TNO Information and Communication Technology

Nederlandse Organisatie voor
toegepast-natuurwetenschappelijk
onderzoek / Netherlands Organisation
for Applied Scientific Research

Brassersplein 2
P.O. Box 5050
2600 GB Delft
The Netherlands

T +31 15 285 70 00
F +31 15 285 70 57
info-ict@tno.nl

TNO report

Privacy & federated authentication and identity management in the infoservice society

Date	1 October 2007
Author(s)	Gabriela Bodea & Marc van Lieshout
Assignor	TNO
Reviewer	Dr.Ir. J.G.E. Olk, TNO ICT
Project number	035.31600
Report number	34564
Classification report	
Title	FAIM deliverable: Privacy & federated authentication and identity management in the infoservice society
Number of pages	54 (incl. appendices)
Number of appendices	5

TNO Information and Communication Technology

Nederlandse Organisatie voor
toegepast-natuurwetenschappelijk
onderzoek / Netherlands Organisation
for Applied Scientific Research

Brassersplein 2
P.O. Box 5050
2600 GB Delft
The Netherlands

T +31 15 285 70 00
F +31 15 285 70 57
info-ict@tno.nl

Abstract

The present paper examines some of the privacy issues related to forms of federated authentication and identity management (FAIM) employed in the delivery of electronic services (mainly of the government). The paper should be read as a merely exploratory exercise. It starts by defining briefly the context in which current forms of federated authentication and identity management (FAIM) are being employed. For this purpose, a new concept has been introduced, that of the infoservice society. Subsequently, the paper takes a closer look at the situation in three countries: the Netherlands, Austria and the United States. The brief inventory of developments in the three countries will be used to distil some insights into related privacy issues, formulate conclusions and policy recommendations.

Contents

1 Introduction and definitions

"A stone is a stein is a rock is a
boulder is a pebble."
Ernest Hemingway
("A rose is a rose is a rose is a rose."
Gertrude Stein)

This paper was written in the context of the TNO-ICT project FAIM. FAIM is an abbreviation of Federated Authentication and Identity Management. The project FAIM set itself the task to explore the various facets and, insofar as possible, address the questions around the concept of FAIM, in order to allow TNO ICT to formulate a vision on the subject.

The main aim and objective of this paper, as part of the FAIM project, was to develop our own understanding of current developments, the impact of ICT on society, and in particular privacy-related issues pertaining to FAIM.

In the title, we introduced a new term, that of the ***infoservice society***. The infoservice society refers to a new stage in the development of the information society. Regarding the information society and for the purpose of this paper we chose to restrict the period to which we referred in this paper to the post-digital revolution era. The purpose of introducing the new term is a practical one. It is meant to describe more accurately specific recent developments.
During the past decade western societies witnessed the explosive growth and broad availability of information and knowledge. (Advances in) information technologies were instrumental in making this possible. The access to information and, to a certain extent, the production or the making available of information have lost their spatial and, arguably, temporal dimensions. These developments had a profound social and economic impact. During the alpha, or preliminary stage of development the available information in terms of sheer quantity, grew exponentially. Particularly, the internet had a democratizing effect on information. Established roles, especially gate-keeping roles, were challenged, and new roles and competencies were negotiated. A certain sense of chaos became prevalent and with it the need for structure. This stage, the beta stage, could be equated with a prototype and experimental stage. From a technical perspective, information systematization became imperative (from basic search engines to information management). From a social perspective, new configurations emerged: whether as new networks or changed power positions. From an economic perspective, the commercial potential of information was recognized and began to be exploited (from information itself as a commodity to information technologies as new and effective means to deliver services). The three perspectives, however, should not be seen separately but together, constituting an entity. This stage corresponds to the infoservice society.
A case in point are the various forms of electronic governments. Providers of services are no longer exclusively businesses, but also governments. The pervasiveness of internet, especially broadband internet makes possible the delivery of complex services over the internet. The issue of federated

authentication and identity management is characteristic for this phase, and often at the core of e-Gov and other types of services. FAIM have the *potential* to increase efficiency, reduce costs, and enhance privacy.

Definitions of concepts
The Liberty Technical Glossary defines ***federation*** as an association comprising any number of service providers and identity providers. The same Glossary defines ***identity*** as the essence of an entity. One's identity is often described by one's characteristics, among which may be any number of identifiers.[1]

1.1 Scoping the exercise

This contribution to the FAIM project focuses on the broader social, juridical, ethical and political – and to a certain extent on the historical and cultural – context in which federated identification and authentication management evolves. FAIM cannot be seen isolated from the socio-political context in which it is developed. Interestingly, one could see in FAIM an attempt to rectify the societal discourse on dealing with personal data in a direction in which more respect is paid to privacy concerns. This societal discourse has been guided in the direction of collecting and aggregating more personal data and use of these personal data for identification purposes. Previous attempts of states to introduce central administrations with one central personal number for the citizens are documented in, amongst others, 'The Electronic Eye', published in 1994 by David Lyon. He sketches the resistance against the introduction of centralised personal identification numbers in a number of European countries (Germany, United Kingdom). The Netherlands could be added to this list. Today, most of these countries have adopted one or another form of centralised registration. In the Netherlands, for instance, this has been accomplished by broadening the scope of the social number (introduced in the late eighties) to that of social-fiscal number (mid-nineties) and using it as the basis for a further development, the so-called Citizen Service Number (burgerservicenummer), introduced in 2007. Privacy concerns are still raised, but they appear to have lost some of their bargaining power.

Federated Identification and Authentication Management systems could constitute a tool able to swing the pendulum back in the direction of enhancing the protection of (personal) data, by restricting access to and use of these data to specific sectors and specific objectives. Objectives for introducing various FAIM constructions are manifold and range from increasing efficiency in data processing to ensuring data quality. Still, as is also shown by the cases we have studied, the enhancement of privacy protection – for instance by enhancing barriers to exchange of personal data or by offering tools to improve transparency of data processing – is an important consideration in developing specific FAIM constructions. In order to develop a shared understanding of the relation between FAIM and privacy protection, we will offer a concise interpretation of the concept privacy and identity.

[1] Liberty Alliance Project, Liberty Technical Glossary, projectliberty.org/liberty/content/.../file/liberty-glossary-v2.0.pdf

One of the first modern definitions of ***privacy***, as 'the right to be let alone'[2], belongs famously to Warren and Brandeis. It goes back to 1890 and has distinct juridical connotations. In 1967, the American scholar Alan Westin differentiated in his study[3] between four 'spheres' of privacy: solitude, intimacy, reserve, and anonymity. Privacy, according to Westin, has three dimensions. Firstly, a spatial and relational one – the intimacy of physical spaces, such as the home; of physical distances towards each other; and the relational distance towards other people). Secondly, an informational one: personal information. And thirdly, a bodily one. For all three dimensions, the right to decide about how to engage with other people and other objects is part of the private sphere. They all deal with the autonomy of the individual subject. The socio-cultural background of privacy is the need people have to be able to withdraw from public life, in order to 'recharge the life battery'; to contemplate, to reflect in isolation; or to be together with people who are very close and intimate. Privacy thus defined is a socio-cultural phenomenon, much more than a strictly juridical. The interpretation given to the different dimensions of privacy are likely to vary widely over time and contexts. TV reality shows constitute an interesting and, to some, bemusing example of a new take on the meaning of privacy, with participants apparently all too willing to 'expose' themselves fully, often in intimate setting, to an unknown public. Certain categories of webcam broadcasts over the internet constitute a similar example. Privacy can thus be regarded as a remarkable and interesting socio-cultural phenomenon in which social relations and socio-cultural values and conventions are interwoven in an intricate manner. Except for this socio-cultural dimension, we can also discern a juridical and an ethical dimension to privacy. Juridical, in the sense that regulations and laws describe the legal boundaries to the intrusion in the daily lives of people (be it physical or informational), one such example being the European Directive on Data protection 95/46/EU. The ethical dimension relates to the kind of society we want to live in and the consequences this has for respecting one's own and other people's privacy.

The informational dimension of privacy has been embedded in national Data Protection Acts (DPAs). Originating from the European Directive on Data protection, they focus more on the protection of data rather than on the protection of privacy. DPAs show a strong link between security and privacy issues. Most DPAs tend to include provisions meant to protect data quality and to ensure that proper security mechanisms are in place in order to prevent abuse and misuse of data. Specific requirements are usually included regarding the handling of sensitive personal data (as, for instance, race, sexual disposition, health could be interpreted in certain contexts)[4]. Data Protection Acts are based on the OECD Guidelines on the Protection of Privacy (see appendix A) which define the rules governing the proper use of data. Two of the principles of

[2] Warren, Samuel and Brandeis, Louis, The Right to Privacy, Harvard Law review, vol. IV, no. 5, December 15, 1890, www.law.indiana.edu/instruction/fcate/3162/resources/Warren_Brandeis.html

[3] Westin, Alan F., *Privacy and freedom*, Atheneum, 1967

[4] Although one could argue that any data can become sensitive depending on the context in which it is used (such as address information made public with the purpose of threatening someone).

particular relevance in the context of this paper are those referring to limiting the collection of data to what is strictly necessary; and to clearly specifying the purpose of data collection. The emergence of new ICT raises new challenges for the observances of these principles. The sheer amount of data which are and can be collected has increased greatly over the past decades, as have the possibilities of linking data and making them personally identifiable. In the case of RFID, for example, a simple consumer good, such as a wallet, may be used to identify its owner; the data stored on the RFID chip of the wallet may thus become personal data.

This relation between a person and his or her attributes is especially problematic in relation to public services. Personal data are often needed in order to exercise certain rights and obligations (such as paying taxes, voting, or for insurance purposes). Datamining technologies enable the creation of links between data in heaps of seemingly unrelated events. Personalization of data, such as in using previous purchases to create a purchase preference profile of a consumer, for the purpose of customizing the offer to that customer, may hold advantages for both the customer and the organisation. However, it could also lead to an intrusion of privacy and/or inaccurate or data. This enhances the demand for safeguarding the quality of the collected data, leading to more (and potentially more privacy intrusive) measures and procedures.

Another trend is that towards introducing unique identifiers for individuals (such as a personal number), thus enabling the identification and authentication of individuals in specific circumstances. The rise of biometric identification methods (such as through fingerprints, facial scans, etc.) heighten the technological complexity. They are, however, seen as part of a security approach in which the use of unique personal attributes will lower the possibilities of misidentification. This is all too important in the fight against criminality and terrorism.

FAIM may contribute to having the best of both worlds: proper identification without sharing of personal data beyond what is strictly necessary. In this paper we will look into more detail at the opportunities and threats presented by FAIM for the protection of privacy. We will do so by investigating the introduction of identity technologies in three countries: the Netherlands, Austria and the USA. The Netherlands has been chosen for obvious reasons, being a country in which the discourse on electronic identity technologies has been pursued since many years and in which a number of interesting developments are expected to take place in the coming years. The USA is of interest since there has always been a discourse on the position of the government vis-à-vis the protection of privacy of citizens while the tension between privacy and terrorism is probably highest in this country. Austria is an interesting country since it has chosen for the introduction of FAIM in the entire public sector and is a leading European country in its pursuit for finding the balance between the efficiency of the public sector and the privacy concerns of its citizens.

Approach

In the next chapter we will start by presenting some key elements of the (intended) introduction of FAIM in governmental services, illustrated by the situation in the Netherlands, the United States of America and Austria. The cases are presented in a concise manner, focusing on some of the characteristics, giving the reader some feeling for the different policy contexts and the varying

approaches that can be found. We will subsequently use the cases to discuss the relationship between FAIM and privacy on a number of dimensions.
The threats towards privacy are summarized in a number of topics and they will be combined with the strengths and weaknesses of FAIM to encounter these threats and to promote the opportunities that come with FAIM.

1.2 Methodology

Owing to the limited resources, the paper had to rely primarily on desk research. The paper made use of existent research undertaken in the field, online databases, government and industry resources available online, and other publications. The research was carried out between April and September 2007.

2 Case studies

2.1 The Netherlands[5]

Table 1 The Netherlands - Information Society indicators

Networked Readiness Index world ranking[6] (NRI), 2006–2007[7]	*6* • *(score: 5.54)*
Internet access • *% of households (2006)* • *% of enterprises(2004)*	*80%* *88%*
Broadband adoption (2006) • *% of households* • *% of enterprises*	*66%* *82%*
% of % of individuals using the Internet at least once a week (2006)	*76%*
e-Commerce (2006) • *% of individuals having purchased/ordered online in the last three months* • *% of enterprises having received orders online within the previous year*	*36%* *23%*
e-Government (2006) • *% of individuals using the Internet for interacting with public authorities:* o *obtaining information* o *downloading forms* o *returning filled forms*	*46%,* *27.3%,* *29.7%*

[5] The information in this section is based largely on the following documents:
- Progress report e-Government published by the E-Government Knowledge Centre of the Dutch Ministry of the Interior and Kingdom Relations, www.e-overheid.nl/data/files/publicaties/ProgressReportOctober2006.pdf;
- (Modernisering van de overheid, Actieprogramma Elektronische Overheid) *Wet algemene bepalingen burgerservicenummer, Memorie van Toelichting Burgerservicenummer*, www.paspoortinformatie.com/dsc?c=getobject&s=obj&objectid=4406&!sessionid=1a5dbo5!z8ZWns7p!8nhb9o!M9xXGAuyBTegM35YuUC!RV1zyOvofxaqyo3h50uV&!dsname=BPRextern; and
- the Netherlands Senate (Eerste Kamer der Staten-Generaal), Algemene bepalingen betreffende de toekenning, het beheer en het gebruik van het burgerservicenummer (Wet algemene bepalingen burgerservicenummer), Memorie van Antwoord, 19 December 2006.

[6] The Networked Readiness Index (NRI) is used to measure a nation's degree of preparation to participate in and benefit from ICT developments. The NRI is composed of three components, assessing the environment offered by the country in question, the attitude of its key stakeholders, and the uptake of ICT among those stakeholders. http://ec.europa.eu/idabc/en/document/6850/5652

[7] www.webforum.org/pdf/gitr/rankings2007.pdf

• *% of enterprises using the Internet for interacting with public authorities:*	
o *obtaining information*	*63%*
o *downloading forms*	*64%*
o *returning filled forms*	*61%*

Source: Eurostat, IDABC, http://ec.europa.eu/idabc/en/document/5858/406

Background and timeline

The programme Electronic Government started in the Netherlands in 1998. Its first stage covered the period 1999-2002. By 2002, the Netherlands had one of the highest internet penetrations in the world. e-Gov services that had been set up by that date included:
- www.overheid.nl, a portal for over 1,400 internet site of the national, regional, and local governments (launched in 1999);
- over 30% of all public services of the government, to citizens and businesses alike, had been made available online;
- intranet to which most government organizations were connected.

Research into the introduction of chip cards (the Dutch electronic identity card or eNIK) as means of personal identification enabling citizens' access to public services dates back to 2002. It coincided with the introduction of the government PKI. The evaluation carried out at the time revealed the inopportunity of the eNIK. Reasons included the limited number of electronic services available at the time; marginal use of available services by citizens; limited support services made available to citizens using the electronic services; high costs related to the introduction of the eNIK.
Whilst the introduction of the eNIK was postponed, other related activities continued. Among them, developing new electronically available services, infrastructure, legislation, administration, etc.
In the meantime, following the increased availability of services and access of users to these services, and a new evaluation of the current situation, the initiative has been found opportune. Pending the adoption of new legislation, it is expected that the new electronic identity card will be introduced in 2007 or 2008.

According to the progress report of 2006, 65% of the e-Gov services were expected to become available by the end of 2007.

Some of the services and facilities already available or soon to be introduced are described below and illustrated in Table 2.

Table 2 The Netherlands – selection of current and future e-ID facilities & related e-Gov services

Public sector

	Current	***Future***
(e)ID	• *Dutch passport* • *Dutch identity card* (Since August 2006, both the passport and the identity card include a chip with personal information and facial biometrics. As of 2009, fingerprint biometrics shall be included.) • *DigiD* – eID for public services	• *Dutch electronic identity card* (eNIK) with the following planned functionalities: electronic identification, electronic signature, secure electronic transfer of data. • *BurgerServiceNummer* (BSN) & Bedrijven- en instellingennummer (BIN) – single citizen and business/organization number respectively
Electronic services	• *e-Gov services portal* www.overheid.nl including links to • *income and company tax return* filing • *cadastre* • *subsidies* • *unemployment benefit* • *permits (e.g. construction permits)* • *general government information*	• *Personal Internet Page/e-file* (PIP/ e-dossier) - Personalized means of conducting business and communicating with the government, any time, anywhere
National Electronic Databases/Registers	Registers: ▪ Persons ▪ Businesses/organizations ▪ Cadaster ▪ Topography ▪ vehicles ▪ income, work and social securities	• non-residents (RNI)

Infrastructure	• *PKI* - for what: electronic signature, secure transfer of information and eID - for whom: government (all levels) to government, citizens and businesses (G2G, G2C, G2B) • *DigID*	• *PKI* – extended functionality to include B2C, B2B, etc
Standards & interoperability	▪ Organization for Common Administration (GBO.Overheid) - manages DigID, PKI etc as well as developing standards for the exchange of data between government, citizens and businesses ▪ Use of open standards ▪ National E-forms	▪ Programme register Streamline (SBG) ▪ Data routing – Gegevensroutering – merge government transaction port with RINIS to create one data transfer route for all government organizations. ▪ Interoperable catalogues/No wrong Door – connecting all public products and services

Existing and planned **national electronic databases and/or registers** include those for persons, businesses/organizations, cadastre, topography, vehicles, income, work and social securities, and non-residents.

DigiD is an authentication system to access number of government services. It provides two levels of security. The basic (lower) level uses a combination of user name and password, and the medium level uses an additional code sent to users by SMS.
It can be used by various levels of government in delivering services to citizens and companies. Over 100 municipalities had already introduced DigiD by the second half of 2006. By the same date, DigiD had over one million users. The number of users is likely to increase as more Municipalities will adopt DigiD and the Tax and Customs Administration employs DigiD for electronic income tax filing. Other administering bodies of the Dutch Government to have introduced DigiD included the Informatie Beheer Groep (the Dutch organization that administers student funding), the Land Registry, the Social Insurance Bank, the Centre for Work and Income, the UWV (the organization that administers employee insurance schemes). A higher security system, personal key infrastructure or **PKI**, is used for the following of communications: government (all levels) to government, citizens and businesses (G2G, G2C, G2B). Functionalities of PKI include electronic signature, secure transfer of information and eID.

Standardized electronic forms are being developed and introduced, such as notification, complaint and appeal e-forms; electronic application forms for grants, licences and permits; etc. The electronic forms can be linked to DigiD, and, in the future, to central (national) databases or registers. Combining these links is in line with the principle of 'collecting once, using many times'. It refers to one of the principles of the Dutch e-Gov policy meant to improve the (cost) efficiency of public service delivery.

Planned measures to improve **interoperability** include register streamlining, a single data transfer route for all government organizations, and interoperable catalogues connecting all public products and services.

Citizens are given **access** to their private data as recorded electronically by the various public bodies. In the near future, access to all individual data as recorded electronically in government databases will be possible from a central point. A ***Personal Internet Page****/e-file* will be made available to each citizen and will serve as central point of access and personalized means of conducting business and communicating with the government, any time, anywhere. Via the personal internet page, each citizen will be able to view and manage (update, change) his personal information and will have direct access to all digital public services available.

A new **single citizen number**, the *BurgerServiceNummer* (BSN), will be introduced soon. It will replace the existing one, the so-called SOFI-number, a single citizen number used for public administrative purposes (tax filing, health insurance, driving licence, etc.). Companies and other organizations will be assigned unique numbers as well, the Bedrijven- en instellingennummer (BIN).

Existing means of **personal identification** include the national passport and identity card. Since August 2006, both the passport and the identity card include a chip with personal information and facial biometrics. It is planned that, as of 2009, they will also include fingerprint biometrics.

The soon-to-be-introduced Dutch **electronic identity card** (eNIK) is likely to have the following functionalities: electronic identification, electronic signature, and secure electronic transfer of data. DigId, regarded as a simplified means of electronic identification available to citizens and used in their electronic dealings with the government, is likely to remain in use even after the introduction of the eNIK.

The introduction of new and/or altered means of identification, with added electronic functionalities and incorporating new features such as biometrics, requires adapting the existing legislation, and in some instances adopting new laws. The process is a lengthy one and in some cases it has delayed the introduction of new electronic products and services.

The new law regarding the single citizen number is expected to be passed in 2007. The law provides exclusively for the use of the single number for public sector products and services. However, the text of the law refers to the possible future use of the single citizen number in conjunction with the electronic identity card for additional purposes outside the public realm (e.g. in the private sector). In the middle-long term, a new law can be expected regulating the use of the unique citizen service number by non-public organization.

EU guidelines are (to be) observed with regard to all new eID, privacy, etc national legislation.

The Dutch private sector differs significantly from the public sector, with regard to federation. The use of federated methods of authentication and identification lags behind not only compared to the Dutch public service, but also compared to the private sector in other countries.
Additional **private sector (e)IDs** are limited in the Netherlands compared to other countries, such as the USA, and may include credit cards; bank cards (which also double as debit/credit cards); loyalty cards; and health insurance cards, etc. The use of credit cards in the Netherlands remains limited compared to the US for example. This has always been attributed to the early introduction of a typical Dutch payment method, the payment card. This was a guaranteed debit card which could be used in shops, theatres, in public places, etc, i.e. in every place which today uses PIN-passes (electronic purse).
Private sector services available in the Netherlands include most forms of e-commerce.

Authorities
The Dutch ministry responsible for most of the e-Gov initiatives is the Ministry of the Interior and Kingdom Relations. Other ministries with shared responsibilities for a number of projects are the Ministry for Economic Affairs, the Ministry for Housing, Spatial Planning and the Environment, the Ministry of Social Affairs and Employment, the Ministry for Finance, etc.

Other relevant organizations at national level include the College bescherming persoonsgegevens (CBP), the Dutch data protection authority.

A *public register* recording changes of personal data and a register of appointed and registered data protection officials, have both been started in 2001.

2.2 The United States of America

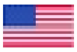


Table 3 The USA - Information Society indicators

Networked Readiness Index world ranking[8] (NRI), 2006–2007[9]	*7* • *(score: 5.54)*
Internet access • *% of inhabitants (2005)* • *% of enterprises(2005)*	*31.19%[10]* *n.a.*
Broadband adoption (2006) • *% of inhabitants (2006)*	*19.6%[11]*
e-Commerce (2005)[12] • *e-commerce as a % of total retail sales(excluding travel services, financial brokers and dealers, and ticket sales agencies)* • *e-commerce as a % of total selected services industries revenues* • *e-commerce as a % of total Merchant Wholesalers, including Manufacturing Sales Branches and Offices sales*	*2.5%* *1.6%* *18.3%*

Sources: OECD, Communications Outlook 2007, OECD Publishing, 2007, http://213.253.134.43/oecd/pdfs/browseit/9307021E.PDF (read-only version);
US E-Gov Programme, www.whitehouse.gov/omb/egov/index.html
US Census, www.census.gov/eos/www/2005/2005reportfinal.pdf

(USA population = 300mil.)

Background and timeline

All recent measures and accompanying (proposed) legislation regarding authentication, identification, privacy, etc. have been adopted in light of the events of the 11th of September 2001. As such, there is a distinct emphasis on homeland security and anti-terrorism.

[8] The Networked Readiness Index (NRI) is used to measure a nation's degree of preparation to participate in and benefit from ICT developments. The NRI is composed of three components, assessing the environment offered by the country in question, the attitude of its key stakeholders, and the uptake of ICT among those stakeholders. http://ec.europa.eu/idabc/en/document/6850/5652

[9] www.weforum.org/pdf/gitr/rankings2007.pdf

[10] OECD, Communications Outlook 2007, OECD Publishing, 2007, http://213.253.134.43/oecd/pdfs/browseit/9307021E.PDF (read-only version)

[11] OECD, Communications Outlook 2007, OECD Publishing, 2007, http://213.253.134.43/oecd/pdfs/browseit/9307021E.PDF (read-only version)

[12] www.census.gov/eos/www/2005/2005reportfinal.pdf

Worth mentioning is that the issue of a national identity card represents one of the more sensitive issues in the US. For historic and constitutional reasons, the idea of a national identity card is largely regarded with suspicion. (Although current social security numbers and driver licences can be seen as constituting de facto IDs.) Also, the Privacy Act[13] does not allow the establishment or maintenance of unauthorized cross-agency national data banks. Therefore, the proposal for the introduction of RealID (see below) was considered controversial.

Table 4 The USA – selection of current and future e-ID facilities & related e-Gov services

	Current	***Future***
(e)ID	- *US passport* - *state identity card* - social security number (SSN)	- *RealID* - electronic credentials issued by commercial entities, such as banks, -
Electronic services	government-wide official web portal including links to: - online tax filing - online loan grant applications - e-training, travel, recruitment and payroll processing for federal employees - reservations for Federal recreation sites - separate Business Compliance Portal - E-Rulemaking also for consultations - etc.	-
National Electronic Databases/Registers	Registers: ▪ social securities	- (Temporarily) cancelled proposal for a centralized government-wide gateway architecture
State Electronic Databases/Registers	▪ driving licences ▪ vehicles	

[13] The Privacy Act of 1974 (amended), http://www.usdoj.gov/oip/privstat.htm

Cross-Federal Databases / Registers	▪ The EINSTEIN Program[14] ▪ The US-VISIT Program[15]	• ICE Electronic Travel Document System (eTD)[16] • The Homeland Security Information Network (HSIN)[17]
Infrastructure	• RSA(R) Federated Identity Manager stand-alone solution	•
Standards & interoperability	▪ open	▪

The four levels of US government include the Federal Government, the State Government, the Local Government, and the Tribal Government. Given the complexity, we have limited the examples given below to Federal initiatives.

[14] The United States Computer Emergency Readiness Team's (US-CERT's) EINSTEIN Program (2004) is an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government. By collecting information from participating Federal government agencies, the US-CERT builds and enhances cyber-related situational awareness to facilitate identifying and responding to cyber threats and attacks, improve network security, increase the resiliency of critical, electronically delivered government services, and enhance the survivability of the Internet.

[15] (January 4, 2004, initial deployment of US-VISIT).

- includes the visa waiver program (VWP) travellers in US-VISIT, expansion of US-VISIT to the 50 busiest land border ports of entry (POE) and changes in the business processes used by DHS to share information with Federal law enforcement agencies.

- includes the Live Test to read ICAO-compliant biometrically enabled travel documents by October 26, 2005.

- includes: (1) Implementation of technology (Exit devices) and processes for recording the exit of covered individuals from air and sea ports by December 31, 2005; and (2) The proof of concept for technology and processes for automatically recording the entry and exit of covered individuals at U.S. land border POEs using Radio Frequency Identification (RFID)-enabled I-94 Arrival/Departure Forms. The proof of concept of the capability was originally scheduled to begin in August 2005 and, if successful, to be deployed to the 50 busiest land ports by December 31, 2007.

[16] The Electronic Travel Document System (eTD) will maintain personal information regarding aliens who have been ordered or have been removed from the United States. The eTD will also maintain information on U.S. government employees and foreign consular officials required to access the system. The eTD system will present and share alien information with the foreign consular officials and associated governments for their use in the expedited issuance of travel documents.

[17] Operations Directorate Homeland Security Information Network Database, The Homeland Security Information Network (HSIN) Database supports the HSIN user community by enabling approved users to research and analyze information with a nexus to terrorism. The HSIN is a secure internet-based system of integrated communication networks designed to facilitate information sharing between DHS and other Federal, state, county, local, Tribal, private sector commercial, and other non-governmental organizations involved in identifying and preventing terrorism as well as in undertaking incident management activities.

Additionally, the US Government sectoral approach shapes the way in which measures are taken.

The US carries out an active policy of making all government service available electronically to all citizens. The 24 government-wide **e-Gov** initiatives are part of the President's Management Agenda program.[18]

USA.gov, previously **FirstGov.gov.,** is the U.S. government-wide official web portal. It allows citizens access to all U.S. government information and services available on the web. USA.gov is an interagency initiative administered by the U.S. General Services Administration's Office of Citizen Services and Communications. [19]

The US General Services Administration (GSA) is responsible for the **E-authentication** Initiative. This initiative will provide a uniform process for establishing electronic identity and eliminate the need for each initiative to develop a duplicate approach to verify identity and electronic signatures. GSA abandoned original plans for creating a centralized government-wide gateway, as the US General Accounting Office deemed it risky for GSA to take on a central role as an online authentication broker. GSA is currently focusing on a decentralized, federated approach to e-authentication. [20] E-authentication's distributed architecture will also allow citizens and businesses to use non-government-issued credentials (such as those issued by banks) to authenticate themselves in order to conduct transactions with the government.
Authorized credential services companies and, in some cases, government agencies will issue electronic credentials to users before they submit address changes to the US Social Security Administration, for example. In the literature studied, the practice is also referred to as a **federation of federations**. There are certain requirements to be met by circles of trust outside government in order to connect to the government federation(s), but they refer primarily to interoperability and security and allow for no further exchange of credentials (therefore insuring pseudo-anonymity).
The exchange of trusted identities with other agencies takes place via the General Services Administration's E- Authentication Portal.

PIV (Personal Identity Verification of Federal Employees and Contractors). Federal employees are the object of separate rules regarding credentialing. A special directive issued in 2004 (HSPD-12), the Policy for a Common Identification Standard for Federal Employees and Contractors, is meant to enhance security, reduce identity fraud, and protect the personal privacy of those issued government identification.[21]

[18] Leslie Pang, Ph.D., A Manager's Guide to Identity, Management and Federated Identity, Information Systems Control Journal, volume 4 , 2005

[19] www.usa.gov/About.shtml

[20] www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/12-19-2005/0004236199&EDATE=

[21] www.idmanagement.gov/drilldown.cfm?action=whatis_hspd12 , http://csrc.nist.gov/piv-program/

The Federal Identity Credentialing Committee (FICC) implements the Government-wide identity credentialing policy.[22]
The U.S. Office of Personnel Management (OPM), responsible for the Federal workforce (departments and agencies, etc) serves as both a Relying Party and an Asserting Party -- organizations which generate and provide the trusted identity credential.

PKI (public key infrastructure) The Federal PKI Steering Committee (FPKISC) is responsible for the development of a public key infrastructure to support secure electronic commerce and electronic messaging as well as other Federal agency programs requiring the use of public key cryptography.[23]
The Federal Public Key Infrastructure (FPKI) Policy Authority is an interagency body set up under the CIO Council to enforce digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities.[24]
The FBCA (fpkia.gsa.gov) is an information system that facilitates an entity accepting certificates issued by another entity for a transaction. It has evolved into the Federal Public Key Infrastructure Architecture (FPKIA) that encompasses CAs by multiple vendors designating each CA to support a different FPKI policy and function.
There is a Prototype and a Production FPKIA. The Production FPKIA has gone through Certification and Accreditation and was granted Approval to Operate.
The General Services Administration, E-Authentication Program Management Office has been appointed as the Federal PKI Operational Authority (FPKI OA), to manage the design, development, implement and operate the Production FPKIA.[25]

REAL ID[26] The REAL ID Act of 2005 aims to establish minimum standards for state-issued driver's licenses and identification cards in order to prevent terrorism, reduce fraud, and improve the reliability and accuracy of identification documents issued by State governments.
The act was passed by Congress following recommendations from the 9/11 Commission.
The REAL ID Act requires that a REAL ID driver's license be used for "official purposes".[27]
Certain changes are to be expected following the results of the privacy assessment and they refer to the connectivity of the databases; the protection of the personal information stored in the State databases; and the protection of the personal information stored on machine readable technology on the DL/IDs.

[22] http://www.cio.gov/ficc/

[23] http://www.cio.gov/fpkisc/

[24] http://www.cio.gov/fpkipa/ , http://www.cio.gov/fpkipa/crosscertFPKI.htm

[25] http://www.cio.gov/fbca/

[26] Notice of Proposed Rulemaking: REAL ID , Department of Homeland Security, www.dhs.gov/xprevprot/laws/gc_1172765386179.shtm

[27] Accessing a Federal facility; boarding Federally-regulated commercial aircraft; and entering nuclear power plants. DHS may consider expanding these official purposes through future rulemakings to maximize the security benefits of REAL ID.

Social Security Number (SSN) or existing **state-issued driver's licenses** and identification cards. An argument exists that both the SSN and existing state credentials already create de facto national identifiers.

ExpectMore.gov developed by the U.S. Office of Management and Budget and Federal agencies assesses all Federal programmes twice a year. Privacy assessments accompany all Federal programmes.

2.3 Austria

Table 5 Austria - Information Society indicators

Networked Readiness Index world ranking[28] (NRI), 2006–2007[29]	*17* • *(score: 5.17)*
Internet access • *% of households (2006)* • *% of enterprises(2004)*	*52%* *94%*
Broadband adoption (2006) • *% of households* • *% of enterprises*	*33%* *69%*
% of % of individuals using the Internet at least once a week (2006)	*55%*
e-Commerce(2006) • *% of individuals having purchased/ordered online in the last three months* • *% of enterprises having received orders online within the previous year:*	*23%* *23%*
e-Government (2006) • *% of individuals using the Internet for interacting with public authorities:* o *obtaining information* o *downloading forms* o *returning filled forms* • *% of enterprises using the Internet for interacting with public authorities:* o *obtaining information* o *downloading forms* o *returning filled forms*	*28%,* *22.2%,* *12.1%* *56%* *76%* *54%*

Source: Eurostat, IDABC, http://ec.europa.eu/idabc/en/document/6631/385

Background and timeline

Austria boasts a successful strategy in implementing e-government both internally and in the information and communication processes with its citizens.

[28] The Networked Readiness Index (NRI) is used to measure a nation's degree of preparation to participate in and benefit from ICT developments. The NRI is composed of three components, assessing the environment offered by the country in question, the attitude of its key stakeholders, and the uptake of ICT among those stakeholders. http://ec.europa.eu/idabc/en/document/6850/5652

[29] www.weforum.org/pdf/gitr/rankings2007.pdf

Being a front-runner in previous years (4th in 2004 and 2nd in 2005). Austria now is European leader in eGov services, according to the European benchmark on e-government services. 95% of Austrian eGov services are yet in the transactional stage (Stage 1 – Information: online information about public services; stage 2 – Interaction: download of forms; Stage 3 – Two-way interaction: processing of forms, including authentication; Stage 4 – Transaction: full case handling, decision and delivery, including payment).

Identification and authentication management is at the heart of the Austrian processes, meant to push eGovernment in Austria. By 2000, Austria already adopted the Electronic Signature Act. The combination of a clear vision on what to realise and flexibility in how this should be done seem to form the basis of the Austrian success. The Austrian approach is based on using encryption technologies in all parts of the communication and information processes and in using a secure layer for service delivery and interaction with citizens. On top of this, citizens and companies are identified by specific numbers which are different for different sectors but which all stem from one unique source number. This source number is protected and can only be released to its rightful owner. This approach prevents data collection across various sectors and offers an interesting starting point for safeguarding privacy. The structure is very flexible as well, as citizens can use various cards for the direct communication with government. Any card that fulfils specific requirements can be used as identification and authentication tool. We'll explain this approach in detail in the next section.

E-government activities in Austria

The figure in Annex D shows the broad range of Austrian activities around e-government over the past years. Above the timeline we have presented the outcomes of the legislative process and we have indicated some features of the organisational and policy making process. Under the timeline we have indicated the activities and events accompanying the introduction and rollout of e-government services. The figure shows a number of interesting elements:

- The legislative process in Austria outpaces that in many other European countries. We have already mentioned the electronic signature act which was in place in 2000 and has undergone a first revision in 2005. Austria also has a separate e-government act which regulates a number of issues regarding identification and authentication.
- One of the successes of the Austrian approach is its strict direction of the entire e-government process. To this end, Austria created dedicated platforms and committees to guide the process. In 2003, it initiated the e-Government Platform, for which the Federal Chancellor bears responsibility and acts as chairman. The e-Government Platform is broadly composed of representatives of the national government, regional and local authorities and a number of social interest organizations (such as the Main Association of Austrian Social Security Institutions). In 2005, it has been restructured in Platform Digital Austria, a Platform with a broader objective than its predecessor.
- The ELAK (Electronic File System) organises the digitisation of governmental processes with the aim to have the full process of document handling digitised. All processes can be dealt with in a digital way. Citizens and the business sector can digitally communicate with Austrian government about all aspects concerning the timely and efficient delivery of the electronic services, using electronic identification and authentication means (sector specific PINs and electronic signatures).

- The Electronic Service Delivery is part of the digitisation of Austrian government. Upon identification and authentication, services may be delivered in a fully digitised form. Upon delivery, the person who has requested the service is notified, originally in electronic form but after two notifications a final notification will be delivered by postal service.
- June 2006, the first electronic passport has been issued in Austria.

The activities of Austria with respect to Identity management are summarized in the following table.

Table 6 Austria – selection of current e-ID facilities & related e-Gov services

	Current
(e)ID	• *Citizen Card* In February 2003 the first Citizen Card was issued by the Austrian Computer Gesellschaft. • *E-Card*. The e-Card is a health insurance card; a pilot of the e-Card started in December 2004; full roll-out of the e-Card commenced as from November 2005; in a relatively short period of time over 8 Million cards were issued. The e-Card is able to cope with electronic signatures and can be used as identity card for communication with the government. • *E-Passport.* Austria started in June 2006 with issuing e-Passports, containing a facial scan.
Electronic services	• *Electronic Delivery of Services (March 2004)* • *Electronic Record System (ELAK);* a digital documentary processing system that enabled Austrian civil officers to deliver services in a fully digitized form (completed in January 2005) • *E-Government Conformance Logo* (Güterziel) • *E-Government services*: Austria offers the full range of 12 e-gov services that have been agreed upon with the EU • *Mobile identification service*
National Electronic Databases/Registers	Registers: ▪ Persons: Central Register of Residents (each citizen is issued a citizen registration number (ZMR)) ▪ Address register
Infrastructure	• *Certification Authority*

Sources: Kartenservice Portal, www.sozialversicherung.at/esvapps/page/page.jsp?p_pageid=110&p_menuid=61873&p_id=2
eGovernment Factsheet – Austria, http://ec.europa.eu/idabc/jsps/documents/dsp_showPrinterDocument.jsp?docID=6630&lg=en

Identification and authentication initiatives

Austrian government has followed a rather flexible approach to identification and authentication mechanisms. *Any* card that fulfils specific requirements can be used for access to citizen services. The card needs to be ready to cope with electronic signatures, it needs to have an authentication mechanism to enable loading certificates and it must have sufficient storage capacity. The e-Card (the electronic health insurance card) is an example of a card which has been prepared to enable use as citizen card. Having been piloted in December 2004, full roll-out commenced a year later (November 2005). In a relatively short period of time 8 Million cards were distributed. But also bank cards can be used as citizen card, mobile phones or USB sticks.

The sourcePIN is a secure number which should not leave the card of its possessor. The sourePIN is used to derive sector specific PINs which are different for each sector. Since each sector has its own specific key, it is impossible to exchange data between two different authorities. In this manner privacy of citizens is safeguarded. The flexibility of the procedure means that it is possible to use the same method and procedures for B2C processes as well.

Authorities

As already indicated, the management of the e-government process has been the Cabinet's responsibility, thereby guaranteeing the priority the e-government developments have for Austrian government. The Federal Chancellor chairs the e-Government platform. Initiated in 2003, it has been restructured into the Platform Digital Austria.

The E-Cooperation Board was founded to support the E-Government Platform in achieving its objectives (2003). Chair of this board is the Executive Secretary for E-Government. It is broadly composed as well. The E-Cooperation Board coordinates the introduction of E-Government nationally, regionally and locally. Together with the ICT Board, which bears responsibility for all ICT processes during the transformation, it supports the Platform Digital Austria since the restructuring that took place in 2005.

Within Austrian national government the Austrian Federal ICT Staff Unit (which is lead by the CIO of the Cabinet) advices the Platform Digital Austria. An E-Government Innovation Center supports the ICT Strategy Unit of Federal Government and takes care for Information and Education, for providing technology watch and strategic advice, for communication and international cooperation and for cooperation with the business sector. This ICT Strategy Unit is in the lead for all the various aspects of the E-Government activities.

Legislative and regulatory framework

Austria has been leading in adopting the **Electronic Signature Act** (2000). This act has been updated in 2005.

The E-Government Act has been adopted in 2004. This is a major law, regulating various aspects of the e0-government process. It is based on the following principles:

1. users are free in the choice of communication means when submitting a request to public administration
2. technical and juridical means are used to safeguard privacy.

3. people with special needs are offered unhindered access to public administration and services by the end of 2007 by way of compliance with international standards about Web access.

To promote the use of the electronic administrative procedures, there will be no fees charged for these services during the introductory period.

Other relevant laws and regulations are the Data Protection Act (2005) and the Address regulation law and the Re-use of information law (all in 2005).

Conclusions

Identification and authentication management receives special attention within Austria and is one of the main building blocks for the Austrian e-government architecture. A series of measures has been taken in order to prevent the unwanted distribution of personal data within public organisations while at the same time efficiency of public services is improved by the introduction of fully digitised administrative processes.

The Data Protection Commissioner plays an important role in this entire process as the sourcePIN Registration Authority. This offers the DP Commissioner the possibility to check any misuse or abuse of personal data.

The most important and innovative part of the Austrian approach is the reliance on technical measures to safeguard privacy. By using an advanced system in which multiple encryption procedures will minimise the chance that personal data can be collected by public organisations over the boundaries of their own sector, Austrian government has built in safety measures to comply with the European directive on data protection (and the baseline requirements stemming from this directive such as purpose binding and minimal collection and use of data). The combination of sector specific PINs – which are derived from the sourcePIN – and electronic signatures offers a strong security environment. Identification is secured by means of the Identity Link which enables the fully automated processing and checking of identities. Authentication is secured by using the sector specific PINs in combination with electronic signatures.

Beside this security approach, Austria has chosen for a very flexible system which allows all manner of devices to be employed as long as they comply with certain conditions (storage capacity, processing of electronic signatures, processing of identity links).

3 Analysis and federation-related privacy issues

Table 7 Information Society indicators - NL, USA, AU

	The Netherlands	Austria	The USA	
Networked Readiness Index world ranking (NRI), 2006–2007	6 (score: 5.54)	17 (score: 5.17)	7 (score: 5.54)	
Internet access • % of households (2006) • % of enterprises(2004)	80% 88%	52% 94%	**Internet access** • % of inhabitants (2005) • % of enterprises(2005)	31.19% n.a.
Broadband adoption (2006) • % of households • % of enterprises	66% 82%	33% 69%	**Broadband adoption (2006)** % of inhabitants (2006)	19.6%
% of % of individuals using the Internet at least once a week (2006)	76%	55%		
e-Commerce (2006) • % of individuals having purchased/ordered online in the last three months • % of enterprises having received orders online within the previous year	36% 23%	23% 23%	**e-Commerce (2005)** • e-commerce as a % of total retail sales(excluding travel services, financial brokers and dealers, and ticket sales agencies) • e-commerce as a % of total selected services industries revenues • e-commerce as a % of total Merchant Wholesalers, including Manufacturing Sales Branches and Offices sales	2.5% 1.6% 18.3%
e-Government (2006) • % of individuals using the Internet for interacting with public authorities: o obtaining information o downloading forms o returning filled forms • % of enterprises using the Internet for interacting with public authorities: o obtaining information o downloading forms o returning filled forms	46%, 27.3%, 29.7% 63% 64% 61%	28%, 22.2%, 12.1% 56% 76% 54%	**e-Government (2006)** • individuals using the Internet for interacting with public authorities: o obtaining information (no of visits per month, Q4 FY06 & Q1 FY07) o returning filled in tax forms(% of total population) • enterprises using the Internet for interacting with public authorities: o obtaining information (no of visits per month, Q4 FY06 & Q1 FY07) o returning filled in corporate tax forms	301,875 1.3% 440,000 9%

Sources:
Eurostat, IDABC, http://ec.europa.eu/idabc/en/document/6631/385
Eurostat, IDABC, http://ec.europa.eu/idabc/en/document/5858/406
OECD, Communications Outlook 2007, OECD Publishing, 2007,
http://213.253.134.43/oecd/pdfs/browseit/9307021E.PDF (read-only version);
US E-Gov Programme, www.whitehouse.gov/omb/egov/index.html
US Census, www.census.gov/eos/www/2005/2005reportfinal.pdf

(USA population = 300mil.)

The previous chapter presents a brief inventory of relevant initiatives in the Netherlands, the US and Austria. It should be noted that a number of the Netherlands and USA initiatives discussed in this paper refer to *planned* initiatives which have not been implemented yet.

Although succinct, the inventory of relevant initiatives highlights a number of similarities so well as dissimilarities between the approaches of the three countries.

It is evident that all three countries are actively promoting e-Government making more services available to their citizens and creating the condition for them to make use of the services. As the tables reveal, the availability of government e-services currently exceeds their use, with some variations between the three countries. Reasons could be partial functionality, lack of knowledge amongst the public about their existence, public reluctance to use them for reasons of privacy or trust, no access, or other reasons. Also, the use of commercial e-services lags behind, most likely for similar reasons. Although at first sight disappointing, the e-commerce statistics also indicate a large growth potential.

Similar to all three countries is the use of some forms of federation.

Further similarities include the use of unique identifiers. Although efficient for administrative purposes, it can pose distinct privacy risks. In the Netherlands, for example, the social security number can be found not only on passports and identity cards, but also on driving licences, and is mentioned in many (non-secure) communications with the various government agencies. As for the United States, a US report mentions that over 75% of US counties include social security numbers on public documents, exposing as many as 94% of citizens to identity theft.

While Austria and the Netherlands have introduced electronic identity cards for governmental purposes (or about to do so), the USA have so far refrained from introducing a national ID-card. However, as far as the US is concerned and as mentioned earlier in this report, the driving licence can be seen as constituting a de facto ID (and as a result of the introduction of the REAL ID act, a de facto eID). Similar to all countries, however, is the scepticism and reluctance with which such plans for (e-) identity cards are met. If in Europe it recalls war-time sensitivities with regard to such documents, in the United States the resistance is based on the perceived breach of a fundamental principle, federalism, of the US state and democracy.

One of the main dissimilarities refers to the role governments assign themselves in issuing IDs, managing them, managing information, controlling access and use, etc. The Netherlands adopts a, surprisingly, more conservative, or perhaps cautious approach. At the present stage, the government remains the principal issuer of (e)-IDs and their use is restricted to public services. And although proposed Dutch legislation takes into account the possibilities of multiple identities as well as the use of government-issued identities by commercial parties, they are considered to be premature. Changes (preceded by changes in law) should not be expected before existing and soon-to-be-introduced means and measures are past the test-phase, and are considered privacy– and other risk-proof. The Netherlands also scores low on other Privacy Enhancing Technologies, such as unlinkability (personalized data can be communicated between government domains), and user-empowerment (the user is given limited control of his personal data). Austria, at the other end of the spectrum, adopts a more flexible approach to government-issued IDs, both in terms of use for purposes outside the public domain and physical support, whilst ensuring unlinkability and extensive user control of his personal data. Although in carrying out the above-described measures, both Austria and the Netherlands implement EU Directives, we see that the interpretations they each give to the same EU directive are significantly divergent. The United States appear to have adopted a more liberal approach, in that it has not claimed a monopoly of issuing (federal) IDs. On the other hand, however, the privacy protection offered to citizens is very limited. The latter is to a degree offset by the obligatory privacy impact assessments that accompany such measures. It is however unclear what the impact of such privacy assessments is, in terms of conclusions being translated into measures to reduce the privacy risks thus exposed.

What emerges from this brief comparison is that, at least for now, there is no standard approach to how best to implement such measures. That is not only the result of the experimental phase of the infoservice society we are currently traversing, but also the result of socio-cultural differences. That becomes particularly evident when comparing the democratic market capitalism of the United States, a democracy based on the individual values of the Enlightenment (the right to be let alone mentioned in the introduction of this paper), with European countries, where social-democratic models prevail and the emphasis is more on shared values.

But how relevant are such differences, still? In the context of the networked and increasingly globalized infoservice society local events can reverberate globally. One illustration is the way in which many countries have adapted national legislation pertaining to identity (management) as a direct result of the terrorist attacks that took place in the USA in 2001 and subsequent attacks in the UK. (As such, for example, a government-issued identity card and accompanying legislative measures will imply relinquishing some individual privacy rights, presented as a necessary trade-off in relation to increased security). What emerges as critical is the need for international co-operation. The challenge for the coming years will be to reconcile the afore-mentioned socio-cultural differences in the interest of international co-operation. For the foreseeable future, the same social-cultural differences will continue to constitute a large potential for friction (as was the case with the recent agreement between the European Union and the United states on the processing and transfer of passenger name record data by air carriers).

As we have mentioned in the previous chapters, relatively recent technological developments, in particular that of ICT and their mass adoption within a relatively short space of time brought about significant changes in the way citizens communicate/exchange information with their governments and in which consumers communicate/exchange information with commercial organizations. The very distinction between the role of individuals on the one hand as citizens and on the other hand as consumers has become blurred and now they are referred to more often in their new, hybrid quality of citizen/consumer. The amount of virtual dealings, whether commercial or non-commercial transactions, has increased exponentially. Increased technological knowledge combined with the mass use of means of electronic communication made it possible and, indeed, lucrative to both collect and process large and detailed amounts of personal information. Such technology-driven changes and renegotiations of roles between actors are on-going.

Certain concerns are thus inherent to these processes, one of which regards the issue of privacy. With regard to potential infringements of privacy, the behaviour of both public and private organizations constitutes a cause for concern. In the case of the internet, the context of this concern is its largely international and non-regulated character, or where regulated, the absence of uniform or harmonized international regulation and flawed enforcement.

Virtual interactions of commercial organizations with their customers often differ significantly from face-to-face interactions. Not only are such commercial organizations now *able* to collect, record and process more technical information regarding the user (from type of operating system, to number of visits, page views and surfing path), they can also *require* (sometimes excessively detailed) personal information or the use of cookies as a prerequisite for site or service access. On the basis of information collected in this way, the organizations can then create customer profiles, calculate trends, and in some cases sell on the information thus collected. Personalized service to customers and targeted marketing are two of the more often mentioned reasons for data collection. Such claims, however bear little relation to the wishes of customers – such personalization takes place in the absence of an explicit request or wish of the user, and often even without his knowledge. The user is more likely to be given little or unclear information as to what happens to his personal data once that has been collected.

The same can apply to public organizations, too. An added risk to privacy in this case is constituted by the potentially large amount of personal data available to public organizations following the digitalization of many public records as well as services. The use of a unique identifier in conjunction with linked or linkable digitalized public records, registries, data repositories are particularly problematic as regards the risks it poses to privacy.

3.1 Dilemmas

The issues discussed in the previous chapter highlight a number of current dilemmas.

Security vs privacy. Current initiatives, such as the introduction of electronic and/or biometric identity cards, are seen as promoting increased common security to the cost of individual privacy. The trade-off becomes acceptable if one accepts that the overall advantages for the larger community outweigh personal disadvantages.

Convenience of use and customized services vs security and privacy - Particularly relevant for FAIM at its current stage. The new generation of FAIM has the *potential* to render this dilemma obsolete. Two interesting experiments exploring the possibilities are Microsoft's InfoCard (consistent and secure way to choose an identity to use on a website or for an application; users would have multiple InfoCards) and IBM's Identity Mixer software (which uses artificial identity information, i.e. pseudonyms, to make online transactions anonymous). A third interesting experiment is the **demo developed by TNO ICT** as part of the FAIM project (see other FAIM deliverable, not included in this paper).

ICT and technology changes as moving target vs the slow-grinding mills of bureaucracy. In the EU, the approach to solving this dilemma is to adopt technology-neutral measures/legislation. However, subsequent implementation by individual member states is likely to further lengthen the process.

Centralized and centrally regulated vs decentralised and self- or co-regulated. This dilemma emphasises the need to reconsider the role so well as the reach of national governments in the infoservice society. Additionally, it refers to issues such as standardization.

National vs international/global action. In the infoservice society, an increasing number of issues defy national boundaries taking on an international dimension. Such changes underline the need for international co-operation in tackling such issues. Juridical and, very prominently, political and socio-cultural considerations and traditions are likely to determine both discourse and action.

3.2 Challenges

In this context, there are many **challenges** politicians, legislators, commercial organizations and consumer interests groups alike have to face.
A first challenge is that of ***defining identity*** – a complex issue, certainly in the context of globalization. For the purpose of FAIM, however, a more practical approach should be favoured over the philosophical, cultural, etc ones.
Directly connected to the first challenge is that of establishing what constitutes ***required information*** for the identification of users. New, emerging solutions of identification, such as the use of attributes or identity mixers, might render this challenge obsolete.
Another, fundamental, challenge is to decide if ***regulating the internet*** would be necessary (and practicable). In such a case, whose responsibility would be to draw rules and enforce them, and how feasible is such a perspective, particularly given the global character of the current infoservice society? Left to itself, one can notice strong tendencies towards self-regulation, often initiated by the private sector in order to meet the expectations and/or requirements of their clients (in terms of quality, reliability, security of transactions, post-purchase service, etc). In this context, an increased role is asserted by groups advocating consumer rights (NGOs, etc). The question remains: is this a desirable trend, likely to protect the interests of users whilst having a non-obtrusive effect on market mechanisms? Or is public intervention still necessary or even preferable (in this case as “impartial” mediator, rather than sole authority)?
Last challenge to mention is that of ***defining privacy,*** and not only in terms of what its accurate contemporary meaning has become (see introduction). In 1948, privacy was listed at Article 12 of the Universal Declaration of Human

Rights by the General Assembly of the United Nations[30]. It underlined its universal/global dimension, even more poignant in the context of today's globalized and networked economy. However, in spite of the proliferation of privacy-related legislation of the last years, a clear legal definition has yet to be formulated. In its absence, the principles set by the OECD (which have also been foundational to the European privacy directive EU/95/46) are used.

In a European context, several harmonized legislative measures have been taken to tackle this issue. The EU Privacy Directive, for example, requires specific measures be adopted with regard to the use of cookies, spam, directories, location data, retention and use of data. However, the national adoption of European legislation, the principles of subsidiarity and proportionality, etc. can translate to relatively large variations in the national interpretation given to such European legislation.

Two privacy-related risks in particular require further attention, given their significant material and abstract impact respectively: identity crime and the (breach of) trust.

Identity crime

In assigning additional functionalities to (e)IDs and considering federated forms of authentication and identity management one should take into consideration the various vulnerabilities and risks associated herewith. Two (sub)risks in particular need to be considered: the *infringement of privacy*, as a major concern and breach of fundamental rights; and *identity fraud* (including identity theft). The latter is more often mentioned given its devastating effects (not least of all of a financial nature) on the lives of individuals.
According to a recent US report, the most frequent form of identity theft in the US is the fraudulent use of someone's name and identifying data to obtain credit, merchandise, and services. The report mentions that identity theft is considered an "equal-opportunity crime, affecting victims of all races, incomes, and ages — even the deceased." The negative consequences are not only for the account of citizens, but also for that of public and private organizations.

A Federal Trade Commission survey conducted in 2003 indicated that an estimated 9.91 million adults (about 4.6% of the United States population) were victims of some form of identity theft that year. Approximately 27.3 million adults were estimated to have become victims during the previous five years. The financial losses for businesses and victims associated with identity theft incidents amounted to about $53 billion in 2004. The average loss per incident remained deceivingly limited (an estimated $700). Not taken into consideration are ensuing costs (crime prosecution and prevention costs, incurred legal costs, etc) and long-term consequences for the victims (loss of creditworthiness, damaged reputation, efforts invested in restoring the damage, general

[30] United Nations, Universal Declaration of Human Rights, December 10, 1948 'Article 12. *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'* , www.un.org/Overview/rights.html

psychological distress). Additionally, the majority of identity fraud incidents is not reported by the victims.
The past couple of years registered a marked increase in reported identity fraud incidents which was directly related to the increase in the use of ICT mediated (mainly online) services over not properly secured systems.

Trust

Trust is at the core of FAIM. Image, a volatile yet essential ingredient of trust can be harmed easily by negative publicity generated by, often, incidents given disproportionate attention in the media. Public's trust alone (at best as a form of educated guess) remains an inconsistent tool in measuring privacy. (For example, recently the EU expressed serious concerns regarding the privacy record of Google; at the same time, annual surveys carried out among the United States public by the Ponemon Institute rate Google consistently high as regards the *perceived* trust of the public.)
In order to safeguard trust, a primary requirement is **concerted responsibility**. That is to say that all parties: user, legislator and service providers (in its broadest meaning) share the responsibility. One of the major fallacies of legislations, assuming that it does everything to protect the privacy of citizens/consumers, is that it is inherently outpaced by the rhythm of progress in technology. Permanent updates of the law to accommodate technical changes are impracticable and cumbersome. *Technology-neutral measures* are necessary. Proper *enforcement* of rules and legislations so well as privacy watchdogs/monitors are needed, as opposed to relying solely on self-regulation (in France, in 2006, most complaints about privacy breaches were lodged with the privacy watchdog against financial institutions and other commercial parties).

4 Suggestions and recommendations

4.1 Addressing roadblocks by means of regulatory, co- and self-regulatory measures.

In addressing the challenges and dilemmas described in the previous chapter, we considered it necessary and useful to structure them. The four categories of so-called failures correspond and adapt for the purpose of FAIM those defined by Erik Arnold[31] et al in their analysis of innovation systems:

- Capability failures: *inadequacies in users' abilities to act in their best interest* (user can be understood as consumer/citizen). This can be interpreted as inadequate level of knowledge and information (such as regarding the handling of personal information, storage in databases, exchange of personal information, trust and security issues in an electronic environment in relation to the public and private sector, etc.), and abilities, and can be addressed by governments by setting up adequate educational facilities. Special attention should be paid to bridging the digital divide. In other words, such measures should not be limited to the conventional educational system, and thus aimed primarily at young(er) users. They should include specifically social groups likely to fall outside the scope of such measures, such as the elderly. National awareness and information campaigns using traditional media can be effective means.

- Failures in institutions: *Failure to (re)configure institutions so that they work effectively within a system.* This can refer to both infrastructure and human resources and can be addressed equally by private enterprises and government. Addressing such failures in the context of FAIM is of particular importance in such instances as transferring personally identifiable data between central databases or registers, or between agencies or in outsourcing the management of such databases. Means to compensate for this failure: making relevant training available to own employees; acquiring suitable equipment; incorporating industry standards in the organization's work process; setting clear rules for the handling of sensitive personal data and monitoring the observance of such rules.

- Network failures: *These relate to problems in the interactions among actors in the system* (see also above.) Solutions could include measures to increase the interoperability of networks. They could also include the use of privacy enhancing technologies (PETs). Traditionally limited to 'pseudonymisation tools', PETs are software and systems that allow individuals to withhold their true identity from those operating electronic systems or providing services through them, and only reveal it when absolutely necessary. These technologies help to minimise the information collected about individuals and include anonymous web browsers, specialist e-mail services, and digital cash.[32]

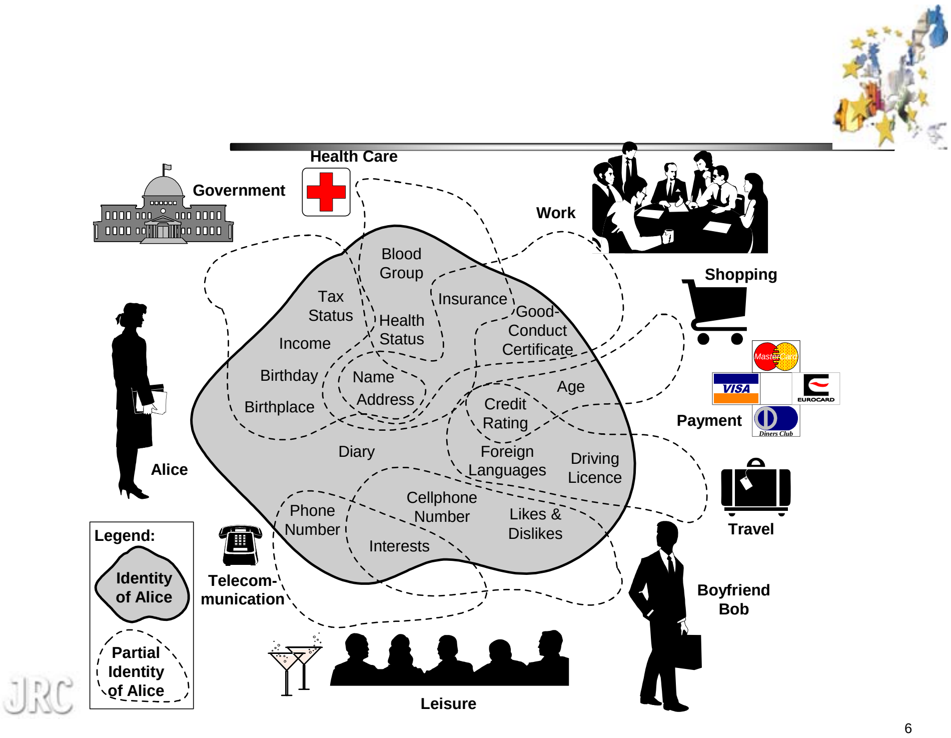
[31] Arnold, Erik (Technopolis), Kuhlman, S. (Fraunhofer – ISI), and Meulen, B. van der (University of Twente), A Singular Council: Evaluation of the Research Council of Norway, December 2001, Technopolis
www.isi.fhg.de/publ/downloads/isi01b45/norway.pdf

[32] Information Commissioner's Office (ICO), Data Protection Guidance Note: Privacy enhancing Technologies (PETs), v2.0, United Kingdom, 29 March 2007, www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies_v2.pdf

According to some data[33], federated identity management systems hold the potential to allow individuals access to the services of organisations without having to provide personally identifiable information to them. They involve one trusted organisation verifying the identity of an individual and then vouching for them, specifying their particular entitlements. This could allow individuals to access the services provided by third parties without having to disclose their identity or other information necessary to prove their entitlement. [34] This would reduce significantly related network failures.

- ***Framework failures:*** *regulatory and self-regulatory frameworks regarding privacy, safety, ethics etc., so well as other background conditions, such as the sophistication of consumer demand, culture and social values.* The main starting point of all regulatory and self-regulatory measures should be principles such as those drawn by OECD regarding the Protection of Privacy and Transborder Flows of Personal Data (see Appendix A).

Figure 1 Partial identities [*]



Source: Marit Hansen, EU privacy workshop, October 2001, www.cosic.esat.kuleuven.ac.be/pampas/workshop/slides/RAPID.ppt#449,6,

4.2 Addressing roadblocks by means of technical solutions

For various ways of addressing roadblocks by means of technical solutions, including an identity mixer developed in the context of this research, please refer to the other deliverables of the FAIM project.

[33] idem
[34] idem

5 Instead of conclusions

The number of transactions, both monetary and non-monetary, carried out in the infoservice society for which identification and authentication are required is likely to continue to grow at an exponential rate. At least until an alternative is found, and whether for economic (such as costs saving) or convenience reasons, it is likely that the need for FAIM will grow as well. Certain forms of FAIM hold in turn the potential to aggravate the problem of invasion of privacy (through the big or multiple smaller brother effects) so well as to offer a (partial) solution to the privacy issue (e.g. through anonymity or pseudonymity). *Pervasive need not mean invasive*.
However, even in its capacity as (partial) problem-solver, FAIM alone, whatever the configuration, cannot constitute the answer to all privacy issues as discussed in the context of the present paper. An informed and educated public, a coherent legislative framework, a proper and consistent enforcement policy and several independent monitors/watchdogs to protect the interests of the various parties involved are equally necessary.

As mentioned before in this paper, the absence of a uniform understanding or at least an accurate definition of the concept of privacy remains problematic. Values and conventions hold different meanings to different peoples and different individuals, and are likely to vary significantly over time. At the same time, the increasingly international character of transactions that take place in the infoservice society calls for a common understanding and a corresponding, generally accepted operational definition of the concept. For these reasons and in the context of this paper we suggest the use of the notion of private space rather than that of privacy. We can define the ***private space*** as *encompassing all representations of self, expressions of self, productions of self, tangible or intangible, physical or virtual, whether in the physical or the virtual world.* The use - in this context alone - of the concept of private space instead of that of privacy could help to avoid some of the pitfalls and biases introduced by culturally laden definitions of privacy. It would also provide a much needed operational definition, essential for defining unambiguous privacy-related rules, regulations, laws etc., which, in turn, would improve conditions for better observance and control thereof.

In many areas of the infoservice society the current trend favours the increased use of open source. However, the correspondent development with regard to (the contents of) the private space should be a shift towards *private property*. Hereby, ***ownership of one's own private space*** and all its contents would be restored to their original and rightful owner: the individual. In this scenario, ownership would have to be restored in an explicit manner and the principle would have to be observed fully. That implies that ownership and use should be not separated, at least not without consent. That would eliminate the opt-out as a generously abused privacy function in favour of ***opt-in***. It would also allow for ***consensual*** access to personal data on a ***need-to-know basis*** only (for example insurance companies' access to personal medical data, or financial institutions' access to credit worthiness data). Ownership and use understood as inseparable rights would also render the subjects of supposedly online-enhanced narcissism, exhibitionism, voyeurism, etc, mentioned briefly in the introduction, to social anthropology, behavioural psychology or other branches of social science, hence underlining the value-free character of the private space as defined in this paper.

The ***opt-in*** stands out as the preferred choice, even in the context of any FAIM construction. Currently, control options over what happens to one's individual data once recorded are limited: poorly publicized and little known; or included in lengthy and sometimes difficult to understand privacy policy statements; and cumbersome, often requiring that the individual contact each firm, institution, etc using his personal data in order to change or remove it from their records. With personal data being resold as a commodity, privacy risks increase while the possibilities of keeping track of the information and hold control over it decrease correspondingly. (In the United Kingdom it is estimated that information about the average working adult is stored in about 700 databases.[35])

Managing one's personal information is only one aspect of what can be regarded as a paradox of the infoservice society, namely the ***increased burden of tasks and responsibilities*** transferred onto the individual. Although one of the aims of electronic governments was to ease and simplify transactions with their citizens, the result is an increase in the number of tasks, previously performed by specialized personnel, which now have to be performed by citizens themselves. The same is true in the case of online interaction with commercial institutions. The individual is in charge of a vast number of new tasks ranging from establishing a secure internet connection, to updating software, to managing online identities, to online filing and managing of official documents, to managing bank accounts. *Meet the modern take on the Renaissance man: the infoservice factotum.*

Additionally, these new responsibilities, many requiring new skills, have to be attended to mostly in the intimacy of one's private sphere, (i.e. in one's home, from one's private PC). This brings about a ***blurring of the border*** between the private and the public spaces – at least symbolically, privacy has been invaded. In many cases, however, that invasion of privacy is more than just symbolical: in any FAIM configuration, increased data collection and collation are posing more privacy risks.

In light of all of the above it becomes imperative that responsibilities be shared fairly between individuals, the public and the private sectors. In the context of FAIM, that should take place with more regard for the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as defined by the OECD (see Appendix A).

[35] BBC, Trust warning over personal data, 13 July 2007, http://news.bbc.co.uk/1/hi/uk_politics/5172890.stm

6 Bibliography

Arnold, Erik (Technopolis), Kuhlman, S. (Fraunhofer – ISI), and Meulen, B. van der (University of Twente), *A Singular Council: Evaluation of the Research Council of Norway*, December 2001, Technopolis, www.isi.fhg.de/publ/downloads/isi01b45/norway.pdf

ARTICLE 29 Data Protection Working Party, *Opinion on More Harmonised Information Provisions*, 11987/04/EN, WP 100, Version November 25 2004, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf

Clarke, Roger, *Information Technology and Dataveillance*, Communications of the ACM, Volume 31 , Issue 5 (May 1988), Pages: 498 - 512 , 1988

E-Government Knowledge Centre, *Progress report e-Government*, Dutch Ministry of the Interior and Kingdom Relations, November 2006, www.e-overheid.nl/data/files/publicaties/ProgressReportOctober2006.pdf

ENISA (European Network and Information Security Agency), ad hoc Working Group on "Regulatory Aspects of Network and Information Security" (WG RANIS), *Inventory and assessment of EU regulatory activity on network and information security (NIS),* Greece, December 2006, www.enisa.europa.eu/doc/pdf/deliverables/RANIS/ENISA%20ad%20hoc%20working%20group%20on%20regulatory%20aspects%20of%20network%20and%20information%20security.pdf

Froomkin, A. Michael, *The Death of Privacy?*, 2000, http://personal.law.miami.edu/~froomkin/articles/privacy-deathof.pdf

Hansen, Marit, *EU privacy workshop*, October 2001, www.cosic.esat.kuleuven.ac.be/pampas/workshop/slides/RAPID.ppt#449,6,

Information Commissioner's Office (ICO), *Data Protection Guidance Note: Privacy enhancing Technologies (PETs)*, v2.0, United Kingdom, 29 March 2007, www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies_v2.pdf

Liberty Alliance Project, *Liberty Technical Glossary*, projectliberty.org/liberty/content/.../file/liberty-glossary-v2.0.pdf

Lindsay, David, *An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law*, Melbourne University Law Review, volume 29, number 1, April 2005, Melbourne, 2005, www.austlii.edu.au/au/journals/MULR/2005/4.html#fn1#fn1

The Netherlands Senate (Eerste Kamer der Staten-Generaal), *Algemene bepalingen betreffende de toekenning, het beheer en het gebruik van het* *burgerservicenummer* (Wet algemene bepalingen burgerservicenummer), Memorie van Antwoord, 19 December 2006

OECD, *Communications Outlook 2007*, OECD Publishing, 2007, http://213.253.134.43/oecd/pdfs/browseit/9307021E.PDF (read-only version)

OECD, *Information Technology Outlook 2006*, OECD Publishing 2006, http://213.253.134.43/oecd/pdfs/browseit/9306051E.PDF (read-only version)

Pang, Leslie, Ph.D., *A Manager's Guide to Identity, Management and Federated Identity,* Information Systems Control Journal, volume 4 , 2005

Ponemon, LarryDr., *2007 Most Trusted Companies for Privacy Study*, Executive Summary, Ponemon Institute LLC, 28 March 2007, www.truste.org/pdf/2007_Most_Trusted_Companies.pdf

PR Newswire/RSA Security Inc., *RSA Federated Identity Manager Enables U.S. Government Organizations to Support the E-Authentication Initiative*, www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/12-19-2005/0004236199&EDATE=

Rosen, Jeffrey, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*, Random House, 2004

Solove, Daniel J. and Rotenberg, Marc, *Information Privacy Law*, Aspen Publishers, New York, 2006

Stanford Encyclopedia of Philosophy, http://plato.stanford.edu/

Warren, Samuel and Brandeis, Louis, *The Right to Privacy*, Harvard Law review, vol. IV, no. 5, December 15, 1890, www.law.indiana.edu/instruction/fcate/3162/resources/Warren_Brandeis.html

(Modernisering van de overheid, Actieprogramma Elektronische Overheid) *Wet algemene bepalingen burgerservicenummer, Memorie van Toelichting Burgerservicenummer*, www.paspoortinformatie.com/dsc?c=getobject&s=obj&objectid=4406&!sessionid=1a5dbo5!z8ZWns7p!8nhb9o!M9xXGAuyBTegM35YuUC!RV1zyOvofxaqyo3h50uV&!dsname=BPRextern

Westin, Alan F., *Privacy and freedom*, Atheneum, 1967

7 Other resources

- Austrian Data Protection Commission, www.dsk.gv.at/indexe.htm
- Austrian Institute for e-Government, www.uni-potsdam.de/db/elogo/ifgcc/index.php?option=com_content&task=section&id=10&Itemid=92&lang=en_GB
- BBC, Trust warning over personal data, 13 July 2007, http://news.bbc.co.uk/1/hi/uk_politics/5172890.stm
- Center for Democracy and Technology', www.cdt.org
- Department of Homeland Security, *Notice of Proposed Rulemaking: REAL ID*, www.dhs.gov/xprevprot/laws/gc_1172765386179.shtm
- Dutch e-Gov information site, www.e-overheid.nl/thema/
- eGovernment Factsheet – Austria, http://ec.europa.eu/idabc/jsps/documents/dsp_showPrinterDocument.jsp?docID=6630&lg=en
- Electronic Privacy Information Center (EPIC), www.epic.org/
- Eurostat, IDABC, http://ec.europa.eu/idabc/en/document/5858/406 , http://ec.europa.eu/idabc/en/document/6631/385
- Federal Identity Credentialing Committee (FICC), various documents, www.cio.gov/ficc/ , www.cio.gov/fpkisc/ , www.cio.gov/fpkipa/ , www.cio.gov/fpkipa/crosscertFPKI.htm), www.cio.gov/fbca/
- IDManagement.gov, *Homeland Security Presidential Directive 12 (HSPD-12),* www.idmanagement.gov/drilldown.cfm?action=whatis_hspd12
- Kartenservice Portal, www.sozialversicherung.at/esvapps/page/page.jsp?p_pageid=110&p_menuid=61873&p_id=2
- Networked Readiness Index (NRI), http://ec.europa.eu/idabc/en/document/6850/5652
- NIST Computer Security Division, Computer Security Resource Center (CSRC), Processing Standard (FIPS) 201: Personal Identity Verification of Federal Employees and Contractors, http://csrc.nist.gov/piv-program/
- OECD Workshop on Digital Identity Management (IDM) - Trondheim, Norway, 8-9 May 2007, www.oecd.org/document/41/0,3343,en_2649_34255_38327849_1_1_1_1,00.html
- PCI PCI Security Standards Council, www.pcisecuritystandards.org
- Privacy Act of 1974 (amended), www.usdoj.gov/oip/privstat.htm

- US Census, www.census.gov/eos/www/2005/2005reportfinal.pdf
- U.S. government's official web portal, www.usa.gov/About.shtml
- Webforum, rankings, www.webforum.org/pdf/gitr/rankings2007.pdf

8 Signature

Delft, <datum>

<Institute>

<naam afdelingshoofd>
Head of department

<naam auteur>
Author

A OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

A. BASIC PRINCIPLES OF NATIONAL APPLICATION[36]

1. **Collection Limitation Principle**
2. **Data Quality Principle**
3. **Purpose Specification Principle**
4. **Use Limitation Principle**
5. **Security Safeguards Principle**
6. **Openness Principle**
7. **Individual Participation Principle**
8. **Accountability Principle**

B. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

C. NATIONAL IMPLEMENTATION

D. INTERNATIONAL CO-OPERATION

[36] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html

B The European and international legal context – a selection

- **Personal data protection**

  Directive 95/46/CE issued by the European Parliament and Council on 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data - Official Journal No. L281, 23/11/1995, p. 0031-0050

  Directive 2002/58/CE issued by the European Parliament and Council, 12 July 2002, concerning the processing of personal data and the protection of privacy in the Electronic Communications Sector (Directive on privacy and electronic communications) - European Community Official Journal No. 1201/37, 31/07/2002 (abrogates directive 97/66/CE)

- **Consumer protection**

  Directive 85/374/CEE issued by the Council on 25 July 1985 on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products - Official Journal No. L210, 07/08/1985, p. 0029 - 0033 Amended by 399L0034 (OJ L 141 04.06.1999 p. 20)

  Directive 91/250/CEE issued by the Council on 14 May 1991 on the legal protection of computer programs - Official Journal No. L 122, 17/05/1991 p. 0042-0046

  Directive 1999/5/EC by the European Parliament and Council held on 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity - Official Journal No. L 091, 07/04/1999, p. 0010 - 0028

- **Electronic signature**

  Directive 1999/93/CE by the European Parliament and Council, 13 December 1999 on a community framework for electronic signatures

European initiatives

- **Internet security**

  Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Regions committee (adopted on 26 January 2001 - COM 2000/890 end): "Create a more secure information society while improving the security of information infrastructures and fighting against cybercrime"

Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Regions committee on network and information security, 6 June 2001 (http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsec_fr.pdf)

European Council Convention on cybercrime
(Treaty open for signature on 23.XI.2001 in Budapest)
For further information about this treaty (status of signatures and ratifications, list of declarations and reserves, explanatory report, etc.), see the Council of Europe site:
(http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185)

Resolution of the European Union Council No. 15152/01, 11 December 2001 on networks and information security.
(http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsecres_en.pdf)

Communication from the commission to the Council, the European Parliament, the Economic and social committee and Regions committee (COM 2002 152): "Proposal for a decision of the European Parliament and of the Council amending decision 276/1999/CE adopting a multiannual community action plan on promoting safer use of the Internet by combating illegal and harmful contents on global networks.
(http://europa.eu.int/information_society/programmes/iap/programmes/followup/index_en.htm)

Proposed Council Framework decision related to attacks on information systems (COM 2002 173 final) published in the European Communities Official Journal C 203 E, 27 August 2002.
(http://europa.eu.int/eur-lex/en/archive/2002/ce20320020827en.html)

Information society

eEurope 2002-2005 action plan: an information society for all prepared by the European Council and Commission and presented at the Seville European Council (21-22 June 2002)
(http://europa.eu.int/information_society/eeurope/action_plan/index_en.htm)

Protection of individuals

European Council Convention for protection of individuals with regard to automatic processing of personal data, 28 January 1981
(http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm)

International/global initiatives

US Visa Waver Scheme

The US Visa Waver Scheme has been instrumental in speeding up the process of introduction of new identity documents - machine readable, containing biometric information, and other chip-stored personal information - in a number of European countries (e.g. Belgium).

C Selection of relevant legislative and regulatory framework & organizations

1. The Netherlands

- de Wet bescherming persoonsgegevens (WBP) – the Dutch data protection act of September 2001

- Wet gemeentelijke basisadministratie persoonsgegevens – the Dutch act regarding the local administration register for personal data

- Wetsvoorstel introductie van het burgerservicenummer (BSN) – legislative proposal regarding the introduction of the citizen service number

In the middle-long term, a new law can be expected regulating the use of the unique citizen service number by non-public organization.

2. The USA[37]

Selection of relevant laws, regulations & miscellaneous (listed by the Department of Homeland Security component agency websites).

- Act of 1974, System of Records Notice for the Department of Homeland Security (DHS), United States Visitor and Immigration Status Indicator Technology, Automated Identification Management System (AIDMS)

- The Privacy Act of 1974 (amended), www.usdoj.gov/oip/privstat.htm

- Homeland Security Act of 2002.

- Critical Infrastructure Information Act of 2002 (CII Act) (seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection responsibilities, thereby reducing the nation’s vulnerability to terrorism).

- Real ID: Notice of Proposed Rulemaking. (Draft regulations in the form of a Notice of Proposed Rulemaking from The Department of Homeland Security to establish minimum standards for state-issued driver’s licenses and identification cards in accordance with the REAL ID Act of 2005.)

• Personal Identity Verification (PIV), Homeland Security Presidential Directive 12 (HSPD-12), issued on August 27, 2004, requiring the establishment of a standard for identification of Federal Government employees and contractors. HSPD-12 directs the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems. This initiative is intended to

[37] www.dhs.gov/xprevprot/laws/

enhance security, increase efficiency, reduce identity fraud, and protect personal privacy.

Publications[38]

- Daily Open Source Infrastructure Report
- National Infrastructure Protection Plan
- National Strategy to Secure Cyberspace

Authorities

- The Department of Homeland Security
- the Department of Transportation
- the Social Security Administration

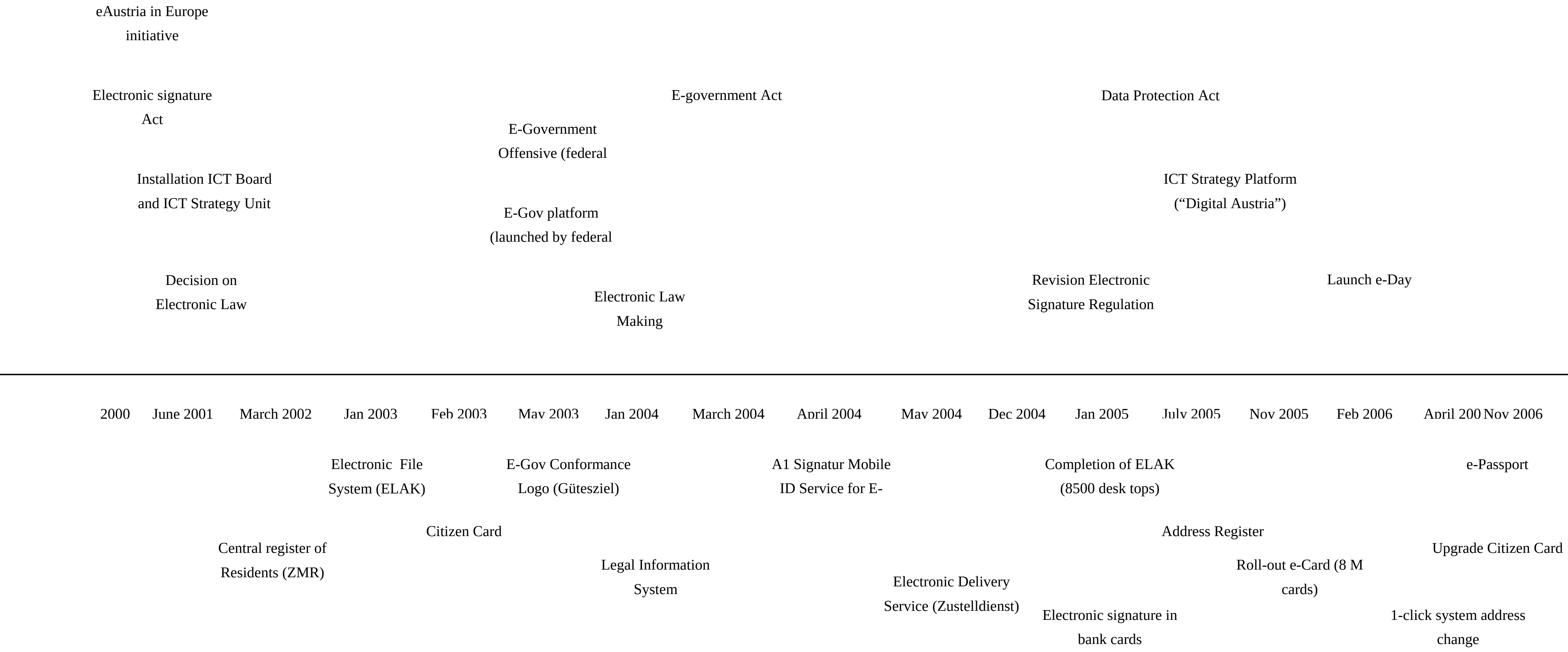
(for other bodies, see text)

3. Austria

- Constitutional Law on Access to Information (1 January 1988)
- Electronic Signature Act (1 January 2000, amended in 2005)
- E-Government Act (1 March 2004)
- Data Protection Act (1 April 2005)
- Regulation on Address Registration (July 2005)
- Re-use of Information Act (19 November 2005)

[38] www.dhs.gov/xprevprot/publications/

D E-Government in Austria - timeline



eAustria in Europe initiative

Electronic signature Act

Installation ICT Board and ICT Strategy Unit

Decision on Electronic Law

E-Government Offensive (federal

E-Gov platform (launched by federal

Electronic Law Making

E-government Act

Revision Electronic Signature Regulation

Data Protection Act

ICT Strategy Platform (“Digital Austria”)

Launch e-Day

2000 June 2001 March 2002 Jan 2003 Feb 2003 May 2003 Jan 2004 March 2004 April 2004 May 2004 Dec 2004 Jan 2005 July 2005 Nov 2005 Feb 2006 April 200 Nov 2006

Central register of Residents (ZMR)

Electronic File System (ELAK)

Citizen Card

E-Gov Conformance Logo (Gütesziel)

Legal Information System

A1 Signatur Mobile ID Service for E-

Electronic Delivery Service (Zustelldienst)

Completion of ELAK (8500 desk tops)

Electronic signature in bank cards

Address Register

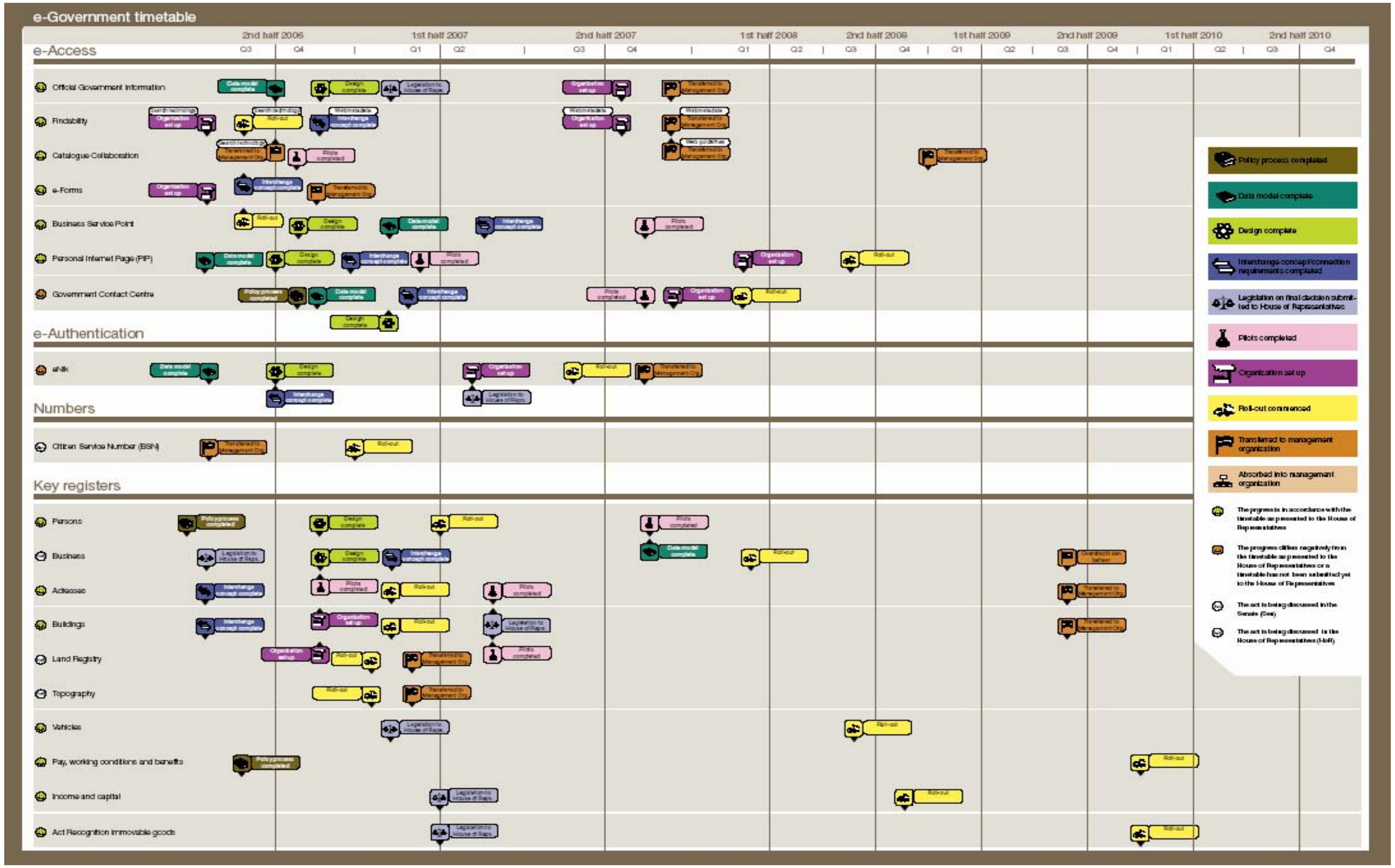
Roll-out e-Card (8 M cards)

e-Passport

Upgrade Citizen Card

1-click system address change

E E-Government in the Netherlands – timeline



Source: Progress report e-Government published by the E-Government Knowledge Centre of the Dutch Ministry of the Interior and Kingdom Relations.

http://www.e-overheid.nl/data/files/publicaties/ProgressReportOctober2006.pdf.