

Table of Contents

TABLE OF CONTENTS	1
EXECUTIVE SUMMARY	3
PART I: RESEARCH ON DIVERSITY MEASURES AND THE EFFECT IN EGOVERNMENT	4
1 Introduction	5
2 Austria	6
2.1 Introduction	6
2.2 Current and planned figures on usage of certificates for online services	7
2.3 Best practice services already existent or planned	7
2.4 Legal policies and laws supporting certificates.....	9
2.5 Relevant authorities responsible for implementation.....	10
2.6 Existence of a roadmap for certificate usage	11
2.7 Time schedule of roadmap for service usage.....	11
3 Denmark	13
3.1 Introduction	13
3.2 Current and planned figures on usage of certificates for online services	14
3.3 Best practice services already existent or planned	15
3.4 Legal policies and laws supporting certificates.....	17
3.5 Relevant authorities responsible for implementation.....	18
3.6 Existence of a roadmap for certificate usage	18
3.7 Time schedule of roadmap for service usage.....	19
4 Italy	20
4.1 Introduction	20
4.2 Current and planned figures on usage of certificates for online services	22
4.3 Best practice services already existent or planned	23
4.4 Legal policies and laws supporting certificates.....	25
4.5 Relevant authorities responsible for implementation.....	26
4.6 Existence of a roadmap for certificate usage	26
4.7 Time schedule of roadmap for service usage.....	27
5 Germany	28
5.1 Introduction	28
5.2 Current and planned figures on usage of certificates for online services	29
5.3 Best practice services already existent or planned	29
5.4 Legal policies and laws supporting certificates.....	31
5.5 Relevant authorities responsible for implementation.....	31
5.6 Existence of a roadmap for certificate usage	33
5.7 Time schedule of roadmap for service usage.....	33
6 EU	34
6.1 Introduction	34
6.2 Current and planned figures on usage of certificates for online services	34
6.3 Best practice services already existent or planned	35
6.4 Legal policies and laws supporting certificates.....	36
6.5 Relevant authorities responsible for implementation.....	36
6.6 Existence of a roadmap for certificate usage	37
6.7 Time schedule of roadmap for service usage.....	38
7 Conclusion	40

PART II: PROBLEMS AND MEASURES ON INTRODUCTION OF THE CITIZEN ID CODE-NUMBER 42

1	Introduction.....	43
2	The Personal Identifier in the e-Government Sphere.....	44
	2.1 Basic Approaches to the use of Personal Identifiers.....	44
3	Personal Identifiers in Different European Countries	46
	3.1 Estonia.....	46
	3.1.1 Evaluation and Critique	48
	3.2 Austria	48
	3.2.1 Evaluation and Critique	49
	3.3 Switzerland.....	50
	3.3.1 Evaluation and Critique	51
	3.4 Germany.....	52
	3.4.1 Evaluation and Critique	53
4	Public Debate on Personal Identifiers.....	54
	4.1 Criticisms of the Introduction of Personal Identifiers.....	54
	4.2 Dealing with Criticism.....	56
5	Conclusions.....	58
	Appendix.....	59
	Acronyms/Abbreviations.....	59
	References.....	60

Executive Summary

The Final Report consists of two parts and relevant attachments.

Part I: Research on diversity measures and the effect in e-government

The advancements of electronic signatures and authentication with certificates will be investigated for EU, Denmark, Germany, Austria, Italy.

For each of these countries a Web search was performed to gather information on: Current and planned figures on usage of certificates for online services, best practice services already existent or planned, legal policies and laws supporting certificates, relevant authorities responsible for implementation, existence of a roadmap for certificate usage in these countries, time schedule of roadmap for service usage.

Part II: Problems and measures on introduction of the citizen ID code-number

Part II is concerned with the use of personal identifiers in various European countries. In this study we will clarify what a personal identifier is, where it occurs and in what form and what it is used for. The possibilities that it opens up will be indicated and the potential for misuse will be identified. Considerations such as what to do with the findings and which aspects of the personal identifier should be studied if it is used will also be addressed. In addition, approaches to personal identifiers and the already implemented national projects addressing their introduction will be examined and assessed and conclusions will be drawn from the public debate on personal identifiers and will be incorporated into the study.

**Part I: RESEARCH ON DIVERSITY MEASURES AND THE EFFECT IN
E-GOVERNMENT**

1 Introduction

The progress in introducing certification services for signatures and authentication into applications and infrastructures is at very different stage in Europe.

Similarities and differences in the implementation and use of electronic signatures and authentication for eGovernment applications exist in the EU member countries. This study focuses on the achievements and plans of four countries - Denmark, Germany, Austria, Italy - and the EU itself. Some drawbacks and respective solutions of these countries to foster the usage of electronic signatures are outlined.

2 Austria

2.1 Introduction

Bürgerkarte

Since February 2003 the "Bürgerkarte" (citizen card) is being introduced in Austria. The "Bürgerkarte"¹ 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:

- National ID card
- Social security card (so-called e-card)
- Students card
- 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

The "Bürgerkarte" today is mainly used in the public sector for identification and authentication purposes. 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.

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.

e-Card

For the e-health system two cards were introduced: one card for the citizens (e-card) and one professional card for the doctors. The combination of the ordination card (o-card) that is owned by the doctor and the e-card which is owned by the patient gives the doctor the authority the access to the patient data in the data processing center. Each doctor has his separate private e-card, as he is also a potential patient.

Bankomatkarte

Moreover about 6.7 million bank-cards (Bankomatkarte) have been issued between 2005 and 2007. But less than two of thousand user did activate the signature function on the bank card (11.2005).

Mobile Signature

¹ EU IST FIDIS project (Future of Identity in the Information Society), D3.6 Study on ID Documents, December 2006, <http://www.fidis.net/>

The mobile signature has been provided by A1² for all Austrian mobiles independent of the mobile provider from 2004 to 2007. According to the transitional provisions in the E-Government Act (Section 25 E-Government Act), advanced signatures can be used instead of qualified signatures until 31.12.2007. As a consequence the A1 signature has finished on 31.12.2007³.

2.2 Current and planned figures on usage of certificates for online services

A 98% coverage for the e-cards is reached in the end of 2007. One million e-cards have to be exchanged annually. About 500.000 cards are lost in the end of 2006, of which about 46.200 cards were reported as stolen and 108.000 were reported as lost and 97.000 as defect or have to be exchanged by other reasons (122.000). Further 500.000 e-cards had to be replaced because of changing the name, title or because of expiring of the European health insurance. Each card costs about four to five euro including the shipping⁴.

The e-card is as described mainly used in the Austrian health system, but has the optional and additional function to be a signature card at no charge⁵. Each owner has to activate this signing functionality in order e.g. to use an online government service. A survey (Fessel-GfK 17.05.2006-02.06.2006)⁶ found out that only 4% of all e-card owners did activate the signature functionality. Further 5% wanted to activate the signature function within three months, 19% till the end of 2006, 39% wanted to activate the card in 2007. About 33% do not think about activating the signature functionality. Due to the problems with the interests at the electronical signature, Austria introduces several online services and a free software called BKU (Bürgerkarten-Umgebung) for Windows 2000/XP/Vista, Linux, and Mac OS X⁷.

Manfred Matzka (Federal Chancellery of the Republic of Austria) expects 100.000 new users activating and using the signatures in 2008, as the current usage is too small (smaller than one million activated citizen-cards)⁸.

2.3 Best practice services already existent or planned

Federal applications using electronic signatures are listed at http://www.help.gv.at/sigliste/sig_bund.jsp, local applications at http://www.help.gv.at/sigliste/sig_region.jsp.

To give examples, the following applications are (among others) citizen card enabled and, thus, employ eSignatures:

² A1, <http://www.a1.net/>

³ Stadtgemeinde Mattersburg, Die Bürgerkarte in Österreich (in German),

http://www.mattersburg.gv.at/index.php?option=com_content&task=view&id=11&Itemid=20

⁴ Salzburger Nachrichten, Der Schwund bei den E-Cards (in German), 13.12.2007,

[http://www.salzburg.com/nwas/index.php?article=DText/yj*7zpzl~980l476zt\\$wmcr&img=&text=&mode=§ion=newsletter&channel=nachrichten](http://www.salzburg.com/nwas/index.php?article=DText/yj*7zpzl~980l476zt$wmcr&img=&text=&mode=§ion=newsletter&channel=nachrichten)

⁵ A-Sit, Die Bürgerkarte (in German) [http://www.a-](http://www.a-sit.at/de/dokumente/publikationen/flyer/buergerkarte.php)

[sit.at/de/dokumente/publikationen/flyer/buergerkarte.php](http://www.a-sit.at/de/dokumente/publikationen/flyer/buergerkarte.php)

⁶ A-Sit, Fessel GfK, Online Study (in German), 06 17.05-02.06.2006, [http://www.a-](http://www.a-sit.at/pdfs/2006_10_05_VIENNA_RFID.pdf)

[sit.at/pdfs/2006_10_05_VIENNA_RFID.pdf](http://www.a-sit.at/pdfs/2006_10_05_VIENNA_RFID.pdf)

⁷ Bürgerkarte (in German), <http://www.buergerkarte.at/bku>

⁸ Futurzoneqorf.at, E-Card wird zum Online-Ausweis (in German), 30.10.2007,

<http://futurezone.orf.at/it/stories/239551/>

Federal applications:

- Pensions (various: validation of entitlements, application of retirement, applications of disability pensions, pensions for widow/widower, ...);
- Electronic delivery;
- Applications for subsidy (family support, health insurance, or living costs);
- Tax online (various taxes, such as VAT declarations, income tax declarations, income tax returns, etc.);
- Application for childcare allowances;
- Centre for reporting of environmental crime, repeat offence, or child porn;
- Electronic confirmation of residence;
- Electronic certificate of Register of Convictions;
- eTendering.

Free Tools

A lot of tools are available for free in order to ensure appropriate handling of signatures and certificates in Austria. The problem that here arises is that a lot of different tools have to be used, developed by different manufacturers supposing different qualifications of the potential user. The tool diversity ranges from keyboard-drivers to JAVA based Windows tools in German language. It is to assume once a user makes bad experiences with software it is very difficult to convince him again to use signatures. One easy to handle and free tool should be produced that does not let the responsibility of security in the hand of a single user. The following examples present some of these free available tools. Some of these tools are only available if a citizen card on the PC is used or the citizen-card emulator called SeLaNext⁹ which is also freely downloadable:

- **Invoice reception book:** In order to promote the use of electronic invoicing, the legitimation for deduction of input tax in Austria is only given if the invoices are electronically signed since 31.12.2005. Each invoice has to be verified whether its signature is valid or not. For this step of validation a free and downloadable tool (called ebRe) has been developed by the Federal Ministry of Economic Affairs and Employment (BMWA) together with the AUSTRIAPRO which is the B2B platform of standardization within the Chamber of Commerce of Austria¹⁰. The usability of the tool itself does not seem to be very high, especially as the user has to copy files by himself, options have to be edited by hand in an ini-file¹¹.
- **A-Sit Zertifikat Status Tool:** In order to be able to check whether a issued certificate is valid or possibly revoked, A-SIT developed a free JAVA-tool called "Zertifikat Status Tool"¹² which is able to retrieve the status of a certificate at any timestamp.
- **Modules for online applications:** In order to support the development of services, by order of the Federal Chancellery of the Republic of Austria and the Federal

⁹ SeLaNext, citizencard-emulator, https://demo.a-sit.at/buergerkarte/security_kapsel/index.html

¹⁰ BMWA, ebInvoice Rechnungseingangsbuch – kostenloses Prüftool für elektronische Rechnungen (in German), <http://www.bmwa.gv.at/BMWA/Schwerpunkte/Wirtschaftspolitik/InnovaTechnol/Initiativen/ebinvoice.htm>

¹¹ EbRe –Dokumentation, <http://wko.at/ebusiness/e-rechnung/EbRe.pdf>

¹² A-SIT, Zertifikat Status Tool (in German), http://demo.a-sit.at/el%5Fsignatur/zertifikats_status/index.html, http://www.a-sit.at/de/dokumente/publikationen/flyer/zertifikat_status_tool.php

Finance Office several modules for online applications (MOA¹³) have been developed. In June 2005 the modules have been set under the Open-source license of the Apache Foundation in version 2.0, hence the distribution of those modules and the associated source code is freely available. In the area of electronic signatures, the following modules are important: MOA-SP for signature validation, MOA-SS for server signatures, MOA-ID for identification.

The concept of giving the possibility to test the system and by this to give the citizen an easy access to the system should help to have confidence in the work with signatures. During testing the system the citizen is able to find out where the benefits are given and could by this find easily motivation to use the system regularly, as told in "On Diffusion and Confusion – Why Electronic Signatures Have Failed"¹⁴. To get used to electronic signatures some best practices are mentioned below.

Public terminal for citizen-card

The municipalities of Engerwitzdorf (Upper Austria) won in a contest the first terminal with citizen-card functionality at Austria's government fair of 2007¹⁵. The terminal has been developed by APC Interactive Solutions AG¹⁶, an Austrian terminal solution specialist. The terminal is connected with already existent eGovernment services and should improve the general usage with signature cards. As the terminal allows the citizens to have an easy "first try" without investing too much time and energy in their home-environment. It is to evaluate whether citizens have a better acceptance and understanding towards signatures if they have the possibility to get to know the system in a prepared environment. But currently this terminal is just the only one terminal where citizen feedback is not yet published.

Software for creating electronic offers

ASFiNAG¹⁷ and ÖBB Infrastruktur Bau AG¹⁸ implemented a free software called @-AVA-ASSI for creating electronic offers which will be introduced at the 14. April 2008¹⁹. The software helps the user to create offers and sign them in the mandatory way. This software allows it to electronically sign just the main part of the document while all other parts will be automatically signed in addition. Furthermore the software is completely accountable for the correctness of signing procedure. As it is only allowed to electronically sign with the statutory qualified signature the software ensures the correct application of the qualified signatures. Since November 2007 first on-road-tests are in progress.

2.4 Legal policies and laws supporting certificates

European Directive 1999/93/EC of 13 December 1999 on a Community framework for

¹³ Digitales Österreich, MOA, <http://www.digitales.oesterreich.gv.at/site/5241/default.aspx>

¹⁴ Trust and Privacy in Digital Business, – Why Electronic Signatures Have Failed, Springer Berlin / Heidelberg, 2006, <http://www.springerlink.com/content/66r68553t2446877/fulltext.pdf>

¹⁵ Digitales Österreich, Erster Bürgerkarten Terminal verlost (in German), 11.10.2007 http://www.digitales.oesterreich.gv.at/site/cob_25167/5236/default.aspx

¹⁶ APC interactive solutions AG, <http://www.apcinteractive.net/>

¹⁷ ASFiNAG, <http://www.asfinag.at/>

¹⁸ ÖBB Infrastruktur Bau AG, <http://www.oebb.at/bau/>

¹⁹ @-AVA-ASSI, Der elektronische Angebotsassistent von ÖBB und ASFiNAG (in German), 22.01.2008,

http://www.oebb.at/bau/de/Pressecorner/Presseinformationen/2008_01_22_-AVA-ASSI_-der_elektronische_Angebotsassistent/2008-01-22_Prsentation_Fachmediengesprch_-_Handout.pdf

electronic signatures was transposed into Austrian legislation²⁰ through: the Signature Act which went into force 1 January 2000 and has been amended in 2000 and in 2001 and the Signature Order of 2 February 2000. The Signature Order has been amended in 2004;

Electronic signatures are defined for natural persons only. Provisions for mandates and representing a company (or another natural person) are given in the citizen card identification model that has been laid down in the E-Government Act.

Austrian legislation did not explicitly introduce the concept of advanced electronic signatures. "Qualified" electronic signatures are however literally taken from the Directive by taking and combining the definitions of advanced electronic signatures and the provisions of article 5 of the Directive into a single definition. Qualified electronic signatures are referred to as "secure electronic signatures" under Austrian legislation. The supervision of electronic signatures is laid down in the Signature Act. Supervision is carried out by Telekom-Control-Kommission which calls RTR-GmbH⁷. Supervision covers all certification services providers and is thus not limited to those issuing qualified certificates.

The SourcePIN Register Regulation defines the activities of the SourcePIN Register Authority that are necessary to implement the citizen card concept and the cooperation with its service providers. This includes the creation of an identity link which is a separate data structure on the citizen card to establish a link between an electronic signature and the unique identity of the citizen derived from central registers.

2.5 Relevant authorities responsible for implementation

An ICT Board was set up by order of the Council of Ministers in June 2001. The body was composed of the Chief Information Officers of all the federal ministries and their deputies. In 2005 a restructuring of eGovernment organisation took place. The Federal CIO continues to exist. An ICT Strategy Unit has been installed at the Federal Chancellery. This group is responsible for the eGovernment Act and the Signature Act. Coordination on the federal level and with provinces, municipalities and local authorities is carried out by the ICT Board. An e-Cooperation Board allocates responsibility for the preparation of implementation projects and coordinates the implementation projects of the participating organisations (ICT Board, eGovernment working groups of the provinces and the public-administration bodies responsible for ICT). The two bodies ICT Board and e-Cooperation Board are coordinated by the ICT strategy platform "Digital Austria" which is led by the Federal CIO.

Thus, the eGovernment structure spans over various levels.

- Federal eGovernment: The ICT Board and the e-Cooperation Board which are coordinated by the ICT strategy platform "Digital Austria". A Federal ICT Strategy Unit is installed in the Federal Chancellery.
- Regional eGovernment: eGovernment implementation of the provinces is carried out by the respective regional units. Coordination with federal initiatives is implemented.
- Local eGovernment: Local eGovernment initiatives are carried out by the local authorities. Coordination with federal initiatives is implemented through the unions of municipalities and local communities.

For implemented eGovernment services the respective Ministries are responsible, as for

²⁰ IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Austria, <http://ec.europa.eu/idabc/servlets/Doc?id=29070>

example: FinanzOnline-Tax declarations online, the Federal Ministry of Finance (www.bmf.gv.at); Electronic delivery (www.zustellung.gv.at), the Federal Chancellery (www.bka.gv.at); Residence certificate (<https://meldung.cio.gv.at/egovMB/>), the Federal Ministry of Interior (www.bmi.gv.at), Social Security, Social Security Organisations (www.sozialversicherung.at).

2.6 Existence of a roadmap for certificate usage

General e-health roadmap

The e-Health-Initiative²¹ did create an e-health strategy recommendation for Austria within a strategy paper²². The roadmap contains

- preconditions
- e-Health-infrastructure / basic components
- e-Health-applications
- accompanying measures

A major part of e-health activities, especially in the content of electronic medical record (ELGA) the following preconditions were defined, which have a strong relation to certificates for electronic signatures and authentication:

- roles and authorization concept
- pseudonymous- / anonymizing services
- long-time archiving.

Program of the Austrian federal government 2007 – 2010

"In the course of digitization, the expansion of transmission channels (broadband, fibreglass) must be accelerated. Austria must position itself amongst the top 3 ICT nations. By the end of 2009 the broadband infrastructure shall be available to the entire population. One single contact person for ICT issues seems necessary. The ICT taskforce already created will stand by this person as an advisory body. This will create the basis for future cooperation with all partners for the best possible conditions throughout Austria in the whole ICT area. The 172 expansion of e-government services as well as the spread and use of the digital signature are also to be accelerated."²³

2.7 Time schedule of roadmap for service usage

Implementation of the i2010 initiative in Austria

In "i2010 Austria"²⁴ (which explains the general goals and the most important i2010 initiative measures to be implemented in the areas of economics, research and development, education, public administration and health in Austria) Austria did identify several goals

²¹ E-Health-Initiative Strategie und Technologien, <http://ehi.adv.at/>

²² E-Health-Initiative Strategie und Technologien, Empfehlung für eine österreichische e-Health Strategie (in German), 01.2007, http://ehi.adv.at/fileadmin/user_upload/adv_author/pdfs/konferenz20070126/Strategie_Empfehlung_der_e-Health-Initiative_Oesterreich_20070126_v2_02.pdf

²³ Programm of the austrian federal government, 23. legislative period 2007 – 2010, <http://www.austria.gv.at/DocView.axd?CobId=19879>

²⁴ i2010 Austria, <http://www.bka.gv.at/DocView.axd?CobId=16635>

where one of the objectives are to guarantee broadband coverage of 98%, which is almost full coverage, by the end of 2007. Due to this Austria wants to accelerate speed-up access and the introduction of qualitative and innovative services and applications and thus increase use and penetration while closing the technological gap. Austria wants to raise the proportion of companies who carrying out part of their purchase and sales transactions over the Internet (eBusiness) until 2010 to 50%. Further objectives are for 75% of all companies to be sending or receiving electronic invoices with electronic signatures (eInvoicing). In the context of signatures Austrians objective is for 75% of all companies to be sending and receiving electronic invoices signed with electronic signatures by 2010.

e-card with qualified certificates

Until the end of 2007 the e-card could be used with an advanced signature (SV-Verwaltungssignatur) which was equated to the secure signature as written in the law of eGovernment. The Main Association of Austrian Social Insurance Institutions decided to change the signature technology for the e-card to the qualified signature²⁵. In order to prevent misuse and to reach higher quality of signatures 50% of all e-cards have to be exchanged (about 4,6 million e-cards) until 2010 by starting in January 2008. The current social insurance administration signature will be replaced by the so called qualified signature and an additional electronic photo that helps to assign the owner to its e-card more clearly. Through the deployment of the qualified signature the Austrian government hopes that the e-card will be easily used with public authorities, the economy and in public life because of the homogeneous underlying signature conditions.

By introducing the qualified signature the possibility is given to use the citizen-card within e-banking or electronic tenders. As the bank-card (Bankomatenkarte) had huge problems with the dissemination of its function to sign, it is expected that this functionality will be declined in the future.

²⁵ Ecard, Die NEUE Bürgerkarte auf der e-card (in German),
http://www.chipkarte.at/portal/index.html?ctrl:cmd=render&ctrl>window=ecardportal.channel_content.cmsWindow&p_menuid=51682&p_tabid=1&p_pubid=134395

3 Denmark

3.1 Introduction

In Denmark no electronic ID-card system like smart cards or other physical token has been distributed. Denmark established a signature system, where the user is able to activate its signature over an internet portal after receiving an activation code in the mail (not email). The OCES (Offentlige certifikater til elektronisk service – public certificates for electronic services) is the initiative of Denmark that establishes the national digital signature solution which is used in eGovernment sector for example. The OCES signature framework applies to both human and legal entities, hence the OCES signatures can be issued as personal certificates, company certificates and employee certificates.

Different payment rules had been set up depending on the status of the receiver of a signature²⁶:

Citizens

- Digital signatures are free to acquire and to use for all citizens.
- Personal signatures will be available to all citizens, including disabled persons.
- Installation support will be available to all citizens.

Public authorities

- Unlimited reception of personal signatures and employee signatures in all public authorities.
- Pay for acquiring a Local Registration Authority function (LRA) and issuing employee signatures.

Companies

- Pay for receiving signatures in their solutions - except employee signatures received from public authorities.
- It is free to acquire and use an LRA and up to 10 employee signatures for external purposes.
- Additional employee signatures require acquisition of a payable LRA and an additional fee per employee signature.

Personal identification numbers are used in the OCES signature process. This personal identification number is a unique and identification number for the entire life of each Danish citizen, as the Act of the Civil Registration System states. The personal numbers of all Danish citizens are stored in the CPR-register (a national data store containing name, address etc.). Due to this only companies registered in Denmark and citizens with a Danish personal registration number (CPRnumber) have access to the electronic signatures.

Denmark's OCES is based on international standards like i.e.:X.509.v3 and ETSI TS 102 042 v 1.2.1 see reference in the OCES CP²⁷.

With the 01.01.2007 a central entrance to public eGovernment services has been established on www.borger.dk. From January 2008 a "my page" will be accessible to all citizens

²⁶ Epractice, Digital Signatures in Denmark, <http://www.epractice.eu/cases/1786>

²⁷ OECS – Digital Signatur, (in Danish), <https://www.signatursekretariatet.dk/certifikatpolitikker.html>

with digital signature based on the OCES standard.

3.2 Current and planned figures on usage of certificates for online services

A total of at least 1.1 million digital signature certificates according to the Danish OCES standard were issued to citizens, workers and businesses by the end of year 2006²⁸, which is about 20 % of all inhabitants.

Approximately EUR 5.7 million € was assigned to the signature project by the Danish Government, the tender won TDC (Tele-Denmark Communications)²⁹ who implemented the signature contract.

About 80% of the citizens are potential users, which mean 4 million inhabitants. The actual penetration (2007) is estimated at 800.000, which are around 20% of the potential users. The actual use is difficult to estimate as the usage cannot be monitored centrally. There are over a 100 public services though and statistics from central services show a constant increase in usage.³⁰

Out of the experiences made in Denmark the following statements can be derived³¹: The most important lesson learned from the implementation of the digital signature has been that if there are no electronic services available, which require digital signatures, there is no motivation among citizens and companies to acquire and use the digital signature. The number and range of electronic services are vital for the dissemination of a public key infrastructure such as the digital signature. This situation has clarified that it takes time to establish a large-scale open infrastructure for digital signatures and a long time to get citizens and companies to use it. Because the electronic services act as drivers for the dissemination of digital signatures in the society, the digital signature cannot be seen as a product in itself. It is therefore vital to focus on how to get the citizens and companies to use the digital signature and clarify what their advantages are as well as how the digital signature can add value to their individual work process/task.

The following results and experiences are derived by Modinis-IDM³² in Denmark

- It is not clear why the Danish government has decided not to issue or create electronic identities for its citizens. The steps that were taken to issue the digital signatures are very similar to the eID initiatives in other member states, for example, a nation-wide public key infrastructure has been set up.
- It is not known whether there are initiatives to promote interoperability with electronic signatures from other member states.
- From this initiative we learn that it is not easy to provide an infrastructure first and to ensure at the same time that it will have successful applications. One could try to think of applications before setting up the infrastructure but it is commonly believed that it works better the other way round.

²⁸ Ramboll Study, Benchmarking of the national administrative and legal practices in the fields of eSignatures, invoicing as well as contract conclusion and implementation, 11.2006, <http://ec.europa.eu/enterprise/ict/policy/legal/2006-bm-cr/ramboll-benchmarking-final-report-draft.pdf>

²⁹ TDC, Tele-Danmark Communications, <http://erhverv.tdc.dk/>

³⁰ IDABC, eID Interoperability for PEGS in Denmark, 2007, <http://ec.europa.eu/idabc/servlets/Doc?id=29592>

³¹ Epractice, Digital Signatures in Denmark, <http://www.epractice.eu/cases/1786>

³² Modinis IDM, National profile for eGovernment IDM initiatives in Denmark, 02.2007, <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/DanishProfile>

3.3 Best practice services already existent or planned

Online Citizen Campaign

In spite of the existence of a whole bunch of digital services and free request able digital signatures the signatures does not seem to have been adopted by the citizens. Due to this problem a huge campaign has been started in whole Denmark. The online citizen campaign called "Netborgerkampagnen"³³ was carried out over a period of three months in the autumn of 2006. The target of the campaign was to inform the citizens, about the public digital self-service options available on the Internet. Denmark tries to focus on the libraries as one of the central places where municipalities and other public institutions could get in touch with as many citizens as possible.

Through the campaign the online public self-services have been presented, like E-box, Digital Signature, the libraries' web guide and bibliotek.dk which are available at borg-er.dk. Moreover services in the area of 'Job and Education', 'Pension and Health' and 'Home and Relocation' have been presented including the optional download of demos in order to give an easy access and to reduce potential fear of the citizens concerning the internet or signature usage.

The employee of the library was available and addressable in case of questions and explained the citizens how to use the different options and introduce to different institutions for further information. The employee itself had been trained and introduced with information and courses.

In the end of 2007 Danish libraries did promote a campaign on the free e-resources which are available to the public in the libraries. Denmark is planning to extend the campaign by starting a seminar for all leaders, employees and politicians in the region who are involved in online citizen services.

ETHICS

ETHICS (Electronic Tender Handling, Information & Communication System)³⁴ is a procurement system. The system has been in operation since 2000. The parties involved in the signature scheme are bidder/vendor, procurer, application owner, TDC (issuer of OCES certificates) and service provider.

To be able to respect the requirement on confidentially, judicial evidence etc. the following conditions have to be met:

- the vendor must submit their proposal digitally signed.
- the contracting authority put a time stamp on the proposals when receiving these.
- it is not possible to open the bids until the deadline for submission of proposals is met.
- Proposals can only be opened by persons authorized.
- Violation of the rules can be traced

No measures have been taken to ensure interoperability with signatures created and/or certificates issued in other countries. No statistics on the use of eSignatures have been provided]³⁵.

³³ The Online Citizen Campaign, 2007, http://www.splq.info/issues/vol40_4/04.htm

³⁴ ETHICS, SKI, <http://www.innovation.dk/ethics/2008.pdf>

³⁵ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Denmark, <http://ec.europa.eu/idabc/servlets/Doc?id=29078>

TastSelv Borger - eTax

The Danish citizens' tax declarations are reported by employers, banks, mortgage institutions, trade unions, and social benefits administration etc. to the Central Customs and Tax Administration. The citizens can report corrections or approve their tax return via the Internet through TastSelv Borger³⁶. The application uses OCES signatures and/or a simple password solution. The parties involved in the signature scheme are SKAT (application owner), TDC (issuer of OCES certificates), CSC (service provider) and the users. Relying party are SKAT. The system TastSelv Borger is not accessible to non-nationals and no measures have been taken to ensure interoperability with solutions from other countries.

In 2005 the application had 3.113.476 logins through password solution and 487.248 logins with OCES signatures. This is an increase in use of OCES of 136% compared to 2004.

According to SKAT it has been a problem that the OCES certificate is not mobile.³⁷

TastSelv Erhverv - eTax

TastSelv Erhverv³⁸ is the parallel to TastSelv Borger for enterprises. The application allows enterprises to report and pay VAT and tax online. The application is accessible to non-nationals who have a SE-number (are paying VAT to Denmark). Non-nationals can only get access by pin-code as OCES signatures are not offered to non-nationals.

App. 300.000 enterprises are using the application. 3% use an OCES signature. 97% use simple password solution.³⁹

Sundhed.dk – eHealth

Sundhed.dk is the joint public health internet portal in Denmark ('sundhed' means health). The Danish health service contains app. 110.000 users with own eSignature. The Digital Certificates are used for identifying the users. When identified by the portal, the user has access to own data and for healthcare professionals to patient data. The external systems are systems in hospitals, national medicine and patient databases, but at the moment no signatures are used between systems. The security between systems is handled by a point-to-point private and secure network. At the moment there are pilot projects (SOSI) validating the exchanges of the signed information between systems.

Especially the fact that healthcare professionals need access to data from every bed in a hospital calls for other solutions than the current software based eSignature. The mobility issue is handled differently from hospital to hospital –but several organizations have started to implement a central certificate store – others consider different hardware solutions.⁴⁰

Virk.dk

Virk.dk⁴¹ is an internet portal delivering a number of fully digital solutions for the benefit of the companies as well as the public administration. Virk.dk contains more than 200 e-forms. A number of the forms may be filled out and signed with an OCES signature. When

³⁶ SKAT, TastSelv Borger, <http://tastselv.skat.dk/>

³⁷ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Denmark, <http://ec.europa.eu/idabc/servlets/Doc?id=29078>

³⁸ SKAT, TastSelfErhverv, <http://www.skat.dk/SKAT.aspx?oID=199625>

³⁹ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Denmark, <http://ec.europa.eu/idabc/servlets/Doc?id=29078>

⁴⁰ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Denmark, <http://ec.europa.eu/idabc/servlets/Doc?id=29078>

⁴¹ Virk.dk, <http://www.virk.dk/>

a user signs the data supplied to an e-form, the signed data is submitted together with an XML instance and a PDF version of the form. Authorities can now retrieve this data on Virk.dk using a common web service. Moreover authorities can build integration between Virk.dk and their back office systems, using the common web services based on the XML schemas. The parties involved in the signature scheme are the Danish Commercial and Companies Agency and the private company KRAK⁴² (application owners), TDC⁴³ (issuer of OCES certificates), all government institutions with transactions forms for businesses – currently 39 institutions and the users (companies). Relying party is the government institutions with transactions forms on Virk.dk.

The number of registered users is app. 15.000. The application owner KRAK considers OCES to be stable and secure but with weaknesses in usability, price and usage.⁴⁴

NemKonto - eBanking

[All citizens and companies in Denmark have to have a NemKonto⁴⁵. When logging on to the website www.nemkonto.dk, the EAS validates the signature with the provider, TDC. For employees in public institutions using an employee digital signature, the signature is used to identify the user profile of the employee. This is done in the safety system "KSP/CICS". The OCES signature is used by app. 40.000 users of the application.⁴⁶

borger.dk

Borger⁴⁷ is a portal for a suite of A2B solutions, where local municipalities can offer self-service to their citizens. A large number of applications of the municipalities are offered from the portal. As borger.dk is an umbrella application with a number of individual applications no general rule covers the use of eSignatures in the application. Until week 43, 2006: app. 800.000 logins, of which app. 25% are using OCES certificates, i.e. 200.000 certificate login⁴⁸.

E-boks

Secure electronic document archive, where public authorities and companies can deliver documents to citizens/consumers. Documents are received through the e-boks portal⁴⁹. The application uses OCES signature, a simple password solution and the common Danish NetBank logon system (NetID) are supported. Approximately 1 million users use the application and the application owner states that 70% use electronic signatures.

3.4 Legal policies and laws supporting certificates

Advanced and "qualified" electronic signatures cannot be issued to legal persons under Danish law⁵⁰.

⁴² KRAK, <http://www.krak.dk/>

⁴³ TDC, Tele-Danmark Communications, <http://erhverv.tdc.dk/>

⁴⁴ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Denmark, <http://ec.europa.eu/idabc/servlets/Doc?id=29078>

⁴⁵ NemKonto, <http://www.nemkonto.dk/wo/default.asp>

⁴⁶ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Denmark, <http://ec.europa.eu/idabc/servlets/Doc?id=29078>

⁴⁷ Borger.dk, <http://borger.dk/>

⁴⁸ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Denmark, <http://ec.europa.eu/idabc/servlets/Doc?id=29078>

⁴⁹ E-books (in Danish), <http://www.e-boks.dk/>

⁵⁰ Interdisciplinary Centre for Law and ICT, European Electronic Signatures Study, http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl#dk

The practical effect of the Danish eSignature Act has been disappointing as no “qualified” electronic signatures are being offered by certification service providers in Denmark. One of the main obstacles has been the requirement for signature holders to meet up and identify themselves in person. Realizing that few people would do this the Government initiated the establishing of the mentioned OCES standard. The OCES signature is a “light version” of the qualified electronic signature with the important difference that the holder of an OCES signature does not have to perform face to face identification.

3.5 Relevant authorities responsible for implementation

Federal eGovernment

One of the projects of the initiative was the establishment of a national digital signature solution to be used (not exclusively) in eGovernment solutions. This solution, called OCES (Offentlige certifikater til elektronisk service – public certificates for electronic services) digital signatures. The OCES project is established within the framework of the Ministry of Science, Technology and Innovation.

Regional eGovernment

After a restructuring reform of the municipalities and regions Denmark consists of 5 regions and app. 100 municipalities (as of January 1, 2007). The main working area of the regions is the health care sector, including responsibility for the public hospitals. Through their organization Danish Regions (www.regioner.dk) the regions are running a national healthcare portal (www.sundhed.dk) which includes a number of applications.⁵¹

Local eGovernment

A number of local eGovernment applications are offered by the Danish municipalities. Many of these applications are used by a large number of the municipalities and provided through the website borger.dk. This website is owned by the organization KL which is the organization of the municipalities (www.kl.dk). The applications of the website is developed and operated by KMD (www.kmd.dk) which is a Danish IT company owned by the municipalities through their organization KL. KMD is operating on market terms but has a very strong position in the Danish market for municipality IT services and applications.⁵²

3.6 Existence of a roadmap for certificate usage

E-government strategy 2007-2010⁵³

The Danish strategy contains general goals as well as 35 specific initiatives. The strategy has three priority areas⁵⁴:

- Digitalization focused on creating improvements in the service to citizens and

⁵¹ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Denmark, <http://ec.europa.eu/idabc/servlets/Doc?id=29078>

⁵² IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Denmark, <http://ec.europa.eu/idabc/servlets/Doc?id=29078>

⁵³ Denmark, The Danish e-Government Strategy 2007-2010 Towards better digital service, increased efficiency and stronger collaboration, http://modernisering.dk/fileadmin/user_upload/documents/Projekter/digitaliseringsstrategi/Danish_E-government_strategy_2007-2010.pdf

⁵⁴ Modernisering.dk, Danish e-government Strategy 2007-2010, <http://modernisering.dk/da/english/>

businesses;

- Digitalization that enables resources to be transferred from administration to citizen-focused service;
- Coordination and prioritization of digitalization efforts in the public sector through more binding, cross-governmental collaboration at all levels.

The strategic plan states that the objective is to spread an improved and user-friendly solution for digital signatures during the strategy period to citizens and businesses, and to make it fully serviceable in the public digital service offering. In 2006, 98 percent of the public authorities were already capable of receiving and sending e-mail signed with a digital signature, and as at mid-2007 more than a million digital signatures have been issued.

3.7 Time schedule of roadmap for service usage

Some strategic targets⁵⁵ of the Danish strategy regarding service usage are:

- From 2008 citizens and businesses will be able to receive text-messages reminders about public sector appointments.
- In 2010 all digital self service solutions will be integrated in the citizen portal borg-er.dk
- In 2012 the evolvement of the citizen portal should be completed as all digital services should be integrated
- In 2009 all businesses should be able to access via single digital-signature sign on all digital-reporting-solutions.
- In 2010, 75% of businesses reporting should be done digitally.
- In 2009 Citizens-portals like „My Home“ or „My Children“ have to offer all major service areas.
- From 2010 all citizens and businesses are able receiving alternatively all letters from the public sector in the appropriate portal digitally
- In 2008, 30 regional and municipal digital citizen services will be fully integrated into the Citizen Portal.
- In 2009 a user should be able to use its signature wherever he has to self-authenticate.

⁵⁵ The Danish Government Strategy 2007-2010, The Danish government, Local Government Denmark (LGDK) and Danish Regions June 2007, http://modernisering.dk/fileadmin/user_upload/documents/Projekter/digitaliseringsstrategi/Danish_E-government_strategy_2007-2010.pdf

4 Italy

4.1 Introduction

As Italy is not a federal state, it must be remarked that there is nonetheless a distribution of the legislative power between the state and the regions.

RUPA (Rete unitaria della Pubblica Amministrazione) is a broadband network interconnecting all public administration bodies across the country. In the course of 2007, RUPA is will be incorporated into a Public Connectivity System (Sistema Pubblico di Connettività - SPC), with increased quality and security standards.⁵⁶

Because of this some regions have created their specific ICT systems, as it is the case of Lombardia with ehealth-Project CRS-SISS or Emilia-Romagna with Project SOLE.

The State entity in charge to decide the applicable standards is currently the CNIPA⁵⁷ (Centro Nazionale per l'Informatica nella Pubblica Amministrazione, National Centre for ICT in the Public Administration).

Some tasks of CNIPA are the following:

- it coordinates the planning of the most notable interventions for development, and sets the norms and criteria for projecting, making, management of Public Administrations ICT systems; in particular, it deals with such issues as service quality and organization; it as well defines the criteria and technical rules concerning security, interoperability and functioning of the systems;
- it supervises the implementation of relevant projects fostering the technological innovation in the public sector, the diffusion of e-government and the development of the great national infrastructures connecting public offices and bringing administrative services to citizens and enterprises.⁵⁸

eIC

The EIC card is issued by municipalities. It was firstly conceived in the second half of the Nineties as a tool for simplifying relations between government and citizens, seeking to achieve a number of objectives:

- greater security in identification for law enforcement purposes;
- use as an identification tool for online services;
- complete interoperability throughout the country.

Initial trials began in 2001 with the distribution of 100,000 cards by 83 municipalities. Currently, however, the distribution process had to be delayed due to relevant initial misconceptions about what the functions of the card have become evident. In particular, it emerged that for security reasons it is hardly feasible to use the same instrument as an id-card and a qualified signature tool. The EIC is recognized as a valid travelling document

⁵⁶ Epractice.eu, eGovernment Factsheet - Italy - National Infrastructure, <http://www.epractice.eu/document/3395>

⁵⁷ CNIPA, [url:http://www.cnipa.gov.it](http://www.cnipa.gov.it)

⁵⁸ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Italy, <http://ec.europa.eu/idabc/servlets/Doc?id=29087>

within EU countries.⁵⁹

NSC / CNS (NSC: National Services Card / CNS: Carte Nazionale dei Servizi)

The NSC is a card issued by public administrations, which embeds a microprocessor having the same features as the EIC and the same running software. The difference to the EIC is that no laser band, holograms, photo etc are used to make the card secure against imitation. The NSC is not accepted through a visual identity check at the border but it can be used to sign electronic documents with a qualified signature moreover it contains an entity authentication certificate and a qualified signature certificate.

Such card e.g. issued by the Chambers of commerce (working also as the CA "Infocamera") allows users to access their data recorded in the registry of enterprises. The NSC is also expected to be used as a common tool for electronic payments toward Public Administrations.⁶⁰

Italy decided to rollout the NSC in order to have a better instrument for being able to sign electronically.⁶¹

INA-SAIA

The objective of the National Centre for Demographic Services (Centro Nazionale per i Servizi Demografici – NSCD) which was founded in 2002, to centralize the IT infrastructures concerning signature data through the eIC in the INA-SAIA system. Several management tasks had to be solved:

- the National Registry Office Index (Indice Nazionale delle Anagrafi - INA);
- the Personal-Data Access and Exchange System (Sistema di Accesso e Interscambio Anagrafico -SAIA);
- the upkeep of Registers of Italians Resident Abroad (Anagrafi degli Italiani Residenti all'Estero -AIRE);
- the automated monitoring of Registry Office records and marital status.

The Personal-Data Access and Exchange System is based on the National Registry Office Index, which is designed to monitor data records of the registry office.

Municipalities have to keep the index constantly up to date with the personal data at their disposal. By managing the so-called "INA-SAIA applications backbone", the National Centre for Demographic Services is also able to manage personal-data exchanges between municipalities and other local authorities. In this way, all municipalities become able to issue Electronic Identity Cards to their citizens.⁶²

IT-MOD Multiservice Card (CMD)

The initial project, named "Milcard", started in year 2000, with a limited extent to the Italian Army. Its main goal was to collect and store on a smart card the health information of every soldier in the region of Balkan. As a secondary goal, the card was used in order to

⁵⁹ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Italy, <http://ec.europa.eu/idabc/servlets/Doc?id=29087>

⁶⁰ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Italy, <http://ec.europa.eu/idabc/servlets/Doc?id=29087>

⁶¹ CNIPA, The perspective of digital identity in Italy and Europe http://www.aipsi.org/eventi/evento_864931ed01aaa9c249356eae29cf5b94f8fab2c2/download/manca_cnipa.pdf

⁶² IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Italy, <http://ec.europa.eu/idabc/servlets/Doc?id=29087>

securely identify the personnel accessing the central databank. Later on, when other Administrations (Justice) issued a tender for the adoption of the same card, the name was changed in "Carta Multiservizi del Dipendente" i.e. Multiservice (Public) Employee Card.

The CMD is a valid ID document (comparable to the eID Card). With respect to the National ID Card the CMD has an interoperable, CNS-like subset of information but also a set of services which are instead specific for its on-field use⁶³. Two interesting examples of these specific services are the military health data structure and the certificate for mail signature and encryption, other services like in the context of the military are access control, digital signature, access to restricted areas, fuel card, central data bank access, weapon retrieval, etc.

The MOD seems to be driven by the military, as they defined the following main objectives⁶⁴:

- Support digital certificates for legally valid digital signature, strong authentication and encryption;
- Become the new electronic ID document of the defense personnel;
- Contain the health data of the IT-MOD employee (emergency card);
- Contain two fingerprint templates (right and left hand);
- Be interoperable with the other relevant electronic ID documents used in Italy (Electronic ID Card (CIE), National Service Card (CNS))
- Be interoperable with international standards for the health data structure (NETLINK standard adopted).

4.2 Current and planned figures on usage of certificates for online services

Above 2 millions of eIC's have been issued at the beginning of 2006. About 40 millions of paper based identity cards replaced with eICs before the year 2010. During 2006 about 16 millions of National Services Cards are planned to be issued, but this could not be confirmed yet.⁶⁵

In Italy the architecture of the national e-Health system features the Electronic Health Record (EHR) that contains information regarding a patient's medical history. In Italy 13 million smart cards have been issued, which can be used as an Electronic Health Card and as an Electronic Identity Card. The diffusion of Electronic Health Cards depends on regional authorities. Lombardy is the region in which smart cards are more diffused (9 millions) among citizens and already in use.⁶⁶

The ANCI (Association of Italian Municipalities) has collected experiences with e-cards and has developed recommendations for the communes. In the first project phases the following problems have been encountered:

⁶³ IDABC, eID Interoperability for PEGS in Italy ,11.2007, <http://ec.europa.eu/idabc/servlets/Doc?id=29602>

⁶⁴ Ministero Difesa, IT-MOD Multiservice Card (CMD), 2007, http://www.inco-health.org/docs/relazioni_26022007/Fattorini_MinisteroDifesa.pdf

⁶⁵ CNIPA, The perspective of digital identity in Italy and Europe http://www.aipsi.org/eventi/evento_864931ed01aaa9c249356eae29cf5b94f8fab2c2/download/manca_cnipa.pdf

⁶⁶ SINCERE, Visionary eHealth roadmap, 14.02.2007, <http://www.be2-aalborg.dk/download/SINCERE%20Visionary%20e-health%20Roadmap.pdf>

- Connectivity to SSCE
- Lack of documentation
- Personnel in communes are not sufficiently trained, causing problems with the use of the technology.⁶⁷

4.3 Best practice services already existent or planned

CRS-SISS

The project CRS-SISS⁶⁸ manages in the Lombardy Region of the healthcare folder of all the citizens of Lombardia Region by collecting digitally signed documents and other information about contacts between the citizen and the healthcare service providers. The professional card is called SISS (Health Care Information System). The modification of health data is only allowed in combination with a second card, the citizen card. Lombardia Region citizens are the final customers of the healthcare services. The core of the CRS-SISS project is an 'Healthcare Extranet', which links operators, social services, organizations and citizens, tracking all the events which occur in the patient treatment (from prescription to administration) and providing value added services. The citizen card is called CRS ("Regional Services Card").

The CRS-SISS project, using its CNIPA credited CA, creates two certificates for each operator:

- authentication certificate
- qualified signature certificate

Currently (end 2007) about 3.450.000 recipes per month are logged and digitally signed. The digital signature of referrals, being still in an early phase of diffusion, logs about 140.000 signed referrals per month. The expectation of the project, when completely deployed, is to reach about 16.000.000 transactions per month, of which about 60% digitally signed. The trend of transactions per month is sustaining the expectations, with a growth of about 15-20% per month⁶⁹. Some statistics of 2006 show that a total of 35.000.000 transactions since 2003 were performed.⁷⁰

In order to guarantee the deployment of ICT infrastructures throughout the system 30€ millions a year over the last 5 years have been to be invested from the regional government.

The biggest hurdles are seen by the project leader in the organizational side. They found out that the problems are less on the technological side but more about how health care professionals are involved in promoting and implementing efficient use of ICT tools to

⁶⁷ Modinis IDM, National profile for eGovernment IDM initiatives in Italy, 02.2007, <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ItalianProfile>

⁶⁸ Carta regionale dei servizi, www.crs.lombardia.it

⁶⁹ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Italy, <http://ec.europa.eu/idabc/servlets/Doc?id=29087>

⁷⁰ Health Leader Innovation Forum, Personal Health Record: view from the top, 05.06.2007, <http://www.healthleadersinnovationforum.com/presentations/Day%20%20Session%20%20Personal%20Record%20View%20from%20the%20top.pdf>

the advantage of their work and of their patients' health conditions.⁷¹

Facts of the CRS-SISS:

- Citizens: around 9 millions CRS delivered with a coverage of >90%, 52% have been activated⁷²
- Professional Cards distributed: 70.000
- Public Health Service (15 Local Health Services, 29 Hospitals and 5 Healthcare Research Institutes), with around 99% coverage
- 2500 Private Healthcare and Social Services Suppliers^{73,74}

All over the country more than 10 eHealth projects started that support digital signatures, like the SOLE project in Emilia-Romagna which can be used for prescriptions, booking of medical services and to store and diffuse Electronic Health Records.

Entratel and Fisconline

Entratel and Fisconline are two web portals providing professional tax middlemen (Entratel) and tax payers (Fisconline) with ICT services for transmitting income-related data to tax administration. Since 2007 a fusion of the two portals has been performed to one portal⁷⁵.

The tax system is available through on Microsoft operative systems or MacOS where a specific software tool, downloadable from Fisconline web service, allows to electronically sign files which have to be transmitted. The files to proceed must have been previously created using an ad hoc tool for tax declarations. Then the system asks for the user's PIN code, and an eSigned encrypted document is subsequently created. After that procedure the document is ready to be sent to <http://telematici.agenziaentrate.gov.it>.

For the future it is planned to create an adaptation to mobile communications. Until the year 2006 650,000 users have electronically signed more than 351 million documents in 8 years.

Unimoney

The unimoney system by unimatica⁷⁶ allows the secure exchange of financial documents between banks and local governments. Unimoney provides also a digital signature based storage system (Unistorage) fully complying with Italian regulations. More than 20 institutions are using Unimoney by signing 300.000 documents each year.

No technical problems did arise, but convincing people to use the system is the main

⁷¹Health Leader Innovation Forum, Personal Health Record: view from the top, 05.06.2007, <http://www.healthleadersinnovationforum.com/presentations/Day%20%20Session%203%20Personal%20Record%20View%20from%20the%20top.pdf>

⁷²SINCERE, Visionary eHealth roadmap, 14.02.2007, <http://www.be2-aalborg.dk/download/SINCERE%20Visionary%20e-health%20Roadmap.pdf>

⁷³Inco Health, The INCO-HEALTH "antennas": experiences and networking, 26.02.2007 http://www.inco-health.org/docs/relazioni_26022007/Beretta_RegioneLombardia.pdf

⁷⁴Health Leader Innovation Forum, Personal Health Record: view from the top, 05.06.2007, <http://www.healthleadersinnovationforum.com/presentations/Day%20%20Session%203%20Personal%20Record%20View%20from%20the%20top.pdf>

⁷⁵Agencia entrate, Service of Entratel and Fisconline (in Italian), <http://telematici.agenziaentrate.gov.it/Main/index.jsp>

⁷⁶Unimatica S.p.a., <http://www.unimatica.eu/default.htm>

problem (especially middle aged and aged persons).⁷⁷

ArchiPRO

The Province of Bologna⁷⁸ coordinates the Project DOCAREA⁷⁹, which aims, as its main target, at creating a back-office technological and managing infrastructure allowing the creation, management and storing of electronic documents. The main objective of Archipro is to make electronic documents legally valid. In the Context of Archipro only smart cards in combination with the DIKE⁸⁰ software application by CA Infocamere⁸¹ which runs under Windows, Linux and MacOS are possible to be used. The whole application is currently configured for the Province of Bologna is set for working with a single signature.

Just 1% of all documents have been digitally signed created or received by using Archipro. Main obstacles result from legal and organizational limitations, and are tied to certificates the validity period of a certificate which is about two years and the procedures for renewal.⁸²

Telemaco

In Italy all companies have to enter specific data like registration, amendment or closure notifications to a Business Register. All documents placed in the electronic Business Register have to be signed by qualified signatures because of legal reasons.

In the year 2005 850.000 electronically signed balance sheets were submitted to the electronic Chambers of Commerce.⁸³

4.4 Legal policies and laws supporting certificates

The first normative action that has established the validity of the digital signature for the subscription of electronic documents has been DPR 513 of 1997, adopted in execution of article 15 of the law n. 59 of 15 March 1997. Subsequently, such norm has been transposed in the DPR n. 445/2000 (Unified Body of Laws on the administrative documentation), modified and updated in the following years. Today, the law that disciplines to the electronic signature is the legislative decree 7 March 2005, n. 82, named "Code of the digital administration", modified from the D.Lgs. 4 2006, n. 159. The norm, in article 1, distinguishes the concepts of "electronic signature", "qualified electronic signature" and "digital signature"⁸⁴.

There are some problems in real life for the application of electronic documents in Italy. Electronic form suits for almost all contracts that should be in written form. The majority of those contracts should be registered by government bodies, and for that it is necessary to put tax stamps on the document, but on electronic document this is still impossible. So

⁷⁷ Ramboll Study, Benchmarking of the national administrative and legal practices in the fields of eSignatures, invoicing as well as contract conclusion and implementation, 11.2006, <http://ec.europa.eu/enterprise/ict/policy/legal/2006-bm-cr/ramboll-benchmarking-final-report-draft.pdf>

⁷⁸ Provincia Bologna (in Italian), <http://www.provincia.bologna.it/provbologna/index.jsp>

⁷⁹ Docarea, <http://www.docarea.it/english/project.html>

⁸⁰ Secure Sign Card, http://www.securesigncard.it/software_d.htm

⁸¹ InfoCamere, (in Italian), <http://www.card.infocamere.it/>

⁸² IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Italy, <http://ec.europa.eu/idabc/servlets/Doc?id=29087>

⁸³ IDABC European Government Services, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE Italy, <http://ec.europa.eu/idabc/servlets/Doc?id=29087>

⁸⁴ Ibls, INTERNET LAW - The Digital Signature in the Italian Legal System, 09.04.2007, http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1723

you have a legally valid contract, but you have problems to register it, so attorneys recommend their clients to sign in classic form. Moreover there does not exist a consistent relevant jurisprudence in the civil law countries.⁸⁵

4.5 Relevant authorities responsible for implementation

CNIPA⁸⁶: The Italian Authority for information technologies in public administration (CNIPA) main tasks are promoting, coordinating, planning and controlling the development of information systems within the government central organizations and agencies, through, interconnection and integration. It also decides about applicable standards.

Infocamere⁸⁷ makes the software for the signature card DIKE⁸⁸ available for free, however there are also products by other Certification authorities available (Postecom, Actalis, National Notary Council, etc.).

4.6 Existence of a roadmap for certificate usage

The plans regarding the National Service Card (CNS) / e-health card are regionally different, as for example:

- New infrastructures will be developed to allow end users and local institutions to access the system. The whole architecture is developed around the Electronic Health File (FSE, Fascicolo Sanitario Elettronico) that contains information regarding a patient medical history.
- This data can be accessed by citizens through the National Service Card (CNS), which is a smart card that can be used as an Health Card or as an Identity Card.
- Local authorities can introduce the National Service Card Since January 2005, following the guidelines issued by the National Centre for ICTs in the Public Sector (4th of January 2005, www.cnipa.gov.it/site/it-IT). A network of regional systems in which medical histories of individuals –Electronic Health Records – will be stored is built. This network will be accessible anywhere in Italy by medical personnel and administrative bodies.
- In Lombardy e-Health sector is quite developed, it has been the first Italian region to introduce Regional Service Cards – in 2006 there were 9 millions digital health cards, of which 52% already active. Electronic Health Records are stored and diffused among local actors through a network called SISS (Informative Social and Medical System).In 2007 this system will be extended also to private medical structures.

Adopting Commission approach the National Service Card can be used as European Health Insurance Card (EHIC), which enables European citizens to receive Health treatment in the whole European Union, according to the rules of hosting countries.⁸⁹

⁸⁵ Katerina Dulcic, LLB Lawyer's perspective on digital signatures in Europe, 2004, http://www.carnet.hr/CUC/cuc2004/program/radovi/a3_dulcic/a3_full.pdf

⁸⁶ CNIPA, CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione, National Centre for ICT in the Public Administration), <http://www.cnipa.gov.it>

⁸⁷ InfoCamere, (in Italian), <http://www.card.infocamere.it/>

⁸⁸ Secure Sign Card, http://www.securesigncard.it/software_d.htm

⁸⁹ SINCERE, Visionary eHealth roadmap, 14.02.2007, <http://www.be2-aalborg.dk/download/SINCERE%20Visionary%20e-health%20Roadmap.pdf>

4.7 Time schedule of roadmap for service usage

CRS-SISS project has been divided into two stages. In the first stage (1999 to 2002) they did set up the organization. In the Region of Lecco they started an prototype on 300.000 citizens. In the second stage, which starts in 2002 and ends in 2009 the planned to extend the system to the whole region of Lombardy and it is planned to select new partner for the CRS-SISS project. They issued more than 90% of all planed cards to the citizens, as just 52% of these cards have been activated in 2006.⁹⁰

⁹⁰Health Leader Innovation Forum, Personal Health Record: view from the top, 05.06.2007, <http://www.healthleadersinnovationforum.com/presentations/Day%202%20Session%203%20Personal%20Record%20View%20from%20the%20top.pdf>

5 Germany

5.1 Introduction

Germany's federal eGovernment 2.0 program was launched on 13 September 2006. eGovernment 2.0 is based on the eGovernment action plan in the EU's i2010 initiative, as well as on experience with Germany's own federal strategy BundOnline 2005 (2000-05) and the national strategy Deutschland-Online (2003-). All federal bodies will be following the program, which will be coordinated by the Federal Ministry of the Interior. The aim is to make eGovernment an integral part of administrative innovation. The government has identified four points for targeted action between now and 2010:

- Portfolio: demand-oriented expansion of the Federal Government's eGovernment services in terms of quality and quantity
- Process chains: electronic cooperation between businesses and public administrations via joint process chains
- Identification: introduction of an electronic identity card and development of eID concepts
- Communication: a secure communications infrastructure for citizens, enterprises and administrations including citizen portals for the provision of a data safe and an electronic address for everybody and including a certification program.

The eCard strategy of the German Federal Government coordinates the different federal e-card initiatives (such as the e-health insurance card, the e-ID card, and the job card/eLENA) as well as the access to important databases and services in the areas of social security and tax procedures:

- ePassport: Called 'ePass', the new German travel document was officially introduced on 1 November 2005. The passport includes an embedded RFID chip that will initially store personal information such as name and date of birth, as well as a digital facial image of the holder. In a second phase – starting in November 2007 – the chip will also store a scan of the holder's left and right index fingerprints.
- eID Card: There are plans for introducing an electronic identity card (elektronischer Personalausweis) end of 2009. The new eID Card shall be used for visual inspection and, in addition, for universal identification and authentication on the Internet for eGovernment and eCommerce services. For this purpose, features for electronic authentication (mandatory) and for digital signatures (optional) will be implemented. The chip on the card will contain the same information which is printed on the card today. The chip will also contain certificates to prove these data. Data from the chip can only be read if the holder agrees by entering a PIN beforehand. As the card shall be used for authentication in the private sector as well, and because in different contexts different parts of the total data are necessary, there will be a function to allow the holder to control which data can be read in a specific situation. For example, when an age control is required, only the data from the age field can be read.⁹¹
- eHealth Insurance Card: The Federal Ministry of Social Affairs and Health plans the

⁹¹ IDABC, eID Interoperability for PEGS in Germany, 2007, <http://ec.europa.eu/idabc/servlets/Doc?id=29591>

introduction of an ehealth card in Germany for citizens. Doctors and pharmacists will get a health professional card, which is equipped with an electronic signature to sign, e.g., prescriptions. Main target of the project is the digital support of already established processes in the health sector. According to the German government, the e-health insurance card is not to be distributed to the broad public before 2010. Producing and distributing cards to about 80 million people will indeed represent a major logistics operation.

5.2 Current and planned figures on usage of certificates for online services

The final report of the BundOnline 2005 initiative counted in excess of 440 online services being used by the federal Government alone. Naturally, only a very small proportion of these 440 online services depend on the use of electronic signatures. Most of the services provided online are made up of information and communication services. This will remain the case in future.

In the institutions of government the digital signature is rarely discussed, seldom used and moderately understood as a study⁹² shows from 2007 for North Rhine-Westphalia. All of the involved administration see a high potential of signatures but do not use signatures or just the weakest form, a standardized e-mail signature. About 30% of the asked people do not use any signatures 26% use the weakest form (standardized mail signatures) and just 8% use the qualified signature. A major problem is a widespread uncertainty concerning the correct handling of signatures.

The electronic signature will certainly gain further impetus in the wake of the two big, radical projects to be implemented within the next years (2009 / 2010) at the instigation of the federal Government – electronic health card/HPC and electronic ID card. Ubiquity does not necessarily translate into intensive use but in combination with appropriate awareness building measures it does reduce inhibitions and other reservations

Germany expects that certificates (authentication certificates) will be used extensively as soon as the new eID card is issued. A variety of public and private services are expected to accept the eID card for authentication. Nevertheless the security infrastructure to support these eID cards is not place yet. A certificate for electronic signatures can be optionally installed on the eID card.

5.3 Best practice services already existent or planned

Because of Germany's federal structure - Germany is organized into 16 federal Länder (states), which exercise responsibility on their own account the federal Government is unable to take any far-reaching decisions on behalf of the federal states and municipalities. As most administrative services in Germany are provided not by the federal Government but by the states and municipalities, their Government activities assume particular significance in the German context. It would be beyond the scope of this study to examine all of the eGovernment initiatives of the 16 federal states. The "Deutschland-Online" webpage contains an up-to-date overview with corresponding links to other sites.

⁹² Informationsbüro d.NRW, Studie, Auswertung Thema: Formulare und Signaturen, 2007, http://www.egovernmentplattform.de/fileadmin/user_upload/PDF/Umfrage/Infobuero_dNRW_Formulare_Signaturen.pdf

Qualified electronic signatures are widely accepted by administrative agencies⁹³.

Some best practice services are mentioned below and a more comprehensive list of services can be found in the IDABC report on Germany⁹⁴.

Public procurement system (eProcurement)

The flagship e-Vergabe project was considered to be one of the most important projects of the BundOnline 2005 initiative. The service will permit the electronic awarding of federal administration (BVA) orders based on communications between the awarding agency and potential bidders that are comprehensive, legally binding and free from media discontinuities. The offering ranges from notification via electronic tender submission through to contract award using the contract award platform. The documents containing the contract terms can be downloaded and bids submitted with an electronic signature. The system is used by companies and by all of the federal Government's awarding authorities as well as by a number of states and municipalities. The eVergabe application currently supports only qualified electronic signatures. As a result of changes in the contract terms advanced signatures (software certificates) have also been accepted since November 2006.

Environmental protection

The German Emissions Trading Authority (DEHSt) within the Federal Environment Agency is the national authority with responsibility for implementing the Kyoto protocol's market based climate protection toolkit: emissions trading and the project based mechanisms that are Joint Implementation (JI) and the Clean Development Mechanism (CDM). In September 2006 DEHSt received the 6th eGovernment prize for federal, state and municipal administration in the category "best virtual organisation" for its fully electronic business processes. As a matter of principle, the system supports unsigned, advanced and qualified signature messages. Currently only unsigned and qualified signature messages are used.

Virtual Postal Center⁹⁵

The Virtual Postal Centre is a central basic component Data Security. It supports secure, clear and confidential communication between agencies and external communication partners such as citizens or companies. As such it works as a central security gateway which provides the functions authentication, signature verification, signature creation, decryption and encryption, e.g. the Virtual Postal Centre supports secure communication via both e-mail and web channels. It also maintains interfaces to back-office applications such as archive systems, workflow and document management systems and application transactions. A VPC provides the following security functionality over prescribed interfaces: Encryption and decryption, creating and checking signatures, creating and checking time stamps, security checks such as checking for viruses and content in e-mails and documents, authentication, status checking in the context of delivery and receipt mechanisms.

The so-called Electronic Court and Administration Mailbox (EGVP) is based on VPC.

⁹³ Points of acceptance for qualified electronic signatures, [http://www.where2sign.de/index.php?id=433&L=1&tx_jwakzeptanzstellen_pi1\[filter\]\[tx_jwakzeptanzstellen\]\[0\]\[uid\]=0&tx_jwakzeptanzstellen_pi1\[filter\]\[tx_jwakzeptanzstellen\]\[0\]\[kategorie\]=4&tx_jwakzeptanzstellen_pi1\[cmd\]=LIST&cHash=3cbdfb6a8f](http://www.where2sign.de/index.php?id=433&L=1&tx_jwakzeptanzstellen_pi1[filter][tx_jwakzeptanzstellen][0][uid]=0&tx_jwakzeptanzstellen_pi1[filter][tx_jwakzeptanzstellen][0][kategorie]=4&tx_jwakzeptanzstellen_pi1[cmd]=LIST&cHash=3cbdfb6a8f)

⁹⁴ IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Germany, April 2007, <http://ec.europa.eu/idabc/servlets/Doc?id=29077>

⁹⁵ BSI, Virtual Postal Center (in German), <http://www.bsi.de/fachthem/vps/publikationen.htm>

eCard API

The German eCard-strategy aims at harmonizing the various government projects which issue or use smart cards for authentication and signature purposes. Against this background the German government developed the eCard-API-Framework⁹⁶ specification which aims at supporting arbitrary smart cards and facilitating the integration of them into various eID-applications. Based on these currently emerging eCard-API applications can use electronic signatures in a uniform way. A test specification and a so-called testbed supports software developers for compliance with the eCard-API.

5.4 Legal policies and laws supporting certificates

The Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway is the competent authority in accordance with §3 of the Signatures Act (SigG). All laws and Ordinances regarding electronic signature can be downloaded here⁹⁷, such as

- Information and Communication Services Act (Informations- und Kommunikationsdienste-Gesetz – IuKDG)
- Framework for Electronic Signatures, Amendment of Further Regulations Act (Signaturgesetz - SigG) of 22 May 2004
- Electronic Signature Ordinance (Signaturverordnung - SigV) of 22 November 2001

The “written form requirement” issue in particular is of great importance as far as the use of electronic signatures is concerned:

- Act on the Amendment of Formal Regulations under Private Law and other Regulations governing modern Legal Transactions (FormAnpG) of 13.07.2001; FormAnpG introduces the electronic format as an optional written form. That means that the qualified electronic signature can be used instead of the handwritten signature in legal relations. But there are exceptions as well, for example termination of a contract of employment, a promise to pay a debt or the writing of a reference are expressly excluded.
- Second Law amending the tax regulations (Tax Amendment Act 2003 – StÄndG 2003)
- Law on the use of electronic forms of communication in the judicial system (JKomG – Justice and Communication Act) of 22.03.2005.

5.5 Relevant authorities responsible for implementation

Deutschland-Online⁹⁸

Deutschland-Online is Germany's national eGovernment strategy of the federal government, federal-state governments and municipal administrations and strives for an integrated eGovernment on all administrative levels.

A joint project management unit was set up at the office of the Conference of State Sec-

⁹⁶ BSI, Das eCard-API-Framework (BSI TR-03112), in German, 3.3.2008
<http://www.bsi.bund.de/literat/tr/tr03112/index.htm>

⁹⁷ Bundesnetzagentur, Legal Underpinnings,
http://www.bundesnetzagentur.de/enid/89fa00a0877e14651df69ff2dba346a5,0/Electronic_Signature/Legal_Underpinnings_z4.html

⁹⁸ Deutschland-Online, <http://www.deutschland-online.de/>

retaries at the Federal Ministry of the interior with responsibility for overall project management, knowledge management, controlling as well as management of the support services for the prioritised projects. Furthermore, the office is also in charge of monitoring the other Deutschland-Online projects.

Conference of State Secretaries

The Conference of Federal and Federal-State State Secretaries responsible for eGovernment with involvement of central municipal organisations on an equal-rights basis meets four times a year. On behalf of the heads of federal and federal-state governments, this Conference co-ordinates federal cooperation in the field of eGovernment and is in charge of the political steering of Deutschland-Online.

Conference of Minister-Presidents and Conferences of Specialized Ministers

The Conference of Minister-Presidents and the Conferences of Specialized Ministers are bodies in which federal states cooperate in their own spheres of responsibility. The federal states use these conferences in order to agree on proceedings in matters of joint interest, develop their position in relation to the federal government and also seek mutually agreed solutions with the federal government.

BSI⁹⁹

The Federal Office for Information Security (BSI) is Germany's National Security Agency. The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions. This work includes IT security testing and assessment of IT systems, including their development, in co-operation with industry.

KBSt¹⁰⁰

The Federal Government Co-ordination and Advisory Agency for IT in the Federal Administration (KBSt) is located within the Federal Ministry of the Interior, the KBSt is an inter-ministerial agency of the Federal Government intended to ensure that the federal administration optimizes its use of information technology for specific fields and in organizational, economic and technical terms.

KoopA¹⁰¹

The Kooperationsausschuss ADV (KoopA ADV) (Co-operation Committee Automatic Data Processing), to which the federal Government, states and municipal umbrella associations belong, is a body that unanimously agrees common principles governing the use of Information and Communication Technologies (IT) and important public administration IT projects.

Bundesnetzagentur¹⁰²

The Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway is a separate higher federal authority within the scope of business of the German Federal Ministry of Economics and Technology. It is the competent authority in accordance with §3 of the Signatures Act (SigG). Information on Certification-Service Providers, products for Qualified Electronic Signatures and testing and confirmation offices can be found

⁹⁹ BSI, <http://www.bsi.bund.de>

¹⁰⁰ KBSt, <http://www.kbst.bund.de/>

¹⁰¹ KoopA, <http://www.koopa.de/>

¹⁰² Bundesnetzagentur, <http://www.bundesnetzagentur.de/>

here.

5.6 Existence of a roadmap for certificate usage

Deutschland-Online action plan¹⁰³

Deutschland-Online is Germany's national eGovernment strategy of the federal government, federal-state governments and municipal administrations and strives for an integrated eGovernment on all administrative levels.

The aim of Deutschland-Online is to create a fully integrated eGovernment landscape in Germany. The necessary standards are set and the strengths of federalism are put into practice in that individual partners lead the way with model solutions which also benefit others (the "one or some for all" principle). In this way, uniform and consistent online services are enabled across all administrative levels.

Besides the basic infrastructure and standardization projects, the Deutschland-Online action plan also includes three other projects which are directly orientated towards the needs of citizens, i.e. motor vehicle registration, civil status registers and citizens' registries.

eID card

A concrete roadmap is not published yet.

e-health card

In January 2006 the electronic health card was introduced in eight pilot regions. The overall objective is to interlink more than 80 million patients with about 270.000 physicians, 77.000 dentists, 2.000 hospitals, 22.000 pharmacies and more than 300 health insurance funds. The electronic health card and the necessary components for its implementation will be tested under laboratory conditions. This test phase is a continuous process where the basic features and further applications will be tested under laboratory conditions and with test data.¹⁰⁴

5.7 Time schedule of roadmap for service usage

Certificate usage will be fostered by the nation-wide distribution of the e-health and eID card in 2009/2010.

e-health card

It was planned to start the first concrete rollout of the e-health card in 2008 which could not be reached as the 100.000 card test did not yet start. Currently it is expected that the nationwide rollout will not start before 2010.

¹⁰³ Deutschland-Online action plan, http://www.deutschland-online.de/DOL_en_Internet/broker.jsp?uMen=c59506d6-81bd-7011-2668-414b826c9940

¹⁰⁴ SINCERE, Visionary eHealth roadmap, 14.02.2007, <http://www.be2-aalborg.dk/download/SINCERE%20Visionary%20e-health%20Roadmap.pdf>

6 EU

6.1 Introduction

i2010 is the EU policy framework for the information society and media. It promotes the positive contribution that information and communication technologies (ICT) can make to the economy, society and personal quality of life.

The i2010 strategy has three aims:

- to create a Single European Information Space, which promotes an open and competitive internal market for information society and media services,
- to strengthen innovation and investment in ICT research,
- to support inclusion, better public services and quality of life through the use of ICT.

i2010 is currently undergoing a mid-term review to make sure that it remains up to date with the rapidly changing ICT environment. The updated strategy will be presented in spring 2008.

Given the importance of ICT for today's economy, i2010 is a key element of the Lisbon strategy for growth and employment.

The i2010 strategy was launched by the European Commission in June 2005 and will be in place until 2010.

EU Action Plan 2010 requesting safe access to services EU wide¹⁰⁵:

When citizens travel or when they move they want easy access to services. EU governments have agreed to facilitate this process by establishing secure systems for mutual recognition of national electronic identities for public administration web-sites and services. The Action Plan foresees a full implementation by 2010. The Commission will help make this happen by supporting wide-scale cross-border demonstrators, identifying common specifications for electronic ID management during 2007 and by reviewing the rules of electronic signatures in 2009.

6.2 Current and planned figures on usage of certificates for online services

In Commission report¹⁰⁶ of 15 March 2006 on the operation of Directive 1999/93/EC on a

¹⁰⁵ EU Press release: eGovernment: Commission calls for ambitious objectives in the EU for 2010, 25 April 2006, <http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/06/523&format=HTML&aged=0&language=EN&guiLanguage=en>

¹⁰⁶ EC Report on operation of Electronic Signature Directive, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2006&nu_doc=120

Community framework for electronic signatures the Commission notes that there has been far less use of qualified electronic signatures than expected. The main reason for this is economic, in that service providers have little incentive to develop a multi-application electronic signature and prefer to offer solutions for their own services. A number of applications in the future might nonetheless trigger market growth, particularly in relation to eGovernment services.

The lack of technical interoperability at national and at cross-border level causes another obstacle for the market acceptance of e-signatures. It has resulted in many “isolated” islands of e-signature applications, where certificates can only be used for one single application. EESSI has worked on common interoperability standards but most of the Member states have specified national standards in order to promote interoperability.

Today, in the PKI environment, the smart card is the mostly used signature-creation-device because the smart card provides a means to store the private key securely. This technology is expensive and requires physical infrastructure investments (distribution of cards and card readers etc). There are already a number of alternatives to the smart card that can be used to store the cryptographic key securely.

Another practical reason for the reluctance to implement e-signature applications is that the archiving of electronically signed documents is considered too complex and uncertain. Legal obligations to keep documents for as long as over 30 years, require costly and cumbersome technology and procedures to ensure readability and verification of such period of time.

In the IDABC “Preliminary study on mutual recognition of eSignatures for eGovernment applications”¹⁰⁷, November 2007, was performed with the following goals:

- identify and analyze the similarities and differences in the use of electronic signatures in eGovernment applications in each Member State both in the legal context, and on the technical implementation aspects;
- assess the impact of the identified similarities and differences on the interoperability of eSignatures and hence of the eGovernment applications;
- prepare conclusions and recommendations on addressing interoperability issues related to the mutual recognition of electronic signatures for eGovernment applications/services.

The report notes that authentication mechanisms are used in many countries as a viable alternative to actual e-signatures, since the required functionality can often be emulated in a sufficient manner by such mechanisms.

6.3 Best practice services already existent or planned

Electronic Signatures

A specific action was initiated by the European Commission IDABC unit to analyze the requirements in terms of interoperability of electronic signatures for different eGovernment applications and services taking into account the relevant provisions of Directive 1999/93/EC on a Community framework for electronic signatures and their national implementation as well as the report on the Directive and the standardization activities on the interoperability of electronic signatures.

¹⁰⁷ IDABC, Preliminary study on mutual recognition of eSignatures for eGovernment applications, November 2007, <http://ec.europa.eu/idabc/en/document/6485>

The current situation regarding the use of eSignatures in national eGovernment applications is represented in a Web site¹⁰⁸ that lists all *EU country's significant applications*.

Identity Management

The EU i2010 Action plan stresses, that eGovernment identity management in the EU should be advanced by addressing interoperability issues as well as future needs, without ignoring differences in legal and cultural practices and the EU framework for data protection. The Modinis study on Identity Management¹⁰⁹ in eGovernment lists the *current plans and status regarding identity management in the different EU countries*.

6.4 Legal policies and laws supporting certificates

Directive¹¹⁰ 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures – the *Electronic Signature Directive* - lays down the criteria that form the basis for legal recognition of electronic signatures by focusing on certification services. These comprise the following:

- common obligations for certification service providers in order to secure transborder recognition of signatures and certificates throughout the European Community;
- common rules on liability to help build confidence among users, who rely on the certificates, and among service providers;
- cooperative mechanisms to facilitate transborder recognition of signatures and certificates with third countries.

The *Public Procurement Directives*¹¹¹, which entered into force on 30 April 2004, complete the legislative framework for the use of electronic signatures in public procurement. Use of e-signatures is central to establishing operational e-procurement systems across the EU. E-procurement can be expected to be one of the major fields of application, especially for more advanced forms of e-signatures. E-procurement illustrates the challenges to be overcome when promoting the use of e-signatures.

6.5 Relevant authorities responsible for implementation

i2010 High Level Group¹¹²

The Commission has set up a High Level Group of Member States' representatives to advise the Commission on the implementation and development of the i2010 strategy. The group reviews the effectiveness of i2010 and gives advice on possible improvements and adjustments, using benchmarking to monitor i2010 implementation and policy evolu-

¹⁰⁸ IDABC, eGovernment applications grouped by country, <http://ec.europa.eu/idabc/eSig-Web/indexd708.html?id=3>

¹⁰⁹ Modinis IDM, National IDM Profiles, <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/NationalProfiles>

¹¹⁰ EU Electronic Signature Directive, <http://europa.eu/scadplus/leg/en/lvb/l24118.htm>

¹¹¹ Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transports and postal services sectors, OJ L 134, 30.4.2004, p.1 and Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, OJ L 134, 30.4.2004, p.114

¹¹² i2010 High Level Group, http://ec.europa.eu/information_society/eeurope/i2010/high_level_group/index_en.htm

tion. The High Level Group is composed of one representative per Member State at Director General level. It is chaired by the Commission and meets up to three times per year. It is open to observers from candidate and EEA countries. The High Level Group is an advisory group and falls under the classification of "experts group".

IDABC

IDABC¹¹³ stands for Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens. It uses the opportunities offered by information and communication technologies to encourage and support the delivery of cross-border public sector services to citizens and enterprises in Europe, to improve efficiency and collaboration between European public administrations and to contribute to making Europe an attractive place to live, work and invest.

By using state-of-the-art information and communication technologies, developing common solutions and services and by finally, providing a platform for the exchange of good practice between public administrations, IDABC contributes to the i2010 initiative of modernizing the European public sector. IDABC is a Community program managed by the European Commission's Directorate-General for Informatics.

6.6 Existence of a roadmap for certificate usage

eIDM

Citizens, as they move across the EU, want easy access to public administrations and services. Businesses often need to verify the identity of their customers. Just like a plastic identify card in your wallet, eIDM guarantees the identity of any entity or person, fast and reliably without the person having to be physically present.

For eIDM, the EU takes a pragmatic approach, seeking interoperability between national identity systems rather than taking on the onerous task of inventing and deploying completely new identity management systems. This way, national regulations can be respected while still creating the essential function of eIDM.

Putting public services on-line requires more than identity: document authentication is critical, too. A physical birth certificate can be examined for its provenance, but currently there is no pan-European digital equivalent. The EU will, therefore, set up a reference framework for authenticated electronic documents across the continent.

The planning for this important topic is reflected in the Electronic Identity Management roadmap table¹¹⁴ and paper¹¹⁵.

Certificates for signatures and authentication are the key enabling techniques to support eIDM.

eSignatures

In the IDABC "Preliminary study on mutual recognition of eSignatures for eGovernment applications is stated that from a regulatory perspective, the most significant provisional conclusion seems to be that the surveyed countries have made a rather extensive (and possibly excessive) use of the possibility allowed by the Directive to impose additional

¹¹³ IDABC <http://ec.europa.eu/idabc/en/home>

¹¹⁴ I2010 eGovernment Action Plan, A roadmap for eID for the Implementation of the eGovernment Action Plan, http://ec.europa.eu/information_society/activities/egovernment/docs/eidm_roadmap_table.pdf

¹¹⁵ A Roadmap for a pan-European eIDM Framework by 2010, http://ec.europa.eu/information_society/activities/egovernment/docs/eidm_roadmap_paper.pdf

requirements to the use of e-signatures in public sector applications. Specifically, and regardless of the precise method followed, all surveyed countries exclusively allow certificates from formally accredited or recognized service providers, where foreign CSPs are rarely if ever accredited or recognized. The practical result of this is that every aspiring user of an e-signature in an e-government application first needs to address himself to the appropriate CSP (typically outside of his own borders), thus creating a significant barrier to uptake by non-nationals. To support interoperability especially for signature validation, the most significant recommendation is to set-up a *Federation of Validation Authorities*, e.g. on the basis of the European Bridge/Gateway CA.

The *EU Services Directive*¹¹⁶ claims for single access points to reach all public agencies. The objective of the Services Directive is to achieve a genuine Internal Market in services by removing legal and administrative barriers to the development of service activities between Member States. The Directive will guarantee service providers more legal certainty if they want to exercise two fundamental freedoms (freedom of establishment and freedom to provide services) enshrined in the EC Treaty. This will make it easier for businesses to provide and use cross-border services in the EU, thus increasing cross-border competition in service markets, bringing down prices and improving quality and choice for consumers.

Therefore, the different ICT systems need to be seamlessly networked together, in particular new innovative systems shall exchange data interoperable with older ICT systems and applications. ICT research shall emphasize new forms of dynamic networked cooperative business processes and optimized work organizations. Research activity will consist in creating a business interoperability framework in regards to short-, middle- and long-term change to prevent over- and under-investments in interoperability technology. To promote ICT enabled public services, both, technical and organizational needs have to be considered. Technically common interfaces, portability of identity, and authentication systems are needed. Organizational changes will require new practices, new skills and different legal grounds.

6.7 Time schedule of roadmap for service usage

European Commission eSignature Workshop – Brussels

Directorates-General for Informatics (IDABC) and for Information Society and Media, jointly organized a Workshop on eSignature Interoperability on 12 December 2007 in Brussels, Belgium. The Workshop¹¹⁷ focused on the ways to achieve interoperability and mutual recognition of eSignatures. The workshop summary report and participation list are available¹¹⁸.

Preliminary conclusions are:

- Issues around interoperability are confirmed: legal, technical, organisational
- A need for clarification and information (awareness raising on) of :
 - certain articles of the Directive
 - the consequences of some technical choices (authentication vs. signature)

¹¹⁶ EU Services Directive, December 12, 2006, http://ec.europa.eu/internal_market/services/services-dir/proposal_en.htm

¹¹⁷ European Commission eSignature Workshop, December 2007, Brussels, <http://ec.europa.eu/idabc/en/document/7310>

¹¹⁸ eSignature Workshop summary report, <http://ec.europa.eu/idabc/servlets/Doc?id=29956>

- clarification of the existing standards (mapping and guidance) and their role (legal compliance)
 - awareness of the existing referenced standards
- There is need to give a response at European level, as for example the creation of a validation structure. This solution implies political will and rules of governance

Follow-up:

- The Commission has issued on 20 November 2007 a Communication on Single Market Review, announcing that "the Commission will present in 2008 a specific Action Plan to further promote the implementation of mutually recognised and interoperable electronic signatures and e-authentication (electronic identity) between the Member States, thereby facilitating the provision of cross-border public services".

7 Conclusion

The main features/activities to support certificate usage in these countries will be summarized.

Austria

Austria promotes the e-card in the context of e-health intensive. In this context the citizen-card functionality is in the hand of every citizen supplied with a health insurance card. An interesting approach to omit that the technology is a too high barrier for some citizen is the citizen-card terminal, which is just in its first instance in pilot action. As further terminals are planned their chances to become accepted and used is good, especially by minorities who do not have a personal computer at their home.

Although the citizen-card functionality is a framework that is able to be used on different card-types, two of three card types seem to have failed. The project for bank-cards does not get enough usage in the context of signature feature and the mobile signature has been stopped in the end of 2007.

Denmark

Denmark has more citizens with internet access than other European countries. Despite of growing regulations for the usage of signatures not every citizen (just 20%) has obtained the signature for itself. As the signature is for free (but not for businesses) and much easier to obtain, because the signature does not need to have a physical token in Denmark, it leads to the conclusion that the citizens do not see a cause for obtaining the signature. Especially the area of digital services is growing in Denmark, but not as frequently used as expected.

In contrast to the citizens the businesses do have direct benefits due to using digital services assisted by signatures. In combination with a law that makes signatures unavoidable compulsory during invoice handling it is possible for Denmark to sell the signatures to companies and pressing the signatures into the economy.

Italy

Italy has a lot of projects concerning signature-cards and the signature. Italy did reach the highest number of issued card in contrast to other region in this study. All over Italy 13 million smart cards have been issued, but 9 million are issued in the region of Lombardy, where just 52% of these cards have been activated. The autonomous competences of each Italian region seem to lead into a rather slow interaction in between these regions however all regions underlay one political directive.

Italy has reached a high level of quality in some single projects but a nationwide implementation that grows out of pilot-project is not seen yet. Reasons for the non acceptance of the usage of signatures are less based on technical aspects but more on cultural and organizational problems. They concrete they hope that younger generation will accept the new card-system better than current generations.

Germany

Even so the PKI is in place for qualified electronic signatures, the usage is not as high as expected for private people. For business activities qualified electronic signatures are used more often, especially in the justice environment and also for procurement and in-

voicing.

With the electronic identity card all citizens will have automatically an authentication certificate, which can be used to “login” to administrative and business services. It is expected that this will lead to a better acceptance of electronic means to authenticate. Nevertheless the signature is an optional feature for electronic identity card.

EU

The EU is concerned with a harmonized infrastructure for cross-border activities. In this respect studies and projects are performed that feature the interoperability aspects. It was observed that the eSignature Directive was implemented in the EU countries but not with the same understanding of what type of signature (advanced or qualified) is used for which service. Identity management is the next goal to achieve, which is concerned with electronic identities and their interoperability in EU countries. Several projects are currently executed regarding IDM.

Part II: PROBLEMS AND MEASURES ON INTRODUCTION OF THE CITIZEN ID CODE-NUMBER

1 Introduction

The following study will begin with personal identifiers in an e-Government context, establishing them as an important element necessary for the implementation of public services. They can also be defined as components within a database that enable a person to be unmistakably identified. In the following analysis the role of the personal identifier in identity management will be explored: it serves as an identifier in government authority databases after prior authentication using certificates. In the following chapter the basic types of personal identifiers will be identified and in turn area-specific and universal personal identifiers will be examined. The next part of the study examines the use of personal identifiers in Europe. An initial general overview will be presented within this context and subsequently the nations of Estonia, Austria, Switzerland and Germany will be examined more closely. The examination will concentrate on the general state of development of these countries in terms of e-Government, e-Government strategies, the use of personal identifiers within this strategy's framework, the relevant technical systems and the progress of the entire project. Furthermore, opinions about the systems in use will be presented. The second main part of the study is concerned with analysing arguments for and against area-specific and universal personal identifiers. The advantages and also the weaknesses of both approaches will be shown and ways in which these weaknesses can be dealt with on both the conceptual and the technical level will be explored. Trust will be identified as a key factor in the acceptance of e-Government processes. The national/cultural context and the legal situation as well as the use of already existing approaches as a starting point for deciding which kind of personal identifiers to use will also be mentioned.

2 The Personal Identifier in the e-Government Sphere

Within the sphere of the public sector's register, e-Government is involved with all administrative aspects of online services between citizens and businesses at various levels of government, between public authorities and between public authorities and businesses. [ITWi08: E-Government]. A singular development approach to new technologies in the public sector and the networking of databases will strive to provide better customer orientation and increase efficiency by developing an e-Government strategy. The aim here must be to work in real time, i.e. to create a system in which all players are constantly exchanging up to date information without any data mismatches occurring and in which personalised data and knowledge of products and services can be provided. [OEST03, 20]

Communication between the above named players at the online level is especially important and this chiefly raises questions to do with trust, communication, integrity and authentication. Identity management plays a central role in this context. An important part of this is the holistic administration of digital identities. To be more exact it concerns creating, registering, changing and deleting identities, classifying roles, rights and attributes and preparing and distributing identities as well as using and inspecting them. [Krause 2007].

During the registration of most services, which are available on non-state run online portals and which occur through the user's autonomous entry which they carry out themselves in a directory (user registration) the use of electronic certificates for authentication is preferred in the field of e-Government as opposed to the use of an access portal for public authorities. This electronic identity can function as a secure access point to a multitude of varying online services for citizens, businesses and other lobby groups. [BEA07: 9] The certificates used are usually issued when the user proves their identity initially and once only at a public authority and it is then saved as an electronic document. Verification of electronic identity occurs during the course of registration with a service e.g. by entering a PIN number or after registering biometric data with the help of a suitable scanner. [BEA07: 4]

The form that this proof takes and the kind of verification which should be used to prove identity is one of the key questions posed by the penetration of new information technologies into the public administration and into the entire public sector in general. In this context the question of which identifiers appear to be suitable for a framework like this also becomes relevant. The term "identifier" stands for a number (a sequence of symbols), that is an element of a database allowing a person or object to be unequivocally identified. [Biaggini02: 5] In this study it will have the same meaning as the terms "personal reference number", "personal identification number" or "personal identifier" which are all terms concerned with the identification of people. In registers of people they are understood to be insurance, register, customer and personal numbers used as register numbers leading to the unmistakable identification of the relevant person. They are therefore not based on ambiguous elements such as personal names, for example.

The following chapter will explain the basic approaches to the use of personal identifiers currently being used in Europe.

2.1 Basic Approaches to the use of Personal Identifiers

Official registers, such as the trade register, the criminal records register and the tax register are part of the public sector's output. Legally significant data about people, objects and procedures pertaining to them are saved in these registers. They can contain a multitude of so called personal identifiers enabling unequivocal identification within a register but they cannot be used outside the confines of the register. These sector-oriented application specific personal identifiers do not merely refer to a concrete subject area or register. [Biaggini02: 5] As e-Government develops it is becoming increasingly essential that official registers communicate with each other in a standardised manner and are able to be networked with each other. [Hristova03, 3]. At this point the sectoral use of such personal identifiers (SPI) as they are used in Germany, for example, reaches its limits rather quickly as the identification number cannot be used across-the-board by different registers. It is therefore difficult to carry out specific administrative procedures which require access to several registers and it is impossible to carry them out in real time.

Another approach is the use of personalised and unique reference numbers at the national level. [DSG-EU03, 8]. As opposed to the methods already presented, the personal identifier can be implemented across all registers. In this case it will be called a "universal personal identifier (UPI) or universal personal identification number and it serves to identify the same person in several official personal registers. [Hristova03, 6]. In order to implement such an approach countries which do not have a centralised register must first set one up. In this case it is conceivable that procedures that have already been used, for example, registers of newborns, could be used as a basis from which unique personal identification numbers could be generated. If the set up of such a system is planned then its legal framework and relevant data protection regulations must be meticulously examined in advance. Alongside both of the procedures presented here there is another approach that is a blend of universal and sectoral personal identifiers. This method would generate a unique personal identification number, known as the root number, but it would not be used directly. Rather the root number would be used to generate several area specific identifiers. The technical approach used with this method ensures that a root number will not be generated from an area specific identification number, derivation can only occur in one direction. Austria and Germany's specific data protection laws, for example, can be taken into account using this system.

3 Personal Identifiers in Different European Countries

The general trend when using personal identifiers is to head towards using already defined unique personal reference numbers or sector oriented reference numbers in order to access online administrative procedures. [DSG-EU03, 9] Germany, Hungary, Switzerland, Great Britain and Portugal use sector oriented reference numbers whereas the use of unique reference numbers may be pushed forward in Ireland, Spain, Slovenia, Italy, the Czech Republic, Denmark, Estonia, Finland, Poland, France, Lithuania and Belgium. Finland, Estonia, Slovenia, Italy, Spain and Belgium already have electronic ID cards and indeed biometric data is already being stored on these cards and used in Italy and Sweden. [Kubic07: 10ff]

Germany and Switzerland have exclusively used sector oriented reference numbers and they have only been used for their originally designated purpose. Yet in the interim Germany and Switzerland have been making efforts to change this. Switzerland has decided to harmonise their official citizens' register with the use of AHV insurance numbers as personal identifiers. On the one hand the new AHV insurance number is a social security number but it should also be able to be used as an administrative personal identification number. [EDÖB07: 3] Germany is examining the Austrian approach to see if it is suitable and to see if an area specific code can be universally used, as it is in Switzerland. Austria has decided upon a unique compromise: to generate area specific identifiers from universal personal identifiers. Estonia has decided to solely use the universal personal identifier.

The following overview will take a closer look at the developments in certain countries. For this analysis the systems used in Estonia, Austria, Switzerland, and Germany will be examined more closely. The aim here is to use these national developments and experiences as a starting point for a discussion about the use of personal reference numbers in their various forms.

3.1 Estonia

Estonia, with a surface of 45 000 square kilometres, is a little bigger than Switzerland but with a population of just under 1.4 million it has significantly fewer inhabitants. [E-INST08]. This relatively small country in northern Europe has far reaching plans and with its "Estonian Information Society Strategy 2013" it wants to create a science based economy and society which also embraces a unique e-Government strategy. This is based on the principles behind a national directive for an "information society" which was passed by Estonian parliament in 1998, as well as on the European strategy i2010¹¹⁹ and sector specific developments. [G-Est06: 4]. In addition, Estonia has the highest Internet usage rate in Europe. 59% of the population between the ages of 15 and 74 used the Internet in 2006. [DOSIS07: 95]. In the field of e-Government, estimates of service providers' online availability places Estonia in second place within Europe. [CAP-G06: 14]

¹¹⁹ „i2010 - A European Information Society for Growth and Employment“ is a European Commission strategy paper dealing with the creation of a fully integrated information society based on the wide use of information and communications technologies (IKT) in the public sector and in small and middle sized businesses. More information can be found at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0229:EN:NOT>>



Figure 1: Personal code number in plain text on the Estonian ID card [Source: Cim06]

The electronic personal identification document, the ID card, together with the unique personal code lies at the centre of these reflections on a unique information and communication strategy. It is an electronic identity document used for unmistakable authentication as opposed to services in the field of e-Government. Every card contains visually identifiable information such as a photograph, the cardholder's name, date of birth, date of issue, card number and the national and universal personal code. It also has special data that includes the above named information and also an email address and two electronic certificates. [Cim06: 9]. Both certificates have electronic keys that are also protected with PIN numbers. One of the certificates is for authentication and the other is for digital signatures. To meet the card's demands only two pieces of information, the name of the card owner and the personal code, are dispatched with the certificate. [Cim06: 16] This is done so that the transmission of personal information can be kept to a minimum and to prevent misuse. A central database with universal personal codes enabling the card owner to be authenticated using the dispatched data is being created in order to meet the planned interoperability requirements. [Cim06: 3]

The "Estonian Government's Citizen and Migration Board" is the institution responsible for distributing ID cards at the national level. The distribution, administration and verification process is, however, carried out by a network of private and public partners. The joint venture AS Sertifitseerimiskeskus consisting of Estonia's two biggest banks is responsible for validating the certificate and managing the entire range of electronic services while the Swiss TRÜB Baltic AS takes care of manufacturing and personalising the cards.

The card can be used for various national services at the e-Government level, which is well developed. In addition, the user logs on to their card with the help of the certificate and an appropriate card reader machine via a central internet portal and from here they can access over 20 databases where they can, for example, fill out an application and/or sign electronic documents.

The electronic ID, which uses a universal personal code and is set out in clear language, has been well accepted by the Estonian populace. By the end of October 2006, 892 957 valid documents were in circulation. [DOSIS07: 23] In southern Estonia 9% of the popula-

tion admitted to using the ID card as electronic identification in 2006.¹²⁰

3.1.1 Evaluation and Critique

With their electronic ID citizens have an easily manageable tool in the hand that can be used for both identification and to sign electronic documents in both public and private sectors. The card will solely be used as a key to access decentralised stored databases. The cardholder's name and personal code only will be used for authentication with an electronic certificate. The ability to access the system using a log file has had a positive effect on the overall acceptance of the entire system, as it allows every ID card user to retrace all requests relating to their personal data. [Cim06: 16] Thus every ID cardholder stays informed of which government department has requested their data and when they requested it.

The use of a unique personal code set out in clear language and the involvement of private businesses in the entire process is not unobjectionable in data protection terms. On the one hand one person can be identified across all departments as they have a universal personal code but on the other hand the state is handing over the most sensitive identification and card manufacturing processes to private businesses. The fragile nature of the Estonian Internet landscape was exposed when a three week long attack on many service providers took place there in 2007. Government sites, parties and media sites were paralysed by the denial of the attacks on services, bank portals were similarly affected and international payment traffic was temporarily stopped. [KÖT08] In this context various Internet service providers also fell under the control of crackers. It is unknown whether identities were stolen from users at this time. This scenario does show, however, that a well constructed e-Government structure, including its networks, can be attacked using fairly simple methods.

3.2 Austria

Austria, which lies in central Europe, has a surface of 84 000 square kilometres and a population of 8 million. Like Estonia, Austria is a relatively small yet very successful player in the e-Government context. The benchmarking of the 28 European countries put Austria in first place. [CAP-G06: 14] With its redesign of the national IT strategy in 2001 and an e-Government law, which has been in force in Austria since 01.03.04, Austria is one of the first European nations to have implemented laws in the field of e-Government [F-NET05]. Internet usage is also very high in Austria and in 2006 it was just under 60%. This places it within the upper third in Europe. [TCUSM07: 2]

Strategies for e-Government solutions are based on three categories. On the one hand there are the elements necessary for organisational implementation. This includes the help.gv.at portal, a cross government department platform in the Internet and FinanzOnline, the federal ministry for finance's website as well as various e-business portals. In addition there are various technical coordination elements to consider such as the citizens' card and the form style guide as well as structural measures such as knowledge management, qualifications and financing. [Bundes06: 19]

¹²⁰Comparison I. http://www.riso.ee/en/files/eSeire_uuringu_IDkaardi_kasutamine_2006_I_ENG_0.pdf



Figure 2: Citizen card [Source: <http://www.digitales.oesterreich.gv.at>]

At the heart of the system lies the citizen card, an electronic identity document with a particular model relating to the personal code. This is not allowed to be stored outside a specialised government department. Instead, it can only be used to generate sector-oriented codes. [DSG-EU03: 9] Austria is following an approach that represents a mixture of both basic versions: the universal personal identifier and the sector-oriented, application specific personal identifier. In order to implement this version every naturally registered individual receives a root number for unambiguous identification. This root number is derived from what is commonly known as the ZMR number of Austria's centralised register of residents¹²¹ and encrypted and it can only be exclusively stored on the citizen card so that it remains under the citizen's control. [Bundesk06: 124] For people working in legal professions the first number to be used will be the company's book number, company registration number or identity number. The root number for natural unregistered individuals will be generated with the help of a supplementary register. A root number register government department will be created with the help of the data protection commission in order to administer the root numbers. This department will also deal with related administrative¹²² queries. A sector specific code can only be generated with the participation of the affected party and implemented using the citizen card. The institution which requires an area specific code then generates this using a special encrypting procedure which makes a retrograde calculation of the root number used here impossible. The root number itself is not allowed to be stored at the processing institution. [Bundesk06: 125] This should ensure that an area specific personal code number cannot be (mis)used for identification outside department boundaries.

3.2.1 Evaluation and Critique

With its concept for a root number derived from a centralised registry of residents that is used to generate area specific personal identifiers, Austria has created a much observed solution based approach in the field of e-Government which satisfies the requirements of the country's far reaching data protection regulations. By centrally storing data and using area specific personal codes they have created a model that incorporates legal data protection issues in a far more thorough manner than Estonia has, for example.

However, the concept has still received some criticism. In *Datenschutz.de* (a data protection portal) Hans Zeger, a member of the Austrian Data Protection Council, addressed the topic of e-Government as follows: "...technically error-prone, not transparent and far too

¹²¹ The centralised registry of residents controls a database which has an Austria-wide overview and history of a person's registered places of residency.

¹²² This becomes necessary when, for example, information about a person pertaining to a particular administrative procedure comes from another sector specific department.

complicated."¹²³ A gap appears to have opened between such proclamations and the reality. The Austrian Society for Privacy and Data Protection is critical of the fact that from more than 1000 administrative procedures only 6 were inter-regional applications and 36 of them were only available at particular locations. The FinanzOnline portal, that had more than a million users in 2006, recorded afterwards that exactly 3500 users had authenticated themselves using the citizen card. The large majority of users had used the classic user name and password method, which raised significant doubts about the system's level of acceptance. [ADAT07: 2] The possibility of connecting with administrative steps, an approach they were striving for despite the sector specific codes, opened up the question as to whether identities could not be assignable across sector borders using this method after all.

3.3 Switzerland

Switzerland, with its surface of approximately 42 000 sq. km and its population of 7.4 million, is one of the smaller but relatively densely populated countries on the European continent. [STOR07]

In the field of e-Government it is considered to be at the tail end of Europe, according to an appraisal commissioned by the European Commission by the management and IT advisors Capgemini. [CAP-G06: 14] This is quite astonishing, as a study by the "Economist Intelligence Unit" in cooperation with the "IBM Institute for Business Value" ranked Switzerland in third place for their state of development in terms of information and communications technologies and also for their ability to use them in government, business and private contexts in their worldwide ranking of the most economically important nations. [EIU06: 5] The Swiss have a very high rate of Internet usage in any case. In 2006, 62% used the Internet at least once every quarter. [HEISE07: 1] Because of their federal structure Switzerland has a multitude of rules for running their official register. It is a similar problem to the one in Germany as due to these circumstances there is a problem that registers of residents are based on different systems and thus people are entered into the system using differing codes and the systems are barely able to communicate with each other. [Hristova03, 20]

In order to achieve a harmonisation of the register and also with a view to future e-Government applications, a federal law was passed in June 2006 to collect data for statistical purposes and to simplify the legal exchange of personal data between registers and also to regulate which identifiers and attributes must be entered into the registers. [Register Harmonisation Law: Article 1] Directives are part of the legal requirements used to administrate the register for resident registration. This register contains personal data such as first name and surname, gender, nationality and also the insurance number and old age and survivors' insurance of every person who has relocated to Switzerland or is resident there. [Register Harmonisation Law: Article 6] Evidently the plan is to turn the original area specific personal identifier AHV number from the old age and survivors' insurance into a cross divisional personal code. A decree about the systematic application of the AHV insurance number outside the AHV determined which authorities and institutions were allowed to use this insurance number. [EDDI07: 1] The law decrees that the insurance number can also be systematically used as a national insurance number which can be used in other areas for implementing premium reductions for health insurance, for social welfare and for enforcing taxation laws, and it can also be used by educational

¹²³ <http://www.datenschutz.de/news/alle/detail/?nid=2372>. Comparison. Also in a similar context: "The Citizen Card – for IT Professionals Only" < <http://oe1.orf.at/highlights/73241.html>>

institutions and by authorities and institutions that are entrusted with enforcing cantonal rights. [Federal law on old age and survivors' insurance: Art. 50c und 50e] As part of these innovations a new AHV number will be introduced in July 2008. This number is completely anonymous and will be composed of Switzerland's 3 digit country code, a 9 digit random number and a 1 digit control number. It will be printed on the AHV identity card in plain text along with the name, surname and date of birth. [AHVIV07: 2]



Figure 3: The AHV number as a personal identifier on the Swiss insurance certificate [source: AHVIV07]

On January 24 2007, the Federal Council passed a national e-Government strategy. This should be developed in collaboration with representatives of the cantons and communities and managed by the federal information technology body. Some of their aims include electronic processing of traffic between government departments and business, electronic handling of processes between government departments, and also between citizens and government departments. [ISOB 2007: 4] There is a catalogue of proposals which have been prioritised for the implementation that is being continually updated and which provides unique personal identifiers in the form of AHV numbers for electronic data exchange between marital status bodies, resident registration bodies, voting registers, the inland revenue, social insurance institutions and trade registers. [SAEGS07: 6]

3.3.1 Evaluation and Critique

The implementation of a cross divisional personal identifier underlines Switzerland's efforts to create a total e-Government strategy for its information and communications systems and to facilitate better networking at a federal level and better processing of cross divisional processes. The AHV number is a tool in Switzerland's hand which can actually create a unique personal identifier. However there is currently no solution to show what a data exchange system will look like. Consequently at the very least Switzerland currently meets the requirements for a uniform e-Government approach, although concrete solutions are still in the early stages of development.

Data protectionists view the fact that a personal identifier deals with a non-spoken number, that it is randomly generated and it does not contain any personal information posi-

tively. However, the greatest danger in data protection terms is the ability to connect different databases. [Zehnd06: 1] The national law on old age and survivors' insurance in Article 50c and 50e allows certain related institutions and organisations to use the AHV number. As the above named players also store personal data about the person concerned, unequivocal identification across sectoral boundaries must occur. In this context the danger that personal data might be improperly used or abused grows considerably, particularly if the personal identifier is stored together with particularly sensitive data such as information about the person's state of health or together with information about criminal proceedings or sanctions pertaining to them. [Biaggini02: 9]

The new regulations are also being viewed critically on the political level. The Swiss Volkspartei (People's Party) opposed the new AHV number citing the reason that through these very possibilities that now exist to link up all this data, a transparent citizen will be created, leading to a surveillance society. There are also peers in the Social Democratic Party (SP) and the Christian Democrats (CVP) who are of the opinion that data protection government departments should be set up at the very least and that the nation's statistical interests should not be allowed to infringe on citizens' personal and privacy rights. [NACH06]

3.4 Germany

Germany, with approximately 82 million inhabitants and a surface of 375 000 square kilometres is one of the largest and most densely populated countries in central Europe. [SADBL07: 1] In terms of online services the country is ranked in the lower midrange [CAMP-G06: 14] German is also only ranked as midrange in the Economist Intelligence Unit e-readiness rankings [EIU06: 5] In terms of Internet usage Germany is above the European average of 53% with approximately 60% and is therefore neck and neck with Switzerland. [HEISE07].

In the field of e-Government there are numerous initiatives for modernising the administrative structure on the national and state levels. Thus between 2000 and 2006 the e-Government initiative Bundonline was put into effect and in 2003 a resolution was passed by the federal government in collaboration with the states to create a joint Deutschland –Online e-Government strategy. Based on the experiences gathered in this project, the interior ministry put forward the "Future Oriented Administration Through Innovation" programme for a trans-sectoral modernisation of the national administration, encompassing the areas of personnel, taxation, organisation and e-Government. [BMI06: 5] This programme was concretised in the following year as part of a 57 project implementation plan.

The E-Government 2.0 programme was a part of this plan with a particular emphasis on modernising the registration process and piloting a country-wide marital status registry. [BMI06a: 17] Some of the aims include secure Internet transactions via a unique electronic identification of citizens, economic sectors and public administrations and the introduction of an electronic personal ID in this context.

In order to implement this plan this registration was introduced in the course of the 2006 federalism reforms as part of the federal government's legislative competence and a method of resolution was developed that includes the creation of a singular federal registry of residents by 2010. It can be assumed that there will not be a trans-sectoral personal identifier in this context and that a more data protection friendly solution should be found instead. [BMI07: 2] Just what this solution will look like remains unclear. In this context it is interesting to consider that alongside the standardisation of the registration process, the introduction of a singular unique identification number is also being pro-

moted in the taxation system which has, until now, been decentralised. In the process the government departments responsible for residents' registration will transfer every citizen's personal data to the Federal Central Tax Office, who allocates a unique identification number that is linked with personal data such as name, pseudonym, gender, date of birth, address or doctor's degree [HEISE07a] and shares this number with the appropriate registration authority. [Bundesr07: Artikel 1, Satz 2b].

3.4.1 Evaluation and Critique

With the establishment of its "Future Oriented Administration Through Innovation" programme, Germany has created a process that should lead to an effective and efficient administration, particularly in the domain of registering processes. This will be supported by the efforts being made to create unique digital identities and electronic identification documents which should, for example, accompany legally binding declarations of intent and authentication possibilities for government departments and also for business. The fact that the public sector has improved, particularly in the area of provision of online services, was recognized by the 2007 Capgemini study. Since then 75% of the most important administrative services have become fully available via the internet, and in addition the provision of online services for business has improved dramatically. [VINN07: 1] Germany was in 10th place in 2007 in a comparison of several countries, an improvement on the previous year when it reached 19th place.

When it comes to the personal identifier there is also the decentralised area-specific model, although the decisions being made about the central registry of residents and the unique tax identification number indicate that a unique personal code has come into favour. This is also the case with the unique tax number, which has been widely criticised. The increase in data exchanges between government departments and other Federal Finance Office locations is creating an enormous pool of data where individual citizens do not know what is happening to their data. [SDZ07] Data protectionists fear that we are entering into "a complete acquisition and recording of the general public's data. The finance departments' private communications partners and employers and the taxpayer's clients could just about, as the civil rights activists have pointed out, use the ID to unambiguously classify data for tax procedures"[HEISE07b]. In this particular context the German Federal Finance Minister was awarded the Big Brother Award¹²⁴ 2007 in the field of politics by a jury composed of members of the German Data Protection Federation, the Chaos Computer Club registered association, the Information Technology and Society Development Association and the International League for Human Rights, as he introduced the tax ID with a prerequisite: "to allow a unique identification of the tax payer as part of taxation procedures". His critics see this as the actual introduction of an unconstitutional personal identifier, as it cannot be reconciled with the German constitutional court's "micro census verdict" of 1969 on human dignity, for if the state were to take rights in and of themselves into account they would not force the people to register and catalogue their very identity, that is, themselves. [BBA07]

¹²⁴ The German Big Brother Awards were founded as a declaration from the initiators to promote public discussion about privacy and data protection – they aim to highlight the improper use of technology and information.

4 Public Debate on Personal Identifiers

As part of the new strategies and progressive technical developments in the field of e-Government, and with the aim of creating a legal foundation, the political players have adapted and indeed recently passed a series of regulations, directives and laws at the EU and national levels. i2010 or the Lisbon Strategy are often named as an underlying principle for the initiative for a European information society, defining the strategic framework for the general political orientation of this sector at the EU level. This initiative envisaged analysing community law in its entirety in information society terms and analysing media services. It also envisaged demonstrating proposals for essential changes if necessary up until 2007. [KDEG05: 6] One of their main aims is to enable secure access to public services through mutually recognised electronic identification and authentication and to make this available Europe wide. (eID). [KDEG05: 29]

Suggestions on how to implement these goals have ignited a debate about how to introduce them and about changes to the ways in which personal identifiers are used. These points are being debated by various community groups, journalists, data protection authorities and political decision makers. In the following the main points of view of the various interested parties that are for or against the introduction of sector specific or universal personal identifiers will be presented. These approaches and the way they are employed in different countries will be examined. Indeed, the interest groups in the different countries vary in size and in the way they are perceived, yet the arguments they put forward are quite similar.

4.1 Criticisms of the Introduction of Personal Identifiers

One of the criticisms chiefly being aimed at the introduction of area specific personal identifiers is based on an outright rejection on principle. This line of argumentation plays with the concept of the enemy, but also deals with concepts of individual freedom and cultural understanding. The English newspaper "The Telegraph" observed that when dealing with the topic of the ID card in England many newspapers saw parallels with Nazi Germany and hailed it as the introduction of a police state. With the introduction of the personal identifier it was feared that by entering a single number police could call up a wide range of information about a person, from their state of health to any previous convictions at any time. [TELEG05: 1] The German weekly newspaper "Die Zeit" quoted Margaret Thatcher in this context, declaring that she had already described personal identification cards as a terrible "Germanic idea" and an instrument of the nanny state that could only be plotted on the European continent, where there has been a bias towards harassment and state control since time immemorial. [Zeit04: 1] In some countries critics base their argumentation on the legal situation and decisions made by the high court. Thus the German Constitutional Court decided that **to render people as mere objects of the state** is not compatible with legally anchored human dignity. [BverfGE 1969: 27] According to the unique personal identifier's critics, this is exactly what would happen if a universal trans-sectoral personal code were to be implemented. In Switzerland one legal opinion specially assigned for this purpose showed that a non speaking personal identifier was not in itself problematic, what could be problematic is its allocation in connection with further procedures such as entering it in a register so that it could be processed further and this could also possibly include particularly sensitive personal data. [Biagini02: 29]

One argument against the introduction of an area specific but also against a universal personal identifier is that it supports procedures that include promoting storage of an individual's personal data in connection with the personal identifier for a very long period of time. Indeed the German personal identifier "tax identification number" is supposed to be valid for a lifetime and stored together with an individual's personal data. Plans to collect data on airline passengers taking international flights Europe wide and to hand this data over to authorities and store it for 13 years feeds theories that this kind of data could be used for very different reasons after all. It cannot be discounted that because of bribes, clerks' disloyalty or for purely political reasons data could be used illegally and misused for criminal or political purposes in one or any of the EU regions. [GRUE07: 1]

Another starting point for criticism portrays the often missing or inadequate inclusion of social groups and the general public as a whole in the government's legislative projects for introducing the personal identifier. Above all the fear of not knowing what is happening with all of the data creates a feeling of apprehension. In addition to the debate about the type of personal identifier to be used, its exact use and purpose is being poorly communicated. The Swiss data protection officer of the canton of Zurich made the criticism that "the citizen as a number stirs up negative associations amongst large numbers of the general public. Despite this sensitivity the federal personal number was introduced and promoted behind closed doors three years ago without explaining how it is intended to be used." [DSB-Z03: 1]

The possibility of identity theft is considered to be a great problem on the technical level. This is particularly relevant if the personal identifier is used in connection with certificates or biometric characteristics for identification on electronic documents. The security standards for IDs have been cast in doubt after an ID card was successfully cloned in Great Britain in an experiment. [TIMES06] Germany's Chaos Computer Club also shows how biometric characteristics that are used in some countries in connection with electronic IDs can be easily falsified. [CCC04]

From this it can be basically deduced that fears about the introduction of the personal identifier, whether area specific or universal, are basically nourished by the interconnection of databases, which thereby primarily provide the potential for abuse that can occur in this context. Thus with Germany's area specific tax identification number, alongside the transparent citizen there is now a transparent patient and a transparent bank customer as well as a transparent taxpayer. [JLB07: 4]

The danger of personal data being misused is therefore particularly high and the risk increases in proportion to the rate of data integration. The possibility of this occurring is seen as a given by data protectionists, particularly with the use of the universal personal identifier, as unique identification makes allocating data across departments much easier. "The unique personal ID leads to a situation where registers can be connected with each other in the simplest of ways. This creates a situation where the potential for abuse is large: this makes across-the-board evaluation possible, placing the transparent citizen within easy reach." [DSB-Z03: 1] However, the use of the area specific identifier is just as disputed. Even data protectionists criticize the fact that the Austrian approach, for example, is error prone, expensive and too complicated.¹²⁵

¹²⁵<http://www.datenschutz.de/news/alle/detail/?nid=2372>. Comparison. Also in relation to „Citizen Card – for IT Professionals Only“ < <http://oe1.orf.at/highlights/73241.html>>

4.2 Dealing with Criticism

Completed studies have shown that in most cases the type of personal identifier is not a key factor in achieving acceptance of the system; it is the level of trust in the carefulness of the contact with the connected personal data that is important. Many debates about the personal identifier itself are being kindled, but after taking a second look it becomes clear that citizens lack trust in the public authorities' competence both conceptually and technically. If this mistrust is confirmed, it can be assumed that it will be difficult to introduce the universal personal identifier in particular, and for it to gain acceptance.

The British government is currently bearing the burden of having dealt with personal data in a lax manner and it is suffering from the general public's loss of confidence. After their tax office lost two CDs containing personal data from just under half of the British public in the post, the critics greatest fears were realised, confirming the English's already strong rejection of centrally storing personal data. [ARD07] After government departments had to confess that they had lost the data from millions of child allowance recipients and driving school applicants and furthermore had to admit that sensitive information about patients was misplaced by the state run National Health Service, the crisis of confidence reached its zenith. [ARD07a]

It is not without reason that a current study commissioned by the European Union has come to the conclusion that trust is important above all for e-Government, and this can be achieved through successful collaborations between public authorities and citizens and the maturation of technical concepts. "Trust-based service systems are required in all areas of European society, and so our governments and citizens must together develop an agreement on the acceptable ways of gathering, storing and using data about citizens within a secure electronic service environment." [Wils07: 15]

If the use of a universal personal identifier is planned a growth in confidence, which could primarily be achieved if convincing control methods are used by non government bodies, must be reached. In this respect Estonia is offering an interesting approach. Each citizen has access to a log file in which all procedures related to the use of their personal data must be stored. If this system is functioning reliably the users of the system can remain informed of any procedures relating to them at all times. This method weakens the argument that citizens no longer know what is happening with their data.

Another possibility is to create a far-reaching statutory basis for data protection. An approach using independent controlling authorities would contradict the idea of the all-powerful state, as the maintenance of data protection laws would be independently monitored. These procedures could be organised as part of the federal data protection law¹²⁶ within the framework of a data protection audit "in order to improve data protection and data security, providers of data processing and programs and storage units can allow their data protection concept and also their technical facilities to be inspected by independent and authorised overseers and allow themselves to be appraised and then publish the results." [Federal data protection law: article. 9a]

The danger of personal data being improperly used can be minimised if area specific personal identifiers are used. Austria's approach to this is to use a limited sectoral identifier derived from a general identifier. However if this is used data will still be exchanged between various divisions, and it is possible that under certain circumstances area-specific

¹²⁶This law is being used in Germany for the implementation of the European Parliament's Directive 95/46/EG under recommendation as of October 1995 for the protection of the natural person in the use of an individual's data and for the freedom of data traffic (ABl. EGNr. L 281, S. 31 ff.).

identifiers could be stored by other institutions from other areas.

The German Federal Ministry of the Interior is proposing an interesting alternative with their pseudonym function for electronic IDs. With this a character string would be generated from both the electronic ID number and a number from the requested online service: without the involvement of an electronic identifier. This pseudonym guarantees an online service that a “real person” is behind these actions, a person that has already documented their identity with an ID application. “ The ID holder can enter verified data for e-business and e-Government services – such as address, age or city – without disclosing their name.” [HEISE08] This would meet some of the data protectionists’ requirements, as they have been demanding a pseudonym function for electronic personal IDs for quite some time.

A level of trust can be achieved as fears are being addressed. It is clear to see that these fears are being taken seriously and that they are being taken into account when technical procedures are implemented. On its website an Austrian municipality explained why the introduction of the electronic citizen card using the area specific personal identifier did not, according to their assessment, create the dangerous situation of the transparent citizen.¹²⁷

The dissemination of information about systems which have already been set up or are about to be set up is generally very important. Advantages such as the saving of costs, an increase in the number of users and prevention of fraud would be noticed by citizens. Indeed, the 2007 Accenture study made citizens the focal point of their e-Government appraisal. It is the citizen who must be addressed when services are being planned. “The fundamental questions of customercentricity then—what it is and how much of it do citizens want – are wrapped up in issues of both culture and personal preference, as well as in the nature of the interaction. [ACC07: 22]

¹²⁷<http://www.hitzen Dorf.at/cms/beitrag/10002060/40127#9>

5 Conclusions

In the e-Government context personal identifiers are specially designed to identify people and to connect personal data to data records and connect them with each other. Many groups in society in different European countries perceive these data records to be particularly sensitive and in need of special protection; they must be handled with great diligence. Concerns that these records may be dealt with carelessly and that the potential for their misuse is ever increasing are shared not only by political parties, federations, associations, and journalists but also by citizens. These concerns are being expressed in surveys, statements, studies, books, articles in the press and Internet blogs. These concerns should be taken seriously and trust should be cultivated. For these reasons measures are being identified to confront these concerns regarding the introduction of the personal identifier so that e-Government services will be more widely accepted. The choice of personal identifier can help with this process. An area specific personal identifier has the advantage that personal data records cannot be so easily used in a trans-sectoral manner, thus eliminating the danger of an all-knowing centralised government department. The disadvantage of such a system is poor networking of administrative steps and the danger of media mismatches occurring in data processing. In addition, such a solution can be extremely complex, which makes it even more error prone and can make it complicated to use. The use of a unique personal identifier would simplify the setting up of services, but this feeds concerns that personal data could be arbitrarily connected, thus creating the scenario of the "transparent citizen". It is important that appropriate protection measures are taken at both the processing and technical levels. Such measures can include, for example, the creation of specially designed data protection laws and data protection audits, user control measures such as access using a log file that informs about the exchange of data, or wide ranging information campaigns on plans to introduce new systems and their advantages and provisions for data protection. Neither systems using area specific personal identifiers, nor those using unique personal identifiers or hybrids have proved to be particularly suitable or unsuitable in the studies that have been conducted. The natural/cultural context, the legal situation and the use of existing approaches are far more important when deciding on a suitable version. They should be thoroughly analysed so that an appropriate decision can be reached.

Appendix

Acronyms/Abbreviations

CA	Certification Authority
CSP	Certification Service Provider
EC	European Commission: The European Commission embodies and upholds the general interest of the European Union and is the driving force in the Union's institutional system. Its four main roles are to propose legislation to Parliament and the Council, to administer and implement Community policies, to enforce Community law (jointly with the Court of Justice) and to negotiate international agreements, mainly those relating to trade and cooperation
EU	European Union: The European Union (EU) is a family of democratic European countries.
IETF	Internet Engineering Task Force
ITU-T	International Telecommunications Union Telecommunications Sector
PKI	Public Key Infrastructure
SSCD	Secure Signature-Creation Device
TTP	Trusted Third Party

References

- [ACC06] Accenture (2006): Building_the_Trust.
URI:http://www.accenture.com/xdoc/en/industries/government/acn_2006_govt_report_FINAL2.pdf.
- [ACC07] Accenture (2007): Leadership in Customer Service, Delivering on the Promise.
URI:http://nstore.accenture.com/acn_com/PDF/2007LCSDelivPromiseFinal.pdf.
- [ADAT07] ARGE DATEN (2007): Gescheitertes Experiment Bürgerkarte - Wann ist Schluss mit diesem Unfug. URI:http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=45653gzg.
- [AHVIV07] AHV-IV (2007): The New AHV Number. URI:http://www.ahv.ch/Home-D/allgemeines/nahv/D_30.02.pdf?lang=de&msg-id=15480.
- [ARD07] ARD (2007): Millionen Datensätze verschlampt.
URI:<http://www.tagesschau.de/ausland/datenverlust4.html>.
- [ARD07a] ARD (2007a): Britischer Gesundheitsdienst verliert Patientendaten.
URI:<http://www.tagesschau.de/ausland/datenverlust8.html>.
- [BBA07] bigbrotherawards.de (2007): Category: Politics. Federal Finance Minister.
URI:<http://www.bigbrotherawards.de/2007/.pol>.
- [BEA07] Bea Systems (2007): Integration der e-ID in die eBuerger-Dienste der Zukunft.
- [Biaggini02] Biaggini, Giovanni (2002): Ein Personenidentifikator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes (Art13BV).
URI:<http://www.edoeb.admin.ch/themen/00794/00819/01081/index.html?lang=de&download=M3wBUQCu/8ulmKDu36WenojQ1NTTjaXZnqWfVpzLhmfnapmmc7Zi6rZnqCkkin0hH9+bKbXrZ2lhtTN34al3p6YrY7P1oah162apo3X1cjYh2+hoJVn6w==>.
- [BMI06] Ministry of the Interior (2006): Zukunftsorientierte Verwaltung durch Innovation.
URI:http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2006/Pogramm__Zukunftsorientierte__Verwaltung,templated=raw,property=publicationFile.pdf/Pogramm_Zukunftsorientierte_Verwaltung.pdf.
- [BMI07] Ministry of the Interior (2007): Bundesmelderegister. URI:http://www.deutschland-online.de/DOL_Internet/binarywriterservlet?imgUid=173218f3-e631-114f-bf1b-1ac0c2f214a8&uBasVariant=22222222-2222-2222-2222-222222222222.
- [Bundesk06] Federal Chancellery (2006): Behoerden im Netz.
URI:<http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=27782>.
- [Bundesr06] Federal Upper House (2006): Verordnung zur Einführung dauerhafter Identifikationsnummern.
URI:<http://www.bundesrat.de/SharedDocs/Drucksachen/2006/0701-800/705-06,templated=raw,property=publicationFile.pdf/705-06.pdf>.

- [Bundesr07] Federal Upper House (2007): Verordnung zur Aenderung der Steueridentifikationsnummerverordnung.
URI:<http://www.bundesrat.de/SharedDocs/Drucksachen/2007/0301-400/307-07;templat%20eld=raw,property=publicationFile.pdf/307-07.pdf>.
- [CAP-G06] Capgemini (2006): Europaweit Steigende Online-Verfuegbarkeit von Dienstleistungen der Oeffentlichen Hand.
URI:http://www.at.capgemini.com/m/at/tl/EU_eGovernment-Studie_2006.pdf.
- [CAP-G07] Capgemini (2007): The User Challenge Benchmarking The Supply Of Online Public Services. URI:http://www.at.capgemini.com/m/at/tl/EU_eGovernment-Studie_2007.pdf.
- [CCC04] Chaos Computer Club (2004): Wie können Fingerabdrücke nachgebildet werden? URI:http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml.
- [Cim06] Cimander, Ralf (2006): eID in Estonia.
- [DOSIS07] DEPARTMENT OF STATE INFORMATIONS SYSTEMS (2007): Information Technology in Public Administration of Estonia Yearbook 2006.
URI:http://www.riso.ee/en/pub/2006it/estonian_it_public_sector_yearbook2006.pdf.
- [DSB-Z03] Datenschutzbeauftragter Kanton Zürich (2003): Resolution zum Personen-Identifikator. URI:<http://www.datenschutz.ch/themen/1205.php>.
- [DSG-EU03] The EU Data Protection Group (2003): work document on electronic administration.
URI:http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/e-government_de.pdf.
- [E-INST08] Estonian Institute (2008): A dozen questions about Estonia.
URI:<http://www.einst.ee/publications/12/>.
- [EDBÖ07] EDÖB (2007): Harmonisierung amtlicher Personenregister und Verwendung der neuen AHV-Versichertennummer als Personenidentifikator.
URI:<http://www.edoeb.admin.ch/dokumentation/00445/00509/01130/01134/index.html?lang=de>.
- [EDDI07] Eidgenoessisches Departement des Innern (2007): Verordnung ueber die Mindeststandards der technischen und organisatorischen Massnahmen bei der systematischen Verwendung der AHV-Versichertennummer ausserhalb der AHV.
URI:<http://www.admin.ch/ch/d/sr/8/831.101.4.de.pdf>.
- [Edelh06] Edelhofer, Edit (2006): Austria online, an overview of the current e-Government proposal. URI:<http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=25037>.
- [eGOV07] cc:eGov (2007): Think Paper 11. Trust and Identity in Interactive Services: Technical and Societal Challenges.
URI:<http://www.ccegov.eu/Downloads/Paper%2011%20-%20Trust%20and%20identity%20in%20interactive.pdf>.
- [EIU06] Economist Intelligence Unit (2006): The 2006 e-readiness rankings.
URI:<http://www.e-gov.zh.ch/internet/sk/e-gov/de/doku/study.SubContainerList.SubContainer4.ContentContainerList.0036.DownloadFile.pdf>
- [EUR-K07] European Commission (2007): Annual Report on the Information Society 2007.
URI:http://ec.europa.eu/information_society/eeurope/i2010/docs/annual_report/2

- 007/i2010_ar_2007_de.pdf.
- [F-NET05] Future Network (2005): The Status quo und future E-government trends in Austria and Hesse. URI:<http://img.pte.at/files/binary/936.pdf>.
- [G-Est06] Government of Estonia (2006): ESTONIAN INFORMATION SOCIETY STRATEGY 2013. URI:http://www.riso.ee/en/files/IYA_ENGLISH_v1.pdf
- [GFK06] FESSEL-GfK (2006): Monitoring E-Government. URI:<http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=21828>.
- [GRUE07] Fraktion Bündnis 90/Die Grünen Schleswig-Holstein (2007): Fluggastdaten. Das Ende der Freiheit über den Wolken. URI:<http://www.sh.gruene-fraktion.de/cms/presse/dok/211/211379.html>.
- [HEISE07] Heise-Online (2007): Internet-Nutzung in Deutschland wächst weiter kräftig. URI:<http://www.heise.de/newsticker/meldung/87528>.
- [HEISE07a] Heise-Online (2007a): Projekt für einheitliche Steuernummer in der Schiefelage. URI:<http://www.heise.de/newsticker/meldung/98943>.
- [HEISE07b] Heise-Online (2007b): Identifikationsnummer für alle Bürger kommt ab Juli. URI:<http://www.heise.de/newsticker/meldung/90890>.
- [HEISE08] Heise-Online (2008): E-Personalausweis soll Pseudonym-Funktion erhalten. URI:<http://www.heise.de/newsticker/meldung/103530>.
- [Horn05] Hornung, Gerrit (2005): Die digitale Identität. URI:<https://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2007113019808/1/DissertationGerritHornung.pdf>.
- [Hristova05] Hristova, Ralitsa (2003): Die Bedeutung des Personenidentifikators in der Entwicklung des E-Government. URI:<http://www.alexandria.unisg.ch/EXPORT/DL/13203.pdf>.
- [ISOB07] Informatikstrategieorgan Bund (2007): E-Government-Strategie Schweiz. URI:http://www.isb.admin.ch/themen/egovernment/00067/index.html?lang=de&download=NHZLpZeg7t,Inp6l0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCEdlR9fGym162epYbg2c_JjKbNoKSn6A--.
- [ITWi08] IT-Wissen (2008): E-Government. URI:http://www.itwissen.info/definition/lexikon/_egovernmentegovernment_egovernmentelectronic%20governmentegovernment_egovernmentegovernment.html.
- [JLB07] Jung Liberale Bochum (2007): Junge Liberale lehnen elektronische Lohnsteuerkarte ab! URI:<http://www.julis-bo.de/presse/index.html>.
- [KDEG05] KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN (2005): i2010 –Eine europäische Informationsgesellschaft fuer Wachstum und Beschaeftigung. URI:http://eur-lex.europa.eu/LexUriServ/site/de/com/2005/com2005_0229de01.pdf.
- [KÖT08] Kötter, Wolfgang (2008): Angriff aus dem Netz. URI:<http://www.freitag.de/2008/05/08050601.php>.
- [Krause07] Krause, Harald (2007): Internationale Standards zum IdentityManagement. URI:http://www.finanzen.bremen.de/sixcms/media.php/13/Medias_res_20

- 07_E-Identity_Krause.pdf.
- [Kubic07] Kubicek, Herbert (2007): E-Identity im E-Government, Nationale und Internationale Entwicklungen.
URI:http://www.finanzen.bremen.de/sixcms/media.php/13/Medias_res_2007_Plenum_E-Identity_Kubicek_Wind.pdf.
- [MEPL06] Mediapulse (2006): Internetforschung 2006.
URI:http://www.mediapulse.ch/de/download/PK2007/Internetforschung_2006.pdf.
- [Moell07] Moeller, Jan (2007): Melderegister, Personalausweis, Bürgerportale-Bausteine einer integrierten eID-Infrastruktur fuer Deutschland(E-PASS).
URI:http://www.finanzen.bremen.de/sixcms/media.php/13/moeller070612_E-Gov_in_medias_res.pdf.
- [NACH06] Nachrichten.ch (2006): 13-stellige AHV-Nummer ab 2008.
URI:<http://www.nachrichten.ch/detail/243568.htm>.
- [OEST03] Österle, Hubert (2003): Real-Time Business.
- [SADBL07] Statistische Ämter der Bundes und der Länder (2007): Fläche und Bevölkerung.
URI:http://www.statistik-portal.de/Statistik-Portal/de_jb01_jahrtab1.asp.
- [SAEGS07] Steuerungsausschuss E-Government Schweiz (2007): Katalog priorisierter Vorhaben.
URI:http://www.sgww.ch/egovernment/071203_bund_egov_priorisierte_vorhaben.pdf.
- [Schedl07] Schedler, Kuno (2007): 4. Bericht zum Stand von E-Government in der Schweiz.
URI:<http://www.e-gov.zh.ch/internet/sk/e-gov/de/doku/study.SubContainerList.SubContainer3.ContentContainerList.0028.DownloadFile.pdf>
- [SDZ07] Süddeutsche Zeitung 2007: Die Deutschen werden durchnummeriert.
URI:<http://www.sueddeutsche.de/deutschland/artikel/611/112499/>.
- [STOUR07] Schweizer Tourismus (2007): Geographie der Schweiz.
URI:<http://www.switzerland.com/de/offer-Switzerland-Geography-200085.html>.
- [TCUSM07] Teleport Consulting und Systemmanagement GmbH (2007): Mediadaten-2007.
URI:http://verkauf.vol.at/files/mediadaten_2007_screen.pdf.
- [TELEG05] The Telegraph (2005): Identity crisis over UK cards.
URI:<http://www.telegraph.co.uk/global/main.jhtml?view=DETAILS&grid=&targetRule=10&xml=/global/2005/03/08/elrob711.xml>.
- [TIMES06] Times-Online (2006): Cloning demo adds to fears over ID card scheme.
URI:<http://www.timesonline.co.uk/tol/news/uk/article602621.ece>.
- [VINN07] Verwaltung innovativ (2007): Deutschland beim E-Government im oberen Drittel der EU-Mitgliedsstaaten. URI:http://www.verwaltung-innovativ.de/cln_047/nn_684536/DE/Presse/Pressemitteilungen/PresseArchiv/2007/20070921__deutschland__beim__e__government.html?__nnn=tr.
- [Wils07] Wilson, Frank (2007): Trust and Identity in Interactive Services-Technical and Societal Challenges.

URI:<http://www.ccegov.eu/Downloads/Paper%2011%20-%20Trust%20and%20identity%20in%20interactive.pdf>.

[Zehnd06] Zehnder, Carl August (2006): Die AHV-Nummer und der Datenschutz.
URI:<http://people.inf.ethz.ch/zehnder/ahv-nr/IW1206-AHVNr-CAZ.pdf>.

[ZEIT04] Die Zeit (2004): Germanischer Charakter.
URI:<http://www.zeit.de/2004/52/gbidcard>.

