure) and electronic ID cards, in order to help ensure secure public and private sector e-transactions in Europe. [163]

At the Porvoo 7 seminar, held in Reykjavik in May 2005, among the topics discussed was a discussion paper by Thomas Myhr entitled *"Regulating a European eID. A preliminary study on a regulatory framework for entity authentication and a pan European ID".* [164] [165]

Hereafter we briefly summarise this study, as well as the comments on the report, some of which were presented at Porvoo 8 in Brussels in October 2005.[166]

4.2.2 Context of the Study

Myhr contributed in the eAuthentication workshop organised by CEN/ISSS in December 2004, which aimed at developing *a strategic vision towards an electronic ID for the European Citizen*.[167]

Regarding legal aspects, their main observation was that, despite an architectural model, standards and technical specifications, there is European regulation missing in the field of electronic *(entity) authentication*. This term, which is further explained below, is often used as a synonym for identification.

The advice of CEN/ISSS was to rely as much as possible on existing regulation. In addition, they pointed out a number of topics, which in their opinion should be regulated within a so-called European eAuthentication framework.[168]

Council of the EU 14390/05 (Presse 296), 2696th Council Meeting, available online at http://www.fco.gov.uk/Files/kfile/JHA_Conclusions_1-2Dec.pdf, p. 35 point 1.

[163] More information about the group can be found at http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/20710B02C6C5B894C2256D1A0048E290/

[164] The study is available at: http://Porvoo 7.fjarmalaraduneyti.is/media/Porvoo 7/Thomas_Myhr.doc

[165] Thomas Myhr is a senior advisor at the Norwegian Ministry of Trade and Industry. He was the project leader of "eRegelprosjektet", a project aimed at identifying and removing obstacles to electronic communication in the Norwegian legal framework (i.e., laws, regulations, etc.). He was also involved in the implementation of the Electronic Signatures Directive and the E-Commerce Directive in Norwegian law.
Programme. He is a member of Porvoo.

[166] More information on the seminar is available at http://www.Porvoo 8.rrn.fgov.be/Porvoo 8/home.php.

[167] The workshop report is available at: http://www.cenorm.org/CENORM/businessdomains/businessdomains/isss/activity/wseaut.asp.

[168] Namely (1) procedures etc. when issuing an eID, (2) the content of an eID and its verification (3) data protection (control information presented to third parties) (4) liability and (5) revocation of the eID and to some extent (6) interoperability (see the mentioned CEN/ISSS report, p. 18-21).

The Myhr study, which is discussed here, has clearly been inspired by the discussions with CEN/ISSS (same topics, same conclusions). It was prepared for and accepted by the Porvoo Group.

At Porvoo 8, the group decided that the report should be included in the Porvoo eID requirements.[169]

This leads us to the key question of the report: *what suggestions do Myhr, Porvoo and CEN/ISSS make in regard to a regulatory framework for entity authentication and a pan European eID[170]?*

4.2.3 Using the Existing Regulation as far as Possible

Their first proposition is that the existing regulation should be used as far as possible. The report verifies whereas the e-Signature Directive[171] can be applied to the context of (electronic) identification.

Before we explain Myhr's opinion in this regard, we should first say something about the two central concepts of the report: *signatures and identification*.

Technicians usually use the term signatures as a synonym for *digital signatures*. They understand it as a cryptographic primitive, which is fundamental in authentication, authorisation and non-repudiation. In a technical context, the purpose of a (digital) signature is to provide a means for an entity to bind its identity to a piece of information. The process of signing entails transforming the message and some secret information held by the entity into a tag called "signature" (Menezes, Van Oorschot, Vanstone 1997).

Depending on the usage of the signature, the signed message can be used for authentication. Authentication is typically subdivided into two separate classes:

- data authentication, to corroborate the origin and the integrity of data (e.g. a contract) and
- entity authentication, to corroborate the partial identity of an entity and a set of its observed attributes. This process is referred to as "identification".[172]

With regards to digital security, *non-repudiation* means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. In other words, non-repudiation of origin proves that data has been sent, and non-repudiation of delivery proves it has been received.

---

[169] At the moment when drafting this article, the new version of the Porvoo eID requirements was not yet available. The current version can be found at: http://www.fineid.fi/vrk/fineid/files.nsf/files/2F38FAA842A30AE5C225703F00253D8C/$file/eID-WP-final-o.pdf

[170] Please note that the Myhr study did not limit itself to the a regulatory framework for the usage of eID (smart) *cards*. The eID can for instance also be contained in another token, such as a mobile phone.

[171] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, available online via http://europa.eu.int/eur-lex/en/

[172] Definitions from the Modinis-IDM glossary: https://www.cosic.esat.kuleuven.be/twiki/modinisidm/bin/view.cgi/Public/GlossaryDoc.

Lawyers have a different conception of a signature. For them a signature is in the first place (there are exceptions) a handwritten depiction of someone's name (or some other identifying mark) that the person writes on data – typically documents – as a proof of identity and will.

Dr. Patrick Van Eecke's doctoral thesis on this topic came to the conclusion that there are a limited number of universal reasons why signatures are used in a legal context, namely:

- to identify a person (identification),
- to provide certainty as to the personal involvement of that person in the act of signing (non-repudiation)[173]
- to associate that person with the content of a document (expression of one's will) (Eecke 2004).

The e-Signature Directive does deal with the (legal or technical) usage of signatures. It explicitly states that it does not intend to cover the question of legal recognition of electronic signatures, or to cover aspects related to the usage of electronic signatures.[174]

The directive defines the term electronic signature as follows: *"data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication"* (Art. 2,1 of the directive).[175]

The **central question** in the Myhr report is whether the e-Signature Directive only covers electronic data authentication signatures, or also electronic entity authentication signatures?

Myhr is convinced that entity authentication signatures should not be excluded from the application field of the Directive, because of the broad definition given to electronic signature.

He underpins his theory, by stating that the ETSI standard which supports the Directive (X.509 v3)[176] also includes the usage of the X.509 certificate for entity authentication *alone.*

We will not go in detail into the discussion, but only mention that there are divergent opinions.[177] Also, even if Myhr would be right, this thesis seems not to have very much

---

[173] As explained below, in consequence of the e-Signature Directive, electronic signatures which are based on a qualified certificate and created by a secure-signature-creation device have the same legal effectiveness as a handwritten signature, and thus include a non-repudiation function. They are called "non- repudiation signatures".

[174] Such topics are partially dealt with by other European legislation, such as Directive 2000/31/EC on e-commerce. Article 9 of this Directive states that "Member states shall ensure that their legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means."
For more information on the e-Signature Directive, see chapter 3 of the book Arno R. Lodder, Henrik W.K. Kaspersen (Eds.), *"eDirectives: Guide to European Union Law on e-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society and Data Protection",* Kluwer Law International, Dordrecht (The Netherlands), 2002, 200 p.

[175] The term "data" in this definition does not refer to the usage of the signature ("data authentication"), but only refers to the above mentioned "piece of information", which is digitally signed. In technical terms, this piece of information is a unique cryptographic code is calculated from the data (hash)

[176] ETSI TS 102 280 V1.1.1 (2004-03), X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons, available after registration from http://www.etsi.org/services_products/freestandard/home.htm.

[177] The EC report on "The legal and Market Aspects of electronic Signature" (contract nr. 28.400, see page 24), conducted by a.o. Prof. Jos Dumortier, excludes entity authentication from the application field of the directive,

practical relevance, because the **key provisions** of the directive (as discussed in the report) are principally relevant in a *data authentication* context.

- Article 5.2 is a non-discrimination principle regarding the legal effect and admissibility of electronic signatures in legal proceedings and
- Article 5.1 guarantees legal equivalence to paper-based signatures to a specific kind of electronic signatures ("qualified electronic signatures"[178]).

Myhr verified what should be regulated when someone disagrees with his thesis, and concluded that the answer is a legal rule for the electronic equivalence of (offline) identification. He believes that the closest one can get to such an electronic equivalence, is to ensure that it is not disqualified only due to the fact that it is in an electronic form.[179]

In addition to such a rule, Myhr considers that there are other issues that need to be addressed in some way or the other, to achieve a functional legal framework for entity authentication and the use of a pan European eID. These issues are briefly summarised hereafter.

4.2.4 Key Issues When Drafting a Directive on Authentication

4.2.4.1 Issuance Procedures of an eID

How to prove the identity of the eID holder?

For a third party to trust an eID and subsequently accept it as a valid eID, it is of vital importance to ensure the link between the natural person holding the eID[180] and the information contained in it.

This issue has bean dealt with in annex II[181] and Article 6.1 of the e-Signature Directive[182]. These rules heavily rely on corroboration of the identity of the holder of the eID done by the certification service provider (CSP).

---

by referring to its recital 8, which states: "Rapid technological development and the global character of the internet necissate an approach which is open to various technologies and services capable of *authenticating data electronically*". The report is available online at: http://europa.eu.int/information_society/eeurope/2005/all_about/trust/electronic_sig_report.pdf.

[178] A qualified electronic signature is an advanced electronic signature (which means that it is an electronic signature which is (1) uniquely linked to the signatory, (2) capable of identifying the signatory, (3) created using means that the signatory can maintain under his sole control, and (4) linked to the data to which it relates in such a manner that any subsequent change of the data is detectable), based on a qualified certificate (conditions in annex I and II of the directive) and created by a secure-signature-creation device (conditions in annex III of the directive). Currently speaking, only digital signatures in a PKI environment comply with these requirements.

[179] If one follows the reasoning of Myhr, such an electronic equivalence would already be covered by article 5.2 of the Directive, and there is a non-discriminatory rule, implemented in all the EU Member States, stating that also non-qualified electronic signatures used for entity authentication, can be given legal effectiveness and legal admissibility as evidence.

[180] A signatory means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents (art. 2, 3° e-Signature Directive).

The issue that Myhr addresses in the report is that the Directive does not state *how* the identity has to be proven to the CSP: Is personal appearance mandatory? Is checking against a national population register needed? Could any other evidential documents serve to prove the identity of the holder?

The ETSI standard on Policy Requirements for Certification Authorities issuing qualified certificates (TS 101 456) answers one of these questions, as it states that the identity of the person to which the qualified certificate is issued shall be checked against a *physical person, either directly or indirectly using means which provides equivalent assurance to physical presence. Submitted evidence may be in the form of either paper or electronic documentation.*

Still, this standard does not clarify which documents are needed to prove the identity of the eID holder, presumably because it is very difficult to find a compromise at the European level (either in regulation or in standardisation work) which is acceptable for all Member States.

Applying the same rules to both eID and visual ID

If an eID shall be given the same legal validity and be used in the same types of transactions as a national accepted visual ID, the requirements on the issuance of the eID should be the same as for the visual ID. Myhr explains that if it were easier to obtain an eID, this would facilitate circumvention of existing rules and regulation and build down existing trust in the ID system.

Today, EU Member States usually have very precise regulations, procedures and document requirements for issuing an ID, but these requirements usually *only apply to visual ID's*.

4.2.4.2 Content and Verification of the eID

The use of unique identifiers

It is imperative that the information in the eID distinguishes holders from each other. There are several (equally good) ways to do this, but when one wants to have a pan European eID, one of these solutions will probably have to be chosen.

According to Myhr, the chosen identifier should have the following features: (1) universality of coverage, (2) uniqueness, (3) permanence, (4) exclusivity and (5) precision.

He raises the question how to make sure that a foreign entity can *verify the identifier*, if it is not used to handle a specific type of identifiers used in foreign eIDs?

---

[181] Annex I, d° states that the certification service provider issuing qualified certificates *"shall verify, by appropriate means, in accordance with national law, the identity […] of the person to which a qualified certificate is issued."*

[182] Article 6.1 states that *"at the time of issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate."*

One external comment on the report[183] was that the report should be complemented with the concept of "certificates", which is the basis for the authentication aspect in eID. These certificates do *not need to include the identifiers of the eID holder*. Linking to these identifiers is (technically) possible without including them in the certificate.

Control of information disclosure

Another issue addressed in the report is how to make it possible for the eID holder to control which information from the eID or certificate is presented to a third party?

It is clear that the need for information that has to be ascertained with information from the eID is different from situation to situation. A hospital for instance, probably needs to know the eID holder's real address, but a company selling widgets over the internet, does only need to know that it will receive due payment for the delivered goods.

Not dealt with in this report, is the relating issue, that a large number of people on the one side declare quite some sensitivity to their personal information being leaked, but on the other side:

- are not very much prepared to accept the overhead or cost of privacy enabled technologies, and
- give large quantities of their (identity) data away to e.g. CRM, profiling programs and questionnaires, where they often cannot control what is done with these data.

Additional research is needed to examine and understand this contradiction. [184]

The use of pseudonyms

The European Union and its Member States have enacted a legal framework to facilitate the exchange of personal data and to provide guidance on processing of personal data while restoring individuals' control over their data.

One of the rules which are relevant in this context is contained in annex I of the e-Signature Directive: the qualified certificate should contain the name or the *pseudonym of the signatory* (under the condition that it can be identified as a pseudonym).

A pseudonym is an *arbitrary identifier of an identifiable entity*, by which a certain action can be linked to this specific entity. The entity that may be identified by the pseudonym is the holder of the pseudonym.

A pseudonym is typically a fictitious name that can refer to an entity **without using any of the entity's identifiers**. In effect, the pseudonym is an additional attribute of a given entity's identity, which allows it to form a set of partial identities which can not necessarily be easily traced to the originating entity. [185]

---

[183] The Comments were formulated by the Ad hoc group on Identification and Authentication, which is currently under Austrian presidency.
[184] In the framework of the FIDIS project, an experiment is currently being performed on valuing the price of location privacy.
[185] Definitions from the Modinis-IDM glossary:
https://www.cosic.esat.kuleuven.be/twiki/modinisidm/bin/view.cgi/Public/GlossaryDoc.

Myhr doubts that there are any visual ID's today issued with a pseudonym instead of a real name, and he assumes that an eID with a pseudonym would most probably have a limited legal and practical value.

He is convinced that when building a legal framework for entity authentication, the right or possibility to use a pseudonym for identification purposes, will need to be addressed.

In this context it is useful to mention an R&D initiative in the field of Identity Management sponsored by the European Commission and the Swiss Government: the PRIME project.

This project proposes building a user-controlled system for managing identities. Their vision is to give individuals sovereignty over their personal data, and enable them to negotiate with service providers the disclosure of personal data and conditions defined by their preferences and privacy policy.

Hence, to a range of risks, there is a corresponding range of responses about disclosing personal data, from full anonymity, to partial anonymity ("pseudonymity") and third-party certified identity. Thanks to the technology, even when anonymous (or pseudonymous), people can still be accountable for their actions.[186]

4.2.4.3 Data Protection

Selective disclosure of data from the qualified certificate

Pursuant to Annex II of the e-Signature Directive, a qualified certificate should not be made public unless the signer/holder has given his approval.

According to Myhr, this rule is insufficient, as it says nothing on the possibility to selectively disclose information, depending on the context in which the eID holder is communicating. However, he believes that the issue could be solved via standardisation work.

Separating authentication and identification data

One of the comments received on the report, was that it should be complemented with the idea of separating authentication and identification data held in the eID.

It is indeed surprising that the report puts entity authentication on a par with identification, but makes no further reference to the different kinds of data to be included in the eID. By application of the general Data Protection rules[187] and the e-Signature Directive, it is clear that:

- data contained in the (qualified) authentication certificate should be limited to what is needed and legally required for authentication purposes;

[186] All this acts within the strict bounds of the law, under anonymity, pseudonymity, or on the basis of explicitly agreed terms between the parties. In all cases technology supports accountability and recourse. For more information on the project, see the project website http://www.prime-project.eu/

[187] Directive 95/46/EC of The European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- data contained in an eID for identification purposes should only be communicated on a need to basis (which mainly follows out of Member State regulation in this regard)

This is particularly relevant when the eID replaces the visual ID, and also contains identification data which previously was available on the visual ID (such as the address, national Registry Number, date of birth or the marital status of the eID holder).

4.2.4.4 Liability, Revocation and Biometry

Myhr mentioned liability, revocation and biometric issues without investigating them in detail. This led to the following conclusions of Myhr that:

- it could be useful to have the same type of reversed burden of proof for issuers of eID in all Member States, akin to the existing rule for certification service providers (Article 6.1 e Signature Directive)
- one could facilitate an enhanced revocation service, via a central European revocation point for the revocation of (all) pan European eIDs
- it should currently not be possible to use the eID as the only "seed document" to apply for a new eID from another issuer, because this would raise additional issues in regard to chain-revocation of eIDs.
- a better way to ensure that the declared holder of the eID is the user of it, could be achieved by adding biometrics.

4.2.4.5 Interoperability

Myhr also raised the question how one could stimulate the eID market to take open industry standards into use? His main finding is that neither the EU nor the Member States can force the market actors to apply such standards, unless these actors deem it beneficial from a commercial point of view.

Although Myhr describes several "interoperability schemes" to implement interoperability in the eID domain, he believes only one of them is realistic: *the authority should have an agreement with one trusted intermediary party, and the intermediary should in its turn have agreements with all certification service providers issuing pan European eIDs*.

4.2.5 Porvoo / Myhr's Suggestions

Myhr's study has been accepted at the seminar which took place in Brussels in October 2005, after having discussed the comments the group received.[188]

[188] After Porvoo 7, the Porvoo members submitted the report for consideration to relevant EU projects i.e. MODINIS, GUIDE, CEN Focus Group on eGovernment and others. For an overview of the (very limited) comments on the report, see the presentation by Ms. Paivi Pösö: http://www.fineid.fi/vrk/fineid/files.nsf/files/AA065D48FCCC3D9EC22570A70045D0C9/$file/Comments_+on+Thomas+Myhr%B4s+report.pdf

One of the resolutions of the seminar is that the study will be included (as is) in the Porvoo eID requirements.[189]

Their main suggestions in regard to a framework for entity authentication and a pan European eID, are:

- to use the e-Signature Directive as far as possible,
- to promote the development and take up of standards for entity authentication, to support the use of eID[190], and
- to conduct legal research to evaluate what the possibilities and limits are of using the existing regulation on passports as a building brick for a legal framework for a pan European eID.

The regulation on passports will take effect in all the EU Member States, which is a non-negligible asset, given the limitations of Article 18.3 of the EC Treaty[191].

Problematic though, is that trust requirements of passport rules require that the eIDs are issued by a public entity, which could hamper the emerging of a market driven solution in the Member States.

4.2.6 Conclusion

Myhr concluded that many of the issues he raised are already regulated by the Member States, via legislation for the handling of visual IDs, or explicitly for the handling of eIDs. Given the limitations of Article 18.3 EC Treaty, he admits that it might be difficult to find a common understanding on (legal) requirements for a pan European eID.[192]

The Porvoo Group probably made the same consideration, but unfortunately decided to not conduct further legal research within the group.[193]

In this context one could make the general remark that, even if Europe would be politically ready for additional regulation in the field of electronic authentication, it would be strongly advisable to first conduct sufficient research on the topic, to have a clear view on:

---

[189] The seminar report of Porvoo 8 is available here: http://www.fineid.fi/vrk/fineid/files.nsf/files/32CEC4054FC5BB5EC22570A7003D9825/$file/Porvoo8+Resolutions.pdf

[190] It is useful to know that a standard is being prepared by CEN TC224 WG15 on the European Citizen Card. For the status of this standardization work, see the presentation by Mr. Lorenzo Gaston at Porvoo 8, available at: http://www.Porvoo 8.rrn.fgov.be/Porvoo 8/doc14/05_Porvoo 8_lorenzo_gaston.ppt

[191] Article 18,3. EC Treaty prevents the Council from drafting regulation on inter alia identity cards. This article sets up legal parameters that have to be observed when drafting a legal framework for a pan European eID: there is a core of legal regulation on "identity cards" that is safeguarded to the EU Member States.

[192] Page 32 of the Myhr report.

[193] The Porvoo 8 report states verbatim: *"After discussion, it was agreed that the legal consolidation will follow the practical developments and that it is therefore of little use to bring this legal issue forward again at next meetings. Instead the Porvoo Group should continue with deployment and demonstrating the usefulness of interoperable IAS services, preferably in appealing use cases, which can then act as the trigger for any required legal developments."* This report is available at: http://www.fineid.fi/vrk/fineid/files.nsf/files/32CEC4054FC5BB5EC22570A7003D9825/$file/Porvoo 8+Resolutions.pdf

- what regulation exists about visual and electronic ID documents in the EU Member States and which "common umbrella" can be found in these regulations,
- what the remaining issues are, and how they can be solved,
- which the limits are for EU regulation and/if the issues can be solved without regulation (e.g. via standardisation).

The Myhr study is a very valuable starting point for research in this domain.

5 Leading Concepts, Prototypes and Implementations

5.1 Introduction

This chapter gives an overview of known concepts, prototypes and implementations of eID documents in Europe. They are listed in Table 5 in chapter 5.2. In the following subchapter leading concepts, prototypes and implementations are introduced and discussed. They were selected because of:

- The time that they have already been used and the subsequent practical experience that is available (Finnish and Belgian ID Card)
- The number of users covered and the introduction of new technologies such as biometrics and RFID (European Passport)
- Privacy enhancing technical (Austrian "Bürgerkarte") or procedural solutions (German e-health card)

The chapters with good practice examples do not follow a homogenous structure, due to the different nature of them and the different phase in which these projects are the content of these chapter shows a big variety.

5.2 Overview on ID Documents in Europe

Country	Name	Card (C) or Procedure (P)	Purposes covered (see Table 1)	Technology or technologies used	Status, Comments, References
Europe	European Passport	C	Ident	RFID, Bio (Face, later Finger)	Concept, prototypes and early implementations (e.g. in Germany); implementation until October 2006, see chapter 5.3.
Austria	"Bürger-karte"	P	Sign	Cert, ElSig, requires PKI	Implemented since 2005, especially for e-government, see chapter 5.5.
	e-card	C	e-health (Option: Sign)	SmCh	Implemented since 2005 with 8.3 Mio users.
Belgium	ID Card	C	Ident (Option: Sign)	SmCh, Cert, ElSig, requires PKI	Implemented since 2005, see chapter 5.6.
Finland	FINEID Card	P	Sign	Cert, ElSig	Implemented since 1999, see chapter 5.4.
France	e-ID Card	C	Ident	RFID, Bio (Face, later Finger)	INES concept (Identité Nationale Électronique Sécurisée); implementation planned to start in 2007.[194]
Germany	ID Card	C	Ident (Option: Sign)	SmCh, Cert, (Option: ElSig)	Concept; implementation planned in 2007.[195]

[194] See http://europa.eu.int/idabc/en/document/4100/335, http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050201.pdf
[195] See http://www.staat-modern.de/Buerokratieabbau/Dokumente-,10188.799625/Bundeskabinett-beschliesst-gem.htm?global.back=/Buerokratieabbau/-%2C10188%2C1/Dokumente.htm%3Flink%3Dsmo_liste

	E-Health Card	C	e-health (Option: Sign)	SmCh, Cert, (Option: ElSig)	Prototype, see chapter 5.7.
	"JobCard"	P	Requires Sign, used for SocIn	Requires ElSig and PKI	Concept, planned to start in 2007. Aim is to centralise different procedures concerning social insurance in Germany. The access of the insurance holder to this information shall be possible via electronic signature card.[196]
Greece	Traditional ID card	C	Ident	-	No plans for eID found.
Hungary	HUNEID	C	Sign	SmCh, Cert, ElSig	Concept and prototype. Within the Hungarian Electronic Public Administration Interoperability Framework currently standards are being defined and middleware is being specified.[197]
Italy	ID Card (CIE)	C	Ident, Sign	SmCh, Cert, ElSig, Laser	Prototypes. Includes laser-band to store up to 1.8 mega-byte of data[198]; see chapter 5.8.1.
Malta	eID Card	P	e-Gov, m-Gov	Cert	Launched in 2005.[199]
The Nether-lands	ID Card	C	Ident	RFID, Bio (Face, later Finger)	Prototypes, introduction planned August 2006.[200]
Portugal	"Cartão	C	Ident, SocIn,	SmCh, MagStripe,	Citizen card project approved by Council of Ministers on April

[196] http://www.teletrust.de/fileadmin/files/eCard_Initiative_09.03.2005.pdf, http://www.bmwi.de/Redaktion/Inhalte/Pdf/J-L/job-card,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf, http://cdl.niedersachsen.de/blob/images/C6935489_L20.pdf
[197] See http://interop-esa05.unige.ch/INTEROP/Proceedings/eGovScientific/papers/6b3.pdf, http://europa.eu.int/idabc/en/document/1277/398
[198] See http://vrk.fineid.fi/download/scc/roma/06-%20Electronic%20Identity%20Card%20Iavarazzo%20Porvoo%202004%20r1b.pdf, http://vrk.fineid.fi/download/scc/roma/05-%20Petecchia_Porvoo%206%20-%20EN.pdf, http://www.anci.it/cie/ and http://www.anci.it/cie/documenti/cie-all-b.pdf
[199] See http://www.emalta.gov.mt/, http://www.mobile.gov.mt/, http://www.certifikati.gov.mt/, http://www.miti.gov.mt/docs/ITStrategy.pdf, http://www.gov.mt/egovernment.asp?p=106&l=1 and https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/MalteseProfile
[200] See http://europa.eu.int/idabc/en/document/3752/5785, http://www.edri.org/edrigram/number3.8/ID

	comum do cidadão"		e-health, voting, tax	Bio (finger, other?)	2005. Seems to be in design phase still.[201]
Spain	eID card ("DNI electronico")	C	Ident (Option: Sign)	SmCh, Cert, ElSig (requires PKI), Bio (finger)	1st version presented in 2004. Card scheduled to begin in 2006. Delays probable.[202]
Sweden	eID Card	C	Ident (Option: Sign)	SmCh, RFID, Bio (Face, later Finger), Options: Cert, ElSig; Options require PKI	Issued since 1st of October 2005. Includes contact chip, RFID and biometrics in accordance with the ICAO standards for international passports. Card issued by police, biometric and other identification data is centrally stored at police.[203]

Table 5: Overview on eID documents in Europe

[201] See http://europa.eu.int/idabc/en/chapter/409, http://europa.eu.int/idabc/en/document/1373/409, http://europa.eu.int/idabc/en/document/4298/342 and http://europa.eu.int/idabc/en/document/3769/342
[202] See http://europa.eu.int/idabc/en/document/2154/343, http://www.cert.fnmt.es/ and https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/SpanishProfile
[203] See http://europa.eu.int/idabc/en/document/3247/355 and http://www.swedenabroad.com/pages/general____40960.asp

5.3 European Passport

As the technical components for the European passport are described in chapter 3 and the legal grounds are described in chapter 4 in this chapter procedural aspects of the introduction will be discussed.

The European passport uses two new technologies (RFID and Biometrics) which have not been used with these technical specifications for such a purpose and such a large number of users so far. Biometrics is known to show a number of quality problems when applied to a large number of persons with a large variety of socio cultural backgrounds. For RFID no comparable predecessor application exists.

The combination of these technologies has been developed in a timeframe of two years taking a minimum of privacy, technical and procedural security into account (see chapter 6). Most of the concrete privacy and security requirements for the implementation of biometrics and RFID in MRTD for example stated by the Article 29 Data Protection Working Party were not integrated in the legal European framework for MRTDs.

Until today (December 2006), no coherent and integrated security framework for MRTDs has been disclosed. The publicly available documentation for such a framework is currently limited to '*Protection Profiles for Biometric Verification Mechanisms and MRTDs including Basic Access Control (BAC)*'[204] and '*Technical Guideline v1.0 for Extended Access Control (EAC)*'.[205] This documentation falls short because it does not necessarily consider existing ePassport implementations[206], it consists mostly of suggestions rather than obligations and it fails to include the necessary organisational aspects of an integrated security concept. Several theoretical and scientifically demonstrated threats and conceptual flaws of ePassports have already been published, yet countermeasures have not been analysed nor specified by Protection Profiles or any appropriate technical guidelines. The most significant of these issues are further described below.

Only one field test with about 14,000 participants has been carried out: at the airport Schiphol in The Netherlands in 2005. In addition to the problems stated in the official report (BZK 2005) information that the RFID can be read out from a distance of 0.5 m (officially: 10 to 15 cm) and be eavesdropped from a distance of up to 10 m[207, 208] became public. In addition Basic Access Control (BAC) seems to be cryptographically weak and could be 'brute forced' within two hours as the effective key-length for the encryption applied can be compared to 35 bit[208] or in some cases 28 bit (Beel, Gipp 2005) only. For comparison: the Advanced

---

[204] Protection Profile BSI-PP-0016-2005 and BSI-PP-0017-2005, certified in August and October 2005 respectively by the German Federal Office for Information Security, available via http://www.bsi.de/zertifiz/zert/report.htm

[205] Issued by the German Federal Office for Information Security (BSI) in August 2006 and announced at http://www.bsi.bund.de/fachthem/epass/eac.htm

[206] ICAO first introduced BAC in its Technical Report "PKI for MRTDs offering ICC read-only access", release 1.1, dated 1st October 2004. Only the Belgian ePassports issued after July 2006 support BAC.

[207] Already in 2004 the German BSI published an analysis that the distance to eavesdrop communication between RFID tag and reader can be much bigger than 10-15 cm (Thomas Finke, Harald Kelter): Radio Frequency Identification –– Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf).

[208] See http://www.heise.de/tp/r4/artikel/21/21907/1.html and http://www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf

Encryption Standard (AES) issued by the (U. S.) National Institute for Standards and Technology (NIST) typically uses at least 128 bit key length. Symmetric cryptography works only in case keys remain secret. In this case the key to the data on the document is stored in the MRZ on the document itself. This key management can be compared to a PIN printed directly on a banking card and provides no secrecy if the document becomes lost or stolen. EAC will according to the current version of the draft perform significantly better, but is planned to be applied only for parts of the data stored on the RFID chip and in European countries.[209]

Another potential threat was demonstrated in August 2006: Cloning of RFID tags in the German passport.[210]

These publicly reported problems have had apart from the development of EAC no consequences so far. In Germany the European passport is issued without conceptual modifications since November 2005, the introduction of EAC in 2007 will not solve the described problems. And procedural solutions for the quality problems of biometrics have been required (for example in BZK 2005 or BSI 2005), but not been discussed or co-ordinated on an international level so far.

Compared to the technological and social complexity the introduction of the European passport has been carried out in a remarkable fast, non-transparent, insufficiently co-ordinated and socially not integrated way. Criticism includes:

- Compared to the complexity of the project and the degree of innovation much too short planning and development phase; errors in the design of the overall system are obvious even before start (see chapter 6)
- Insufficient public political discussion of the technology, its impact on society and a democratic basis for the decision of introduction that is at least debateable (see chapter 4.1.5)
- Compared to the sheer largeness of the introduction the project with 280 million users in Europe remarkable small and short laboratory and field testing phases
- Results from the testing did not lead to modified concepts or implementations of ID documents so far

5.4 FINEID Card

Introduction

Finland was the first country in Europe to issue an electronic identity card, the FINEID card. It is a pioneer in the implementation of the electronic identity concept. The project started early in 1998 and the first card was presented to the Finnish Prime minister on 7 December 1999, as a way of starting the application phase. The card is based on Public Key Infrastructure (PKI) and certificates. The certificate consists of a pair of keys comprising the

[209] See http://www.bsi.bund.de/fachthem/epass/EACTR03110_v101.pdf, published end of November 2006.
[210] See e.g. http://www.wired.com/news/technology/1,71521-0.html

public key and the private key. The identity card can be granted to any citizen of Finland or a permanent resident. The FINEID project aims at the creation of an infrastructure, providing secure means of conducting official business in open and insecure networks.

Description of the card

The card is the same size and thickness as an ordinary credit card. It is 86 x 54 mm (3.4 x 2.1 in.) in size and 0.75 mm (0.03 in.) thick. The card chip, which is an electronic component could break due to mechanical stress when the card is bent or the chip is in contact with a metal object. Touching the chip's contact surface should be avoided because of static electricity.

Information included in visual form is the person's picture, name, date of birth/social security number, time it is valid for, the registrar and the serial number of the card.

Information on the chip of the ID card: In addition to technical data, the card chip contains the Population Register Centre's (PRC) so-called Certification Authority certificates (explained later) and the cardholder's identification and signature certificates.

The only personal data included in the cardholder certificates are first name, family name and a unique electronic client identifier (SATU)[211]. In other words, the holder's personal identity number, home address, date of birth or other similar information is not stored on the chip. If the cardholder has notified that his or her e-mail address is to be inserted in the certificate when filing the card application, it will be a part of the information content of the certificate.

Security and PKI

The PRC issues PKI-based certificates. In the PKI method, a person has a pair of keys comprising a public and a private key. The two parts of the key pair are mathematically interdependent. The first key pair is used for authentication and encryption, the second one for electronic signature. Use of the keys is possible only with the related PIN codes. The PIN codes activate the keys, after which the chip is able to provide the required calculation operations.

Private keys are held only by the certificate holder (e.g. on the ID card chip) and can be utilised only after inputting the PIN codes, but even then they cannot be read from the card. The PIN codes are known only to the cardholder, and he or she can change them, when necessary. Three false attempts at inputting the PIN code locks the card.

Public keys are, as their name suggests, public. Certificates containing the public keys are stored in an open directory, where they are freely available.

The Public Key Infrastructure (PKI) can be utilised directly between two points (e.g. a workstation and a server), so there is no need to transfer any identifying information to any

[211] The SATU is a serial number that does not tell anything about its holder, unlike the personal identity number. The SATU identifier ends with a check digit, calculated in the same way as the checksum character of a personal identity number. The SATU identifier is for life.

central system. The PRC has no need, nor is it even technically possible, to monitor the use of the card or certificates, or, e.g., break the encryption or signature made with the card.

Misuse of the card requires BOTH the physical card AND the disclosure of the PIN codes.

Certification Authority

The Population Register Centre shall act as the Certification Authority and issue FINEID Certificates. This FINEID certificate policy has been registered by the Population Register Centre (PRC). The PRC shall be responsible for the administration and up-dating of the policy.

Authenticating the identity of the Certificate Applicant:

An electronic identification card shall be applied for by personally visiting the police authority acting as the Local Registration Authority or an entity authorised by it. The electronic identification card shall be personally picked up from the Local Registration Authority, at which time the identity of the applicant is once again ascertained[212].

Application areas of the certificates: Certificates issued in accordance with FINEID certificate policy are intended to authenticate the identity of the certificate holder, to verify the digital signature and the authenticity of digital documents or other digital objects as well as to secure the confidentiality of electronic communication, electronic transactions or electronic data transfer.

The Identity Card Act (Henkilökorttilaki 829/1999)[213] concerns the Finnish identity cards, both conventional and electronic versions.

The card can be cancelled by the authority who granted it or by the police in these cases: 1. if the owner wishes so; 2. the information on the card has been changed; 3.it is missing or has been stolen; 4.someone else is using the ID card unjustifiably; or 5.certificates have been tampered.

Cancelling the card causes the data or applications on the card to become inoperable. The applicant has to be told about the consequences of cancelling the identity card. The electronic client identifier is activated as a Citizen Certificate when an ID card is issued by the police, for instance. Then the Citizen Certificate is embedded in the ID card's chip. The Citizen Certificate may also be attached to a bank debit card[214] and/or the SIM card of a mobile device[215]

A given person may have several valid Citizen Certificates simultaneously. However, they all have the same electronic client identifier. The certificate's information content and its authenticity is verified with the electronic signature of the Certification Authority.

---

[212] FINEID certificate policy, for personal certificates on an electronic identification card for electronic communication within administration. Official translation from Finnish government website.
[213] http://www.tml.tkk.fi/Opinnot/Tik-110.501/1999/papers/legislation/legislation.html, "The Legislation and requirements regarding FINEID" 24.2.2000 Minna Rompannen and Sanni Vattinen, Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology
[214] For further information on the bank card see http://www.op.fi/
[215] For further information see http://www.etu-klubi.fi/

The Population Register Centre's  (etu) trademark helps consumers to find and identify the online services that use the Public Citizen Certificate. If desired, health insurance information also may be included in the ID card, in which case it replaces the separate KELA card[216]. In online services, the ID card is used with a reader device attached to the computer and card reader software. The ID card costs € 40 and is valid for five years[217].

Services available using the FINEID card

There are a host of services available using the FINEID card[218]. A few examples are -

State public sector applications for individuals:

- Filling out forms online[219]
- Checking all registered data
- Change of address notifications
- Tax returns
- Housing allowance services[220]
- Checking pension and employment history[221]

Public sector services for companies:

- Electronic Reporting between authorities and companies
- Online Services for Patent Applications
- Electronic funding application to National Technology Agency of Finland

Municipality application[222]: Applications for day-care, school, housing, library services, public transportation, reservations of sports facilities.

Take up and Response

The initial take up of the FINEID card was very slow. Since its launch in 2000, only around 16,000 of Finland's roughly 5 million citizens had purchased the card, by mid 2003[223]. By the end of December, Citizen Certificates had been issued to a total of 96,100 people. Of these,

[216] Personal Health insurance card, for more information see http://193.209.217.5/in/internet/english/english.nsf/WebPrintView/5232A0AAA0589750C2256DFF002F3FDA
[217] Information concerning the ID card http://www.fineid.fi/vrk/fineid/home.nsf/pages/2F1722857B8D77C5C2257054002C5C6B,
[218] The complete list of service descriptions and web addresses are available on the official website at http://www.fineid.fi/vrk/fineid/home.nsf/pages/5982EEE5795622DEC225709700387995
[219] See http://www.lomake.fi/, official Finnish government website
[220] See http://www.kela.fi/, official Finnish government website
[221] See http://www.tyoelake.fi/ official Finnish government website
[222] See http://www.aina.fi/ official Finnish government website
[223] Global e-government, Finland to launch alternative ID system, Wednesday, July 30 2003,by Sylvia Leatham http://www.electricnews.net/send.html?code=9370177

81,300 Citizen Certificates were valid. 14,900 people had integrated their health insurance information into their ID cards[224].

The goal of the Finnish government is to have 200 eID services available by the end of 2007[225].

5.5 Austrian "Bürgerkarte"

Introduction and description of the citizen card solution

Since February 2003 the "Bürgerkarte" (citizen card) is being introduced in Austria and has subsequently until January 2005 been developed to the concept we know today.[226] The current implementation is based on the signature law and the corresponding decree in the version from December 2004.[227] The "Bürgerkarte" is not a card with the same features for each citizen, such as e.g. a passport, but it is rather a concept that allows designing secure electronic public administration services. Primarily the "Bürgerkarte" is a procedural signature solution that can include additional functions. For instance it can be used for the identification of the Austrian citizens in the public sector or for their identification in the social national security system, as members of chambers, officers in the public administration or students. Furthermore it can serve for payment functions (so-called Bankomaten Karte). The "Bürgerkarte" can be implemented using various technological platforms for example chip cards or USB token.

Examples of implementations are:[228]

- National ID card
- Social security card (so-called e-card)
- Students card for two regions, in which universities and subsequently students are organised
- Banking card including electronic signature
- Service card for officers in the Austrian public administration
- Signature implementations for mobile devices (smart phones and PDAs) and USB token

[224] Most recent releases from the official finnish government website on the 04.01.2006 http://www.fineid.fi/vrk/bulletin.nsf/HeadlinesFineidEng/E52A37E26E8108E6C22570EC00364805
[225] European electronic Identity Practices. Country Update Finland. Porvoo 6, Rome, Italy, 2004
[226] See http://europa.eu.int/idabc/en/document/1395/385
[227] An overview on the legislation in Austria can be found at: http://www.a-sit.at/informationen/gesetzlich/gesetzlich.htm
[228] See http://www.buergerkarte.at/de/was_ist_die_buergerkarte/auspraegungen_der_buergerkarte.html

Main motivation for the launching of the "Bürgerkarte" was the introduction of e-government in Austria. In order to promote this initiative the Austrian "Bundeskanzleramt" (office of the Chancellor) provides all basic software and needed licenses free of charge.[229] As certificate authorities (CA) and registration authorities (RA) private providers such as A-Trust for chip card bound signatures or the Austrian Telekom for mobile signatures (so-called A1 signature) are used.[230]

Sector specific personal identifier

Basing on the requirements of the Austrian data protection act for authentication purposes in the public sector the certificates for the electronic signatures are not being used to avoid linkability in cases no signature is needed. Instead a specific personal identifier, the so-called sector specific personal identifier (ssPI), is being used in addition to name and date of birth for processing and data storage purposes. The ssPI is calculated from data stored on the "Bürgerkarte". The calculation procedure for the ssPI is the following:[231]

1. For each citizen a registration number (zentrale Melderegisterzahl, ZMR) is stored in a central database at the Citizens Register of Residents (CRR, zentrales Melderegister). This is used as basic data for the calculation of a so called source PIN (sPIN). In cases where no data in the Citizens Register of Residents is available, data from the Supplementary Register (SR, Ergänzungsregister) is used as basic data (see Figure 12).
   The source PIN is stored only on the "Bürgerkarte", not in the registration office (Stammzahlenregisterbehörde, StZRBeh). In cases this number is needed by public authorities or the citizen it has to be recalculated under the supervision of the Austrian Data Protection Commission.

[229] See http://www.cio.gv.at/identity/
[230] See http://www.buergerkarte.at/de/erstinfo/index.html
[231] See http://www.datenschutzzentrum.de/sommerakademie/2005/somak05_kotschy.pdf and http://portal.bmi.gv.at/ref/szr/anwdok.pdf

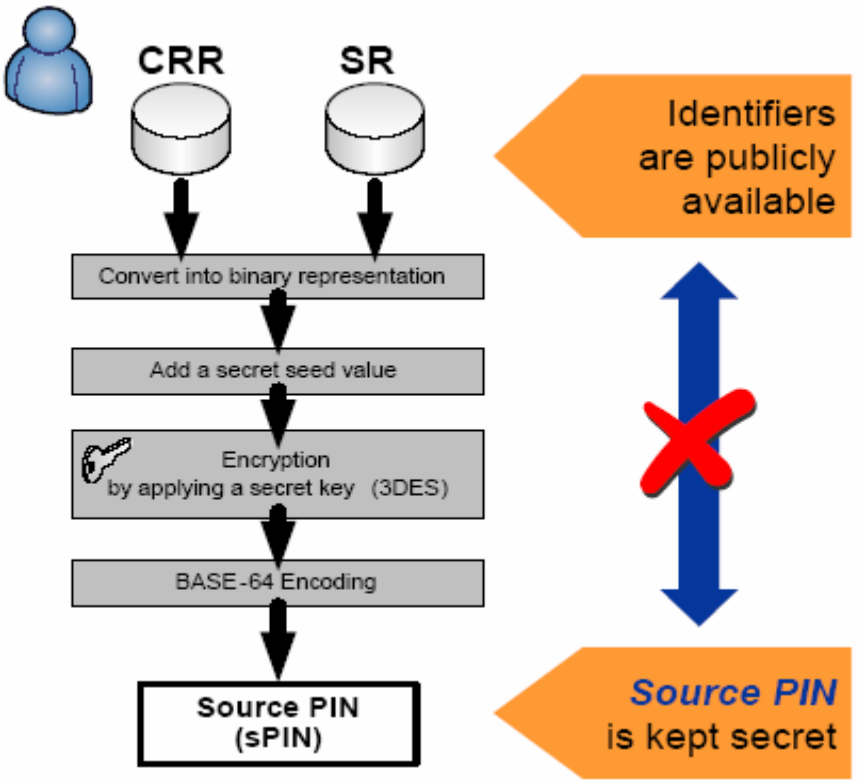

Figure 12: Calculation of the source PIN

2. The public sector in Austria is divided by law (Bereichsabgrenzungsverordnung[232], issued 2004) in 26 sub sectors and 9 sector spanning activities; each division of a public office is assigned to one of these sectors or sector spanning activities. In cases a citizen starts communicating with a public office, his source PIN (sPIN) is one-way-hashed with the sector identification taken from the "Bereichsabgrenzungs-verordnung", resulting in sector specific PIs (ssPI). It needs to be noted that the multiple ssPIs of the citizen can not be linked across the borders of these sectors (see Figure 13). In the private sector the enterprise registration number can be used instead of the sector number to hash an ssPI.

[232] See http://www.a-sit.at/signatur/rechtsrahmen/bgbl_e-gov-berabgrv.pdf

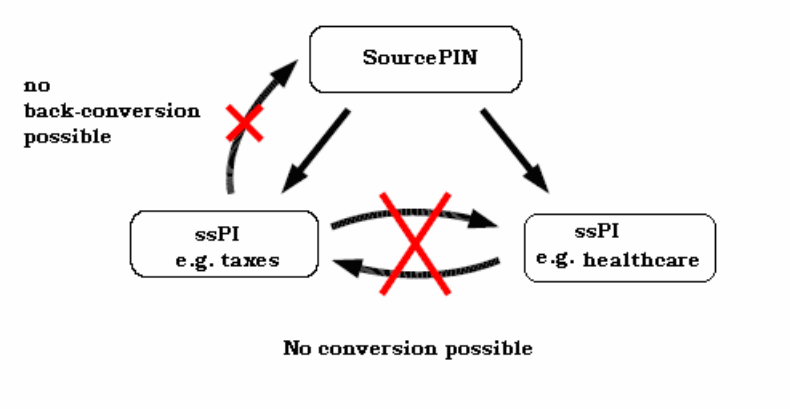

Figure 13: Conversion between Souce PIN and ssPI

3. In cases of inner-sector workflows the sector specific PI (ssPI) must be stored encrypted. In this case the ssPI can be used as symmetric key (see Figure 14).

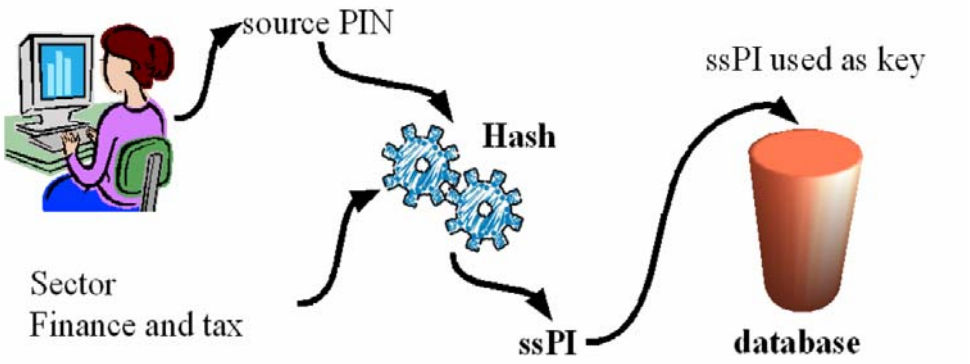

Figure 14: Use of the ssPI for secure data storage

Take up and Response

The "Bürgerkarte" today is mainly used in the public sector for identification and authentication purposes.[233] The most common examples are the request for an attestation concerning data from the criminal record or public registration data, tax declarations and electronic signing (G2G) and receiving (G2C) of official documents.

The concept of the "Bürgerkarte" has gained positive recognition concerning data protection in the public sector by civil right and other non-governmental organisations[234, 235].

[233] Some examples are documented in http://www.buergerkarte.at/de/Videoclips/index.html
[234] For example: http://ffs.or.at/Mitglieder/jack/stellungn_egovg.pdf
[235] A short survey via an internet search engine showed some criticism from 2004 and earlier only. Essential topics raised there do not take privacy and security features of the current implementation into account. Examples for this kind of criticism can be found at http://www.dergrossebruder.org/miniwahr/20040206000000.html or http://www.quintessenz.at/archiv/msg01349.html

Furthermore, in December 2005 the first prize for data protection in the category of European public authorities was awarded to Austria for the concept of the "Bürgerkarte" by the Data Protection Agency of the Community of Madrid.[236]

However some issues remain still open. In addition to the unlinkable ssPI, name and date of birth are used which are in most cases unique and thus create linkability. In case an electronic signature is needed for private or e-governmental transactions, linkability can be established via the single certificate stored on the "Bürgerkarte", as this concept does not include sector specific or pseudonymous certificates for electronic signatures.

From an economic perspective the number of issued digital signatures is still limited. Until end of 2005 only 56,000 electronic signatures (0.7% of the population of Austria) were issued.[237]

5.6 Belgian ID Card

Introduction

Due to new challenges, both on the side of electronic commerce and security, more and more countries decide to replace their paper-based identity cards by electronic ones. Belgium is currently the only European country that has decided to issue an electronic identity (eID) card to all its citizens aged 12 years or older. Estonia also has very extensive coverage; and Austria, Italy and Spain are also making good progress in deploying eID cards. Each of these countries has implemented their individual eID system. This chapter outlines some of the design issues and practical consequences of the Belgian eID card.

Card Description

Figure 15: Belgian eID card's visual aspects

The Belgian eID card is the size of a normal smart card, e.g., a bank card. The visual design (cf. Figure 15) is similar to the previous identity card and contains name (family name, up to two given names, and the initial of a third name), title, nationality, place and date of birth,

[236] http://www.austria.gv.at/DesktopDefault.aspx?TabID=4951&Alias=bka&infodate=19.12.2005 and http://www.ptapde.gr/news/PR_e-PRODAT_20051215.pdf
[237] See http://www.heise.de/newsticker/meldung/68944 and http://www.heise.de/newsticker/meldung/69316

gender, and a photo of its holder. Moreover, it contains a hand written signature of its holder and also of the civil servant who issued the card. It also mentions the validity dates of the card (the card is valid for five years), the card number, the national number of its holder, and the place of delivery of the card. All this information is also stored on the chip in a so-called "identity file." The identity file is around 200 bytes long, and is signed by the National Register (RRN). In addition to the identity file, there is also an address file (about 150 bytes). This file is kept independently as the address of its holder may change within the validity period of the card. The RRN signs the address file together with the identity file to guarantee the link between these two files. The corresponding signature is stored as the address file's signature. As biometric feature, Belgium decided to use a photo (3 kBytes, JPEG format). This photo is (indirectly) signed through the RRN, as its hash is part of the user's identity file.

The chip on the card can perform digital signatures and key generation. There are no concrete plans to integrate decryption functionalities in the eID card.

Roll-out

Initial Planning. On September 22, 2000, the Belgium council of ministers approved an eID card concept study. This study was a direct consequence of the publication of the European Directive, cf. [15], on electronic signatures. The contract to implement the system specified in the study was assigned in January 2002 to the private company NV Steria. In particular, it was decided to issue certificates for individual citizens, and to start with a pilot phase in 11 selected municipalities. In addition, it was decided *not* to integrate the social security card or the citizen's driving license with the newly developed national identity card because of incompatibilities with the Belgian legal framework. From a technical point of view, this integration would have been easy.

Pilot Phase. The pilot phase started in March 2003 by issuing the first 4 eID cards to civil servants. The contract to prepare and produce the first eID cards had been awarded to the private company NV Zetes. This company still takes care of the logistics (transport of the eID card request forms and of the eID cards), and of all the other practical issues: physical assembly of the eID card, printing of the front/back of the card, the electronic initialisation of the cards (key pair generation, initialisation of data files, etc.). All the eID card-related certificates are issued by the Certipost consortium, which is a joint venture of the Belgian Post Group and Belgium's largest telecommunications operator Belgacom.

The first municipality started issuing eID cards to its residents on May 9, 2003, the eleventh on July 25, 2003. An overview of the number of eID cards that have been produced, activated and revoked since the start of the pilot phase is available at[238].

During the pilot phase, a few technical difficulties were discovered and fixed. In particular, the holder's address was removed from the visual part of the card and is now only present in the chip.

Otherwise, it would have been necessary to re-issue cards as soon as holders change their address. For cost reasons, this option was discarded.

[238] Danny De Cock. Non-official information on the Belgian Electronic Personal Identification Card. https://www.cosic.esat.kuleuven.be/belpic/.

Nation-wide roll-out. The national roll-out started September 27, 2004. All citizens may now request an electronic identity card. All 589 Belgian municipalities are equipped to issue and process eID cards. Belgian citizen who wish to obtain their eID card, even before they are invited to do so, can initiate the eID card issuing process themselves.

By the end of 2009, the transition from paper based identity cards to electronic identity cards will be completed. Moreover, by that time, all non-Belgium residents who stay for more than 5 years in the country will also be issued an eID card. For cost reasons, non-Belgium residents who stay a shorter period of time (typically one year), will *not* be issued an eID card but a paper based version.

Cryptographic Details

In total, a Belgian eID card holds *three* different 1024-bit RSA private signing keys: one to authenticate the citizen, one for non-repudiation signatures, and one to identify the card itself towards the Belgian government. The eID card is able to compute digital signatures with all three private keys. For the citizen's authentication key and non-repudiation signature key, this is only done after the card holder entered a PIN. This PIN must be entered by the citizen, preferably using some trusted hardware, e.g., a smart card reader with stand-alone key pad.

Each of the first two key pairs is accompanied by a certificate. These certificates are issued to the citizen: one authentication certificate for use in client authentication, e.g., with SSL/TLS. The second certificate is a qualified certificate that binds the non-repudiation key to the card holder and that can be used to produce electronic signatures that are equivalent with handwritten signatures. Neither of these certificates contains an email address of the citizen. The private key of the card's third key pair is used when the card communicates with the National Register (RRN) for mutual authentication, e.g., to update the card holder's details (typically the address), the national certificates, etc. The RRN keeps in its databases a copy of the public key to verify the signatures calculated with this third key.

It is the smart card initialiser that starts the key pair generations during the initialisation phase of the eID card. The smart cards are produced by Infineon (chip type SLE66CX322P) and are equipped with the JavaCard operating system of Axalto. The cards use their on-board hardware random number generator to seed the key pair generation function of the card. The private part of the key pair never leaves the card. The public exponent of the 1024-bit RSA key pair has a fixed value and equals 65537.

The smart card in itself is not able to calculate the cryptographic hash value on which it produces a digital signature: an eID card digitally signs the 16 or 20 bytes that it receives from an external application. The card is instructed during the initialisation of the signing session to expect 16 or 20 bytes, depending on the padding type (MD5withRSA or SHA1withRSA) that it needs to apply before calculating the actual signature. It is impossible to have the card calculate a signature on other information than these 16 or 20 bytes.

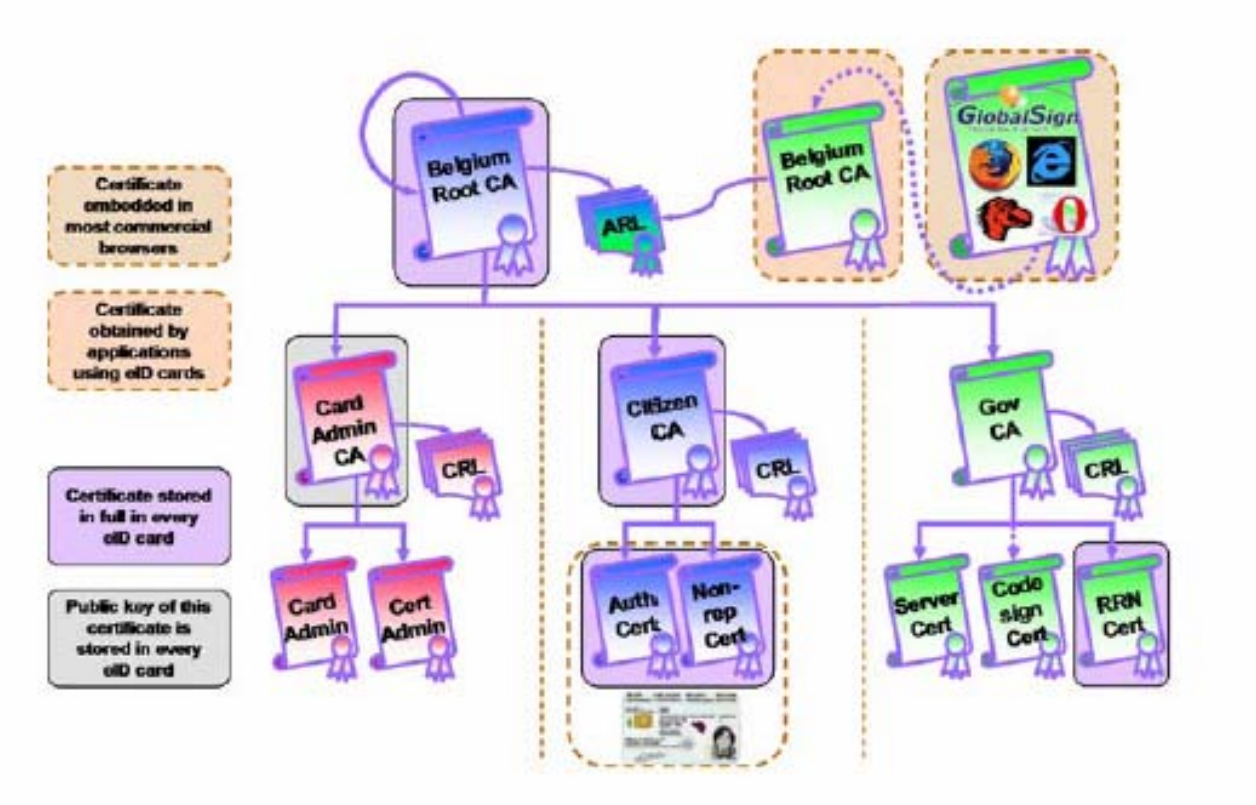

Figure 16: Belpic eID CA structure

The card also holds, in addition to the two card holder certificates, three government-specific certificates: the Belgium Root CA certificate, the Citizen CA certificate, and the National Register (RRN) certificate. The overall certificate hierarchy is summarised in Figure 16.

The Belgium government decided to use a 2048-bit RSA key for its CA certificates. Certificates for individual users (e.g., card holders, servers) and for the RRN include 1024-bit public keys. It was decided to issue 1024-bit RSA key pairs for use by the citizens during the first phase of the national roll-out. In the second part of the national roll-out, a gradual migration to 2048-bit moduli is envisaged.

Figure 16 shows that the Root CA certifies other CA certificates, e.g., for the card administration and government-specific servers. The key pair used for the Self-signed Belgium Root CA certificate has also been certified by the commercial certification authority GlobalSign so that the certificate chain of, e.g., a citizen certificate → Citizen CA certificate → Belgian Root CA, can be validated by mainstream applications (email clients, browsers, etc.). The Citizen CA issues the two citizen certificates.

Carrying an identity card is a legal obligation in Belgium. Hence, the loss of such a card has to be reported swiftly, after which the corresponding certificate is suspended for up to 7 days. If the citizen finds his/her eID card back before this 7-days period ends, then the card can be unsuspended. In the other case, the card becomes irreversibly revoked.

Each CA implements this functionality by issuing, next to certificates, also certificate revocation lists (CRLs) in which it enumerates all the certificates that have not yet been activated by the citizen (i.e., if the eID card has not yet been delivered to the citizen), that

have been suspended (e.g., if the citizen lost his/her eID card), or that have been revoked (e.g., if a citizen's eID card has been stolen).

All the CRLs that have been issued in the last year can be accessed through the Internet (CRLs that are older than one year can also be accessed, but this is not an online service). So far, no certification authorities have been revoked with the Authority Revocation Lists (ARLs). At present (November 2005), the overall revocation list has a size of 36 MB. To facilitate the handling of revoked keys, the CA provides delta CRLs, issued every three hours. Hence, individuals or organisations who wish to update their database with certificate status information only need to download these delta CRLs.

Usually, they have a size of much less than 100 kBytes. To reduce the total size of an individual CRL, the CA has also started, since the beginning of 2005, to keep thirteen active CRLs. It issues certificates that point to a particular CRL in a Round-Robin scheme: the certificates issued for a batch of eID cards refer to one of the active CRL, the next batch to another active CRL, etc.

As each eID card has been initialised with a genuine copy of the Belgian Root CA certificate, the card can be used as a "trusted source": each user can verify the chain of trust within the Belgian PKI system by loading the Belgium Root CA certificate from her/his smart card. Hence, the whole eID project can be seen as a nation-wide PKI – with strong user authentication during the issuing phase, as each citizen has to present her/himself at the municipality.

Apart from revoking the use of an eID card's keys when it is stolen, card holders also have the possibility to have the electronic signature capability of an eID card revoked, even before using a card ("opt-out"). This way, the card holder expresses that she/he is not interested in using the signature or authentication features of the card.

Comments

During the pilot phase, only very few (cryptographic) problems had to be fine-tuned, such as using RSA signatures by PKCS#1v2.1 instead of PKCS#1v1.5. Hence, from a technical point of view, the Belgian eID card relies on a sound architecture. For example, having two different private keys for each citizen prevents specific types of attacks, e.g., by asking to authenticate a "random number" during a session which could in fact result in a digital signature on a contract.

From a practical perspective, the lack of smart card readers installed in home computers performs a serious obstacle for the wider use of the eID card. However, by promoting government applications such as "tax on web", registered mail, social security registration of new personnel, online consultation of government data, together with the distribution to twelve-year olds of a free smart card reader when they get their eID card, the home penetration with readers is expected to increase in the short term.

As soon as it is high enough, we also expect an increasing interest by companies using the eID card as a mean of authenticating their customers and entering legally binding electronic contracts with them.

The main concern with the Belgium eID card is privacy: a Belgian eID card can be used in citizen-citizen, citizen-business, and citizen-government communications. Currently, no privacy enhancing technologies have been implemented with the eID card. While technically

possible, this has not yet been included in the specifications of the eID card. These improvements are expected in a later revision of the eID card system.

5.7 German E-Health Card[239]

Coordinated by the Federal Ministry of Social Affairs and Health the introduction of an e-health card[240] in Germany is planned for 2006. In eight so-called "Modellregionen"[241] pilot implementations and prototypes of the e-health card are being tested until end of 2005. In 2005 it was decided to have a second, extended testing phase in 2006 within the same "Modellregionen".[242] The project of the "Modellregion" in the Federal Land of Schleswig-Holstein is called "Gesundheitskarte Schleswig-Holstein"[243].

The project "Gesundheitskarte Schleswig-Holstein" currently is the farthest developed "Modellregion" within the pilot phase of the e-health card in Germany. Main target of the project is the digital support of already established processes in the health sector which are mainly done on paper today. Important examples are:

- Identification of a patient as insurant of the public health system at the office of a medical doctor or in hospital (today already supported by a chip card)
- Transfer of information which is stored on paper today such as allergy data, permanent medications, blood type and immunisation certificates if needed by the medical doctor
- Referral to other medical doctors
- Prescriptions and purchase of medicine at a pharmacy

Access to emergency data currently is impossible even in cases when they are needed by a medical professional. The introduction of emergency data on the e-health card is a functional enhancement compared to the situation in Germany today.

The storage of data from the medical doctor's file on patient data (such as history of visits, diagnoses etc.) on the card is not planned. In addition the card is not integrated in the invoice procedures of the medical doctor to the insurance companies; these procedures are mainly electronic today and remain unchanged.

Apart from the authentication and the emergency data all the data stored on the card is encrypted and secured by a PIN under control of the user. The user has unrestricted reading

---

[239] This chapter bases on the Backhouse, J. (Ed.), *FIDIS Deliverable D4.2: Set of requirements for interoperability of Identity Management Systems* Frankfurt a.M. 2005, pp. 106-108. The corresponding description of the project was modified with respect to the good-practice elements of the project and to current developments in the status of the project.

[240] See http://www.staat-modern.de/Buerokratieabbau/Projekte-im-Ueberblick-,11922.553645/Elektronische-Gesundheitskarte.htm?global.back=/Buerokratieabbau/-%2c11922%2c3/Projekte-im-Ueberblick.htm%3flink%3dsmo_liste%26link.orderby%3ddatum%26link.orderdir%3ddesc

[241] See http://www.telematik-modellregionen.de/content/index_ger.html

[242] See http://www.bmgs.bund.de/cln_041/nn_600110/DE/Presse/Pressemitteilungen/Presse-BMG-1-2006/pm-3-1-06,param=.html

[243] See http://www.gesundheitskarte-sh.de/

access to all the data stored on his card (e.g. by using an own card reader or a public terminal). If used to transfer data such as referrals or prescriptions, a health professional card is needed to access the data on the e-health card of the patient. Such health professional cards are held by medical doctors and pharmacists. The health professional card is equipped with an electronic signature to sign, e.g., prescriptions. Emergency data on the e-health card is encrypted, but may be accessed by taking a health professional card without needing the PIN of the e-health card holder.

An abstracted view on the data stored on the e-health card is shown in Figure 17. In addition to the storage on the card in some cases the data are stored in a post box on a central server. This post box essentially is a transfer directory from which the data can be received and processed by the corresponding recipients (e.g. medical doctors or pharmacists). The concept to store information concerning organ donation and maternity for a longer period is not finally decided yet.

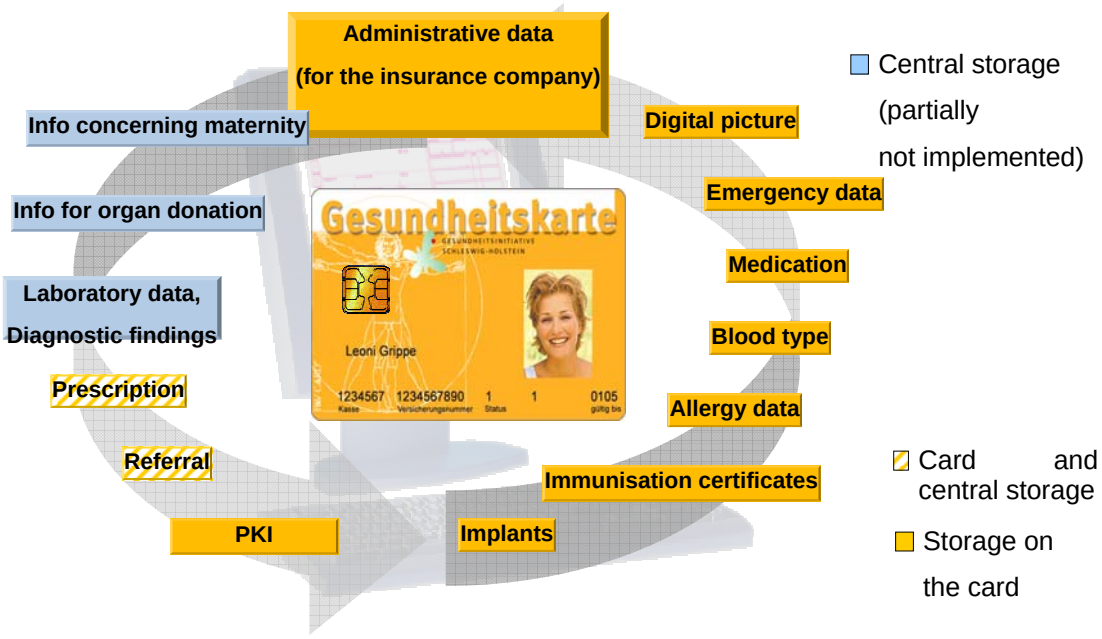

Figure 17: Concept of the storage of data in the German e-health card

Currently more than 1,000 e-health cards are issued within the pilot project. It is planned to extend the number up to 10,000 within 2006. Currently numerous medical doctors organised in the “Gesundheitsnetzwerk Flensburg”, numerous pharmacies, two hospitals in Flensburg and a number of partners from industry are integrated into this project. The server structure and a secured network for data transfer purposes is available, together with PKI infrastructure and interfaces for a number of software systems used by medical doctors, pharmacies, and hospitals. The introduction of the “Gesundheitskarte” is planned for 2007.

In this project a number of positive factors can be observed, that will likely result in a broad success of this project. Among them are:

- Focussing of the concept on existing workflows and broadly accepted procedures
- Decentralised storage of data on the card under the control of the user where ever possible
- Intensive technical field testing in two phases and eight "Modellregionen" and laboratory testing (so called "Hacker Tests")
- Integration of responsible Privacy Commissioners on a central and local level; for example the "Gesundheitskarte Schleswig-Holstein" is observed by the Privacy Commissioner of the Federal Land of Schleswig-Holstein.

5.8 Alternate Implementations and Ongoing Research

5.8.1 Laser Band Technology in the Italian eID Card

In difference to other European eIDs the Italian eID card (carta d'identità elettronica (CIE)) uses a so called laser band. The laser band is a laser optical engraved zone on which up to 1.8 MByte of data can be stored. This makes the laser band technology superior to smart chips or RFID that have less storage capacity today (up to 64 kBytes of data). The problem of this technology is that a proprietary reader infrastructure is needed; only Italy is issuing such an infrastructure so far. For the most European countries the laser band and the data stored there is not be usable and will not be usable in future.[198]

5.8.2 Principles for eIDs and Suggestions for Advanced eID Concepts

After having read the Report of the LSE Identity Project[244]**Fehler! Textmarke nicht definiert.**, Niels Bjergstrom developed criteria for the design of eID systems which will be mentioned briefly in this section.[245] He proposes the following as some necessary criteria (yet not comprehensive):

The Root Identity of a person in the digital world should be an irrefutable electronically readable document with the following properties:

- It must present an irrefutable link between its user and itself.
- It must be able to participate in authorisation procedures without leaking any identity information ("Is this individual allowed to do this in this context?").
- It should be able to facilitate authentication processes without compromising identity – allowing anonymity or pseudonymity most of the time is a fundamental requirement of any eID system in a free society.

[244] See http://csrc.lse.ac.uk/IDcard/identityreport.pdf
[245] Niels Bjergstrom: Editorial of Information Security Bulletin Oct. 2005; http://www.chi-publishing.com/samples/ISB1008Editorial.pdf

- It should be able to uniquely represent (exactly) the legitimate holder in public key cryptographic protocols.
- It should be able to participate in identification processes if identification is required and legitimate.
- It must not depend on irreplaceable personal characteristics to cope with the problem of compromised or lost/changed characteristics.
- The token containing the eID must be replaceable without unwanted consequences, i.e. theft or loss of a token must not enable impersonation.
- All its functions, including any disclosure of information in the token, must be fully controlled by the owner.

Niels Bjergstrom (Bjergstrom 2005) proposes an approach where the linkage between eID and user is performed by DNA which thereby is the basis of eIDs without leaking information or compromising personal details. In any case he sees the necessity for a system which is as decentralised as possible, building on information inside the eID token.

5.8.3 Server Derived IDs

Within the project "Provide eGovernment Good Practice Portability" (PPP) the eforum has constituted[246]. Within this eforum stakeholders of eIDs from the public and the private sector analyse good practice and try to transfer knowledge. A working group within the eforum currently is working on privacy enhancing concepts for authentication of citizen that is able to use existing PKI. Basing on the concept of reverse proxies and on user's certificates from cards for electronic signatures sector specific personal identifiers similar to the Austrian ssPIs are generate by trusted third parties (identity management providers). It is planned to use technical elements of the Austrian solution for example the modification of identifiers by hashing data from certificates with sector data. In difference to the Austrian ssPIs this solution can be used with already established PKI and signature solutions by adding identity management providers. The use of specially coded citizen cards and additional client side software does not seem to be necessary. In addition the use of X.509 compliant certificates is planned to establish compatibility with security standards such as SSL/TLS V1.0.

Within this year the publication of a concept and a pilot implementation are planned.

5.9 Summary and Conclusions

In this chapter an overview on existing concepts and implementations of eIDs is given. Most European countries plan to implement eIDs or have done this already. In addition the European passport is issued in some European countries since November 2005; by August 2006 most European countries plan the introduction of the new passport.

Within this chapter five eID projects were described and analysed with respect to take up and response of the users. These projects are:

[246] See http://www.eu-forum.org/article.php3?id_article=258

- The European passport (large project with the application of new technologies in eIDs)
- The FINEID (established since 1997; this is the oldest eID in Europe)
- The Austrian "Bürgerkarte" (privacy preserving use of sector specific personal identifiers (ssPI))
- The Belgian ID card (high numbers of issued electronic signatures in Belgium)
- The German "Gesundheitskarte" (example for a specialised eID solution in the e-health sector and good practice for the project planning and implementation)

In addition innovative technological concepts were described. This includes:

- The laser band technology used in the Italian eID (CIE)
- Principles for eIDs developed by Niels Bjergstrom
- Server derived IDs as a privacy enhancement basing on established electronic signatures and compliant to existing PKI

From the analysis of the investigated projects obvious factors of success concerning the introduction of eIDs can be concluded. They are:

- Careful planning especially concerning the purpose of the eID and the appropriate technical solution (keep it small and smart); this should include technical, formal and informal aspects of interoperability
- Intensive laboratory and field testing of prototypes
- Refinement of the concepts using the results of the testing phase
- Open communication within the project including all stakeholders of the eID and external experts
- Appropriate education and qualification of the personal involved in the project

6 Security and Privacy Aspects

6.1 Introduction

To describe threats that have to be taken into account when discussing security and privacy of ID documents a short and non-comprehensive overview on threats already being discussed in academic and non-academic communities is given. Basing on that overview in this chapter security and privacy aspects of four basic technologies used in ID documents are presented and discussed. This includes:

- Biometrics
- RFID
- Chip card technology
- Electronic signatures and PKI

Back-office systems are not part of this chapter, as an analysis of security and privacy issues of these systems clearly would exceed the scope of the FIDIS Network of Excellence.

Biometrics and RFID are technologies that have not been used in ID documents until recent times. In these cases the legal requirements for privacy and security are described and analysed in addition to a technical view. The reason is that the introduction of these technologies for the use in ID documents in Europe is politically very much driven by specific European Regulations and related documents. This chapter concludes with a summary and gives recommendations which users, policy makers and technicians should take into account when using current or developing future ID documents.

6.2 General Threats

A number of different threats to security and privacy of ID documents and related systems have already been discussed in academic and non-academic communities. Some of them are very obvious and lead to a increasing use of technical components in ID documents in all European countries in the last 10 years. These are for example: [247]

- Theft of ID documents and the correlated (partial) identities
- Copying or cloning of ID documents basing on existing identities (identity theft) or totally faked and non-existing identities (identity creation)
- Modification of (lost or stolen) ID documents for example to make the identifiers fit to a different person or to change attributes such as date of validity or name of birth

[247] See for example http://www.wdr.de/online/news2/ausweis_sicher/index.phtml

These threats have a limited impact in cases where ID documents are used for a limited number of specified purposes. Traditionally ID documents were used to authenticate a citizen against public authorities of his home or a foreign country. In cases a document gets lost or stolen, this information can be entered in a database for stolen ID documents easily. Within an authentication procedure ID documents can easily be checked against that database by public authorities. In case of a match appropriate measures can be taken.

MRTDs are deploying technologies that are used in different environments and systems as well. This is especially true for biometrics such as fingerprinting. Storage of raw data (photos) of fingerprints and templates are options for future MRTDs. Fingerprints are also used in a forensic context (crime investigation etc.) or as an access solution for buildings, rooms or IT systems. This raises a number of scenarios where biometric data from ID documents could be abused in the context of other biometric systems, for example via spoofing of sensors or manipulating back-office systems such as reference databases. Security (for example access control) of ID document systems and the format in which biometric data is stored in ID documents thus has an impact on the security or the performance of other biometric systems using the same biometric methods or features. This is especially the case where we have unobserved sensors with limited capability of liveness detection. From the perspective of the owner of the passport this kind of abuse of biometric data may result in identity theft.

In difference to traditional ID documents European passports as a prototype of current MRTDs are remotely and non-interactively (from the perspective of the bearer of the passport) readable through a distance from 2 to 10 m, when the access control can be circumvented or hacked. This creates the risk of ubiquitous, unobserved authentication by authorised or unauthorised third parties, when carrying a MRTD equipped with RFID. This enables tracking of people carrying a passport, for example when staying as tourist in a foreign country. Even the abuse of this kind of non-interactive authentication for smart bombs has already been discussed (see chapter 6.3.2).

In addition to traditional and well understood scenarios to abuse ID documents new MRTDs offer numerous additional threats. In particular they base on scenarios for remote and unobserved authentication of bearers of MRTDs and the use of biometric data stored on ID documents for additional purposes in the public and private sector.

6.3 Biometrics

6.3.1 The Legal and Procedural Perspective

The idea to use biometrics to secure ID documents is fairly recent**.** Nevertheless, after mid 2006, the inclusion of biometrics is mandatory for the EU Member States when issuing new passports to their citizens[17]**.** Based on US policy and enhanced international security requirements at borders**,** and the decisions taken on the EU level to increase and harmonise the security features of travel documents, national initiatives have emerged to include biometrics in national ID documents as well. Some EU countries (e.g., Italy) have initiated pilots to test the inclusion of biometrics in national ID documents[248]. Few countries, however,

[248] See also, for a useful overview of the implementation of biometrics in the EU, Bacque, E., 'Overviews. Biometric Implementations in European Union Member States' for the European Biometrics Portal, 29 September 2005, and 'A Hyperlinked Listing of Other Documents available at the EBP website as of November

actually employ biometrics in national ID documents. One of the few countries in the world that have and use national ID card which include biometrics is Malaysia.

Generally, the purpose of the use of biometrics in ID documents is to enhance the authenticity of the documents and to secure the use thereof. In other words, the inclusion of biometrics is aimed, on one hand to make it more difficult to counterfeit the documents, and on the other hand to provide additional means to verify and authenticate that the user of the ID document is the owner to whom the ID document has been issued (to counter the look-alike fraud, often incurred if ID documents are only secured by a (digital) picture of the owner). However, it remains possible that biometrics collected for the issuance of the new generation ID documents are also used for other purposes, sometimes without knowledge of the individuals involved. This is the fear of human rights organisations in the debate about the use of biometric data (e.g., use for face recognition surveillance, etc).

The processing of biometric data for ID documents by the public authorities is subject to the national general data protection legislation (implementing the Privacy Directive 95/46/EC). The requirements under the data protection legislation have to be respected by the controller(s) (for example, the government agency and responsible minister for the ID scheme) and the processors. These general data protection principles which apply are not analysed in this report. Reference is made to Deliverable 3.2 of FIDIS (p.101 et seq.)

In this section, we will briefly describe some of the 'procedural' security and privacy aspects of biometrics in ID documents which are important. The description, however, is not exhaustive. With 'procedural' security and privacy aspects, we mean some overall requirements which are important for the protection of biometrics in the procedure of the issuance, the operation and the use of ID documents. Some of these aspects relate to the use of biometrics whether stored locally, or stored centrally, and are relevant for biometrics in ID documents in general. These aspects are described based on the research done in the IST-2002-001766 BioSec (Biometrics and Security) project[249] (BioSec project). Other aspects have been described or are required in legislation or standards and have sometimes been commented by the Article 29 Data Protection Working Party (WP 29). The security and privacy aspects which are inherent to the characteristics of biometrics in general, e.g., uniqueness, possibility that sensitive information is included, FAR, FFR, and so on will be discussed in the section below (see chapter 6.3.2).

Importance of the enrolment and issuance procedure

It is clear that one of the most basic and essential security and privacy requirement for biometric ID documents is the reliability and security of the enrolment and issuance of the documents to the right person. The enrolment process for biometric ID documents is not standardised and not subject to specific requirements. The basic principle, however, is that upon enrolment all information to be provided by the applicant (in particular the information relating to the identity and the biometric information) shall be rigorously checked. How this is done, is sometimes not disclosed, as publishing such information could obviously have a

22, 2005' assembled by Biometric Bits. The Key to Identity Management Information, Impress, 2005, at http://www.europeanbiometrics.info/images/resources/93_338_file.pdf

[249] See http://www.biosec.org/

negative effect.[250] During subsequent identity checks based on submission of ID documents, it is important to realise that biometrics are not the only means or solution to check or verify that the user of the ID document is the rightful owner. Additional checks with information which are not stored on the ID document could prove to be very valuable.[251]

Technological, data communication and architectural and procedural security aspects of biometric systems

When using biometrics to enhance and secure eIDs, it is essential that one is aware of the multiple vulnerabilities and possible attacks to the various components of a biometric system. Attacks on the technological level include spoofing (creating artefacts from traces left by e.g., fingerprints on objects, to access the system), the installation of specific program code on a component of a biometric system by an attacker, use of unpredictable conditions such as power fluctuations and noise in order to obtain unpredictable system behaviour, power and timing analysis for breaking software code (including cryptographic algorithms and matching mechanisms), use of the residual biometric characteristics on sensor (e.g., fingerprint) to access the system, exploitation of similar templates to deceive the system, and even brute force. For each of these problems, appropriate security measures need to be taken[252]. These security features could include aliveness detection and multimodality, both researched in the BioSec project.

On the data communication level, the attacks could be directed towards many communication points, as shown in the figure below:

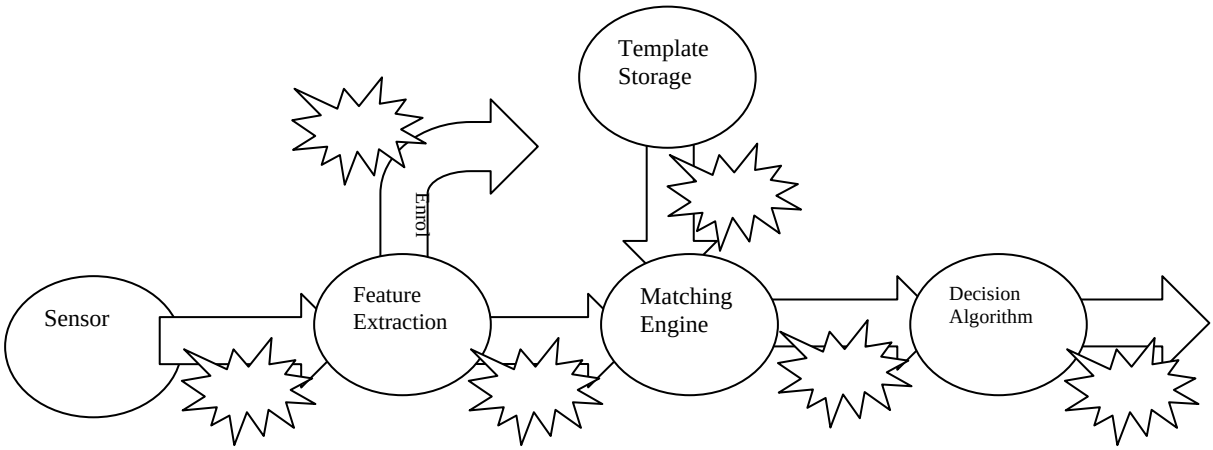

Figure 18: Possible attacks on the communication points of biometric systems[253]

[250] See Lettice, L., '"RFID the lot of them". UK ID card to use ICAO reader standard', *The Register,* 25 July, 2005, at http://www.theregister.co.uk/2005/07/25/id_card_goes_icao/page2.html (last visited on 7 February 2006).

[251] See Grijpink, J., 'ICT als strategische uitdaging', 30 September 2005, Nederlands Biometrie forum, available on http://www.biometrieforum.nl/bio/contents.php?cid=86 (last visited on 14 February 2006).

[252] A very useful and complete description of these and the other vulnerabilities which have been identified see Dimitiadis, CH. K., 'Security recommendations : biometric systems integration, basic research on security, network protocols and PKI', deliverable 3.3 of the BioSec project, see http://www.biosec.org/.

[253] Figure based on ibid, p. 13.

The attacks can be directed towards the biometric data and templates and include capture/replay attacks, whereby biometric signals are captured and replayed, TCP hijacking, man in the middle attacks, whereby the attacker places himself between two communication elements, digital spoofing, whereby a digital pattern that mimics a real one is maliciously injected, use of digital residual data by e.g., memory exploitation, hill-climbing attacks and denial of service. Specific security measures are needed to counter these attacks[254]. It is clear that each of these attacks not only endanger the privacy of the owners of the biometric data, but the operation of the biometric system as such. Finally, security considerations at an architectural and procedural level remain also important and appropriate remedies shall be taken. In general, a security policy should be customised to the specific characteristics of the biometric authentication system. For the management of biometric data, it is noteworthy that there is a standard, ANSI X9.84 (Biometric Information Management and Security) that can be used as a minimum guideline for formulating some of the security requirements. Additional standards relevant for biometrics and which are being developed in ISO/IEC JTC 1, in particular in the subcommittees 27 (security) and 37 (biometrics) should also be followed up[255]. In general, the security policy could be based on the ISO 17799 standard.

The importance of the authentication protocol

If biometric data are to be sent over public networks, such as internet, the importance of a protocol that secures the confidentiality and integrity of the biometric information during the remote authentication process is of utmost importance. Therefore, it is necessary that a protocol which fits the biometric requirements, is chosen. Some of the possible protocols have been examined in the BioSec project, including a biometric Extensible Authentication Protocol (EAP), both in a centralised and decentralised scenario[256].

Need for a security architecture set out in a so-called 'Protection Profile' (PP)

The implementation and use of biometrics in a chip is vulnerable to many security attacks. For this reason, it is essential that all security challenges are addressed in a way which guarantees a secure exchange. WP 29 has stressed the need to create a so-called 'Protection Profile' according to the Common Criteria for Information Technology Security Evaluation[257], which needs to be elaborated by experts, including experts which are fully aware of the privacy problems (Article 29 Data Protection Working Party 2005c, 10). Such PP should also address the characteristics and vulnerabilities of a Public Key Infrastructure which in many cases is the framework for the operation of ID documents. WP 29 further states that this PP should be part of the work to be done by the Committee set up by Article 5 of the Regulation 2252/2004.

---

[254] See also the description in Deliverable 3.2 of FIDIS.
[255] See Dimitriadis, C. K., 'Security recommendations : biometric systems integration, basic research on security, network protocols and PKI', deliverable 3.3 of the BioSec project, see http://www.biosec.org/.
[256] Dimitriadis, C. K., Picco-Marchetti Prado, R., 'Guidelines for biometric-enabled secure access protocols and protocols for secure remote biometric authentication', deliverable 3.4 of the BioSec project, see http://www.biosec.org/.
[257] For an overview, see http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2.

Basic Access Control and Extended Access Control

Basic Access Control (BAC) is a security feature which is aimed at preventing that the data and the biometric data in particular (i.e., the digitalised facial image) which is stored in the (RFID) chip in the ID document can be accessed without knowledge of the owner of the ID document. The reader therefore has to authenticate itself. The way this is done is by an access key built from the machine readable zone (MRZ) of the passport, and which is calculated from the number of the passport, the data of birth and the date of expiry. BAC is a recommendation of the International Civil Aviation Organisation (ICAO)[258] and has been imposed upon the EU member states for the issuance of passports. The problem, however, is that the data of the MRZ are not secret and that the risk exists that the algorithm for the key for access to the data stored on the chip will soon become in the public domain[259]. As pointed out by the WP 29, BAC is therefore a not sufficiently secure access protocol (Article 29 Data Protection Working Party 2005c, 10). For fingerprints and any other additional biometric features, Member States shall define and implement Extended Access Control.[260] Details about this feature, however, have to be further clarified.

Register with details about use and access by authorised authorities

In order to have a view on who has got access to the data stored and when, the European Parliament has stated the request that Member States keep a register of the competent and authorised bodies referred to in Article 2 § 1a of Regulation 2252/2004[261]. Purpose of this register would be to guarantee that only competent authorities have access to the (biometric) data stored. Whether such register will be efficient to limit access to a small number of authorised authorities based on a justified need to know is unsure.

---

[258] ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, version 1.1, published 1 October 2004, p. 17.

[259] See also in the Netherlands, where the public authority, responsible for the issuance of the new passports, admits, to allegations in the press, that there is possibly a security problem with the BAC. An external company alleges since mid 2005 that it can decrypt the personal data contained in the chip. ICAO has been informed thereof by the Dutch public authorities, and this will be followed up. See http://www.minbzk.nl/persoonsgegevens_en/reisdocumenten/nieuwsberichten/feiten_nederlands

[260] ICAO Technical Report : PKI for Machine Readable Travel Documents offering ICC Read-Only Access, version 1.1, published 1 October 2004, p.17, 21 and 22.

[261] European Parliament legislative resolution of 2 December 2004 on the proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)), available at http://www.europarl.eu.int/omk/sipade3?PUBREF=-//EP//TEXT+TA+P6-TA-2004-0073+0+DOC+XML+V0//EN&LEVEL=2&NAV=X

Local storage – match-on-card versus match-of-card

It becomes generally accepted that the risks for abuse of biometric data considerably lower if the biometric data are stored locally, this is on the object under the control of the user. For ID-documents, this means that the building of central databases is avoided and that the biometric information is only stored in the ID document itself. If the biometric data are stored locally, the data shall be stored in a secure way. In practice, this means storage of the biometric data in an encrypted way. This is, however, not sufficient. Upon verification, there remains a considerable privacy and security risk if the (encrypted) data stored on the card leave the card for the matching process (match-off-card). This is necessary because the card lacks an end-user interface and the user has to use the interface provided by a terminal which may not always be trustworthy. The matching is hence in an open environment, vulnerable for attacks and abuse (see also above). During the communication between the card and the card reader, the biometric information could be stolen or changed. Therefore, storage on the local device contains only limited privacy and security advantages, unless the matching process between the biometric credentials submitted and the ones stored, takes place on the card or subject under control of the user itself (match-on-card/match-on-token). In that way, the biometric information never leaves the token or card, which is a closed and more secure environment, than the communication in the open matching environment. Match-on-token as an enhancement of the privacy and security risks has been further researched and demonstrated in JavaCard first prototypes in BioSec project for fingerprint and iris as an enhanced security solution to privacy threats. It might be possible to employ this approach to be further researched and enhanced in ID documents as well, enabling a biometric-on-card verification. This technology could then possibly overcome the critics related to the BAC (see above). Presently, however, there remain for this technology hurdles to overcome, such as the required power consumption which is not compatible with power supply.[262]

Restriction to verification

In conformity with the proportionality principle of the data protection legislation, WP 29 states in its abovementioned opinion that the use of biometrics in ID documents should be technically restricted for verification purposes, whereby the data contained in the document is only compared with the biometric data provided by the holder upon presenting the ID document.

Distinction between biometric data used for ID documents and biometric data for contractual purposes

Finally, WP 29 states that a distinction should be made between the processing of biometric data for ID document purposes, (e.g., for border control), and for which a legal basis is enacted, and the processing of biometric data obtained on the basis of consent, e.g., for contractual purposes (Article 29 Data Protection Working Party 2005c, 11).

[262] See also presentation of Stephan Beinlich, Giesecke & Devrient, 4th BioSec workshop, Brussels, 29 November 2005, at http://www.biosec.org/

6.3.2 The Technical Perspective

Biometrics both has and causes security problems that are investigated in the following.

6.3.2.1 Security Problems of Biometrics

As with all decision problems, with biometric authentication/identification, two kinds of failures occur:

- Persons are wrongly not authenticated or wrongly not identified.
- Persons are wrongly authenticated or wrongly identified.

This leads to the dilemma of (biometric) pattern recognition (Jain, Hong, Pankanti 2000): If the similarity test is strict, people will be wrongly accepted or identified only rarely – but wrong non-acceptance and non-identification will happen more often. If the similarity test is less strict, people will be not accepted or not identified only rarely – but wrong acceptance and wrong identification will happen more often.

Practical experience has shown that only the frequency of one error type can be kept small – and the price to be paid for that is that the frequency of the other error type increases.

A biometric technique is more secure for a certain application area than another biometric technique if both error types occur more rarely. It is possible to slightly adapt the strictness of similarity tests used in biometrics to various application areas. But if only one of the two error rates should be minimised to a level that can be provided by well managed authentication and identification systems that are based on people's knowledge (e.g., passphrase) or possession (e.g., chip card) today's biometric techniques can only provide an unacceptably high error rate for the other error rate.

Since more than two decades we hear announcements that biometric research will change this within two years or within four years at the latest. In the meantime one might begin to doubt whether such a biometric technique exists, if the additional features promised by advocates of biometrics shall be provided as well:

- user-friendliness, which limits the quality of data available to pattern recognition and
- acceptable costs despite possible attackers who profit from technical progress as well (see below).

In addition to this decision problem being an inherent security problem of biometrics, the implementation of biometric authentication/identification has to make sure the biometric data come from the person at the time of verification and are neither replayed in time nor relayed in space (Schneier 1999). This may be more difficult than it sounds, but it is a common problem of all authentication/identification mechanisms.

6.3.2.2 Security Aspects of Biometrics

Biometrics does not only have the security problems sketched above, but biometrics' use also causes security problems. Examples are given in the following.

- Devaluation of classic forensic techniques: Widespread use of biometrics can devaluate classic forensic techniques as sketched for the example of fingerprints as a means to trace people and provide evidence:
    - Databases of fingerprints (especially biometric raw data) essentially ease the fabrication of finger replicas and thus leaving someone else's fingerprints at the site of crime.
    - If biometrics employing fingerprints is used to secure huge values, quite probably, an "industry" fabricating replicas of fingers will arise.
    - As infrastructures, e.g. for border control, cannot be upgraded as fast as single machines (in the hands of the attackers) to fabricate replicas of fingers, a loss of security is to be expected overall.
- Chopping off and taking away of body parts (Safety problem of biometrics): In the press you could read that one finger of the driver of an S-class Mercedes has been cut off to steal his car. Whether this story is true or not, it does exemplify a problem we might call the safety problem of biometrics when using unobserved sensors:
    - Even a temporary (or only assumed) improvement of "security" by biometrics is not necessarily an advance, but endangers physical integrity of persons.
    - If checking that the body part measured biometrically is still alive really works, kidnapping and blackmailing will replace the stealing of body parts.
- Wanted multiple identities could be uncovered as well: The naive dream of politicians dealing with public safety to recognise or even identify people by biometrics non-ambiguously will become a nightmare if we do not completely ignore that in our societies accepted and often useful multiple identities for agents of secret services, undercover agents and persons in witness-protection programs do and have to exist. The effects of a widespread use of biometrics would be:
    - To help uncover agents of secret services, each country will set up person-related biometric databases at least for all "foreign" citizens.
    - To help uncover undercover agents and persons in witness-protection programs, in particular organised crime will set up person-related biometric databases.

These problems gain even more importance by the fact that biometrics in the European Passport are not implemented in a revocable way. As a consequence a lost or stolen passport can be accessed and used together with spoofs for biometrics in an unauthorised way for a long time (up to 10 years).

6.3.2.3 Privacy Problems caused by Biometrics

Biometrics is not only causing security problems, but privacy problems as well:

- Each biometric measurement contains potentially sensitive personal data, e.g. a retina scan reveals information on consumption of alcohol during the last two days, and it is under discussion, whether fingerprints reveal data on homosexuality (Forastieri 2002), (Hall, Kimura 1997).
- Some biometric measurements might take place (passive biometrics) without the data subject getting to know of it, e.g. (shape of) face recognition.

In practice, the security problems of biometrics will exacerbate their privacy problems: Employing several kinds of biometrics in parallel to cope with the insecurity of each single kind, multiplies the privacy problems (cf. mosaic theory of data protection[263]). Please take note of the principle that data protection by erasing personal data does not work on the Internet, since it is necessary to erase all copies. Therefore even the possibility to gather personal data has to be avoided. This means: no biometric measurement.

6.3.2.4 Conclusion

Especially because biometrics has security problems itself and additionally can cause security and privacy problems, one has to ask the question how biometrics should be used and how it should not be used at all.

- **Between data subject and his/her device:** Even biometric techniques that often accept people erroneously, but rarely reject people erroneously, can be used between a human being and his/her personal devices. This is even true if they were too insecure to be used in other applications or would cause severe privacy or security problems in these other applications:
    - Authentication by possession and/or knowledge and biometrics improves security of authentication.
    - No devaluation of classic forensic techniques, since the biometric measurements by no means leave the device of the person and persons are not conditioned to divulge biometric features to “foreign” devices.
    - No privacy problems caused by biometrics, since each person (hopefully) is and stays in control of his devices.

[263] The mosaic theory describes that a collection of a person's data is more than the sum of its parts. This means that not only the data themselves are sensitive and have to be protected, but also the links between them.. See for example Egger, E., ‘Datenschutz versus Informationsfreiheit. Verwaltungstechnische und verwaltungspolitische Implikationen neuer Informationstechnologien.’, *Schriftenreihe der Österreichischen Computer-Gesellschaft (52)*, Wien/München: Oldenbourg 1990.

  - The safety problem remains unchanged. But if a possibility to switch off biometrics completely and forever after successful biometric authentication is provided and this is well known to everybody, then biometrics does not endanger physical integrity of persons, if users are willing to cooperate with determined attackers. Depending on the application context of biometrics, compromises between no possibility at all to disable biometrics and the possibility to completely and permanently disable biometrics might be appropriate.

- **How not at all?** Regrettably, it is to be expected that it will be tried to employ biometrics in other ways:
  - Active biometrics in passports and/or towards "foreign" devices is noted by the person. This should help him/her to avoid active biometrics.
  - Passive biometrics by "foreign" devices cannot be prevented by the persons themselves – regrettably. Therefore, at least covertly employed passive biometrics should be forbidden by law.

  What does this mean in a world where several countries with different law systems and security interests (and usually with no regard of foreigner's privacy) accept entry of foreigners into their country only if the foreigner's country issued a passport with machine readable and testable digital biometric data or the foreigner holds a visa containing such data?

- **Visas including biometrics or passports including biometrics?** Visas including biometrics do much less endanger privacy than passports including biometrics.
  - Foreign countries will try to build up person-related biometric databases of visitors – we should not ease it for them by conditioning our citizens to accept biometrics nor should we make it cheaper for them by making our passports machine readable.
  - Organised crime will try to build up person-related biometric databases – we should not ease it for them by establishing it as common practice to deliver biometric data to "foreign" machines, nor should we help them by making our passports machine readable without keeping the passport holder in control (cf. insecurity of RFID-chips against unauthorised reading[264]).
  - Since biometric identification is all but perfect, different measurements and thereby different values of biometric characteristics are less suited to become a universal personal identifier than a digital reference value constant for 10 years in your passport. Of course this only holds if these different values of biometric characteristics are not always "accompanied"" by a constant universal personal identifier like the number of your passport.

Like the use of every security mechanism, the use of biometrics needs circumspection and possibly utmost caution. In any case in democratic countries (like the countries of the EU) the widespread use of biometrics in passports needs a qualified and manifold debate. After a

[264] http://dud.inf.tu-dresden.de/literatur/ Duesseldorf2005.10.27Biometrics.pdf

discussion on how to balance domestic security and privacy, an investigation of authentication and identification infrastructures[265] that are able to implement this balance should start:

- Balancing surveillance and privacy should not only happen concerning single applications (e.g. telephony, e-mail, payment systems, remote video monitoring), but across applications.
- Genome databases will possibly undermine the security of biometrics measuring inherited physiological characteristics.
- Genome databases and ubiquitous computing (= pervasive computing = computers in all physical things connected to a network) will undermine privacy primarily in the physical world.
- Privacy spaces in the digital world are possible (and probably needed) and should be established – instead of trying to gather and store traffic data for a longer period of time at high costs and for (very) limited use (in the sense of balancing across applications).

6.4 RFID

6.4.1 The Legal and Procedural Perspective

Electronic identification documents (hereafter ID documents) are seen as a necessary upgrade of important paper documents. RFID tags are considered to have enough storage capacity to store biometric images and they are believed to ease the identity checks and enhance security. The equipment of ID documents with RFID tags is claimed to reduce fraud and prevent identity theft as the ID document will not be easily tampered. Furthermore the limiting of human inspection of the documents would help to lessen the amount of errors made.

6.4.1.1 Standards and Legal Requirements

Legal sources with respect to RFID are described in chapter 4.1.6.

The ICAO Document 9303[266] for epassports mandates that the RFID chip contains the passport holder's name, nationality, date of birth and sex as well as the passport number and its date of issue and expiry. Biometric information shall also be included, containing at a minimum a photograph.[267] Similar information (holder's name, date of birth, nationality etc. but sometimes also other information such as the place of birth or national register number) is

[265] Pfitzmann, A., 'Wird Biometrie die IT-Sicherheitsdebatte vor neue Herausforderungen stellen?', *DuD, Datenschutz und Datensicherheit 29*, Vieweg-Verlag, Wiesbaden 2005, pp. 286-289.
[266] The ICAO technical reports and specifications for the integration of biometric identification information into passports and other Machine Readable Travel Documents (MRTDs). are also known as the 'ICAO blueprint' and are available online at http://www.icao.int/mrtd/Home/Index.cfm
[267] Machine Readable Travel Documents – Technical Report *Development of a logical data structure – LDS for optional capacity expansion technologies,* Revision –1.7, 18.05.2004, http://www.icao.int/mrtd/download/documents/LDS-technical%20report%202004.pdf.

included in every kind of electronic ID document. The ICAO blueprint does not require that the information stored in the RFID tag has to be encrypted[268], a fact that increases the dangers against the privacy of the holder.

All the aforementioned data that are saved on the RFID chip are *information relating to an identified or identifiable natural person* (in our case the 'ID document holder') and can therefore be considered as personal data according to the definition of the Data Protection Directive[269].[270] The ID document holder needs to be informed about the data that are going to be included in the RFID tag and about the ways, in which she can access, rectify, erase or block incorrect data that is stored in the tag. The passport authorities need to have reading devices which enable the citizens to access their data stored on the chip and ask for their eventual rectification, erasure or blocking[271].

A basic principle in the field of data protection is the data minimisation principle; according to this principle the data shall be *adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*[272]. The data stored in the RFID tag shall be the data needed for the identification of the holder[273] and be kept to the minimum.

Personal data shall be processed *fairly and lawfully*.[274] The data shall be collected for a specified, explicit and legitimate purpose and be processed only for this purpose (finality principle)[275]. That means that the data collected for the issuing of an ID document cannot be further processed in a way incompatible with those purposes.

6.4.1.2 Privacy Threats

One of the major dangers regarding the use of RFID tags in electronic ID documents is the fact that the RFID tag can be read by any reader and not just the ones of the competent authorities. The unauthorised reading of the tag violates especially the finality principle and underestimates the consent of the ID document holder; therefore it must be guaranteed that only competent authorities are able to have access to the data stored in the chip (Article 29 Data Protection Working Party 2005c). The ID holder shall give her prior unambiguous

---

[268] The data stored on the RFID chips of the Norwegian passport are not encrypted, while the data stored on the German epassport chips will be encrypted, information available online at http://europa.eu.int/idabc/en/document/4792/194

[269] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 p. 0031-0050

[270] However it is to be mentioned that a Member State can adopt legislative measures to restrict the scope of several provisions of the directive, if it considers it necessary to safeguard national security, public security or the prevention, investigation, detection and prosecution of criminal offences […] (Art. 13 Data Protection Directive).

[271] For Germany see http://www.bfd.bund.de/Presse/pm20051028.pdf (accessed on 15.12.2005)

[272] Art 6 (1) c Data Protection Directive

[273] As to this issue see the very interesting decision of the Greek Data Protection Authority on the identity cards (510/17/15-05-2000), available online at http://www.dpa.gr/Documents/Eng/DEC.IDcards510-17-15.05.2000.doc. According to the Greek Data Protection Authority several information that was written on the identity card, such as the profession, the name and last name of the spouse as well as the religion of the holder, was not useful for her identification.

[274] Art 6 (1) a Data Protection Directive

[275] Art 6 (1) b Data Protection Directive

consent[276] for a legitimate data processing to follow.[277] However in the case of clandestine scanning or even eavesdropping she is not even aware that the collection and processing of her data is taking place and therefore she cannot consent to something of which she has no knowledge.[278] ICAO admits[279] that 'although it is unlikely that unauthorised reading will occur, […] ***this cannot [be] completely ruled out'*** (emphasis added). As already mentioned the ICAO blueprint does not require authenticated or encrypted communications between passports and readers. Consequently, an unprotected epassport chip is subject to short-range clandestine scanning (up to a few feet), with attendant leakage of personal information.[280]

The solution ICAO proposes[281] is the use of 'Faraday cages'[282] as a countermeasure to clandestine scanning. In an epassport, a Faraday cage would take the form of metallic material in the cover or holder that prevents the penetration of RFID signals. Passports equipped with Faraday cages would be subject to scanning only when expressly presented by their holders, and would seem on first blush to allay most privacy concerns**.**[283] However the use of Faraday cages does not eliminate the danger of illegal listening into an existing communication between the reader and the RFID chip (eavesdropping).

Repeated unauthorised collection of personal data from a specific RFID tag does not only enable the tracking of the ID document holder, but can also lead to the creation of her profile. If the identity of the ID holder is linked with a unique RFID tag number, the ID holder could be tracked everywhere and thus easily profiled without her knowledge or consent.

The creation of a central database of European Union passports and travel documents containing all EU passport holders' biometric and other data was one of the thorny issues between the European Parliament and the Council. The Committee on Civil Liberties, Justice and Home Affairs had proposed the inclusion of the following provision[284] in the Council Regulation:

'No central database of European Union passports and travel documents containing all EU passport holders' biometric and other data shall be set up'.

According to the Parliament Report[285] *the setting up of a centralised database would violate the purpose and the principle of proportionality**.** It would also increase the risk of abuse and function creep. Finally, it would increase the risk of using biometric identifiers as 'access*

---

[276] Art. 7 a Data Protection Directive

[277] Of course this is not the case for the legitimate scanning of the RFID tag by the authorised personnel. They 'exercise official authority', as mentioned in Art.7 e Data protection Directive and therefore the consent of the ID document is not necessary.

[278] Jay R. & Hamilton A., *Data protection – Law and practice*, London Sweet & Maxwell 2003, p. 91

[279] Annex I Use Of Contactless ICs in Machine Readable Travel Documents, Version 4.0 5 May 2004, p. 25, available online at http://www.icao.int/mrtd/download/documents/Annex%20I%20-%20Contactless%20ICs.pdf

[280] http://www.e-passport.su/

[281] Another solution proposed by ICAO that can apply on identity documents that have the form of a booklet is to place a metal surface on an adjacent page. Under this scheme the RFID tag will not be readable while the booklet is closed. To read the RFID tag the booklet must be opened causing the antenna of the tag to be moved away from the metal surface.

[282] A Faraday cage is a metallic surface enclosing a volume that prevents electromagnetic waves form entering or exiting, definition from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci942282,00.html

[283] http://www.e-passport.su/

[284] Amendment 5: Parliament Report on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports, FINAL A6-0028/2004, 28.10.2004

[285] Ibid

keys' to various databases, thereby interconnecting data sets. However this amendment was not included into the final version of the Council Regulation. As already stated in the Parliament Report the setting up of a centralised database of European Union passports and travel documents violates the principle of proportionality and the same shall be accepted for the setting up of central databases for ID cards[286].

The use of RFID tags in identity documents is not free of problems. The fact that unauthorised machines and consequently persons, who control these machines, may read the tags raises a number of privacy and data protection issues. The most common solution proposed against this treat is the use of 'Faraday cages' and the encryption of the data saved on the RFID tag.

6.4.2 The Technological State-of-the-Art

RFID technology has many application areas, but none of them in the past has come close to the kind of application we are introducing with ID documents. Typically RFID has been used for identification of things (in supply chain management and retail) and persons (for example proximity cards, SpeedPass system) using unique identifiers. So most technical privacy and security features that are currently discussed are focused on these types of RFID and the corresponding back-office systems. The use for more complex micro controller type RFIDs as they are introduced in the European passport is fairly limited. This chapter focuses on the use of RFID in the retail and in MRTDs. As both applications use RFID chips with different capabilities, they show very well the state-of-the-art.

RFID technology is being introduced for use in the retail supply chain (*Luckett 2004*). Many large retailers have instructed their suppliers to tag pallets and cases with RFID tags carrying the Electronic Product Code (EPC™), a "license plate" with a hierarchical structure that can be used to express a wide variety of different, existing numbering systems. EPCglobal[287] has approved a new communications protocol for UHF tags that will standardise tags and readers for the retail supply chain throughout the world. Eventually, many billions of tags will be needed for pallets and cases alone.

If the initiative of the retailers for the tagging of pallets and cases proves successful, then the next step in the process may be to tag individual items. Even though some experiments on item tagging have been conducted by retailers, the enormous number of tags needed, in the many trillions, and the current costs of tags, US $0.25 to $0.50, indicate that it will be several years before large-scale item tagging becomes a reality.

Given that the ultimate vision is to tag all products at the item level, consumers will be affected. Compared with bar codes, the wireless nature of the communication provides significant qualitative and quantitative advantages: tags can store and communicate many more bits of information, multiple tags can be interrogated by the same reader, and readers do not require line-of-sight to the tag. Tags can be read without explicit user action (Floerkemeier et al. 2004). Although tags that can be read at a distance[288] cannot be as small

[286] I.q. Fn. 20
[287] EPCglobal Inc. is a joint venture between EAN International and the Uniform Code Council (UCC).
[288] There are low frequency tags as small as a grain of rice including the antenna but with short read ranges of 1-2 cm.

as a grain of rice, as stated for example in (Weiss 2003), the aforementioned characteristics of RFID tags have raised privacy concerns; see for example (McGinity 2004, Want 2004).

Shaping of public opinion has been started by consumer advocacy groups, for example, by Consumers Against Supermarket Privacy Invasion And Numbering – CASPIAN, followed by numerous articles in journals and newspapers and not only in those specialised in technology and business (Want 2004) but also in the popular press. Perceptions of RFID differ dramatically – ranging from fuzzy fear ("spy chips", "Orwellian Eyes") to unlimited belief in its not yet completely discovered potential.

Ever since the "sensitivity" of RFID-tagged products was recognised, an informed debate has been taking place. For example, the possible economic consequences are discussed by Fusaro in form of a fictional case study (Fusaro 2004). Consumer organisations and data protection commissioners have taken a proactive stands on privacy, and develop policies and guidelines for appropriate implementation of RFID technology. Data protection commissioners have reacted and propose guidelines or regulations. On the other hand, there are RFID proponents who argue that RFID privacy concerns are exaggerated and legislation is premature (Brito 2004). The RFID Position Statement of Consumer Privacy and Civil Liberties Organizations of November 20, 2003, raises the following privacy concerns with RFID:

- hidden placement of tags;
- unique identifiers for all objects worldwide;
- massive data aggregation;
- hidden readers; and
- individual tracking and profiling.

But what are the problems with RFID? Most of today's RFID tags have a static identifier, which never changes throughout its lifetime and is transmitting unassumingly to any reader requesting it. RFID tags, whose identifiers are globally unique and follow a standardised structure,[289] enable inferences about the tagged item to be made. In the following, we describe possible attacks on privacy.

Detecting tag presence often implies signalling the presence of a human being. By correlating multiple observations of the tag's identifier, an adversary tracks the item and may profile an individual's associations. Next, the adversary may have a ``hotlist'' of items/tags in advance that it wishes to detect. Once the adversary succeeds in establishing a link between a tracked item and the owning individual, the individual's history becomes open. If there exists unlocked memory on the tag, an adversary could even write a `cookie' and thus track tags and bypass other mechanisms intended to prevent tracking or hotlisting (Molnar & Wagner 2004).

In the retail space, consumer privacy could be affected by target marketing, where the set of products carried by a consumer or the shopping history if known is then used to classify that

[289] Due to their structure, RFID tags with EPC reveal information about the manufacturer and class of product they are attached to.

consumer for focused marketing efforts. It has further been argued that this knowledge about a customer might also lead to price discrimination or embarrassing situations.

In 2002, Garfinkel proposed "An RFID Bill of Rights", inspired by the Principles of Fair Information Practices, in which consumers should have the following rights (Garfinkel 2002):

- **[Notice]** The right to know whether products contain RFID tags, the right to know when, where and why the tags are being read.
- **[Choice]** The right to have RFID tags removed or deactivated when a product is purchased, the right to use RFID-enabled services without RFID tags.
- **[Transparency]** The right to access an RFID tag's stored data.

Organisations followed to state RFID policies such as Data Protection Commissioners (Cavoukian 2004), the German Computer Society (GI), the European Commission (Article 29), and EPCglobal.

The technologies for protecting consumer privacy can be categorised according to who must provide the technology. Technology deployed by the consumer consists of physical means to detect or block RF signals. A Faraday Cage around the item with an embedded or attached RFID tag will prevent radio waves from reaching the tag. This approach works well with small items, which fit into a purse or bag lined with aluminium foil,[290] but has its limits when goods are large or if the consumer is not aware of tags.

RFID sensor detectors indicate the presence of an RFID reader, and, correspondingly, an RFID reader can be used to search for RFID tags by the consumer by scanning products after purchase.[291] A drawback of the sensor detector is that (almost) any source of electromagnetic waves, a wireless LAN for example, may trigger an alarm.
There is also the possibility of jamming RF signals. Such jamming stations have been used to disable the operation of cell phones. A device that broadcasts radio signals to block/disrupt nearby RFID readers could work. However, this crude approach raises legal issues relating to illegal broadcasting. Alternatively, the RSA blocker tag (Juels et al. 2003) is an elegant mechanism to interfere with the reading of RFID tags.

On the other hand, RFID tag manufactures and researchers have developed technologies embedded into RFID tags to protect consumer privacy. The most prominent example of this class is the "kill command" specified by EPCglobal, which allows the deactivation of tags at the point of sale. There is a steadily increasing number of proposals for "smart" tags. These proposals include hash locks, re-encryption, silent tree-walking, or other cryptography-based approaches to prevent the unauthorised reading of RFID tags.

[290] As an example, see the products of mobileCloak (http://www.mobilecloak.com).
[291] Prototypes are already available, either in the form of a bracelet or as a self-assembly kit to function at 13.56 MHz (`RFID-Detektor' and `Tag-Finder' at eMedia, http://www.emedia.de).

6.4.2.1 Technical Approaches to Improve Privacy of RFIDs

An interesting example of a consumer self-protection device is the proposal by RSA for a blocker tag (Juels et al. 2003), which prevents the reading of other RFID tags in its proximity by spamming the RFID reader. In its basic form, the blocker tag responds in the singulation phase to any query by simulating all possible serial numbers for tags, thereby obscuring the serial numbers of other tags. When carried by a consumer, it effectively mounts a denial-of-service attack.

Selective blocker tags, however, only simulate a given subset of serial numbers. Such ranges of serial numbers may constitute "privacy zones". Each zone (subtree) is identified by its common prefix or, equivalently, by the position of the last common bit on the serial number (the "privacy bit"). Tags can be transferred to a privacy zone if the corresponding privacy bit is switched on. The selective blocker tag responds only to queries related to tags whose identifiers are in the privacy zone. Otherwise, it is silent and only the tag responds to queries related to its ID.

When a reader at a cash register scans an item for purchase, it also transmits a tag-specific key to the RFID tag on the item. This causes the privacy bit in the serial number of the tag to flip to a "1". However, a password needs to be managed for each standard RFID tag, to authorise it to change privacy zones. Further, the reader protocol must be augmented with a special query to ask whether there is a sub-tree blocked by a selective blocker tag ("polite blocking"). Otherwise, the reader may never get around to reading identifiers outside of privacy zones.

Blocker tags are expensive and place the onus of privacy protection solely on consumers (Cavoukian 2004). A blocker tag can only be similar in size and cost to a conventional RFID tag if produced in high quantities. It also suffers from the heterogeneity of current RFID technology: different frequencies, air protocols, etc. It is not likely that tag manufacturers will produce blocker tags as they could be used to interfere with the legitimate reading of RFID tags. Furthermore, retailers have to provide appropriate equipment at checkout where either staff or the consumers disable tags if wanted. Finally, it may be possible that the jamming can be overcome in time (Floerkemeier et al. 2004).

Concerned over public perceptions of RFID tags embedded in products (Benetton, Gillette), chip makers have introduced a "kill command" into their RFID chips.[292] This special command causes a permanent state change in the tag, which prevent it from responding to any interrogations from any readers. Applied upon purchase of tagged products, ``a killed tag is truly dead and can never be re-activated'' (Juels et al. 2003), and thus provides post-purchase privacy.

While the kill command requires only limited changes to tag hardware, there are also some weaknesses. First, it is an "all or nothing" privacy mechanism. Once deactivated, the tag cannot be used for after-sale purposes, no matter how interesting they might be for the consumer. Emerging applications may require that tags still be active while in the consumer's possession. Secondly, consumers have no way of knowing whether the tag has actually been deactivated. The command may have not been received by the tag, or tags can appear to be "killed" when they are really "asleep" and can be reactivated.

As with the blocker tag, "passwords" are needed to prevent unauthorised killing of tags. Depending on the RFID tag specification, passwords range from trivial eight bits up to 32

[292] The EPCglobal Class 1 Generation 2 protocol contains a "kill" command specification.

bits. However, if the password(s) become known, the consequences for the retail supply chain are severe, as this would allow a malicious customer or competitor to silently deactivate numerous tags while walking along the shelves.

The tag killing option could be easily halted by government directive. Retailers might offer incentives or disincentives to consumers to encourage them to leave tags active.

Current RFID technology for the retail space imposes severe constraints on deploying cryptography on the RFID tags. Because of stringent cost pressure, tags are passive and have extremely few gates (Weiss et al. 2003). As an RFID tag is only powered when within range of a reader, it only has an extremely limited amount of time to carry out computations. Pre-computation of results is also impossible when the tag is out of range (Molnar, Wagner 2004). Although recent breakthroughs have been reported in implementing ciphers, for example NtruEncrypt, with no more than 3000 gates (Gaubatz et al. 2004) we assume that encryption, hash functions, or pseudo-random functions are not possible on today's RFID tags. Realistically, only simple password comparison and XOR operations can be expected.

Privacy-preserving authentication protocols have only recently been proposed that are based on randomised hash-lock, re-encryption, hash chains, one-time authenticators, PIN-protected read commands to authenticate readers against tags and others. In the remainder of this section, we briefly elaborate on their basic characteristics and limitations. For a more in-depth discussion on many of these protocols, we refer to (Avoine, Oechsle 2004, Juels et al. 2003, Molna, Wagner 2004).

Even if a tag only transmits a fixed identifier, it can be used to trace an object in time and space. However, as noted earlier, a tag must first be singulated before the reader can start to send commands. Thus, any tag that uses a static identifier in the collision-avoidance protocol can be uniquely identified.

Many of the proposed protocols take advantage of the asymmetry in signal strength, as it is much harder for attackers to eavesdrop on signals from tag to reader. By sending secret information only on the back-channel, these protocols make it harder for passive eavesdroppers.

To achieve location privacy, the information sent by the tag to the reader has to change at each identification. This information is either the identifier of the tag or an encrypted value of it. It implies that the information sent by the tag has to be indistinguishable (by an adversary) from a random value and must be used only once. When the reader is involved in the regeneration of the information, access to a central database is needed. Otherwise, the tag must be able to generate new information by itself, which requires corresponding cryptographic primitives.

Passwords and secret keys for RFID tags must be securely managed. Good security practice further demands that different passwords or keys per tag are used. This may impose a workload on the reader that is on the order of the number of keys. Only Molnar and Wagner have shown a private authentication scheme, for which the reader workload is logarithmic in the number of tags (Molnar, Wagner 2004). On the other hand, this protocol needs a logarithmic number of message exchanges. Because of chip cost and time consumption, it therefore does not offer an alternative technology for today's retail business.

6.5 Chip Card Technologies (Smart Cards)

6.5.1 Security Aspects

The essential characteristic of a smart card in comparison with other data storage media, such as a magnetic-stripe card, is that it provides a secure environment for data and programs. Thus smart cards are all about security. An essential requirement for this is chip hardware that is tailored and optimised for this purpose, along with suitable cryptographic methods for protecting confidential data. However, security depends on more than just special microcontroller hardware and algorithms implemented in operating system software. To discuss security, the PC is a good starting point to show security or rather the lack of it. When the PCs first started to emerge back in the 70s, or later when IBM launched the PC in 1983 who conquered the world, the requirement for security was not there. The indifference with respect to security is still reflected in today's computer architectures (see Fig. 2 left). The software has a hierarchical layer structure and operates above the hardware. This allows a hardware independent interface between the BIOS (basic input/output system) and the Windows/Linux operating system. Therefore the operating system offers the applications a hardware independent interface. Due to this well defined separation between BIOS and the operating system, the hardware as well as the operating system can continuously and independently be upgraded. This was one of the reasons for the fast penetration of the market for todays PCs. In theory any application program should pass all its requests for peripheral services to the Windows/Linux operating system. The BIOS further translates these commands into direct interaction with the hardware devices (input/output, disk, memory, etc.). However, in practice an application program once executing can totally ignore the Windows/Linux and even BIOS layers and can thus interact with the hardware directly. This is often done to improve the efficiency for applications. As an application is allowed direct access to the BIOS and hardware, including memory which contains all the application data, it is evident that any concept of security is a figment of imagination.

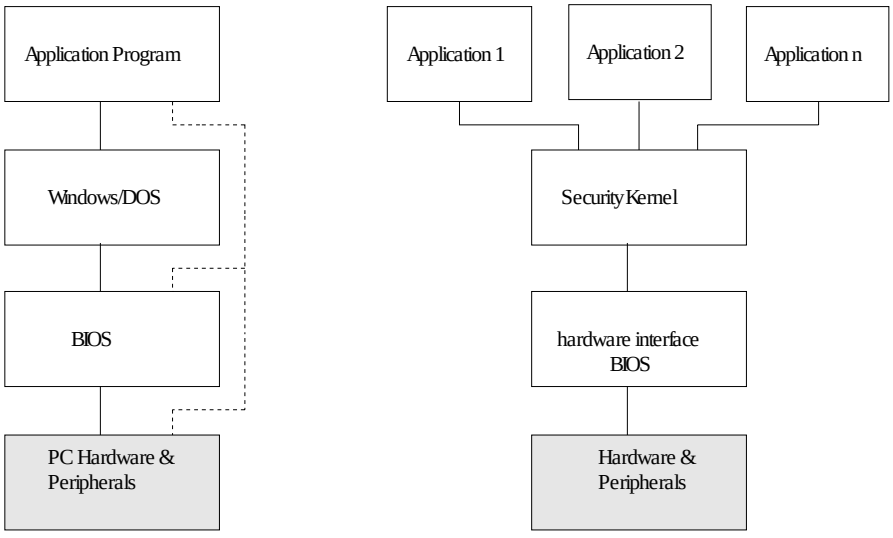

Figure 19: Architecture of today's PCs; application data can have direct access to the BIOS or hardware peripherals (left); secure architecture principle in smart cards where the applications must pass through a security kernel to have no direct access to the hardware & peripherals.

In secure systems for example, an authorised user wishes to be assured that only he can read and modify his personal data. In other words, the service provider and the user want controls to prevent unauthorised access to their data. We distinguish between logical access and physical access control. Logical access control concerns with such familiar principles as password checking or the more sophisticated cryptographic mechanisms for authentication. Physical access control relates to the difficulty of a perpetrator physically breaking into a store of data, by for example connecting wires to the disk drive directly and bypassing the rest of the computer completely. The secure architecture (see Fig. 2 right) must thus prevent any application to access hardware peripherals directly (especially memory) or gain any sort of control of the microprocessor. A security kernel prevents applications to take control of the processor in an unrestrained way, enforces the mapping of the data between application and the data stored and provides for each application its own security controls. The security kernel can for example be realised by an interpreter or a virtual machine where all resource requests are checked against a rights matrix.

An emerging technology for such an interpreter architecture is the Java language defined by SUN microsystems, resulting in the Java Card Platform technology (SUN 2006) for smart cards. Java instructions are translated in a hardware independent bytecode suitable for a virtual Java processor. The Java technology with the necessary Java Virtual Machine and its bytecode interpreter is a natural candidate for the security need of smart cards as its interpreter acts as a security software wall. It is also possible to achieve control mechanisms by security hardware walls in the microprocessor where an application can be constrained from direct accessing secure memory domains using special hardware circuitry. Such software or hardware measures can ensure that an application can only access the date to which it is authorised and in the prescribed way. To preserve security segregation between the various applications, in addition each application implements its own security mechanisms. State-of-the-art cryptographic controlled security mechanisms can be implemented in smart cards, like authentication, data integrity, confidentiality and non-repudiation. It is important to know that all these cryptographic controls involve key attack management which requires the secure distribution of cryptographic keys into various entities and the need for these entities to provide a tamper resistant environment.

It is naturally practically impossible to configure a complete system, or even a smart card, such that it has a perfect security that is proof against everything and everybody. If the effort expended on the attack is raised to a high enough level, it is possible to gain access to any system or manipulate it. However every potential attacker makes a cost/benefit analysis for himself and his target. The rewards of breaking into a system must be worth the time, money and effort that the potential attacker must expend to attain his objective. The security of a smart card is as strong as the weakest of the following four components:

1 application
2 operating system
3 integrated chip hardware
4 card body

The card body can be a simple chip housing or a more complicated body for securing complex multi-chip hardware. In the former case the body is a component which is not only machine readable, but can also be visually checked by humans, in the latter case precautions

against physical opening attacks need to be applied. The data and programs in the smart cards are in addition protected by the remaining three components, the integrated chip hardware, the operating system and the application. If any of these components fail, the smart card is no longer secure, as the components are strongly coupled to each other.

Basically, attacks on smart cards can be divided into three different types of categories:

- *Attacks at the social level* are primarily directed against people that work with smart cards. These can be smart card engineers at the various design and production stages. Further on in the life cycle of the card these are card-holders. Social level attacks can only partially be countered by technical measures and must therefore be countered by organisational measures.
- *Attacks at the physical level* require technical equipment as it is necessary to obtain physical access to the smart card microprocessor hardware. Here we distinguish between attacks during operating (power is applied to the hardware) and attacks during non-operation (no power is applied to the hardware).
- *Attacks at the logical level* have been reported as the most successful attacks up to now. This category includes classical cryptoanalysis, as well as attacks that exploit known faults in smart card operating systems and Trojan horses in executable code of smart card applications.

Attacking methods and protection measures is like a never ending ping pong game. As soon, or better before new attacking methods are known, new and sophisticated protection measures are introduced. As an example, since researchers published a method to draw conclusions about stored cryptographic keys from observing execution speed (Kocher 1995) of cryptographic algorithms or from observing the dynamic power consumption (Kocher 1998) of the smart card microprocessor, more secure implementations of the encryption/decryption algorithms very fast became state-of-the-art. Smart card attacks at the physical level demand exceptionally high effort and expensive equipment. In the following text some of the numerous countermeasures are mentioned to get an impression of the complexity effort to block attacks:

- On the card body level at complex multi-chip smart cards, the objective of the first level of protection is to prevent aggressors to open the box and facing working electronics. Different kind of sensors, like current loops and light sensors are placed in the box to detect attacks and thereupon immediately delete the cryptographic keys.
- On the smart card chip level even more sophisticated countermeasures are necessary: Data buses from the microprocessor to memory sections within the smart card chips are often dynamically scrambled and data transferred on these buses encrypted. Moreover data buses are optically invisible as they are buried in deeper layers of the integrated silicon chip. In addition the busses are covered by metal layers and intrusion sensors.
- Analysing the electrical potentials on the chip surface while it is operating represents serious threat. With a suitably high scanning resolution, this technique can be used to measure charge potentials on very small regions of the chip crystal. With such information it would be possible to draw conclusions about the contents of the

memory while the chip is operating. A very effective countermeasure is to place current-carrying metalisation layers on top of the memory region. If the intruder removes such metalisation layers by chemical etching, the chip will no longer work properly since the layers are not only needed to distribute the power but are also as sensors to detect intruders.

- A similar attack scenario tries not to read but to alter memory contents of the smart card. EPROM cells can be discharged by exposing them to ultraviolet light or X-rays. By a collimated beam of light or light from a laser, the attack point can be focused on a fine point and thus the contents of an individual memory cell can be altered. Such a theoretical attack could be applied to a random number generator in such a way that no longer random numbers would be generated but instead always generates the same number. If this were possible, authentication on the smart card terminal could be broken by a replay attack using a previously employed number. Countermeasures for such attacks again are light sensors at critical hardware circuitry.
- Integrated chip are qualified and work properly as long as voltage, frequency and temperature are within the defined specifications. A strategy of an attacker might be to put the smart card chip out of its specifications of correct working in order to provoke uncontrolled program jumps. Such faulty behaviour could again be used to determine secret keys. To prevent such attacks, every smart card chip has voltage, frequency and temperature monitors to detect environmental irregularities and to switch off the smart cards immediately.

6.5.2 Privacy Aspects

As every other technological system used for processing personal data, chip cards and their background system have to adhere to the legal regulations concerning privacy and security.[293] Apart from that, chip cards offer the possibility to store and process personal data in a decentralised way instead of central data bases. Central data bases can be regarded as a major problem for privacy and security which is pointed out in the strategic vision of CEN [CEN 2005]. In this document Amitai Etzioni, head of the US Institute for Communication Policy studies, is quoted: 'There is always a balance between privacy, security and trust. The more reliable the card is, the more privacy you have, both in the off-line as in the on-line environment. Once the identity is verified, there is no need for alternative searching in databases, archives etc.' Thus eID cards can reduce privacy threats because of 1) their decentralised concept, 2) the support of user control for all transactions (at least if an interactive action is needed), and 3) the on-card chip which can carry out security checks itself.

One problem – not only valid in the context of chip cards – became explicit when the discussion on privacy requirements for chip cards began: Because of the transparency principle each holder of a chip card should know which data are stored on it and how they are processed. Usually (in naïve implementations) this means that the holders can also show the information stored on the card to other parties. If there are specific information stored, e.g. about the holder's health, healthy people may use their chip card to get some benefits (e.g. a

[293] E.g. elaborated in Gardeniers, H.J.M., Chipcards en Privacy. Regels voor een nieuw kaartspel [Chipcards and privacy. Rules for a new card game] Dutch DPA, September 1995. Background studies & Investigations 6, http://www.dutchdpa.nl/documenten/en_AV_06_chipcards_and_privacy.shtml.

cheaper insurance or a job). Those who would not prove their good health status via chip card access would suffer from disadvantages. Even if law prohibited to ask people to see data on their chip card (e.g. in a job interview), they could do it voluntarily – and thus set a standard. This is in particular relevant in (less regulated) civil law. Of course a landlord would prefer a person who has provided evidence for good creditworthiness over others who do not give this information. As the health area has to be treated in a very sensitive way, this problem was addressed by the German Data Protection Commissioners in 1995.[294]

6.6 Electronic Signatures and PKI

The process of creating using and verifying a digital signature provides important functions that can be utilised for ID documents in an e-government context:[295]

- *Firstly,* the asymmetric cryptography (PKI) ensures a high level of security in e-communications and of confidentiality of the context of a message sent over the Internet.
- *Secondly,* digital signatures provide authentication of the identity of the signer by attributing the message to the signer; so it is known who participated in a transaction. The rationale of this function is based on the fact that digital signatures cannot easily be forged, unless the signer loses control of his private key either accidentally or intentionally.
- *Thirdly,* the digital signature protects the integrity of the transmitted data so the recipient can be sure that there has been no alteration to the original message.

The non-repudiation of digital signatures can be guaranteed by the involvement of trusted third parties, the certification authorities (CAs). The CAs issue a certificate, which attributes explicitly a public key to a specific identity and confirms the identity of the subject of the certificate.

Even though these functions of digital signatures can guarantee security over open networks, certain challenges need to be confronted. The big question is how secure is the security provided by digital signatures?

6.6.1 Risks of Using PKI

The incorporation of PKI can be very valuable to ID documents, however, it should be remembered that it is not without flaws. There are certain basic questions that need to be

[294] Entschließung der 50. Konferenz am 09./10. November 1995 zu datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen, http://www.datenschutz-berlin.de/jahresbe/95/anlage/an2_10.htm.
[295] 'A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication', Spyrelli, C., JILT 2002 Issue 2 http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html

answered and precautions that should be taken while incorporating PKI in order to make it sufficiently secure and trustworthy.

Private keys are usually stored on a conventional computer, which may not have a secure computing system, adequate network security and other protections. If it is protected by a password, how difficult is it to guess the password? If the key is stored on a smart-card, how attack resistant is the smart-card? If it is stored in a truly attack-resistant device, can an infected driving computer get the trustworthy device to sign something that was not intended to be signed?[296]

For example, Alice's digital signature does not prove that Alice signed the message, but that her private key did. If her computer were appropriately infected, the malicious code could use her key to sign documents without her knowledge or permission. Even if she needed to give explicit approval for each signature (for example, via a fingerprint scanner), the malicious code could wait until she approved a signature and sign its own message instead of hers[297].

If an attacker can manage to add his own public key to an existing list of legally registered keys, then he can issue his own certificates, which will be treated exactly like the legitimate certificates. They may match legitimate certificates in every other field except that they would contain a public key of the attacker instead of the correct one.[298]

A key has a cryptographic lifetime. It also has a theft lifetime, as a function of the vulnerability of the subsystem storing it, the rate of physical and network exposure, attractiveness of the key to an attacker, etc. From these, one can compute the probability of loss of key as a function of time and usage. What probability threshold is used to consider a key invalid?[299]

Certification authorities (forming the backbone of PKI) are vital to the use of digital signatures. However, some jurisdictions have no specific regulation dealing with certification authorities. The EU Directive prohibits mandatory prior authorisation schemes but does allow member states to set up voluntary accreditation schemes for certification authorities.[300] If the PKI system has to have any value in terms of security, the certificate authorities have to be trusted sources. In certain countries, the government itself assumes the role of being the Certification authority.

6.6.2 Conclusion

The use of PKI in ID documents can guarantee time and cost-efficiency in the bureaucratic procedures by facilitating the handle, process, storage and transmission of data. However, countries have to find a means to overcome security problems arising from the use of PKI.

---

[296] Based on "Ten risks of PKI: What you're not being told about Public Key Infrastructure", Carl Ellison and Bruce Schneier, http://www.schneier.com/paper-pki.pdf
[297] Based on "Risks of PKI: E-Commerce", Carl Ellison and Bruce Schneier, http://delivery.acm.org/10.1145/330000/328123/p152-ellison.pdf?key1=328123&key2=0901199311&coll=GUIDE&dl=GUIDE&CFID=68457300&CFTOKEN=14129309
[298] Supra, See 2
[299] Ibid
[300] "Digital Signatures: Addressing the legal issues", Robbie Downing, Ross McKean, Baker & Mckenzie, http://www.nacm.org/bcmag/bcarchives/2001/articles2001/may/feat1.5_01.html

For instance, in the Finnish eID system, private keys are held only by the certificate holder (e.g. on the ID card chip) and can be utilised only after inputting the PIN codes, but even then they cannot be read from the card. The PIN codes are known only to the cardholder, and he or she can change them, when necessary. Three false attempts at inputting the PIN code locks the card.

It remains to be answered as to whether the questions and problems as stated above have been considered by member states and if so, if they have been effectively overcome in identity documents using PKI.

6.7 Summary and Conclusions

6.7.1 Technology related conclusions

In this chapter four basic technologies currently used in ID documents have been investigated with respect to security and privacy. While smart chips and electronic signatures have been used for eIDs for almost ten years now, the use of RFID and electronic readable biometrics in ID documents is relatively new and especially driven by the European passport.

Chip card technology has been discussed, used and further developed for many years now. As a result this technology is accepted as mature by technicians and privacy commissions in Europe. Of course, the combination of chip cards with other technologies such as biometrics can result in new questions concerning security and privacy.

PKI also has been used for ID document systems in some European countries for 9 years now, though the number of issued certificates still seems to be limited. Apart from the above mentioned risks no major security problems were published. PKI currently does not implement privacy in an optimised way because of the existing linkability of transactions performed via the information in the certificates. The linkability can be reduced by using alternate technical solutions such as digital credentials (see FIDIS Deliverable *D3.1: An Overview on Identity Management systems*, (Meints, Hansen, Bauer 2005) pp. 57-61) or sector specific personal identifies (see chapter 5.5) where no electronic signatures are needed. In some European countries (for example Germany) pseudonymous signatures can be used (Gasson, Meints, Warwick 2005, pp. 32-40). A new technical and from the privacy perspective promising approach currently is being discussed in the European eforum. This approach includes so-called server derived IDs to implement unlinkability of electronic credentials basing on X.509 certificates across the borders of communicational sectors (see chapter 5.8.3).

In difference to these established technologies the use of biometrics and RFID in ID documents raises a number of obvious privacy and security issues. In addition to security aspects, for example with respect to (1) the quality of biometric identification, (2) identity theft and (3) devaluation of classic forensic techniques, a number of privacy aspects still needs to be addressed. This includes (1) minimisation of linkability, (2) enforcement of the purpose binding principle and (3) avoidance of additional, in many cases health concerning, information in biometric raw data. Advanced technical approaches for authentication using biometrics (Gasson, Meints, Warwick 2005, pp. 105-107) have not been tested for or implemented in ID documents so far.

6.7.2 Conclusions with respect to MRTDs

RFID originally have been designed for unrestricted remote access to the information stored on them. For the use of RFID in current ID documents especially the European passport basic security measures, for example Basic Access Control (BAC), have been applied to restrict the access. BAC seems to be cryptographically weak (see chapter 5.3) and uses information stored in the Machine Readable Zone (MRZ) on the document itself; this is like storing the key of a cash box directly under it. Together with well documented projects of non-European countries aiming at the storage of biometric data of foreign visitors in large databases[301], this creates a significant risk of identity theft via biometrics in cases the document is (even properly!) used or gets lost. And scenarios of fast boarder controls using unobserved terminals[302] in addition to well documented methods to spoof biometric sensors (Geradts, Sommer 2005) show how the stolen identities could be used quite easily in future.

A number of additional security and privacy methods currently in discussion or development such as applying a "Kill Command" cannot be used in a meaningful way with RFID in ID documents. Other methods such as integrating a faraday cage in the cover of the European passport are not implemented. Extended Access Control (EAS) does not solve the described problems.

To sum the findings up a convincing security concept is missing. The use of European Passports enables tracking of citizens under certain circumstances, e.g., by equipping door frames with RFID readers, and exposes raw biometric data for additional purposes in the private and public sector. As these passports are valid for up to 10 years and subsequently will be used in that time, the described vulnerabilities also will remain for this timespan.

Concerning the use of the European passport we follow some of the suggestions made by consumer protection organisation[303]. In this case we suggest:

- The European passport should be used and carried around only when necessary.
- In case the European passport is not used, it should be kept in a Faraday cage (for example aluminium foil) to hamper unauthorised access to data stored on the RFID-chip.
- In case the European passport is not used, it should be locked carefully to avoid loss or theft of the document.

Basing on the Budapest Declaration[304] concerning the further development of the European passport the following suggestions should be taken into consideration:

1. Since MRTDs with inherent weaknesses have already been introduced and will inevitably be used in future, we recommend the following measures for immediate

[301] For example: USA; see http://de.wikipedia.org/wiki/Biometrie
[302] This kind of future scenario was discussed on the word eID conference (September 21st and 22nd 2005 in Sophia Antipolis)
[303] For example Foebud; see http://www.foebud.org/rfid/was-kann-ich-tun/
[304] See http://www.fidis.net/press-events/press-releases/

implementation to reduce the risk of security failure and identity theft. These recommendations include scenario-based back-up procedures and technologies which require an international level of development and agreement (i.e. ICAO):

a. Organisational implementation and enforcement of the purpose binding principle especially for biometrics used in MRTDs (where the defined purpose is authentication of international travellers). The use of MRTDs should not be extendable to authentication in the private sector.
b. Citizens need to be informed of the risks inherent in owning new MRTDs and the corresponding security measures which can be undertaken by them (for example avoiding the release of the documents to private organisations such as hotels etc.)
c. Available yet unimplemented security measures such as Faraday cages should be integrated immediately into current MRTDs by the European member states.
d. Organisational procedures are necessary to cater for the failure of biometric authentication due to inherent biometric issues such as false rejection rates (FRR) and error to enrol.
e. Organisational and technical procedures are required to prevent abuse of personal data from MRTDs.
f. Organisational and technical procedures are necessary to deal with identity theft using data from MRTDs or complete MRTDs.

2. In the mid term (within the next three years) a new convincing and integrated security concept covering MRTDs and related systems needs to be developed and communicated. In particular, this must take into account:

a. A definition of required security levels.
b. Protection of European citizens' personal data (including biometrics if still utilised).
c. Multilateral technical and organisational security aspects of the deployment of MRTDs considering different operators in different countries and the MRTD users (exemplary question: How can abuse of personal data by foreign countries be prevented?)
d. Risks and threats emerging from the combination of different technologies used in the context of MRTD such as RFID, biometrics, and security features of paper-based documents.
e. Based on the defined security levels and risk analysis, a complete re-evaluation and re-design of the technical solutions adopted for current MRTDs, especially RFID and biometrics, should be performed. It should be considered whether these technologies are actually necessary, or if technologies which are more secure and privacy-preserving (such as contact smartcards instead of contactless mechanisms) are sufficient. Ways in which the implementation of technologies utilised can be improved (e.g. for biometrics through the use of on-card matching and on-card sensors) should also be investigated.
f. The security concept should be publicly debated by security and privacy experts on a European level.

3. Technical and organisational measures developed need to be standardised (ICAO), implemented in the next generation of MRTDs, and audited world wide.

7 Economic Aspects

It is beyond doubt that one of the most important aspects that need to be considered prior to the deployment of eIDs is the economics of any scheme that seeks to be viable. The importance of economics and the underlying issues that are related to accounting for different cost-projections are critical and typically play a fundamental role in decision-making. For the political world, cost-projections and related economic aspects are also extremely important as they often become the source of debate for a variety of reasons, the foremost of which is public spending that is always prone to heavy criticism. As citizens' expectations are high when tax-collected monetary funds are put to use, research and considerations concerning such schemes becomes extremely important, particularly when public spending escalates towards exorbitant amounts of money that have not been properly considered, or even worse, considerably underestimated. The sheer scale whereby such schemes have to be launched (typically the entire population of a country) means that depending on the complexity of the scheme, there is a distinct possibility that initial estimations concerning cost-projection could be utterly mistaken or considerably dislocated from the end result. Research towards the multitude of issues that influence economic aspects related to eID implementations is therefore necessary, and it is the purpose and target of this section to provide a guide and outline several issues that need to be considered for the implementation and adoption of eID schemes and that should be factored into the economic aspects of implementation.

7.1 Complexity Factoring into the Economics of eIDs

Before going into the actual consideration of outlining some of the critical cost-projection factors for eID implementation, an argument has to be made for the complexity that is inherent in such large-scale projects and that argument is simple; *there are different degrees of complexity of implementation of eID schemes and the higher the complexity, the more ambiguity is induced into the economic projections and estimations.*

The aforementioned statement on the complexity that is influencing the economic projections can be ultimately broken down to *systemic* and *environmental* economic complexity and those two can be described as follows:

a) *Systemic* complexity that generates economic ambiguity concerning the cost-projection of an eID scheme and can be – up to a certain extent – modelled by the government and/or institutions involved in the design and implementation of the scheme.

b) *Environmental* complexity that generates considerable economic ambiguity concerning the post-implementation cost-projection of an eID scheme and is typically contingent upon a variety of elements that cannot all be *a priori* accounted for.

The differentiation between *system* and *environment* occurs under the theoretical framework of Systems Theory and it is within framework that further elaboration can be attempted (Bertalanffy 1969). The theory has itself been through a series of transformations, each enriching the conceptual subtleties and also its applicability to a variety of different domains for analytical purposes (Luhmann 1995).

There are various issues that should be considered here before we go into describing some of the proxies for considering cost-projection but it is useful to say that the aforementioned classification will be used to categorise the proxies. Furthermore, there also needs to be a clarification on the difference between *systemic* and *environmental* complexity. Whereas *systemic* complexity can be attempted to be modelled more accurately (though never fully) by collaboration between different government departments and/or the industry, *environmental* complexity resists modelling attempts *as it is contingent upon societal, political, and technological aspects that are emergent and create a feedback to the economic system in a multitude of ways,* the most prevalent and obvious of which becomes the unpredicted financial costs of the project itself (following the eID implementation). There are other ways however that could potentially affect the economy and these will also be factored into our considerations, for example, the creation of a highly skilled workforce that can potentially enjoy financial gains from transferring skills, processes and a variety of knowledge-driven procedures to other implementation sites and/or integrating the skills and processes into already existing infrastructures.

Finally, before we go into more detail about the elements of the cost projection, we have to clarify that the use of the term *cost* is hereby used – in several occasions – instead of *price.* Interchangeable use between the two terms might neglect the fundamental economic difference between them, namely that *price* reflects and projects a monetary value (say €10billion) whereas an economic interpretation of the cost encompasses price and also includes a variety of other elements that may have an impact on the price itself but do not solely restrict their influences there. *Whereas the price of a scheme might appear to be fixed, the costs are observer-relative and accrue from here to eternity whereas they can also involve intangible aspects that harm the societal fabric in a multitude of ways (i.e. loss of privacy).*

7.2 Cost Projection Elements (of Systemic Economic Complexity)

As analysed above, the elements that can be more easily modelled for the cost-projection of an eID scheme conform to the *systemic economic complexity.* Some of the proxies that should be considered for cost-projection are individually discussed below:

a) **Enrolment cost-projection for staff:** The proxy for the cost-projection here does not include the types of cards to be used[305]. While estimating the cost of enrolment there are sub-proxies that need to be considered. ***Enrolment staff*** needs to be hired for the initial roll-out of the system and the staff also needs to be ***trained*** to use the systems that will be commissioned for the enrolment phase. Due to the sensitivity of the task of identity and the risk for potential fraud there needs to be a careful ***vetting[306] process*** of the employees to be involved in the scheme of the enrolment phase. *Such a vetting process can itself be considerably differentiated and hence constitutes one of the many cost-elements that need to be carefully considered.* Depending on the depth of the vetting process, considerable costs can be further incurred (i.e. companies specialising in the vetting process can carry out standard checks or carry out extensive research on employees' backgrounds involving university diplomas, references, working

[305] Used under the proxy 'equipment'.
[306] Background checks of a variety of characteristics about employees.

experience, certificates, criminal records, and a variety of other elements). Furthermore, staff that will be involved in the enrolment phase need to be trained on ***security aspects*** for potential cases of fraudsters that would try to manipulate the system to their benefit and/or colleagues that try to willingly jeopardise the enrolment. Finally, the involvement of *enrolment staff* in the enrolment phase needs to be properly managed and managerial processes need to be carefully developed and considered within the specific characteristics of the context of implementation.

b) National Identity Register Staff: Independently from the staff that would participate in the enrolment phase, similar elements for cost-projection could be considered (with a few modifications) for the personnel working in the national identity register. Personnel in the National Identity Register would perhaps need to go through a more detailed vetting process than those in the enrolment centre. The need for such a detailed vetting process could be justified once one considers the variety of operations that can be carried out on identities from those that have access to the National Identity Register (NIR hereinafter). Depending on the level of security that would be required – *typically security in the NIR would have to be of the highest possible standards* – then different processes will be have to be setup and scrutinised. Security training of the employees, high-level security procedures for verification of changes to the register and assistance in case of problems will all have to be factored into the cost-estimates. Considerable costs might incur from handling complaints, several issues that might require face-to-face meetings and verification of changes to the register will have to be dealt with and so on. An example from the US comes with the implementation of the no-fly list for terrorist suspects, administered by the department of Transportation Security Administration. The Department of Transportation had paid $2million just to handle complaints but it swiftly proved that this allocation was insufficient, ***as a quarter of that money was used to handle voicemail backlog*** a situation that quickly escalated as people were leaving numerous messages to the automated service and in some occasions it took up to **nine months** before people could be cleared off the list (Singel 2005) (i.e. like the head of Catholic Education in the US, Sister McPhee that was mistakenly identified as a terrorist suspect). **It is therefore important to realise that such *positive systemic feedback*[307] generates economic costs for the scheme and that it has to be swiftly identified, monitored and managed before further costs incur.** It could prove that integration of an eID into day-to-day operations (like financial transactions) could cause much more severe disruptions as a problem in the verification of a person's identity would have to be dealt with efficiently, effectively and consistently, without jeopardising security.

c) Equipment & surrounding issues: A good percentage of the amount of money for rolling out an eID scheme goes to the *purchasing of the devices* themselves (i.e. biometric smart cards) for the entire population. However there is a variety of other cost elements related to the cards themselves like printing, renewing the cards or re-issuing cards. Carrying out effective *auditing* and setting up appropriate policies and procedures prior to the issuing of the cards is also something that needs to be considered and factored into the estimations while *purchasing readers for the public*

[307] The act of a systemic escalation that tends to disrupt the functionality of a system (in this particular scenario being the excessive number of calls done to the Department of Transportation for complaints, quite often from people whose cases would not be dealt with on time).

> *sector* (at selected points of use), *including secure communications to the National Register* are also a considerable cost. The problem that remains to be examined with technological equipment is that new technologies (ultimately both hardware and software changes) may render parts of the broader system obsolete and would therefore signal the need for replacing the technology and/or upgrading parts of the system to cope with more elaborate security requirements. When one considers the *scale that these replacements* need to be carried out then we have a considerable and significant additional cost for which we can only speculate.

The scale and complexity of such schemes is one of the major reasons behind differences in cost-projections. Below is an estimate for the UK example of introducing biometrically equipped ID cards; the estimate was carried out by the London School of Economics[308] and at the time caused a series of debates *as the cost-projection was three-times higher than that* of government's estimations[309]. According to the research findings, the lowest possible estimation for the proposed eID scheme of the UK government came to be £10.6billion with a maximum estimation close to £19.2billion (these figures refer to the cost-projections during operation of the first ten years of the scheme).

	Low	Median	High
Issuing Identity Cards Over a 10-Year Period	814	1015	1216
Passports (Based on Passport Service Figures)	3936	3936	4065
Readers for Public Sector (As Specified in the Bill)	291	306	317
National Identity Register	1559	2169	2910
Managing the National Identity Register	2261	3658	5341
Staff Costs Over a 10-Year Period	1719	3368	5308
Miscellaneous	22	64	117
TOTAL	**10602**	**14516**	**19274**

Cost Projections – All figures are in £millions. See Appendix 2 for more information.

Figure 20: Costs for the issuing of the eID card in UK

(Source of Figure 20 The LSE Identity Project report[310], June 2005)

Differences between the low, median or high cost-projections relate to a variety of elements that can be accounted for individually within each broader category but depending on uncertainty differences the estimations vary.

An analytic breakdown of the cost-projections from the study carried out by the LSE Identity Project for the UK eID scheme involving biometrics is shown below. The analytic breakdown

[308] http://is.lse.ac.uk
[309] Recently the House of Commons passed the Identity Card Bill and dismissed all cost projections itself. The House simply stated that cost-monitoring will be taking place throughout the project's implementation and every six months. The House of Lords has rejected the Identity Card Bill thus far.
[310] http://is2.lse.ac.uk/IDcard/default.htm

can serve as a sample for cost-projections for similar eID schemes, extrapolating categories and considering the variety of issues that should be accounted for whilst performing similar estimations[311]*:*

Appendix 2: Cost Projections

All figures are in millions. These are ten-year rollout figures based primary on Government statistics. Where information is inconsistent, median figures have been brought down toward the lower estimate.

	Low	Median	High
Issuing Identity Cards Over a 10-Year Period			
Initial costs to establish issuing processes			
Includes			
- Set up of policies, procedures			
- Audits and dealing with exceptional cases	8	12	16
Purchase of biometric smartcards			
- 67.5 million population at full rollout	270	338	405
Printing personal information on cards	14	14	14
Renewal of cards			
- Assumes that cards will have to be re-purchased and re-issued every four years			
- This figure covers the ten year rollout period	405	506	608
Re-issuing of cards			
Includes			
- Projected defective rate of 0.25%			
- New cards issued because of change of circumstances during application and enrolment phase			
- Data errors			
- Damaged cards			
- Lost or stolen	117	145	173
Total Cost of Issuing Identity Cards	**814**	**1015**	**1216**
Passports (Based on Passport Service Figures)			
Total cost of issuing existing booklet passports	1994	1994	1994
Total cost of issuing new passports			
- Personal interviews for first time applicants			
- Changing passport-centric system to passport-holder-centric system			
- Placing digital photograph on passport			
- Basic UKPS staffing costs	1814	1814	1814
Replacement passports			
Includes			
- Projected defective rate of 0.25%			
- New passports issued because of change of name			
- Lost or stolen passports	128	128	257
Total cost of passports	**3936**	**3936**	**4065**
Readers for Public Sector (As envisioned in the Bill)			
Purchase of Readers			
Includes			
- Card, Fingerprint, Face, Iris, and combined readers			
- For use at selected public service points envisioned in the Bill			
- Replacement technology every three years			
- Replacement of damaged readers (faulty readers catered for in three-year warranty)	261	261	261
Interfacing with Register			
- Secure communications to National Identity Register for each reader and/or public service point	30	45	56
Total cost of readers	**291**	**306**	**317**

Figure 21: Cost projection of the eID card in UK (1/3)

[311] Appendix 2 of *The LSE Identity Project Report*: June 2005, pp. 315-317.

National Identity Register			
System Contract over 10-year period (database only)			
Includes			
- Research, analysis and development of system			
- Security assessment and certification			
- Hardware and software costs			
- Replacement hardware, software, updates, dealing with system down-times and failure, recertification			
- IT Department operational costs			
- Risk margin	298	298	429
Deployment and Adaptation of Systems			
- Establishing 'pull' from various Government systems required for basic information verification			
- Adaptation of first-round Government systems for 'push' of information, in accordance with the Bill (various Home Office information systems, Police Databases, Department of Work and Pensions systems)	1261	1871	2481
Total cost of National Identity Register Infrastructure	**1559**	**2169**	**2910**
Managing the National Identity System			
Enrolment of UK population, including			
- Set up costs			
- Planning and logistics (policies, practices, audits)	208	213	556
Running costs (maintenance, overheads)			
- Property leasing and mobile registration centres			
- Property servicing charges	608	810	1013
Updating information			
- Changing information on the registry due to change of circumstances			
- Verifying individual's prior circumstances through verification of biometrics at a registration centre			
- Verification of the veracity of the new information	203	540	675
Servicing verification			
- Verification queries from a variety of public sector organisations, in accordance with the Bill			
- Verification queries from employers			
- Call centre management	203	540	1013
Verifying biographical footprint of enrolees			
- Contacting various public sector databases			
- Contracts with private sector data aggregators and credit bureaux			
- Document vetting and verification			
- Verification of individual's prior circumstances, including through verification of biometrics at registration centre			
- Verification of the veracity of the corrected information	675	878	1013
Correction of entries in the National Identity Register, including			
- Policies, procedures, and documentation			
- Regular data integrity checks and compliance with Data Protection Act (including servicing of Subject Access Requests)	53	75	113
Enforcing enrolment of the UK population	65	130	195
Re-enrolment for altered biometrics			
- Verifying prior information			
- Collecting new biometrics			
- Audit	203	405	675
Identifying and policing fraud	43	67	88
Total cost of managing the National Identity System	**2261**	**3658**	**5341**

Figure 22: Cost projection of the eID card in UK (2/3)

Specific Other Staff Costs Over a 10-Year Period			
Enrolment Staff			
- Staffing of registration centres for the initial roll-out			
- Training for use of systems			
- Security training			
- Background checks			
- Management	838	838	1118
Staff for the National Identity Register			
- Security training			
- Background Checks			
- Call centre employees			
- Staff for face-to-face meetings to verify changes to the register			
- Full public interface (taking into account non-co-operators)	813	2433	4056
Staff training for public service points			
- Accessing Register			
- Use of biometric readers	68	97	134
Total staff costs	**1719**	**3368**	**5308**
Miscellaneous			
Design, feasibility, business case (already awarded)	12	12	12
Consultancy and other costs	10	52	105
Total miscellaneous costs	**22**	**64**	**117**
TOTAL	**10602**	**14516**	**19274**

Figure 23: Cost projection of the eID card in UK (3/3)

(Source of the figures: The LSE Identity Project (2005)[308])

7.3 Cost Projection Elements (of Environmental Complexity)

As previously discussed, the elements that *conform to an environmental economic complexity* can not be easily accounted for; they are intimately related to increased uncertainty and are also prone to increased speculation about future economic conditions. These will typically include economic aspects other than immediate cost-projections that could refer to the reaction of other markets and countries. Starting however with the contingent and contextual aspects at a national level we can distinguish several issues:

a) **The Economics from the Threat to Privacy:** With the proposed changes of eID schemes and the underlying technological infrastructure that can support it, citizens are becoming increasingly aware of the threats to Privacy (Arndt 2005). The idea behind a disproportional exercise of power from the government is at the very core of emergent problematic phenomena as far as privacy is concerned, and furthermore acts as a trigger towards expressing resistance to change and reaction to excessive control (Foucault 1977). With implementations of eID schemes, it is often – and not mistakenly – perceived that the balance between those that have the potential of exercising the control (and power) over those on

whom control is being exercised is considerably displaced and the possibility remains strengthened that people are constantly being categorised, profiled and monitored while their personal data becomes jeopardised like never before. Coupled with activities from civil liberties groups, resistance to change might be reinforced and produce several effects. *If we treat the imposition of eID schemes to the population of a nation (or a number of nations through EU Directives) as a purely political decision*[312] *then it becomes evident that Civil Liberties and Privacy Groups that oppose such initiatives are engaging into contrary political acts.* ***Depending on the degree of penetration in influencing public opinion, subsequent reactions from the social stratum can swiftly transform into economic reactions.*** There simply is no way of knowing the changing degree of penetration and/or the sensitivity to privacy whereas the penultimate risks in getting such eID schemes wrong manifest themselves into two distinct directions:

> ***a1)*** *Lack of public confidence in the scheme creates mistrust to the level where the eID is constantly being undermined and misused (security implications also arise)*

> ***a2)*** *The scheme might actually inhibit economic activity if increased vigilance and sensitivity to privacy concerns makes people reluctant as users and might at the same time force them to seek alternative ways of either verifying their identity or bypassing the system itself. Such a risk is particularly relevant to cases where an eID scheme is related to other industry sectors that are themselves heavily reliant on identity verification (with the financial services being the most likely candidate)*

b) **Information Exchange, New Markets and Labour:** The issue of interoperability as analysed at different levels (see previous section) creates and reinforces the need for information exchange and for *generating information out of information.* Depending on the level of interoperability reached across a wide variety of eID schemes, different services could utilise aspects of such schemes and create opportunities for businesses on the basis of schemes that are controlled and/or significantly operated by governments. The creation of new markets is something that should also be considered in terms of the long-term economic effects of such large-scale technological implementations. *Potential uses of the eID scheme (or aspects of it) could open up opportunities into markets that might benefit from incorporating or basing future implementations on the eID scheme, or even create totally new markets based on needs that will eventually emerge and cannot be a priori determined.* Politicians however that use this as a core argument for the proposals (namely that even in problematic scenarios new opportunities and markets emerge) usually forget that a balance must also be struck *with the already existing infrastructure.* Changes, new opportunities and markets will have to be based on the evolution of pre-existing schemas and in the cases where this process is severely disrupted then one cannot easily foresee the extent of the consequences. Labour will also be based upon such a distinction and balance of new opportunities but that is also something that has to be properly coordinated and governments

[312] Assisted by technology and sourcing from a variety of motives (fight against terrorism, control of the state, etc)

must actively pursuit and encourage new directions for the workforce and assist in new opportunities, be those in research, development or business.

7.4 Conclusions

From the aforementioned elements and the analysis that has been carried out, it becomes evident that there is a variety of factors that influence both the cost-projections for an eID scheme, but also, that there are other several elements at play that make the examination of a scheme's economic impact considerably difficult. The complexity of any proposed eID scheme is a major presupposition behind such a statement and it is argued that the more complex the proposed scheme, the more difficult it becomes to carry out an effective, reliable and as close to the reality of the actual implementation, cost-projection. There are also highly contextual aspects within each implementation context (at a national level) which can only be taken into account after careful and considerate research in each context. *In this respect, interoperability can be seen as creating problems rather than dissolving them.* The logic behind such a statement is simple; interoperability is necessary in order for the pan-European effectiveness of a scheme, however interoperability means also that schemes will have to conform to particular structures, whereas the same set of rules, structures or processes cannot be diffused with the same success across different cultural contexts. On the basis then of increased interoperability in eID schemes, cultural differences become more visible and can potentially inhibit rather than support mobility (coupled with privacy concerns and use of sensitive information). Further reflection and identification on these aspects can also lead towards particular studies of interoperability that will account for such cross-context implementation.

A number of elements critical in cost-projection are:

- Period of implementation
- Number of participants
- Enrolment phase
- Type of Identity Document chosen for the implementation
- Resistance to change
- Cultural Aspects

The aforementioned elements however refer only to the implementation phase. From that, we can distinguish two important phases before and after the implementation of Identity documents. Considerable research needs to be undertaken prior to the implementation itself something that might include surveys, pilot tests, and/or other research methods. This is even more critical when Identity Documents themselves are used for access to a variety of services apart from identification purposes alone.

Post-implementation there are also critical aspects that influence the actual cost of the scheme (ongoing costs). For example:

- Security aspects
- Privacy aspects
- Renewal of Identity documents and Register updates
- Handling of complaints and false negatives
- Internal Audits
- Costs of management of the register
- Infrastructural costs and Integration

Governments need to consult extensively with industry bodies and organisations that might assist in both the implementation and the cost-projection of any scheme, but also take into consideration the more subtle aspects that are relevant for their people within the national context, provide training where needed and ensure the viability of the scheme without jeopardising privacy or security.

8 Summary, Conclusions and Outlook

In this document basic technologies used or proposed for official electronic ID documents have been described and analysed with respect to privacy and security.

Chip card technology has been discussed, used and further developed for many years now. As a result this technology is accepted as mature by technicians and privacy commissions in Europe. Of course, the combination of chip card technology with other technologies such as biometrics can result in new questions concerning security and privacy.

PKI also has been used for ID document systems in some European countries for 9 years now, though the number of issued certificates still seems to be limited. No major security problems have been published. PKI currently does not implement privacy in an optimised way because of the existing linkability of transactions performed via the information in the certificates. Current technical approaches to improve the privacy compliance for authentication purposes using eIDs have been presented and analysed.

In difference to these established technologies the use of biometrics and RFID in ID documents is relatively new. The first European ID document using both of these technologies is the **European passport**. RFID and biometrics raise a number of obvious privacy and security issues.

In addition to well documented security aspects of biometrics, for example with respect to (1) the quality of biometric identification, (2) identity theft and (3) devaluation of classic forensic techniques, a number of privacy aspects still needs to be addressed. This includes (1) minimisation of linkability, (2) enforcement of the purpose binding principle and (3) avoidance of additional, in many cases health concerning, information in biometric raw data. Advanced technical approaches for authentication using biometrics have not been tested for or implemented in ID documents so far.

RFID originally have been designed for unrestricted remote access to the information stored on RFID tags. For the use of RFID in the European passport basic security measures, for example Basic Access Control (BAC), have been applied to restrict the unauthorised access. BAC seems to be cryptographically weak and uses information stored in the Machine Readable Zone (MRZ) on the document itself; this is like printing the corresponding PIN on a banking card. Together with well documented projects of non-European countries aiming at the storage of biometric data of foreign visitors in large databases[313], this creates a significant risk of identity theft via biometrics in cases the document is (even properly!) used or gets lost. A number of additional security and privacy methods currently in discussion or development such as applying a “Kill Command” cannot be used in a meaningful way with RFID in ID documents. Other methods such as integrating a Faraday cage in the cover of the European passport are not implemented.

From the technological perspective biometrics and RFID as implemented in the European passport do not seem mature. For the use of the European passport as issued currently we suggest:

- The European passport should be used and carried around only when necessary.

[313] For example: USA; see http://de.wikipedia.org/wiki/Biometrie

- In case the European passport is not used, it should be kept in a Faraday cage (for example aluminium foil) to hamper unauthorised and unrecognised access.
- In case the European passport is not used, it should be locked carefully to avoid loss or theft of the document.

Organisational implementation and enforcement of the finality principle is required, especially for biometrics used in European passports, where the defined purpose is identification of international travellers. Passports should not be used for authentication purposes, e.g., in the private sector. Citizens need to be informed of the risks inherent in owning, carrying and using their passports and the corresponding security measures which can be undertaken by them (see above). Security measures such as Faraday cages, which are available but not widely implemented, should be integrated into newly issued Passports immediately. In addition organisational and technical procedures are required to prevent abuse of personal data from Passports, including tracking and identity theft.

For the next generation of the European passport, a new convincing and integrated security framework covering MRTDs and related systems needs to be developed. It should be investigated how the implementation of technologies utilised can be improved, e.g., on-card matching and on-card sensors for biometrics and it should be considered whether inherently more secure and privacy-preserving technologies such as contact instead of contactless mechanisms should in fact be used.

In addition the criteria for eIDs suggested by Niels Bjergstom (see chapter 5.8.2) should be taken into consideration. In this context the following criteria seem to be especially important:

- It must not depend on irreplaceable personal characteristics to cope with the problem of compromised or lost/changed characteristics
- The token containing the eID must be replaceable without undesirable consequences, i.e. theft or loss of a token must not enable impersonation
- All its functions, including any disclosure of information in the token, must be fully controlled by the owner

Concerning future ID documents and the further development of the European passport the following suggestions subsequently should be taken into consideration:

- The use of RFID should be considered carefully, especially as many problems concerning unauthorised and unobserved access from distances up to 10 m are not sufficiently technically solved today. Alternatively chip card technology can be used.
- The use of biometrics should be considered carefully due to security and privacy problems this technology potentially causes. In cases biometrics is needed, advanced implementation taking security and privacy aspects into consideration should be used.

This includes (1) the use of templates, (2) decentralised storage of data in the documents only and (3) on-card matching procedures for authentication.

In the legal chapter current European initiatives regarding machine-readable documents with biometrics have been described: Eurodac (the EU central fingerprint database in connection with asylum seekers), the Visa Information System (VIS – the EU central database set up to create a common visa policy) and the European Passport (requiring fingerprints and facial images as biometrical identifiers). These initiatives are analysed with respect to the European data protection and privacy framework resulting in the following conclusions:

- The European data protection and privacy frameworks apply to the Regulations but in no case this means that the Regulations are a priori compliant neither with the Data Protection Directive nor with the ECHR. In addition machine-readability of people and of their documents may turn out to be excessive, hereby surpassing the necessity and proportionality criteria set out by the European Court of Human Rights.
- The legal basis itself of the VIS and EU passport Regulations is questioned. While the VIS is in fact a 'first pillar' database, the Proposal provides for access possibilities by 'third pillar authorities' – for which normally other legal grounds than Articles 62 and 66 of the TEC must be invoked. While the EU regulates its passport on the basis of standards established by non-democratic standardisation bodies (ICAO), Article 18 (3) of the TEC even excludes the adoption of provisions by the EC on passports, identity cards, residence permits or any other such document.
- Eurodac, the EU passport and the VIS are subject to possible function creep that is not foreseeable. The impact of this deployment and the future of identity can – regrettably – not be entirely assessed at this moment. A step-by-step approach seems the essential requirement to safeguard the fundamental rights and freedoms.

In the following chapter a study written by Thomas Myhr with respect to a European legal framework for ID documents is compared with the results of a similar discussion in the Porvoo group. Still a lot of research in this area is necessary to get a clear view on:

- what regulation exists about visual and electronic ID documents in the EU member states and which "common umbrella" can be found in these regulations,
- what the remaining issues are, and how they can be solved,
- which the limits are for EU regulation and/if the issues can be solved without regulation (e.g. via standardisation).

In addition to an overview on existing eIDs five existing projects for the implementation of eIDs and three innovative technological concepts have been analysed in this document with respect to factors of success concerning the implementation. The following factors could be concluded:

- Careful planning especially concerning the purpose of the eID and the appropriate technical solution (keep it small and smart); this should include technical, formal and informal aspects of interoperability
- Intensive laboratory and field testing of prototypes
- Refinement of the concepts using the results of the testing phase
- Open communication within the project including all stakeholders of the eID and external experts
- Appropriate education and qualification of the personal involved in the project

Finally economic factors that are relevant for eIDs were analysed. A number of elements that are critical for the cost projection have been elaborated and described. In addition the post implementation costs have to be calculated carefully to get a view on the Total Costs of Ownership (TCO) for an eID solution. Relevant factors in this context are:

- Security aspects
- Privacy aspects
- Renewal of identity documents and register updates
- Handling of complaints and false negatives
- Internal audits
- Costs of management of the register
- Infrastructural costs and integration

9 References

27th International Conference of Data Protection and Privacy Commissioners, *Resolution on the use of biometrics in passports, identity cards and travel documents*, Montreux 16th of September 2005. http://www.edps.eu.int/legislation/05-09-16_resolution_biometrics_EN.pdf.

'2b or not 2b – Evaluatierapport Biometrieproef 2b or not 2b', Ministrie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Amsterdam 2005. http://www.minbzk.nl/contents/pages/43760/evaluatierapport1.pdf.

Alterman, A., 'A Piece of yourself: Ethical issues in biometric identification', *Ethics and Information Technology* 5, 2003, pp. 139-150.

Arndt, C., 'The loss of privacy and identity', *Biometric Technology Today,* 2005.

Article 29 Data Protection Working Party (2003), *Working Document on Biometrics*, 12168/02/EN, WP 80, adopted on 1 August 2003. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf.

Article 29 Data Protection Working Party (2004), *Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)*, 11224/04/EN, WP 96, adopted on 11 August 2004. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_en.pdf.

Article 29 Data Protection Working Party (2005a), *Working Document on Data Protection Issues Related to RFID Technology,* 10107/05/EN, WP 105, 19 January 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

Article 29 Data Protection Working Party (2005b), *Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final*, 1022/05/EN, WP 110, adopted on 23 June 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_en.pdf.

Article 29 Data Protection Working Party (2005c), *Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (WP 112), 1710/05/EN-rev, WP 112, Official Journal* L 385, 29 December 2004, pp. 1-6, adopted on 30 September 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_en.pdf.

Avoine G., Oechslin P., 'RFID Traceability: A multilayer problem', *Financial Cryptography* – FC'05, Lecture Notes in Computer Science, Springer, Heidelberg, 2005.

Backhouse, J. (Ed.), *FIDIS Deliverable 4.1 – Structured account of approaches on interoperability*, Frankfurt a. M. 2005. See http://www.fidis.net/fidis_del.0.html

AXSionics.AG, 'About Us'. http://www.axsionics.ch/. Accessed on 10.08.2005.

Backhouse, J., 'Information @ Risk', *Information Strategy,* December/January 2000, pp. 33-35.

Backhouse, J., Hsu, C., McDonnell, A., 'Technical Opinion: Toward Public-Key Infrastructure Interoperability', *Communications of the ACM,* 46 (6), 2003, pp. 98-100.

Beel, J., Gipp, B., *ePass – der neue biometrische Reispass*, Shaker Verlag, Aachen 2005. Chapter 6 "Fazit" can be downloaded via http://www.beel.org/epass/epass-kapitel6-fazit.pdf.

Bennett, C. J., 'Evidence of Policy Convergence' in *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, Cornell University Press, New York, 1992, pp. 95-115, Chapter 3.

Bennett, C. J., Raab, C. D., 'The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response', *The Information Society,* 13 (3), 1997, pp. 245-264.

Bertalanffy, L., *General System Theory,* George Braziller Inc., New York, 1969.

'Biometric Deployment of Machine Readable Travel Documents – ICAO TAG MRTD/NTWG', Version 2.0, ICAO, Montreal 2004. http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf.

Bjergstrom, N., 'Basic Man-Machine Introductions', *Speech on InfoSeCon*, Dubrovnik, 8 June, 2005.

Borchers, D., 'Kritik am ePass', *c't* (21) 2005, p. 60, Heise Zeitschriften Verlag, Hannover 2005.

Brito, J., 'Relax, do not do it: Why RFID privacy concerns are exaggerated and legislation is premature', *UCLA Journal of Law and Technology*, 8 (2), Fall 2004. http://www.lawtechjournal.com/articles/2004/05_041220_brito.pdf.

Brooks, L., 'Structuration Theory and New Technology: Analysing Organizationally Situated Computer-Aided Design (Cad)', *Information Systems Journal,* 7 (2), 1997, p. 133.

CAP Gemini Ernst Young, 'Online Availability of Public Services: How Does Europe Progress?', Brussels, 2003.

Cavoukian, A., 'Tag, you're it: Privacy implications of radio frequency identification (RFID) technology', February 2004. http://www.ipc.on.ca/images/Resources/up-rfid.pdf.

CEN/ISSS (2004), 'Towards an electronic ID for the European Citizen, a strategic vision', *CEN/ISSS Workshop eAuthentication,* Brussels, 03.10.2004, pp. 1-71. http://europa.eu.int/idabc/servlets/Doc?id=19132.

Chen, W., Hirschheim, R., 'A Paradigmatic and Methodological Examination of Information Systems Research from 1991 to 2001', *Info Systems,* 14, 2004, pp. 197-235.

Chua, W. F., 'Radical Developments of Accounting Thought', *Accounting Review,* 61, 1986, pp. 601-632.

CIA, 'The World Factbook 2002'. http://www.faqs.org/docs/factbook/. Accessed on 15.03.2005.

Cowcher, R., '*Current Issues on Interoperability* 09.03.05'. (Personal communication.)

.De Hert, P., Gutwirth, S., 'Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence' in IPTS, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*. *Report to the European Parliament Committee on Citizens' Freedoms*

and Rights, Justice and Home Affairs (LIBE), July 2003, IPTS-Technical Report Series, EUR 20823 EN, pp. 111-162.

De Hert, P., Gutwirth, S., 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of the power', in Claes, E., Duff, A., Gutwirth, S. (Eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2005, pp. 61-104.

Der Standard, 'Bei E-Card drohen Millionen an Mehrkosten'. http://derstandard.at/. Accessed on 05.08.2005.

Dhillon, G., Backhouse, J., 'Current Directions in Is Security Research: Towards Socio-Organisational Perspectives', *Information Systems Journal,* 11 (2), 2001, pp. 127-153.

Engberg, S. J., '*FIDIS WP 5 Workshop* Open Business Innovation', Tilburg, 2005.

Enterprise DG, 'Networking of Public Administrations – the Ida Mission'. http://europa.eu.int/idabc/en/document/78/25. Accessed on 07.03.2004.

Etzioni, A. (Ed.), *The Limits of Privacy*, Basic Books, New York, 1999, pp. 183-215.

European Commission, 'The Role of eGovernment for Europe's Future', 2003.

European Commission, 'e-Europe 2005 Midterm Review', 2004a.

European Commission, 'Linking up Europe: The Importance of Interoperability for eGovernment Services', 2004b.

European Commission, 'Vol. June 2005 (IDABC) European Commission', 2005, p. 25.

European Data Protection Supervisor, 'Opinion of 20 January 2006 on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM (2005) 600 final)'. http://www.edps.eu.int/.

European Parliament, 'Vol. Article 8 European Parliament', 2000.

European Parliament, 'Fact Sheets 1999-2002', 2002. http://www.europarl.eu.int/factsheets/default_en.htm. Accessed on 22.08.2005.

Eurostat, 'European Demography in 2003'. 31 August 2004. http://epp.eurostat.cec.eu.int/cache/ITY_PUBLIC/3-31082004-BP/EN/3-31082004-BP-EN.PDF.

Fishkin, K. P., Roy, S., Jiang, B., 'Some methods for privacy in RFID communication', *European Workshop on Security in Ad-Hoc and Sensor Networks* (ESAS 2004), Lecture Notes in Computer Science 3313, Springer, Heidelberg, 2004, pp. 42-53.

Floerkemeier, C., Schneider, R., Langheinrich, M., 'Scanning with a purpose – supporting the fair information principles in RFID protocols.' Paper presented at *2nd International Symposium on Ubiquitous Computing Systems* (UCS 2004), November 2004. http://www.vs.inf.ethz.ch/publ/papers/floerkem2004-rfidprivacy.

Forastieri, V., 'Evidence against a Relationship between Dermatoglyphic Asymmetry and Male Sexual Orientation', *Human Biology* No. 74/6, Wayne State University Press, Detroit, 2002, pp. 861-870.

Foucault, M., *Discipline and punish: the birth of the prison.* Harmondsworth: Penguin, 1977.

Freh, S., 'Analysis of Global eID Projects with Focus on Interoperability by Using the TFI Model', 2005a.

Freh, S., 'Talent & Income Statements: The New "Freihändler" of Europe', 2005b.

Friedrich, E., Seidel, U., 'The introduction of the German e-passport. Biometric passport offers first-class balance between security and privacy', *Keesing Journal of Documents & Identity*, Issue 16, 2006, pp. 3-6.

Fusaro, R. A., 'None of our business?', *Harvard Business Review*, 82 (12): December 2004, pp. 33-38.

Garfinkel, S., Rosenberg, B. (Eds.), *RFID – Applications, Security, and Privacy*, Addison-Wesley, New York 2005.

Garfinkel, S., 'An RFID bill of rights', *MIT Technology Review*, Oct. 2002, p. 35.

Gasson, M., Meints, M., Warwick, K. (Eds.), *FIDIS Deliverable 3.2 – Study on PKI and Biometrics*, Frankfurt a. M. 2005. See http://www.fidis.net/487.0.html

Gaubatz, G., Kaps, J.-P., Sunar, B., 'Public key cryptography in sensor networks – revisited', in Castelluccia, C., et al. (Eds.), *European Workshop on Security in Ad-hoc and Sensor Networks* (ESAS 2004), Lecture Notes in Computer Science 3313, Springer, Heidelberg, 2004, pp. 2-18.

Geradts, Z., Sommer, P., *FIDIS Deliverable 6.1 – Forensic Implications of Identity Management Systems*, Frankfurt a.M., 2005. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf.

GUIDE, 'Creating a European Identity Management Architecture for eGovernment'. http://istrg.som.surrey.ac.uk/projects/guide/. Accessed on 20.03.05.

GUIDE, 'Deliverable D1.2.1.B Identity Interoperability Service Report: Core Service Descriptions', Version 2.0, Brussels 2005. http://istrg.som.surrey.ac.uk/projects/guide/files/documents/D1.2.1.B.pdf.

Hall, J. A. Y., Kimura D., 'Dermatoglyphic Asymmetry and Sexual Orientation in Men', *Behavioral Neuroscience*, No. 108, APA Press, Washington, 1994, pp. 1203-1206. http://www.sfu.ca/~dkimura/articles/derm.htm.

Hansen, M., et al., 'Identity Management Systems (IMS): Identification and Comparison Study', *Independent Centre for Privacy Protection Schleswig-Holstein and Studio Notarile Genghini,* 2003. http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf.

Hayat, A., et al., 'Survey on EU's Electronic-ID Solutions', Vienna, 2004.

Hes, R., et al., *At face value. On biometrical identification and privacy*, Registratiekamer, The Hague, September 1999. http://www.dutchdpa.nl/downloads_av/AV15.pdf.

Hildebrandt, M., Backhouse, J. (Eds.), *FIDIS Deliverable D7.2 – Descriptive analysis and inventory of profiling practices*, Frankfurt a.M., 2005. See http://www.fidis.net/.

Hildebrandt, M., Gutwirth, S. (Eds.), *FIDIS Deliverable D7.4 –* I*mplications of profiling on democracy and the rule of law*, Frankfurt a.M., 2005. See http://www.fidis.net/.

Hoepman, J.-H., Jacobs, B., 'E-passports without the big picture', eG*ov monitor*, 20 February 2006, available through http://www.egovmonitor.com/node/4716.

Hollosi, A., 'Requirements for Interoperability in IMS at the Example of Austria's Bürgerkarte', 2005. (Personal communication.)

Hollosi, A., Karlinger, G., 'Die Österreichische Bürgerkarte: Einführung', 2005.

Home Affairs Committee, Vol. Fourth Report (Committee, H. A.), 2004.

Jain, A., Hong, L., Pankanti, S., 'Biometric Identification', *Communications of the ACM* No. 43/2, New York, 2000, pp. 91-98.

ICA 35th Conference Report, 'Round Table Report: Austria'. http://egov.alentejodigital.pt/Austria/ICA_austria.pdf. Accessed in October 2001.

Information Society and Media DG, 'eGovernment Interoperability and Pan-European Services', 2005a. http://europa.eu.int/information_society/activities/egovernment_research/focus/interoperability/index_en.htm#projects.

Information Society and Media DG, 'Search for Individual Research Projects Funded under FP5 and FP6 by the IST Programme', 2005. http://www.cordis.lu/ist/projects/projects.htm.

International Civil Aviation Organization, 'Document 9303' and 'Standard for ePassports', Montreal 2004. Download: http://www.icao.int/mrtd/publications/doc.cfm.

International Organization for Standardization / International Electrotechnical Commission: Numerous standards mentioned in the chapters 3.2 and 6.5.

Jacobs, B., 'Biometrische gegevens horen niet in een databank' (translated: Biometrical data do not belong in a database)', *Volkskrant Forum*, 28 February 2006. http://www.cs.ru.nl/B.Jacobs/PRESS/volkskrant-28-2-06.txt.

Juels, A., 'Minimalist cryptography for low-cost RFID tags (extended abstract)', in Blundo, C., Cimato, S. (Eds.), *Fourth International Conference on Security in Communication Networks* – SCN 2004, Lecture Notes in Computer Science 3352, Springer, Heidelberg, 2004, pp. 149-164.

Juels, A., 'Strengthening EPC tags against cloning.' Manuscript, October 2004.

Juels, A., Pappu, R., 'Squealing Euros: Privacy protection in RFID-enabled banknotes', in Wright, R. (Ed.), *Financial Cryptography*, Lecture Notes in Computer Science 2742, Springer, Heidelberg, 2003, pp. 103-121.

Juels, A., Rivest, R. L., Szydlo, M., 'The blocker tag: selective blocking of RFID tags for consumer privacy', in *10th ACM Conference on Computer and Communication Security*, ACM Press, New York, 2003, pp. 103-111.

Kinder, T., 'Mrs Miller Moves House: The Interoperability of Local Public Services in Europe', *Journal of European Social Policy,* 13 (2), 2003, pp. 141-157.

Klischewski, R., 'Top Down or Bottom Up? – How to Establish a Common Ground for Semantic Interoperability within E-Government Communities', 2000.

Kocher, P. C., *Timing Attacks on Implementations of Diffie-Hellmann, RSA, DSS, and Other Systems,* Internet 1995.

Kocher, P. C., Jaffe, J., Jun, B., *Introduction to Differential Power Analysis and Related Attacks,* 1998. http://www.cryptography.com/resources/whitepapers/DPATechInfo.pdf.

Krissler, J, Kurz, C., 'Die Ergebnisse der BioP2-Studie zur Leistungsfähigkeit biometrischer Systeme', *FIfF Kommunikation* (4) 2005, FIfF, Bremen 2005.

Leitold, H., 'Requirements for Interoperability in IMS at the Example of Austria's Bürgerkarte', 2005.

London School of Economics and Political Science, 'The Identity Project: An Assessment of the UK Identity Card Bill & Its Implications' *The Department of Information Systems,* London, 2005.

Luckett, D., 'The supply chain', *BT Technology Journal*, 22 (3), London, July 2004, pp. 50-55.

Luhmann, N., *Social Systems,* Stanford University Press, Stanford, 1995.

Lyon, D., 'The Electronic Eye: The Rise of Surveillance Society', *Polity Press,* pp. 22-39, Chapter 2, 1994.

McGinity, M., 'RFID: Is this game of tag fair play?', *Communications of the ACM*, 47 (1), New York, 2004, pp. 15-18.

Markus, L., Robey, D., 'Information Technology and Organizational Change: Causal Structure in Theory and Research', *Management Science,* 34 (5), 1988, pp. 583-599.

Martin, B., in *eGovernment Workshop* Vienna, 2004.

Martin, B., in *FIDIS Workshop D3.5,* IKT-Stabstelle, Frankfurt, 2005.

Mayer-Schönberger, V., 'Generational Development of Data Protection in Europe' in *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, Cornell University Press, New York, 1992, pp. 219-241, Chapter 8.

Mead, G. H., *Mind, Self and Society*, Chicago Press, 1934.

Meints, M., Hansen, M., Bauer, M. (Eds.), *FIDIS Deliverable D3.1 – Overview on Identity Management Systems*, Frankfurt a.M., 2005. See http://www.fidis.net/fidis_del.0.html

Miller, B., 'Towards a Framework for Managing the Information Environment', *Information, Knowledge, Systems Management,* 2, 2001, pp. 359-384.

Mingers, J., 'Combining Is Research Methods: Towards, a Pluralist Methodology', *Information Systems Research,* 12 (3), 2001, pp. 240-259.

Molnar, D., Wagner, D., 'Privacy and Security in Library RFID: Issues, Practices, and Architectures', in *11th ACM Conference on Computer and Communications Security* (CCS), ACM Press, New York, 2004, pp. 210-219.

Müller, L., *Discussion of the Possibilities of PETs Nowadays and in the near Future* 21.06.2005. (Personal communication.)

Nabeth, T., Hildebrandt, M. (Eds.), *FIDIS Deliverable D2.1: Inventory of topics and clusters*, Frankfurt a.M., 2005. See http://fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.1_Inventory_of_topics_and_clusters.pdf.

NETC@RDS, 'Project Information'. http://www.netcards-project.com/projectinfo.php. Accessed on 03.08.2005.

News aktuell GmbH, ZDF, 'ZDF-Reporter zeigt, wie EU-Bürger Arbeitslosengeld II kassieren können'. http://shortnews.stern.de/shownews.cfm?id=584278. Accessed on 22.08.2005.

OECD Working Party on Information Security and Privacy, *Background material on biometrics and enhanced network systems for the security of international travel*, 23 December 2004, 53 p. http://www.oecd.org/dataoecd/16/18/34661198.pdf.

ORF.at, 'Die unendliche Geschichte der E-Card'. http://www.orf.at/050805-89910/89915txt_story.html. Accessed on 05.08.2005.

Orlikowski, W.J., Baroudi, J.J., 'Studying Information Technology in Organizations: Research Approaches and Assumptions', *Information Systems Research,* 2 (1), 1991, pp. 1-28.

Orwell, G., *Nineteen Eighty Four,* Harmondsworth: Penguin, New York, 1949.

Otter, H., *Requirements for Interoperability in IMS at the Example of Austria's eCard* 30.06.2005. (Personal communication.)

Otter, H., *Managing Identity,* German Embassy Info Center, 2005b.

Ouksel, A., 'A Framework for a Scalable Agent Architecture for Cooperating Heterogeneous Knowledge Sources' in Klusch, M. (Ed.), *Intelligent Information Age: Cooperative, Rational and Adaptive Information Gathering in the Internet*, Springer, Chapter 5, 1999.

Ouksel, A.M., Sheth, A., 'Semantic Interoperability in Global Information Systems', *SIGMOD Record,* 28 (1), 1999, pp. 5-12.

Payette, S., et al, 'Interoperability for Digital Objects and Repositories', *D-Lib Magazine,* 5 (5), 1999, pp. 41-68.

Peers, S., 'The Legality of the Regulation on EU Citizens' Passports', 26 November 2004, pp. 1-4. http://www.statewatch.org/news/2004/nov/legal-analy-bio-passports.pdf.

Pfitzmann, A., Hansen, M. (Eds.), Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, v0.28, 29 May 2006. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.

Posch, R., Holzbach, M., 'The Austrian Citizen Card – Citizen Card Concept.' http://www.buergerkarte.at/en/was_ist_die_buergerkarte/konzept_buergerkarte.html. Accessed on 05.07.2005.

Posner, R. A., 'John A. Sibley Lecture: The Right of Privacy', *Georgia Law Review,* 12 (3), 1978.

Prins, J. E. J., 'Making our body identify for us: legal implications of biometric technologies', *Computer, Law & Security Report*, 1998, Vol. 14, No. 3, pp. 159-165.

Privacy International, *About Privacy International,* 2005. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65428. Accessed on 18.07.2005.

Rankl, W., Effing, W., *Smart Card Handbook*, John Wiley & Sons, New York, 2003.

Realini, A., 'G2G E-Government: The Big Challenge for Europe', Master's Thesis. Version: 1.1, 2004. http://www.ifi.unizh.ch/egov/Diplomarbeit_Realini.pdf.

Riedl, R., *Affordance in E-Government. In Electronic Government: Second International Conference, Proceedings / eGov 2003,* Springer, Prague, Czech Republic, 2003.

Ringwald, A., 'Electronic Identity: eEurope Smart Cards / Trailblazer 1 "Public Identity"' *eEurope* Paris, 2003.

Schnittger, B., 'Introducing IDABC: European Integration by Electronic Means', *SYNeRGY,* (01), 2005, pp. 3-6.

Schreurs, W., Hildebrandt, M., Gasson, M., Warwick, K. (Eds.), *FIDIS Deliverable D7.3 – Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, Frankfurt a.M., 2005. See http://www.fidis.net/.

Sozialversicherungs-Chipkarten Betriebs- und Errichtungsgesellschaft m.b.H., 'Leistungen'. http://www.chipkarte.at/esvapps/page/page.jsp?p_pageid=220&p_menuid=51921&p_id=5. Accessed on 16.07.2005.

Sun Microsystems, *Java Card Platform Specification v2.2.2*, 2006. Download: http://java.sun.com/products/javacard/index.jsp.

Stalder, F., Lyon, D., *Electronic Identity Cards and Social Stratification,* Routledge, New York, 2002.

Stamper, R., et al., 'Understanding the Roles of Signs and Norms in Organizations: a Semiotic Approach to Information Systems Design', *Behaviour & Information Technology,* 19, 2000, pp. 15-27.

Singer, R., 'Nun Terrorized by Terror Watch', Wired 2005. http://www.wired.com/news/privacy/0,1848,68973,00.html?tw=wn_tophead_1, 2005.

Swann, P., Temple, P., Schurmer, M., 'Standards and Trade Performance: The UK Experience', *The Economic Journal,* 106 (438), 1996, pp. 1297-1313.

Teodori, M., *L'Europa Non Ê L'America,* Arnoldo Mondadori Editore, Milano, 2004.

University of Ottawa, *Legal Systems,* University of Ottawa, http://www.droitcivil.uottawa.ca/world-legal-systems/eng-presentation.html. Accessed on 01.08.2005.

'Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen – BioP II', German Federal Office for Information Security (BSI), Bonn 2005. http://www.bsi.de/literat/studien/biop/biop_2.htm.

Vanfleteren, M., Kindt, E., *Use of Credentials Systems in E-Commerce*, Katholieke Universiteit Leuven, London, 2005.

Van Kralingen, R., Prinis, C., Grijpink, J., *Het lichaam als sleutel. Juridische beschouwingen over biometrie [translated: The body as key. Legal observations on biometrics]*, ITER 1997.

Want, R., 'RFID: A key to automating everything', *Scientific American*, No. 290(1), New York, 2004, pp. 46-55.

Warren, S., Brandeis, L., 'The Right to Privacy', *Harvard Law Review,* (193), 1890.

Wayman, J., 'Linking Persons to Documents with Biometrics. Biometric systems from the 1970s to date'*, Keesing Journal of Documents & Identity*, Issue 16, 2006, pp. 14-19.

Weis, S., Sarma, S., Rivest, R., Engels, D., 'Security and privacy aspects of low-cost radio frequency identification systems', *First International Conference on Security in Pervasive Computing*, Lecture Notes in Computer Science 2802, Springer, Heidelberg, 2003, pp. 201-212.

Weiss, A., 'Me and my shadow', *ACM netWorker,* 7(3), New York, 2003, pp. 24-30.

Westin, A. F., 'The Function of Privacy in Society', in *Privacy and Freedom,* New York, 1967, pp. 8-21, Chapter 1.

10 Glossary and Abbreviations

AES	Advanced Encryption Standard; cryptographic algorithm developed by Joan Daemen and Vincent Rijmen in 1996 and selected 1997 by the National Institute for Standards and Technology (NIST) in the US to be the successor of the old Digital Encryption Standard (DES)
AFIS	Automated Fingerprinting Identification Systems
ARLs	Authority Revocation Lists used in the context of the Belgian ID card
AP	Authentication Provider
ASP	Attribute Service Provider
Authentication	Verification of the identity of a person, a technical system or a process
BAC	Basic Access Control, security mechanism using cryptographic algorithms to protect the RFID of a MRTD against unauthorised access
CA	Certificate Authority
CIE	Carta d'Identità Elettronica, Italian ID card
CRLs	Certificate Revocation Lists used in the context of the Belgian ID card
CRR	Citizens Register of Residents (Zentrales Melderegister) used in the context of the Austrian "Bürgerkarte"
CSP	Certification Service Provider
DC	Digital Certificates
DNS	**D**eoxyribo**n**ucleic **A**cid
EAC	Extended Access Control, security mechanism proposed by the German Federal Office for Information Security (BSI) to enhance the protection of RFID used in MRTDs against unauthorised access compared to BAC
ECHR	European Charta of Human Rights
EDPS	European Data Protection Supervisor
EER	Error to Enrol Rate
eID	Electronic IDentity
EPC	Electronic Product Code
FAR	False Acceptance Rate; successful authentication of a using biometric systems caused by failure of these biometric authentication systems

FRR	False Rejection Rate; failed authentication using biometric systems caused by failure of these biometric authentication systems
G2C	Government to Citizen
G2G	Government to Government
ICAO	International Civil Aviation Organisation
IP	Identity Provider
MRZ	Machine Readable Zone of ID documents
MRTD	Machine Readable Travel Document
NIR	National Identity Register
OCR	Optical Character Recognition
PEGS	Pan-European Governmental Service
PET	Privacy Enhancing Technologies
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
PRC	Population Register Centre used in the context of the FINEID
RA	Registration Authorities
RFID	Radio Frequency Identification
RFID tag	Silicon chip with directly attached antenna for radio frequency transmission of data stored on the chip
RSA	(1) Asymmetric cryptographic algorithm developed by Rivest, Shamir and Adleman in 1977 (2) RSA Security Inc.; American enterprise specialised on security solutions and products
SATU	Unique electronic client identifier used in the context of the FINEID
SIM	Subscriber Identification Module
SR	Supplementary Register (Ergänzungsregister), used in the context of the Austrian "Bürgerkarte"
sPIN	Source Personal Identification Number used in the context of the Austrian "Bürgerkarte"
ssPI	Sector specific Personal Identifier used in the context of the Austrian "Bürgerkarte"
TEC	Treaty establishing the European Communion
TFI	Model to analyse interoperability in three layers: Technical, Formal and Informal

TTPS	Trusted Third Party Services
UHF	Ultra High Frequency (500 to 1000 MHz)
VIS	Visa Information System
XML	eXtensible Markup Language
WP29	Article 29 Data Protection Working Party

11 Appendices

11.1 List of Figures

Figure 1: Overview of important international standards for smart cards. 18

Figure 2: A transparent sample epassport showing the normally visible MRZ at the bottom and the normally hidden RFID loop antenna with the small RFID tag in the antenna top left which holds the biometric data..... 19

Figure 3: Electromagnetic spectrum showing the broad range of the radio wave frequency component 20

Figure 4: The two main components of the RFID system 20

Figure 5: International authentication and authorisation using GUIDE interfaces and services 26

Figure 6: Gateways transforming nationally used data formats and standards for authentication 27

Figure 7: Modified TFI model, influenced by the Open Systems Framework of Social Interaction..... 30

Figure 8: Number of Global Countries (EU 25 excluded) Supporting Various eID Functionalities 34

Figure 9: Number of EU 25 Countries Supporting Various eID Functionalities..... 35

Figure 10: eID Solutions in Countries Categorised by Legal Systems World-Wide..... 36

Figure 11: eID Solutions in Countries Categorised by Legal Systems in the EU..... 37

Figure 12: Calculation of the source PIN..... 92

Figure 13: Conversion between Souce PIN and ssPI..... 93

Figure 14: Use of the ssPI for secure data storage 93

Figure 15: Belgian eID card's visual aspects..... 94

Figure 16: Belpic eID CA structure 97

Figure 17: Concept of the storage of data in the German e-health card..... 100

Figure 18: Possible attacks on the communication points of biometric systems 107

Figure 19: Architecture of today's PCs; application data can have direct access to the BIOS or hardware peripherals (left); secure architecture principle in smart cards where the applications must pass through a security kernel to have no direct access to the hardware & peripherals. 123

Figure 20: Costs for the issuing of the eID card in UK..... 136

Figure 21: Cost projection of the eID card in UK (1/3)..... 137

Figure 22: Cost projection of the eID card in UK (2/3)..... 138

Figure 23: Cost projection of the eID card in UK (3/3)..... 139

11.2 List of Tables

Table 1: Purposes of ID documents 14
Table 2: Overview on technologies used for eID documents 15
Table 3: Biometrics summary table 57
Table 4: Candidates and preferred technologies 58
Table 5: Overview on eID documents in Europe 84