FIDIS

Future of Identity in the Information Society

Title:	"D16.1: Conceptual Framework for Identity Management in eGovernment"
Author:	WP16
Editors:	J.C. Buitelaar (Tilburg University, The Netherlands), M. Meints (Unabhängiges Landeszentrum für Datenschutz, Kiel, Germany) and B. van Alsenoy (K.U. Leuven, Belgium)
Reviewers:	J. Vyskoc (VaF, Slovakia) and M. Gasson (Reading University, U.K.)
Identifier:	D16.1
Type:	Deliverable
Version:	1.03
Date:	18th November 2008
Status:	[Final]
Class:	[Public]
File:	2008_11_18_D16.1_Framework_IDM_in_eGov_Final[2]

Summary

The main goal of deliverable D16.1 is to find an agreement within the different disciplines represented in the FIDIS NoE on the basic building blocks needed to allow dialoguing on the very specific research field of privacy-friendly identity management in eGovernment.

Concretely, this means that the conceptual framework explores the basic concepts of (1) privacy and data protection, (2) identity management and (2) eGovernment, and brings them together in a conceptual framework.

This framework will, in the next phase, be used to define the requirements for privacy friendly IDM in a multi-level eGovernment context.

Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

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

[1] Legal name: Stichting Katholieke Universiteit Brabant
[2] Legal name: Ministerie van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	March 29th, 2008	• Initial release (all authors and Brendan van Alsenoy, Hans Buitelaar, Martin Meints)
0.2	May 2008	• Hans Buitelaar, Martin Meints, editors
0.3	October 2008	• Hans Buitelaar, Martin Meints, editors of version ready for reviewers
1.01	October 29th , 2008	• Comments Mark Gasson, Jozef Vyscok and executive summary included (HB)
1.02	November 6th , 2008	• Final version (HB)

Foreword

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

Chapter	*Contributor(s)*
1 Executve Summary	Hans Buitelaar (TILT)
2 Introduction	Hans Buitelaar (TILT)
3 Identity Management in eGovernment	Martin Meints (ICPP) and Brendan van Alsenoy (ICRI)
4 Privacy-friendly identity management in eGovernment	4.1 Data Protection principles for IDM in eGovernment: Brendan van Alsenoy (ICRI) and Hans Buitelaar (TILT) 4.2 Identity Management Evolution: Bart Priem and Martin Pekarek (TILT); Martin Meints (ICPP)
5 Summary and conclusions	Martin Meints (ICPP)
6 The EU perspctive on eGovernment	Brendan van Alsenoy (ICRI) and Bart Priem (TILT)
7 Switzerland	Eric Dubuis (VIP)
8 United Kingdom	Ruth Halperin (LSE)
9 Netherlands	Hans Buitelaar, Marleen Knapen and Karolina Owczynik (TILT)
10 Belgium	Jacqueline v.d. Velden (ICRI)
11 Germany	Martin Meints (ICPP) and Suad Cehajic (TILT)
12 Austria	Martin Meints (ICPP) and Suad Cehajic (TILT)
13 Summary and conclusions	Martin Meints (ICPP)

Table of Contents

Terminology definitions

These definitions are based on the Modinis IDM Terminology paper.[4]

The prefix 'e' in all cases (e.g. eID, eIDM) means an electronic version of the concept the term defines.

Assertion	An assertion is synonymous with a credential
Attribute	An attribute is a distinct, measurable, physical or abstract named property belonging to an entity
Authentication	Authentication is the corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence
Authorisation	Authorisation refers to (1) the permission of an authenticated entity to perform a defined action or to use a defined service/resource; (2) the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource
Context	A context is a sphere of activity, a geographic region, a communication platform, an application, a logical or physical domain
Credential	A credential is a piece of information attesting to the integrity of certain stated facts
Digital Identity	A digital identity is a partial identity in an electronic form
Entity	An entity is anyone (natural or legal person) or anything that shall be characterised through the measurement of its attributes
Federated Identity	A federated identity is a credential of an entity that links an entity's partial identity from one context to a partial identity from another context
Identification	Identification is the process of using claimed or observed attributes of an entity to deduce who the entity is
Identifier	An identifier is an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context
Identity	The identity of an entity is the dynamic collection of all of the entity's attributes. An entity has only one identity
Identity Management (IDM)	Identity management is the managing of partial identities of entities, i.e., definition, designation and administration of identity attributes as well as choice of the partial identity to be (re-) used in

[4] Modinis IDM Study Team, *Common Terminological Framework for Interoperability Electronic Identity Management. Version 2.01*, available at <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc>, last consulted 29 August 2008.

	a specific context
Identity Management System (IMS)	An identity management system is the organisational and technical infrastructure used for the definition, designation and administration of identity attributes
Principal	A principal is synonymous with an identifiable entity
Pseudonym	A Pseudonym (syn.: nym) is an arbitrary identifier of an identifiable entity, by which a certain action can be linked to this specific entity. The entity that may be identified by the pseudonym is the holder of the pseudonym
Registration	The registration of an entity is the process in which the entity is identified and/or other attributes are corroborated. As a result of the registration, a partial identity is assigned to the entity for a certain context
Role	A role is a set of one or more authorisations related to a specific application or service

1 Executive Summary

In this Fidis deliverable a broad analysis is undertaken of the concepts that together might be said to constitute a theoretical framework for privacy friendly identity management (IDM) in eGovernment. The various disciplines, that are part of the Fidis Network of Excellence, are brought to bear on this important topic. One of the objectives of this network is to contribute to the shaping of the requirements, definitions and conception of specific security, trust and privacy technologies, needed for the future management of identity in the Information Society. This is also one of the objectives of this deliverable, applied to the context of eGovernment. Concerning the conceptual framework, this deliverable mainly provides an overview on requirements and member state concepts. This is already an important part of the framework. The next deliverable in Workpackage 16 will provide more parts.The conclusions provide an analysis of what is special in the context of governmental Identity Management Systems (IMS) and which important problems are currently not addressed properly. One of these is privacy in interoperability, but this is, de facto, an important issue in identity management.

Over the past decades, eGovernment has proven its usefulness beyond a doubt. At a pan-European level, the European Union has increasingly promoted and supported the development of eGovernment. The Commission defines eGovernment as: "*the use of information and communication technologies in public administration combined with organisational change and new skills in order to improve public services and democratic processes and strengthen support to public policies.*"[5] From the point of view of the Commission, this requires:

- An open and transparent public sector, with governments that are understandable and accountable to the citizens, open to democratic involvement and scrutiny;
- A public service, that is at the service of all, excluding no one from its services and respecting each person's individuality by providing personalised services;
- A productive public sector, that delivers maximum value for taxpayer's money (cutting red tape, reducing errors and administrative burdens – both towards citizens as well as civil servants).

Because the digital processes that are involved in providing these services, rely heavily on secure identification processes, it is a natural tendency to collect as much information as possible for governments to be sure they are dealing with the right person. In this respect IMS are also considered by the European Union a key enabler, in achieving these ambitious goals. By constructing these systems robustly the rights of the persons that make use of the governmental services will receive maximum protection. A privacy-friendly IDM – in spite of its many qualities – still is not very popular with government managers. The research, presented in this deliverable, consists of defining models and requirements of an IDM system, that is suitable for large scale implementation in eGovernment. These models also take into account privacy and data protection requirements in the basic architecture design.

[5] European Commission Communication, 'The Role of eGovernment for Europe's future', SEC (2003) 1038, COM (2003) 567 final, adopted 26 July 2003, p. 7.

The study consists of two parts. The first part delineates the perspective, from which identity management can contribute to creating the right conditions for privacy-friendly IDM in eGovernment. The second part describes the situation with respect to the state of development of eGovernment in six European countries. These countries are the United Kingdom, The Netherlands, Germany, Austria, Switzerland and Belgium. Special attention is given in these descriptions to efforts made to protect the privacy interests of citizens. The initiatives the EU itself takes for its own organisation, as well at a pan-European level, are also scrutinised. In addition, in the context of the i2010 initiative, an eGovernment benchmark has been carried out since 2000. The results indicate that there are significant qualitative differences in the implementation of eGovernment throughout Europe. The results of the benchmark are also referred to with respect to the countries scrutinised.

Part 1 of this document gives an overview of which types of identity management are used in which way and to what purpose. Governmental IDM is carried out in an organisation centric way, relying on centralised or distributed data repositories under the control of governmental administrations.

This includes operational practice, in the sense of

- Management of the life cycle of identities and ID documents
- Centralised and distributed identity management schemes
- IT-service or IT-operations management, based on internationally established good-practice frameworks, namely IT Infrastructure Library (ITIL) and CobiT
- Information Security Management, in many cases referring to international standards such as the ISO 27000 series, CobiT or ISO/IEC 15804
- Quality evaluation and management for identity management related processes
- Data protection management and related methods, especially Privacy Impact Assessment.

In addition, requirements for governmental IDM, from the perspective of public administrations and citizens, are listed. This covers

- Functional requirements such as the reliability of identity related information attributors, data quality etc.
- Data protection requirements
- Security requirements and
- Requirements regarding transparency and opacity of governmental procedures relying on IMS.

Besides these technical and security measures, the relevant legal framework is of special relevance, considering eGovernment finds its origin in the public service. The answer is sought for the question whether the legal data protection measures, that already exist, are sufficient in the eGovernment setting. Three specific data protection issues are focused on. These are the finality principle, the legitimacy principle and transparency. These data protection principles are then put in the broader context of privacy principles in general. Furthermore, in order to place these measures in their relevant context, a description is given of the theoretical models, that can be discerned in the evolution of IMS in eGovernment development.

It is observed, that the Directive provides little or no guidance as to how to construe a sound legal basis for the essential characteristic of eGovernment processing, viz the re-use of personal. Nevertheless, ample consideration of the DPD and ECHR art 8 indicates that, under certain circumstances, 're-purposing' of personal data may be legitimate. It can be argued, that such is the case, if these operations stand up to the assessment, that they comply with the reasonable expectations of the data subject taking into account the nature of the data processed as well as possible prejudices towards the data subject. In these cases a Privacy Impact Assessment may be useful. Once again it may be underlined, that legal constraints do not need to form an obstacle if they are applied conscientiously. Reference to the proportionality principle may be of special interest here. ECHR art 8 after all stipulates, that there must be a reasonable relationship between the limitation to the right of privacy on the one hand and the legitimate goals, that are being pursued, on the other.

As mentioned, the application of the IMS, espcially in the field of authentication, and corresponding legal measures, described in Part I, are, in Part II, investigated in member countries and at the pan-European level. It becomes clear that the measures discerned show similar targets with respect to governmental IMS. The main target is the creation of one (or more) reliable authentication mechanisms that serve in identifying citizens in the real and the electronic world. These identity management systems show a similar structure. In addition to an identity card (ID or eID), a register with reference data is kept. The investigated European countries also have a strategy how to deal with these registers. In most cases, a number of existing registers, kept by different governmental agencies, is linked either (a) by introducing a unique identifier (The Netherlands, Switzerland), or (b) by linking them in a defined way (Austria, Belgium, Germany). As historic starting points (e.g. no established ID card and citizen's register schema in the U.K., in difference to the other investigated EU member countries), governmental structures (federal versus centralistic) and the number of citizens, differ widely, the implementation of these concepts shows significant differences. While in the U.K., a national (e)ID document is still in preparation, in Belgium an eID was introduced already since 2004. In 2009 all citizens will have such an eID.

For the "real" (physical) world, in addition to the electronic passport, traditional paper based documents or identity cards (credit card format plastic cards) are used. In general, national ID cards are used for more purposes than identifying citizens in the context of governmental procedures. Traditionally, they are already used as travel documents in the Schengen countries and for authentication purposes in the private sector. Recently, a trend can be observed to introduce biometrics to strengthen the binding between the card and the card holder in the physical world (U.K., Germany). ICAO standards increasingly seem to play an important role in guaranteeing compatibility with electronic passports.

For the electronic world, electronic signature schemes are available in most of the investigated countries for many years now. However, not in all cases are they designed to fulfil authentication requirements (e.g. in Austria, Germany), mainly because the required information is not stored in the citizen's certificates and/or the enrolment does not cover this information. In these cases, an additional authentication scheme for citizens is introduced in citizen cards (Austria) or will be part of the planned future national identity card (Germany). In the political debate, security also seems to play an important role – frequently prevention of "identity theft" is one of the security targets of national eID schemes. However, security of the corresponding registers is not part of the public debate equally. A possible exception is the U.K., because of a number of recent security problems concerning various governmental databases.

From a data protection point of view, the Austrian concept to enforce technically the borders between defined governmental sectors, is most notable. However, apart from the health sector there seems to be no common understanding and definition of governmental sectors to date. Some of the investigated eGovernment concepts try to avoid different sectors and explicitly aim at linking them via a unique identifier (The Netherlands, Switzerland). In Switzerland a privacy debate has started, as this identifier obviously seems to be attractive for uses apart from the intended purpose, especially in the private sector.

In the light of the many and various complexities and shortcomings in the technical and legal components of the desired theoretical framework and not in the least, the significant differences, found in the analysed concepts in the country reports, it is quite clear that a lot of work still needs to be done.

PART I - IDM in eGovernment: an approach for a theoretical framework

2 Introduction

With the introduction of eGovernment, the importance of digital identification assumes ever greater proportions. Whereas in the past the citizen and the public service provider got into contact with each other in the front office, eGovernment concepts attribute an increasingly crucial role to the back office. ICT is an essential part of this service. To resolve the question of the lack of identifiability of the citizen in the backoffice, organisations increasingly gather as much personal information as possible to ensure they are dealing with the right person. This development suggests the assumption that citizens are more and more identified by the government through electronic provision of public services. Electronic identities are, therefore, at the center of many services provided within eGovernment, and will increasingly be needed when eGovernment reaches the stages of transaction and interaction. Moreover, the scale of eGovernment services is expanding, which is a result of the increasing amount of eGovernment applications on a national and pan-European level.

For eGovernment applications to come to full fruition citizens need to be able to electronically prove their identity-related claims for access to such applications, and government services need to be able to use and exchange electronic identities and identity related information. To achieve this, European Member States have autonomously taken the initiative to adopt and design systems for electronic Identity Management (eIDM), which required significant resources of these States. This autonomous adoption of eIDM through member states has resulted in a non-harmonised eID landscape. As a result of this, there also exists a varied privacy-landscape for European electronic Identity Management.

In the various European eGovernments differences have occurred in eIDM implementation on both a technical and operational level. This is not very remarkable, as for example national legislation may have demanded specific eIDM design features,[6] or because the concrete organisation of public services has stimulated the use of a specific eIDM model[7]. Moreover, because the implementation of eIDM requires significant investments and efforts, this might have resulted in Member States choosing an eIDM system that meets their budget requirements and organisational capacity.

From a privacy-perspective, interesting initiatives to be noted are for example the focus of several Member States on ‘reusability’ of personal data and the exchange of information between governmental systems and divisions. Moreover, the storage of identity-related information in central databases or the use of key registers is worth mentioning, just like the linkage of such databases. In addition, the emerging use of biometric data and the application of (single) unique numbers, ‘smart cards’, and card readers is noticeable just as the implementation of electronic identities in combination with new passports.

This study purports to be a brief tentative exploration of the building blocks which in a following Fidis deliverable will result in a conceptual framework for privacy friendly identity management in eGovernment. It starts with referring to the Fidis types of Identity Management Systems (IMS). Next a description is given of how IMS are used in an eGovernment setting. In essence this is of course not substantially different from other settings. However the scale of the identification processes and the required level of

[6] For example in the field of using unique identifiers (e.g. Germany).
[7] For example there can be a difference between federal states and states with central government.

confidence in this specific setting calls for special measures, as will be seen. Furthermore the fundamental purpose of eGovernment i.e. the multi-level use of the corroborated entity, necessitates this even more. Therefore this study also considers the role of the authorisation process and the electronic signature somewhat more in detail. Subsequently the life cycle of eGovernment IMS and the measures which can be taken to run them securely, receive attention.

The typical IDM framework which forms the basis of the eGovernment processes is followed by a study of the legal framework, that bears on identity management in eGovernment. The aspect of data protection is of special relevance here. Because much work has been done on this already, three specific issues are focused on. These are the finality principle, the legitimacy principle and transparency. In the light of the target of the study these data protection principles are then put in the broader context of privacy principles, that are available to assess the building blocks of IMS. Because, it is concluded, some additional measures are needed to achieve a better protection of the privacy of the identified entities. In order to place these measures in their relevant context, a description is given of the theoretical models, that can be discerned in the evolution of IMS in eGovernment development. Some of the measures that are considered to be most conducive to privacy enhancement in the architecture of IMS in eGovernment receive brief attention.

These considerations are followed by a study of the EU perspective on eGovernment and consecutively a description of the situation in six countries viz Switzerland, United Kingdom, The Netherlands, Belgium, Germany and Austria. The study is concluded with an analysis of the measures already taken in these countries and on the pan-European level in an attempt to answer the question whether they are sufficient to ensure the desired level of data protection while at the same time attaining the goals of eGovernment. This analysis is put in the perspective of the IDM models with which the study began.

3 Identity Management in eGovernment

3.1 Identity Management Systems

In the FIDIS-deliverable D3.1[8] identity management systems (IMS) are introduced as technical platforms supporting the management of digital identities or digital identity data. IMS are obviously an integral part of eGovernment IdM. It is important to note that the identity management infrastructure however also includes many processes that take place in an offline environment (e.g. registration, quality measurement), although some of these processes are becoming increasingly "electronified". It is the purpose of this chapter to identify the main components and techniques used in eGovernment today. Before proceeding with this analysis, we must first delineate the scope of our study.

As the procedures used for the management and data managed differ, a typology of identity management and related systems was developed. In this context **three types of identity management systems (IMS)**[9] were introduced:

- *Type 1: IMS for account management,*
  implementing authentication, authorisation, and accounting,
- *Type 2: IMS for profiling of user data by an organisation,*
  e.g. detailed log files or data warehouses which support e.g., personalised services or the analysis of customer behaviour,
- *Type 3: IMS for user-controlled context-dependent role and pseudonym management.*

In addition **three classes** of IMS-solutions could be identified:

- Class 1: Pure IMS whose main objective is to support or implement identity management functionality
- Class 2: Systems/applications with another core functionality, but based on and thereby supporting at least some identity management functionality
- Class 3: Systems/applications which are independent from identity management functionality, but nevertheless offer at least some identity management functionality, such as add-ons

In this deliverable identity management systems of type 1 are investigated only, as control by governmental institutions (or partners in the context of outsourcing) in most cases is an important requirement. In addition the focus of this deliverable is put on class 1 IMS, especially IMS supporting governmental procedures and related work flows.

[8] Bauer, M., Meints, M. and Hansen, M. (eds.), *D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 29 August 2008.

[9] Nabeth, T., et al, *D.2.1: Models, Fidis deliverable*, 2005, pp. 11-12, available at <www.fidis.net>, last consulted 29 October 2008.

3.2 IMS in eGovernment – what are they used for?

3.2.1 Identification and authentication

In first instance, eGovernment IMS serve to identify and authenticate (valid) users of governmental systems or services. The term "identification" covers many meanings and is consequently used in various ways in IdM literature:

- often the term is used to refer to the registration or enrolment process: here identification consists in the process of using claimed, observed or assigned attributes of an entity to establish a partial identity for that entity;[10]
- certain authors also use identification in terms of entity authentication, understood as the verification of the link between an entity and the asserted identity;[11]
- finally, identification is also used in terms of identifiability, i.e. the process of "individualizing" a particular entity within a set of subjects.[12]

These different denotations of the term identification can be combined by defining identification as the process of *establishing* the link between an entity and a (partial) identity; be it for later authentication or account management purposes, or when individualizing the entity (e.g. in the context of fraud detection).

Authentication is understood as the verification of a claim by an entity and may involve identification.[13] In the context of eGovernment IMS, authentication may be defined as the process of corroborating a claimed set of attributes or facts with a specified or understood level of confidence.[14] During an authentication protocol, an asserting entity will most often be required to present some form of corroborative evidence to assure the relying party that the entity is in fact who it claims to be (or that it in fact holds the prerequisite attribute(s); e.g. a group affiliation).

IMS in the context of eGovernment have two different subjects of management:

- Members of governmental institutions and
- Citizens and businesses; mainly understood as clients of governmental institutions or as data subjects.

According to the required level of authorization (cf. infra) different strengths of authentication, typically implemented using different factors for authentication (knowledge, possession and biometric features,[15] and corresponding reference data repositories are used.[16]

---

[10] See also Nabeth, T. and Hildebrandt, M., (eds.), *D2.1: Inventory of topics and clusters, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 29 August 2008.
[11] See e.g. Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997.
[12] See e.g. Leenes, R. (ed.), *D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research, FIDIS deliverable*, 2006, available at <www.fidis.net>, last consulted 29 August 2008.
[13] Kent, S.T. and Millett, L. I. (eds.), *Who goes there?: Authentication through the lens of privacy*, The National Academies Press, Washington DC, 2003.
[14] See glossaries from Modinis IDM Study Team, *Common Terminological Framework for Interoperability Electronic Identity Management. Version 2.01*, available at <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc>, last consulted 29 August 2008.
[15] Gasson, M., Meints, M. and Warwick, K. (eds.), *D3.2: A study on PKI and biometrics, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 29 August 2008.

Examples of corresponding pairs of factors for authentication and reference data used in eGovernment include:

- User name / password and reference database (typically directory services)
- Passport / ID card / biometric reference data and citizens registers
- Administration cards and reference databases
- eHealth cards and reference data of health insurance holders
- Signature cards and Public Key Infrastructure (PKI)

It is important to note however that not only users of governmental systems or resources can be authenticated, but that the origin of data as such can (and often should) be authenticated as well. This is for instance relevant when an asserting and relying party are exchanging messages with some delay (and cannot authenticate each other "in real time").[17]

Furthermore, authentication does not only need to be thought of in terms of factors, but also in terms of "ways" (one-way vs. mutual authentication)[18] and "channels" (depending on whether more than one communication channel is used during an authentication protocol).

An increasing amount of EU Member States have introduced an electronic identity card scheme based on traditional PKI, to allow citizens to securely authenticate themselves in online transactions.

3.2.2 Authorization

Authorization is the process or act of determining the permissions of an entity, through the evaluation of applicable policies, to perform a defined action on a protected or controlled resource.[19] The set of defined actions corresponds to the set of possible uses of the controlled or protected resources (typically 'read', 'modify', 'create' and/or 'delete'). In the operational sense, authorizations are granted or denied based on the result of data or entity authentication, and on the policies defined within the system.

Authorization also implies management of roles and rights. For governmental processes such management focuses on

- Rights of user, operators, administrators etc. in the context of applications used to support governmental processes
- (Physical) access control to governmental property (mainly buildings, rooms etc.)

The authorization profile of an entity says which types of resources it may access, for what period of time and under which conditions (depending on the capacity in which the entity is

---

[16] See also Leenes, R. (ed.), *D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research, FIDIS deliverable*, 2006, available at <www.fidis.net>, last consulted 29 August 2008, p. 83.
[17] Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997, p. 24.
[18] See also Leenes, R. (ed.), *D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research, FIDIS deliverable*, 2006, available at <www.fidis.net>, last consulted 29 August 2008.
[19] The definition is based on Robben, F., *1st Modinis Workshop on Identity Management in EGovernment*, 2005, available at http://www.law.kuleuven.ac.be/icri/frobben/presentations/20050504.ppt>, last consulted at 29 March 2008; Nabeth, T. and Hildebrandt, M., (eds.), *D2.1: Inventory of topics and clusters, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 15 October 2008; Slone, S. (ed.), *Identity Management. A white paper*, 2004, available at <http://www.opengroup.org/online>, last consulted 29 March 2008, p. 13.

registered). In other words, an authorization profile is an aggregation of the rights (privileges) of an entity. These rights of an entity may vary according to the context or domain at hand.

When considering the scale of eGovernment applications, it is important to think of authorizations not only at object or user level, but also at policy level. Provided that the policies within the IMS allow for sufficient granularity, they can be most useful tools in preventing unlawful data processing .

Needless to say, rights and policy management also plays an important role in ensuring confidentiality. Confidentiality is generally understood as keeping the content of information secret from all but those authorized to access it.[20] There are numerous approaches to providing confidentiality, ranging from physical protection to the use of cryptographic algorithms.[21] Encryption is a means of transforming data from a readable form (known as plain text or clear text) to one that is unintelligible (referred to as cipher text).[22] It may be applied during transmission as well as during storage.

Another example of how cryptography plays an important role in furthering the policy objectives of eGovernment is the use of digital signature techniques, which is elaborated in the following section.

3.2.3 Digital and electronic signatures

As indicated earlier, many of the recent electronic identity cards allow citizens not only to authenticate themselves in online transactions, but also to place qualified & advanced electronic signatures within the meaning of Directive 1999/93/ EC on a Community framework for electronic signatures. While cryptographers generally speak of digital signatures, lawyers usually speak in terms of electronic signatures.

Digital signatures can be seen as the 'counterpart' of asymmetric encryption schemes: there is a secret key for signing a message and a public key for verifying. A digital signature is generated by first applying a hash function to a message and afterwards using the core signature algorithm to sign just the resulting hash value. Digital signatures can be used to convince a relying party that a message has not been altered (integrity), and to establish the origin of a message (data origin authentication).

The signature acts implementing Directive 1999/93/EC aim at defining levels of security including authenticity and non-repudiation for the signing of certain types of electronic documents. An 'advanced' electronic signature as defined in Article 2 of the EU directive 1999/93/EC is mainly a digital signature with four requirements: "(a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;"

Of special interest are advanced electronic signatures which are based on a qualified certificate—which is basically a digital certificate as issued by a certification authority —and

[20] Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997, p. 32.
[21] Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997, p. 32.
[22] Based on http://www.businessdictionary.com/. Schneier, B., *Applied Cryptography*, Addison-Wesley, New York, 1996, p. 1.

which are created by a "secure-signature-creation device". This kind of signatures has legal effects as defined in Article 5 of 1999/93/EC.

From a technical point of view the requirements above introduce some (sometimes controversially discussed) challenges and problems. Of special importance are the demands on a secure-signature-creation device that "the signature-creation-data used for signature generation can be protected in a reliable way by the legitimate signatory against the use of others" and that "secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process." in conjunction with the requirement of an advanced electronic signature that "it is created using means that the signatory can maintain under his sole control".

One of the problems is that the secret keys used for signing are typically created by certification authorities and not by the users themselves. Thus a user can never be sure to have the process of signing "under his sole control".

Another problem is that today's standard PCs with standard operating system cannot be used as secure signature-creation devices. Given all the security weaknesses of PCs they can neither ensure that "the signature-creation-data used for signature generation can be reliably protected" nor "what I sign is what I see". Therefore specialized hard- and software is needed. Such devices need at least some means for input to authorize the signing process and some display (or other means of output) to inform the user about what he will sign. So from an organizational and usability point of view electronic signatures are somewhat impractical and costly.

For more information regarding legal and technical aspects of electronic signatures, see FIDIS D3.2.[23]

3.3 eGovernment IMS – How are they run?

3.3.1 Life-cycles of the IMS

Technical products, in this case IMS, and the related processes and procedures run through a life-cycle. This life-cycle typically includes at least the following steps:

[23] Gasson, M., Meints, M. and Warwick, K. (eds.), *D3.2: A study on PKI and biometrics, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 29 August 2008.

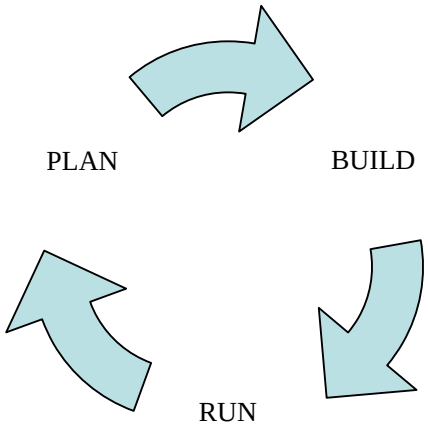

Figure 3.1: Life-cycle of products and related procedures, derived from the Baseline-Protection Catalogues (BSI 2006)

The planning and building phase has a project character. These phases are completed in a non-repeatable way. Proceedings used when going through the planning phase the first time typically can not be reused as such when going through the planning phase again for the next version of the IMS.

The operational or running phase clearly has a process character. Proceedings used here are used repeatedly and are rarely modified. The identity life cycle introduced in the following section is carried out in this phase. In addition IT service, quality and security management are carried out, to maintain the IMS and to ensure the required level of quality and security of the processes in the identity management life-cycle.

3.3.2 The identity life cycle

One of the core functions of identity management relates to the secure management of the 'identity information' of entities. This management, which is performed by one or more Identity Providers, can also be thought of in terms of a *lifecycle*:

- At first, a (partial) identity is created for the entity, which often implies the association of one ore more unique identifiers with that entity;
- the entity is subsequently granted the appropriate credentials, in accordance with applicable policy;
- these identifiers and credentials are then used in later interactions, within one or more contexts or sectors;
- the usage of these identifiers and credentials is generally monitored for a variety of purposes (ranging from fraud detection and quality management to profiling);
- where appropriate, the credentials and/or identifiers of the entity may be revoked or modified (e.g. in case of card loss or role change).[24]

[24] International Telecommunication Union - Telecommunication Standardization Sector. Focus Group on Identity Management. Report on Identity Management Framework for Global Interoperability, pp. 4-5. For a more detailed account of the interrelated processes, see Slone, S. (ed.), *Identity*

Identity data is of course managed for a reason. The primary purpose is usually to enable secure consumer-to-business transactions or to manage access to protected resources. This may require (and enable) a wide variety of other activities, which is well illustrated by the following figure[25]:

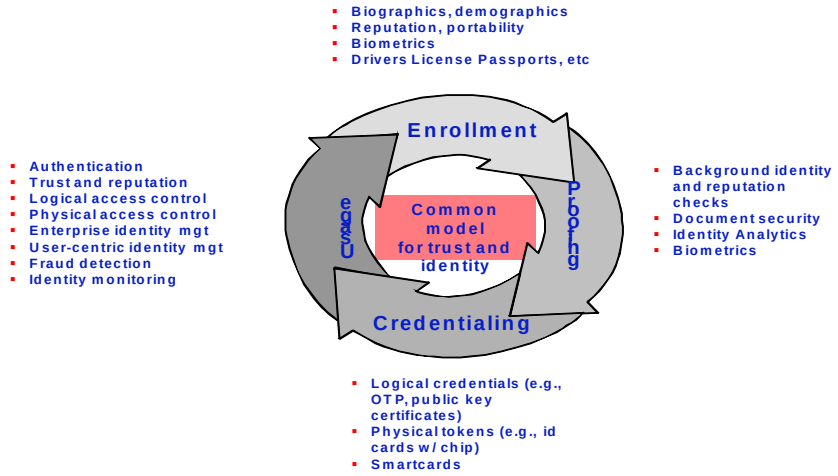

Figure 3.2: the Identity Life Cycle[26]

The policies and practices that govern these activities serve as the *primary basis of trust* for the relying parties involved in any given communication. It is thus essential for the establishment of trust relationships that the relevant entities are duly informed of (and satisfied with) the policies that govern these activities.

In order to perform the lifecycle referenced above, one typically needs to incorporate the following functionalities and services in the IdM infrastructure:

- Registration;
- Identification and authentication mechanisms;
- Access control and other authorization mechanisms;
- User management (provisioning/credentialing);
- Accountability mechanisms (e.g. identity monitoring, fraud detection, logging & auditing);
- Data storage and communication.

Management. A white paper, 2004, available at <http://www.opengroup.org/online>, last consulted 29 March 2008.

[25] International Telecommunication Union - Telecommunication Standardization Sector. Focus Group on Identity Management. Report on Identity Management Framework for Global Interoperability, p. 5.

[26] International Telecommunication Union - Telecommunication Standardization Sector. Focus Group on Identity Management. Report on Identity Management Framework for Global Interoperability, p. 5.

It is obvious that not every IMS contains all of these elements. Yet we believe that the main operational components of IDM systems can be described in terms of one or more of these functions or services. In the subsequent sections we elaborate on two of these elements in an attempt to clarify the operational management requirements for eGovernment IDM. We do so primarily from the perspective of the service provider in a FIDIS type 1 IDM architecture.

3.3.3 Registration

Entity authentication is a service that provides assurance of the claimed identity of an entity, as it corroborates the (claimed) partial identity of an entity and a set of its observed attributes.

Regardless of the chosen authentication level or authentication strength, entity authentication only attests the origin and the integrity of stated facts (i.e. the identity that is being asserted). It says nothing about the accuracy of the data that is exchanged during the authentication protocol. This is why the registration process is of crucial importance: the service provider assigning an identity must carefully verify that the claimed attributes are true before the entity is registered into the system.

In more technical terms, registration may be described as the process of collecting and corroborating a specific set of attributes of an entity, which typically relate to the partial identity (such as a characteristic or mandate) of that entity, with sufficient certainty, before putting at the disposal means by which the entity can be authenticated, or the characteristic or mandate can be verified.[27]

The overall registration process can be described as follows: a new user (or other entity), as an applicant, first registers with a registration authority (RA). This RA authority is an entity which is entitled and trusted to perform the registration service, i.e., the service of identifying entities and registering them in a way that allows the secure assignment of credentials. The registration authority must typically perform some form of identity verification (or "proofing"). Verification of the claimed identity is typically done through the evaluation of paper credentials and by records in databases (e.g., showing a national identity card or a driving license). In order to differentiate the new entity from other entities in the IMS the entity is typically assigned one or more unique identifiers (which will allow the entity to later be recognized in the domain of applicability).[28]

It is important to note that registration services do not only apply to identity attributes. Characteristics (e.g., being a doctor, civil servant) and mandates (acquired through legal or other form of delegation) are equally important, especially when it comes to granting access to protected resources.

3.3.4 User management

Another important piece of the identity management puzzle lies in user management. Two mechanisms for user management warrant some further elaboration, namely:

- provisioning and de-provisioning;
- delegated administration;

---

[27] Based on Robben, F., *1st Modinis Workshop on Identity Management in EGovernment*, 2005, available at <http://www.law.kuleuven.ac.be/icri/frobben/presentations/20050504.ppt>, last consulted at 15 October 2008.
[28] International Telecommunication Union - Telecommunication Standardization Sector. Focus Group on Identity Management. Report on Identity Management Framework for Global Interoperability, p. 5 et seq.

Provisioning[29]

Provisioning can be defined as the automation of all the steps required to manage (setup, amend and revoke) user or system access entitlements.[30] It relates to account creation as well as to credential delivery. The term 'provisioning' is sometimes also used to refer to the process of putting the appropriate (physical) resources at the disposal of authorized entities.

Resource (or user) provisioning is the process of providing users with access to the (computing and non-computing) resources they are authorized to use.[31] It can be seen as a combination of the duties of the human resources and the IT department of an organization to[32]:

- provide users access to computing systems and services (such as email accounts, disk space), to enterprise portals, to remote access networking services, to data repositories, etc. This is done by assigning the appropriate credentials to each user subsequent to account creation;
- Provide users with appropriate hardware and software resources such as computers, phones, desk etc.

In many organizations, the process for managing user access to resources is very labour intensive. Resource provisioning may be automated, e.g. by providing that as soon as a new employee is entered onto a Human Resources system, the employee's data triggers an automated process in which an email account is created, an ID badge is generated, the network administrator is notified, a network account is created, etc.[33]

The main driver to implement an automated provisioning mechanism in a governmental information system is because it reduces costs: system administrators do not longer have to re-enter the same information about entities for each administrative environment. Other important advantages are an increased accuracy of the system, and an increased productivity of the users (they can be operational in the fastest time possible).[34]

Delegated administration[35]

Delegated administration is a process which allows the offloading of the responsibility for user management to those who know their users best, increasing administrative efficiencies and reducing the level of staff required at the central site. In order to realize this, a "chain of approvers" must be identified to ensure secure delegation of capabilities (even roles) such as account provisioning to appropriate parties in the environment.

---

[29] The section is primarily based on Reed, A., *The definite guide to identity management*, 2002, available at <http://www.realtimepublishers.com>, last consulted 15 October 2008, p. 13, 16 et seq. and 40.
[30] Definition from OASIS Provisioning Services Technical Committee, *SPML FAQ*, available at <http://www.openspml.org/spml_faq.html.> last consulted 29 August 2008.
[31] Based on Slone, S. (ed.), *Identity Management. A white paper*, 2004, available at <http://www.opengroup.org/online>, last consulted 15 October 2008, p. 12; Webopedia, Provisioning, available at <http://www.webopedia.com/TERM/P/provisioning.html>, last consulted 15 October 2008.
[32] Based on Webopedia, *Provisioning*, available at <http://www.webopedia.com/TERM/P/provisioning.html>, last consulted 29 August 2008.
[33] Based on Reed, A. , *The definite guide to identity management*, 2002, available at <http://www.realtimepublishers.com>, last consulted 15 October 2008, pp. 16-17.
[34] Based on Reed, A. , *The definite guide to identity management*, 2002, available at <http://www.realtimepublishers.com>, last consulted 15 October 2008, p. 17.
[35] This section is primarily based on Reed, A. , *The definite guide to identity management*, 2002, available at <http://www.realtimepublishers.com>, last consulted 15 October 2008, pp. 16-17 and 40 et seq.

If an entity in charge of managing the system has a delegable right on a user profile, he or she will generally be able to delegate that authority to a similar entity (subject to applicable policy). The ultimate purpose of delegated administration is to allow individual users to perform certain administrative tasks on their own accounts, the most prominent example being password management.

Delegated administration thus may serve to limit the exposure of administrators by identifying 'chain of approvers' mentioned above to securely delegate capabilities (and even roles) to appropriate entities (mandate holders) in the environment.

More specifically, delegated administration makes it possible to:

- *Decentralize administration* by breaking down responsibilities among administrators by geographic location or areas of expertise (account creation, password management, security, and so on).
- *Delegate responsibilities* to authorized users (managers) who are best suited to assign and monitor the responsibilities of the users that they work with.[36]

The main benefits of delegated administration are that it increases the administrative efficiency and reduces the level of staff required at the (central) entity. Provided that a suitable access control model is used, delegated administration can be applied across the borders of the (central) entity itself, for example in relation to its external partners, customers, clients etc.

In general, delegated administration makes it possible to (1) delegate all permissions, including the ability to view, create, modify, and delete users, (2) change passwords, (3) add or delete a user in a security group and (4) approve or reject requests. To make delegation of administration worthwhile there is a certain level at which the desired efficiency can be attained. This varies from about 250 managed accounts (delegation of all permissions) to a thousand (change of password) or in some cases (requests approval) to more than a thousand.[37]

It should be noted that the technical meaning of 'delegation' is quite different from the legal one.

In the public service context the issue is in fact broader. In this context the legal processes of mandating and delegation come into view. In public law we make a difference between attribution, delegation and mandate. Attribution means that the law 'attributes' a specific competence to a specific public body. Delegation means that the body that has been attributed a specific competence delegates it to another body, which will exercise the competence in its own name and on its own account. Mandate means that the body that has been attributed or delegated a specific competence mandates it to another body, which will exercise the competence in the name of the mandating body and on account of the mandating body. Delegation implies performing an action on one's own account. On the other hand mandate implies that the action is performed in the name of the mandating body.

[36] Based on Reed, A. , *The definite guide to identity management*, 2002, available at <http://www.realtimepublishers.com>, last consulted 15 October 2008, p. 40.
[37] These are guesstimates by the author of this section.

Therefore delegation is the process whereby a person is conferred the capacity to perform an action with or towards a third party, in his/her own name, but on the account of another person, whereby the effects are directly and solely attributed to that other person.[38]

A mandate is a right granted by an entity (the mandate issuer) to an identified entity (the mandate holder) to perform well-defined legal actions in the name and for the account of the mandate issuer.[39]

From the legal perspective the concept of a mandate implies acceptance by the receiving identified identity.

3.3.5 IT Operations and IT Service Management

When operating IMS certain tasks need to be fulfilled repeatedly. These tasks are typically also related to management processes in the context of data protection and security. Most important in the context of operational processes are:

- Handling of incidents (incident management) and closely related: handling of security incidents
- Documentation of the configuration of hard- and software (configuration management); the documentation provides necessary input for data protection and security audits
- Planning, testing and formal releasing of new versions of hard- and software (release management; this is also important from a data protection and security point of view)
- Management of changes in hard- and software procedures and underlying infrastructure (change management)
- Availability (includes redundancy planning), capacity (planning computational and communicational resources required) and service continuity management; these tasks are directly related to the security target of availability
- Management of service levels (service level management); this includes security services required

Since the mid 1980s standards for IT operations became available. Most important in this context are the "IT-Infrastructure Library" (ITIL)[40] and the "Control Objectives for Information and related Technology" (CobiT).[41]

ITIL is a suite of a number of service management processes; while the still largely used version 2.0 contains ten processes, the number increased with the current version 3.0 to 30 because aspects of life cycle management of services and related infrastructure were

---

[38] Samoy, I.,'"What's in a name?" Het "in naam van-vereiste" bij de vertegenwoordiging vier jaar na Schoordijk' [What's in a name? The "in name of requirement" in representations four your after Schoordijk], *Tijdschrift voor Privaatrecht*, vol. 41, issue 1, 2004, pp. 563-576. Input by Mireille Hildebrandt during D16.1 Workshop in May 2007.

[39] Based on Robben, F., *1st Modinis Workshop on Identity Management in EGovernment*, 2005, available at http://www.law.kuleuven.ac.be/icri/frobben/presentations/20050504.ppt>, last consulted at 15 October 2008, slide 5.

[40] British Office for Government Commerce (OGC), *ITIL*, available at <http://www.ogc.gov.uk/guidance_itil.asp>, last consulted 15 October 2008.

[41] US American Information Systems and Audit Control Association (ISACA), *CobiT*, available at <http://www.isaca.org>, last consulted 15 October 2008.

introduced into the process suite. Information security management is not a core process in the context of ITIL – for this purpose reference to the British Standards (formerly BS 7799, now ISO/IEC 27000 series) is made. ITIL is mainly used in Europe.

Cobit, mainly used in the USA and companies with a close business relationship to the USA, has a more complete approach compared to ITIL. Cobit therefore also is referred to as "IT governance framework". In addition to operational aspects of IT quality management, compliance and security management are also integrated in this framework.

The structure of ITIL and Cobit differs significantly. While ITIL contains a relatively small number of concretely described processes and relating supporting infrastructure, Cobit describes mainly in so called control objectives and controls the requirement processes in this framework need to fulfil. Concrete process examples are not described in Cobit.

However, to reduce costs, to standardise internal procedures and interfaces with service providers and to meet data protection and security requirements in a standardised way, the described frameworks for IT operations provide a very important and widely used platform.

3.3.6 Quality and security management

When one wants to ensure compliance of the organization's activities with the established policies, procedures, and applicable legislation, as well as verify that an IMS is performing according to expectations, a variety of measures need to be implemented.

For the management of quality and security, international standards on this topic are the natural point of reference. Well established are the ISO/IEC 9000 series for quality management and the ISO/IEC 27000 series for information security management. According to these standards, information management systems consist in several layers:

- a *strategic* layer, in which e.g. policies and management hierarchies are defined;
- a *tactical* layer, in which e.g. processes and concepts are elaborated; and
- an *operational* layer, in which e.g. technical and organizational measures are defined.

An introduction to all these standards and types of management systems is far beyond the scope of this document. However, the two from the point of view of the authors very relevant requirements from these standards are outlined in this chapter.

For the evaluation of the quality and the security of the identity management processes, in addition to an accepted methodology (which can be taken from the standards mentioned above), reference data and specific documents are needed. This may include a set of policies (including security policies), operational concepts (including security concepts) and key performance indicators (KPI) for processes involved. In addition reliable logging and corresponding auditing mechanisms support post factum verification and strategic modification of these policies and indicators when appropriate. We now elaborate further on two of these components, namely KPI and logging and monitoring.

Metrics for quality measurement (KPI)

To assess the quality of an IMS (or any information system for that matter), one needs *qualitative evaluation systems* or *quantitative metrics* to measure against. In this context measurement can be carried out in at least two relevant areas:

- Processes along the life cycle of identities and

- Identity Management Systems (IMS) including related (technical) services.

For the qualitative evaluation of processes the *Process Maturity Model (PMM)*, developed from the Capability Maturity Model[42] often is used. PMM today is applied in the context of IT (operations) management systems such as ITIL and CobiT. The model allows the evaluation of the maturity of processes typically in five maturity levels. To reach a certain level of maturity higher than the initial level, the processes need to meet certain criteria. These criteria including (a) definition of in- and output, (b) documentation of sub-processes included tasks and steps etc. (c) definition of Key Performance Indicators (KPI) and (d) a certain level of usage of KPI.

The following picture illustrates the Process Maturity Model in five levels:

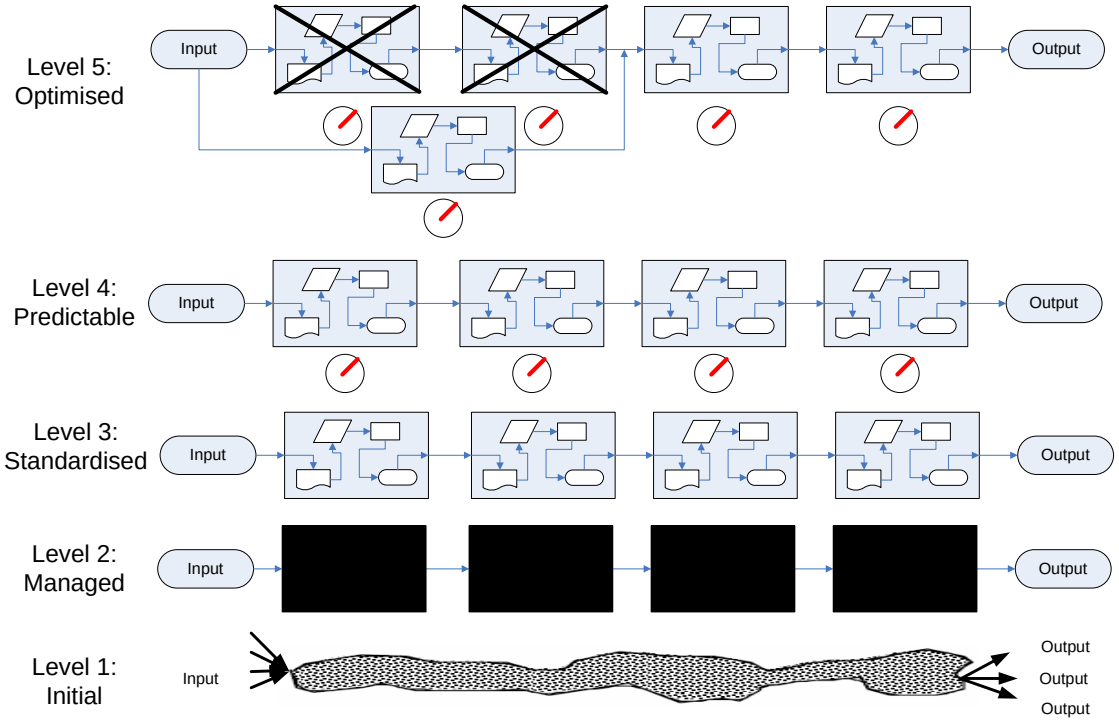

Figure 3.3: Levels of the Process Maturity Model (PMM)

The usage of KPI allows a quantitative quality evaluation. They have to be defined carefully with respect to the aspect of quality that is to be measured. For example with respect to the performance of a process the average time needed to complete the process and the average resources required in a certain time period may be appropriate, while for capacity management the development of these values in this time period may be more suited.

In practice, quality requirements with regard to the IMS and related services are often agreed upon in so-called “service level agreements (SLAs)”.

A **service-level agreement** (SLA) is a part of a contract between one or more service providers and one or more customers that defines the services to be provided, the metrics associated with these services, the expected quality of the services (acceptable and

[42] The Capability Maturity Model originally was developed at the Carnegie-Mellon-University at Pittsburgh (USA) to evaluate processes used for software development, see <http://www.sei.cmu.edu/cmm/>.

unacceptable service levels), liabilities on the part of the service provider and the customer, and actions to be taken in specific instances (e.g. escalation procedures).[43]

The quality of the services provided by the IMS can be measured of a number of properties which allow to establish certain requirements of the IMS, among which:[44]

- Performance: the speed measured and perceived by individual users of the system (latency), or the speed perceived by the total infrastructure, from the point of view of the server (throughput, number of accepted transactions per second).
- Reliability: refers to any system that consistently produces the same results, preferably meeting or exceeding its specifications.
- Affordability this is the level at which the production and operational deployment of the IMS and its applications is cost effective for both the user and the service provider(s).
- Capacity: technical resources provided such as total available disk space, CPU power etc. may be defined. The monitoring of the technical resources used allows for capacity management, which can be understood as part of scalability management.
- Scalability: this metric indicates how well a solution to some problem will work (both from a functional and a performance point of view) when the size of the problem increases by several orders of magnitude.
- Security Service Levels Agreements (SSLAs), which include technical and organizational measures to ensure the required level of security (e.g. confidentiality, integrity and availability) and business (or governmental) continuity, based on a security concepts.
  In the security concepts also the required security level is defined, a risk assessment carried out, a risk treatment plan and a description of residual (or remaining) risks is included. Technical and organizational security measures are the results of the risk treatment plan, elaborated based on the results of the risk assessment (see e.g. ISO/IEC 27001).

Logging and monitoring

Logging is a process that records the linkage between an action and the identity of the entity or role that has invoked the action. It provides an evidence trail of events that have occurred, operations that have been performed or were attempted by (or on) various services or resources.[45] The evidence trail about events and operations is reflected in logs. As this type of logged data always needs to be evaluated in an independent auditing process, the whole process of conceptualization of logging, the logging itself, and auditing also is referred to as "audit logging" in relevant standards for Information Security Management Systems (ISMS)

[43] Definition from Dobler, D.W. and Burt, D.N., *Purchasing and Supply Management*, McGraw Hill, New York, 1996.
[44] Based on ADAPID Project Group, *Requirement Study*, available at <https://www.cosic.esat.kuleuven.be/adapid/docs/adapid-d2.pdf>, last consulted 15 October 2008, p. 128 et seq.
[45] Based on Slone, S. (ed.), *Identity Management. A white paper*, 2004, available at <http://www.opengroup.org/online>, last consulted 29 March 2008, p. 24.

such as the ISO/IEC 27000 series and criteria systems based on them or IT governance frameworks such as CobiT[46].[47]

When information is retrieved from a log, the relying party must be able to determine whether any records were lost and whether the characteristics of the records stored in the log were modified at any time (*integrity*). It must also be able to verify that the log presented emanated from the appropriate entity (*authenticity*).

Logging serves many purposes. Its main task is to provide managers with information they can use for *security management purposes,*[48] *performance monitoring, monitoring compliance with business policies and legal regulations, reporting to the stakeholders etc.*[49]

In the context of security, audit logging aims at preserving the defined level of confidentiality, integrity and availability (CIA, the traditional security targets) of the data processed using the IMS. Additional security targets such as authenticity and non-repudiation also may be included. In any case audit logging does not aim at the IMS only, but also includes all the related processes of identity management. When administered appropriately (and taking into account the relevant legal provisions), the produced evidence trail of events and operations can also serve to establish someone's criminal or civil liability in case of an incident.

It bears noting that logging and monitoring may also have some other legal implications, particularly when the logs contain personal data (at either user- or object level).

[46] CobiT is available via http://www.isaca.org/.
[47] Meints, M. and Thomsen, S., 'Protokollierung in Sicherheitsstandards', *Datenschutz und Datensicherheit*, vol. 31, issue 10, 2007, pp. 749-751.
[48] See relevant standards such as ISO/IEC 27001 (ISMS), ISO/IEC 15408 (Common Criteria), and CobiT.
[49] Based on Slone, S. (ed.), *Identity Management. A white paper*, 2004, available at <http://www.opengroup.org/online>, last consulted 29 March 2008, p. 31. Logging and monitoring mechanisms can also be of significant value for accounting purposes.

4 Privacy-friendly identity management in eGovernment

4.1 Data protection principles for IDM for eGovernment

Assuming that eGovernment increasingly entails more transactions of personal, sensitive and financial data, and moreover requires more linkage of program and authentication information systems, privacy implications are likely to need more and more attention. Governments have the unenviable task of addressing possibly irresolvable tensions in policy and operational requirements. Considering there is ample literature dealing with data protection in general, we focus only on the implications the current approaches in eGovernment will have towards the principles underlying data protection.

4.1.1 Privacy in IDM design

Choices in the design of IDM systems, like the location(s) of stored data, the used identifiers, and the mechanisms of authentication, can influence the citizen's (sense of) privacy. And therefore, even though interoperable, effective, or single sign-on eGovernment services can have an added value for society, privacy needs to be taken into consideration when eIDM systems for eGovernment services are designed and used. Taking privacy into account can reduce the risks of, for example, function creep and identity fraud[50] and can ensure the societal support for the use of eIDM.

The use of personal data in eGovernment applications reveals a 'trust tension': the need to serve the citizen in an effective and efficient manner requires an increasing use and aggregation of data which, on the other hand, can affect the sense of freedom, autonomy, and trust of citizens[51]. Next to this, the obligations and accountability of the government in the field of e.g. national security and fraud prevention may have led to the fact that data collection and data retention are considered necessary. It is a challenge for governments to meet demands for security and efficiency whilst at the same time retaining the privacy of its citizens.

Facing the need to collect more data, the notion of privacy is more difficult to define and can be liable to unclear notions or contextual differences.[52] Nevertheless, several sets of privacy principles exist which can be used to assess the privacy-friendliness of electronic Identity Management systems. For our assessment of eID in eGovernment, we will point out three relevant categories of assessment on the basis of the Data Protection Directive (DPD) and its principles.

The Data Protection Directive (95/46/EC) was drawn up to address the need for pan-European flow of information and the need to have a certain level of data protection. It provides several legal privacy-requirements for personal data to be processed throughout private and public services in Europe.[53] Succeeding the OECD guidelines[54] and Council of Europe Convention

[50] Identity fraud is one of the fastest growing fields of criminality. Information available at <www.antiphishing.org>, last consulted 29 August 2008.
[51] See Dutton, W. et al., 'The cyber trust tension in e-government: Balancing identity, privacy, security', *Information Polity*, vol. 10, issue 1-2, 2005, pp. 13-23.
[52] Introna, L.D., 'Privacy and the computer: Why we need privacy in the information society', *Metaphilosophy*, vol. 28, issue 3, 1997, pp. 259-275.
[53] In principle, the directive does not discriminate between private and public data processing, even though exceptions exist e.g. in Art. 3(2) Dir. 95/46/EC

108,[55] the Directive is based on the consideration to create an internal European market. The Directive is implemented by all Member States in national regulation. Next to the establishment of an internal market, also the consideration to respect private and family life is addressed by this Directive. Thus, it combines the objectives laid down in article 95 of the EC treaty and article 8 of the European Convention on Human Rights (ECHR).[56] Even though the Directive has not been transposed in the same way in all Member States,[57] it is likely that the principles laid down in the Directive are respected by all Member States.

Several principles can be derived from the Data Protection Directive. We can, for example, derive the following six principles on the basis of an assessment by Kosta et al. for the PRIME project, [58] and a description of several privacy principles by Bygrave:[59]

- Fair and lawful processing (art 6(1)a), amongst others consisting of the need for information to the data subject (art 10) and openness of data processing;
- Purpose specification and purpose limitation (art 6(1)b), which also includes the need for a legitimate purpose (art 7) of data processing;
- Data minimisation (art 6(1)c), meaning that processing of personal data needs to be adequate, not excessive, and relevant;
- Data quality (art. 6(1)d), which has a relation with the need for data subject participation (art. 12 and art. 14), and comprises the requirement that data needs to be accurate and up to date;
- Conservation (art 6(1)e), meaning that data must not be kept longer than necessary, and;
- Security (Art 17).

Considering electronic Identity Management in eGovernment, we will assess the privacy-friendliness of eIDM systems in eGovernment more in detail on the basis of three categories which we consider the core themes of interest when it concerns the use of electronic Identities in eGovernment context. These categories are (1) legitimacy, (2) finality, and (3) transparency, and overlap with several privacy principles stated above like for example the principles of fair and lawful processing and purpose limitation. Specific issues considering the

---

[54] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at org >, last consulted 29 August 2008.
[55] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, available at <www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm>, last consulted 29 August 2008.
[56] Cuijpers, C.M.K.C., *Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn* [Privacy law or private law? A private law alternative for the implementation of the European Privacy Directive], Wolf Legal Publishers, Nijmegen, 2005.
[57] European Commission Communication, 'First report on the implementation of the data protection directive' (95/46/ec) (No. COM(2003) 265 final), Brussels.
[58] Inspired by: Bygrave, L.A., 'Core principles of data protection', *Privacy Law and Policy Reporter*, vol. 7, issue 9, 2001; Kosta, E. et al., *Requirements for privacy enhancing tools*, 2008, available at <www.prime-project.eu>, last consulted 15 October 2008; OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at org >, last consulted 29 August 2008; Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, available at <www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm>, last consulted 29 August 2008.
[59] Cf. Bygrave, L.A., 'Core principles of data protection', *Privacy Law and Policy Reporter*, vol. 7, issue 9, 2001.

processing of personal data in eGovernment applications, make it possible that legitimacy, transparency, and finality can not always be satisfied, due to the particular (legal) nature of the eGovernment context.

4.1.2 Making data processing legitimate

Processing of personal data is not permitted without a legitimate basis. Art. 7 and 8 of the Directive specify the instances in which the processing of personal data may be considered legitimate, at least from a 'formal' perspective. For eGovernment applications there appear to be two bases in particular which will typically justify the processing, namely:

- where the processing is necessary for compliance with a legal obligation to which the controller is subject (art. 7, c);
- where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed (art. 7, e).

A task carried out by government administrations in the public interest is only legitimate if it complies with 3 basic principles of public law, namely its (1) legality (2) speciality and (3) proportionality.[60] Thus both legitimacy grounds imply some form of legal basis justifying the processing.

Note that according to the European Court of Human Rights the requirement that the interference must be "provided by law" refers to the law in its broad ("material") sense; i.e. not strictly limited to statutes or acts. In other words it is not in all cases necessary to act upon a statutory basis as such. Even though according to the same Court the legal basis must be sufficiently precise to allow individuals to foresee its consequences and to give them adequate protection against arbitrary interference, this requirement appears less rigid as one might first assume. Furthermore, there appears to be a tendency to interpret existing legal bases broadly, so as not to unduly restrict the administration in the performance of its tasks.

It is important to consider that governmental entities are in quite a different position compared to private controllers. If a governmental entity feels the need to conduct a particular type of processing, it will need some legal basis to do so. One might argue that this significantly restricts the processing capabilities of governmental entities. On the other hand, if the required legal basis is present, the governmental entity will be able to conduct the processing without having to obtain consent of the data subject. Contrary to the private sector, the government is thus in a position to 'legitimize' the processing of such data which it feels necessary to realize its eGovernment goals. Only the constitution and international instruments (such as the ECHR) constrain the government in adopting new bases for processing. Although recent case law of the Strasbourg Court appears to increasingly embrace the principles underlying data protection, it unmistakably leaves the States a significant "margin of appreciation" when subjecting States' processing operations to an art. 8 analysis.

This situation is acceptable only to the extent that the legislative enactments have been preceded by the appropriate parliamentary debate, and the national data protection authorities have been duly heard. This is however not always the case.

[60] See art. 8 ECHR.

4.1.3 Finality principle vs. 'maximal' re-use of personal data

Several European governments consider "back-office integration" as one of the main functional requirements for successful eGovernment. As the reader is aware, the Directive stipulates that data may not be processed in a manner 'incompatible' with the purposes for which it was originally collected (art. 6, b).[61] This requirement has come to be known as the "purpose (or use-) limitation principle";[62] as it serves to set the boundaries of the processing and delineate it vis-à-vis other possible types of data processing. As we will discuss later, the finality principle is closely related to the transparency obligations under the Directive.

Back-office integration and, as witnessed in several Member States (e.g. Belgium, Netherlands) the principles of 'single collection' and 'maximal re-use' of data in eGovernment, appear to be strongly at odds with the principle of finality, or at least with the ideologies underlying it. On the other side of the spectrum is however the finding that data protection is said to act as a "transparency tool"[63]; serving to 'channel' legitimate uses of power, without imposing hard-line restrictions on what these possible legitimate uses may be.[64]

A first observation which needs to be made is that the Directive provides little or no guidance as to what does and does not constitute a "compatible" purpose.[65] Consequently, Member States' interpretations differ substantially in defining what is to be considered (in)compatible.[66] Further processing which is sufficiently "closely connected" with the original purpose will generally be considered compatible.[67] If the further use of the data may rightly be considered "compatible" with the originally stated purpose, there appears to be no conflict with the principle of finality.[68] However, what is the outcome when the new purpose is clearly distinct from the original purposes, to such an extent that it may not objectively be considered "compatible" with the original purposes?

With regard to the private sector, the majority of legal doctrine argue that it is possible to "re-purpose" personal data provided that these processing operations in turn meet all the requirements the law imposes upon data processing operations in general.[69] This may entail: notifying the data subject of this new purpose, obtaining an informed consent, additional

---

[61] Art. 6, 1a) DPD.
[62] See e.g. [Article 29 EHR], p. 6; Bygrave, L.A., 'Core principles of data protection', *Privacy Law and Policy Reporter*, vol. 7, issue 9, 2001; Kosta, E. and Dumortier, J., 'The Data Retention Directive and the principles of European Data protection legislation', *Medien und Recht International*, issue 3, 2007, p. 133.
[63] Gutwirth, S.L., 'Biometrics between opacity and transparency', *Annals of the Italian National Institute of Health (Ann Ist Super Sanita)*, vol. 43, issue 1, 2007, pp. 61-65.
[64] It is important to note that the Data Protection Directive does in fact provide an exhaustive enumeration of the instances in which personal data may be processed. However, it is clear that these basis or defined quite generically. This observation holds particularly in the context of eGovernment, merely stating that a law must be present etc.
[65] The exception of course being further processing of data for historical, statistical or scientific purposes (see art. 6, a) DPD in fine).
[66] Kuner, C., *European Data Protection Law. Corporate compliance and regulation*, Oxford University Press, London, 2007, p. 100.
[67] Kuner, C., *European Data Protection Law. Corporate compliance and regulation*, Oxford University Press, London, 2007, p. 100. See also Bullesbach, A., Prins, C. and Poullet, Y., *Concise European IT Law*, Kluwer Law International, Alphen aan de Rijn, 2006, pp. 44-45.
[68] Bot, D. de, *Verwerking van Persoonsgegevens* [Processing of Personal Data], Kluwer, Antwerpen, 2001, p. 120.
[69] Bot, D. de, *Verwerking van Persoonsgegevens* [Processing of Personal Data], Kluwer, Antwerpen, 2001, p. 121.

notification to the Data Protection authority, etc. This approach thus implies treating the subsequent processing operation as an entirely "new" processing operation, which must meet all the requirements set forth by the Directive.[70]

Several arguments can be made in favour of the latter approach. In fact, the framework set forth by the Directive itself implies that there may be instances in which personal data may be processed where it has not been collected from the data subject.[71] Furthermore, it is equally clear that consent of the data subject is not the sole basis for legitimate processing.[72]

Taking these considerations into account, it of course remains of crucial importance to have some form of criteria to assess "compatibility". The Belgian Data Protection Act for instance stipulates that compatibility is assessed "taking into account all relevant factors, particularly the reasonable expectations of the data subject and the applicable laws and regulations".[73] The Belgian DPA thus advances two specific elements to assess compatibility: the reasonable expectations of the data subject and the applicable laws and regulations. With regards to other 'relevant factors', doctrine states that special consideration may also be given to the nature of the processed data and the possible prejudices towards the data subject.[74]

Although the European Directive makes no reference to such criteria, the elements to assess compatibility advanced by the Belgian DPA (reasonable expectations of the data subject and the applicable laws and regulations) however do not appear to be in contradiction with the Directive in and of themselves. Such is also the case with the elements advanced by legal doctrine (nature of the processed data and the possible prejudices towards the data subject). However, it should equally be clear that the evaluation of compatible use *may not be entirely limited to the presence of some legal basis authorizing the processing.* Reasonable expectations of the data subject, nature of the data processed and possible prejudices towards the data subject should also be taken into account. This follows not only from the language of the Directive, but also from the obligations of Member States under art. 8 ECHR. Furthermore, as mentioned earlier, such legal basis must be *sufficiently clear and precise* to allow individuals to foresee its consequences.

The Data Protection Directive indicates in recital 39 that "re-purposing" of personal data may under certain circumstances be legitimate. One should however be careful not to confuse two distinct notions, i.e. compatibility on the one hand and re-use of personal data (for a clearly distinct purpose) on the other hand. If the latter is the case, the "new" processing operations must in turn meet all the requirements the law imposes upon data processing operations in general. In the field of eGovernment, this will generally entail that a new legal basis must be enacted. As this exercise of regulatory power will generally also need to comply with art. 8

---

[70] Bot, D. de, *Verwerking van Persoonsgegevens* [Processing of Personal Data], Kluwer, Antwerpen, 2001, p. 121.

[71] See in particular art. 10-11 DPD (regarding the right to information of the data subject), which distinguishes between the situation where the data is collected directly from the data subject and the situation where the data was collected from a different source.

[72] Further support for this position may also be found in recital (39) of the Data Protection Directive: "Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, *even if the disclosure was not anticipated at the time the data were collected* from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party".

[73] Art. 4, § 1, 2° of the Belgian DPA.

[74] Bot, D. de, *Verwerking van Persoonsgegevens* [Processing of Personal Data], Kluwer, Antwerpen, 2001, p. 121.

ECHR, the reasonable expectations of privacy of the citizens will have to be taken into account. In such an instance, due consideration should be given to the fact that the data subject will most likely be unaware of this re-purposing.

On the other hand, the principle of finality specifies that no further processing may be done incompatible with the original purposes. However this processing should take into account all relevant factors and particularly the reasonable expectations of the data subject and the applicable laws and regulations. Special consideration may also be given to the nature of the processed data and the possible prejudices towards the data subject.[75] This judgement should be done in the legislative phase. To determine the compatibility with the principles of proper data protection of the individual a PIA may be a useful procedure at this phase.[76]

Furthermore the Data Protection Directive in recital 39 provides some support for providing a sufficient basis for the re-use of personal data by government entities. It states that data can be legitimately disclosed to a third party even if the disclosure was not anticipated at the time the data were collected. Still the data subject should be informed when the data are recorded. If one considers government as one processor the act of disclosure to a third person can be said not to take place. The legal constraints of both the DPD and the other relevant laws and regulations are from this point of view in some sense no longer an obstacle. Additional point of interest to be noted here is that the proportionality principle can be referred to in this context. ECHR art 8 after all stipulates that there must be a reasonable relationship between the limitation to the right of privacy at the one hand and the legitimate goals that are being strived for on the other hand. By giving the aforesaid special attention to the nature of the processed data and the possible prejudices towards the data subject, the balancing test of the proportionality principle may be deemed to receive due attention.

4.1.4 Data quality

Art 6 Data Protecton Directive stipulates precisely the requirements for the quality of the data. It goes without saying that since the matching exercises in the back office of the government are based upon the accuracy of the information provided by the participants, efforts towards accuracy should be of the highest level. The data subjects' view as to the accuracy of his personal data should receive special attention. However in a fully automated operation the incorporation of these views in the processing process will probably be difficult and often be omitted.[77]

In eGovernment the tendency exists to make maximum re-use of data. This need should be brought in line with the principle of proportionality. This principle therefore gets a broad dimension. As a matter of fact, besides the principle of proportionality, the principles of data minimisation and storage duration should be brought to bear here as well. In a sense they can be seen as part of the proportionality principle. As soon as the processor decides upon re-purposing, a new legal basis has to be present. Still even if the processing is being conducted for a legitimate purpose, the processing may not prejudice the data subject in a way that is disproportionate to the interests pursued by the controller. At all times the appropriate balance between the interests of the controller and the data subject must be respected. Moreover one

[75] Data Protection Directive art 4 # 1, 2.
[76] Cf. Holden, S.H. and Millett, L., 'Authentication, Privacy and the Federal E-Government', *The Information Society*, vol. 21, issue 5, 2005, p. 371 for the provisions made for a PIA in the US E-Government Act 2002.
[77] Papakonstantinou, V., 'A data protection approach to data matching operations among public bodies', International Journal of Law and Information Technology, vol. 9, issue 1, 2001, p. 53.

has to adhere strictly to the principle of proportionate storage duration. The nature of the data once again plays an important role here. The processed data may not be kept in a form permitting identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. In terms of necessity of the data only data that is actually necessary to achieve the goals of the processing may be processed. For each purpose specified, a sufficient connection must be established between the purpose and the data collected. In this line of thought this embodiment of the proportionality principle may also be called "data minimization" as it requires that the least possible amount of data is processed taking into account the purpose for which it is being processed.

4.1.5 Transparency in eGovernment?

Under the Data Protection Directive, the controller's obligations regarding transparency are closely related to the finality and proportionality principles. As a rule, the data subjects must be informed of at least of the processing as such, the purposes of the processing and of the identity of the controller.

Because in the eGovernment setting data is often matched and linked beyond the scope of a particular service, the obvious question is whether at every stage of the processing the controller is required to inform the data subject. Relevant to our analysis is the finding that the Directive limits the right to notification in the following two instances:

- when data is collected indirectly and informing each data subject would involve a disproportionate effort;
- when the recording or disclosure is expressly laid down by law.[78]

These limitations cover a large part of the data processing by eGovernment and it can be argued that they *de facto* abolish the requirement for transparent data processing.[79]Although in most legal systems no subject can claim to be 'unaware of the law', citizens may often, as a matter of fact, not be aware of the legal basis warranting the data exchange. Combined with the blanket exemptions to notification under the Directive, this situation leads to a gross lack of transparency vis-à-vis the data subject.

4.2 Identity Management Evolution

The previous paragraph (eGovernment vis-a-vis privacy principles) indicated that IDM systems implemented in eGovernment do not necessarily comply with some categories of privacy principles, especially when it concerns the legitimacy of data processing, the proportionality of the data with regard to its purposes, and the transparency of data processing.

This section will conceptualize the toolbox of techniques and models that can lead to substantial improvement of privacy and data protection in eGovernment. It can also provide additional, specific privacy principles or privacy requirements for eGovernment. We will first describe some of the characteristics of different theoretical IDM models, mainly derived from

[78] Art 11 of the Directive.
[79] Papakonstantinou, V., 'A data protection approach to data matching operations among public bodies', *International Journal of Law and Information Technology*, vol. 9, issue 1, 2001, p. 52.

literature and the general evolution of IDM systems in recent history. After this elaboration, we will describe some characteristics of the different IDM approaches in eGovernment by Member States in the light of the IDM models. After the description of the theoretic models of IDM and the different approaches of Member States, specific instruments to achieve privacy-friendliness are described.

4.2.1 IDM models: from IDM silos to user-centric IDM

In a more theoretical context than the Fidis context (cf section 3.1), we distinguish four different models of Identity Management: 'identity silos', 'centralised IDM', 'federated IDM', and 'user-centric IDM', which all have different implications to privacy.[80]

'Identity silos' are systems in which registration, identification, authentication and authorisation of users is organised by one entity, for a fixed group of users that are served by this entity only. In this system, individuals will need to identify and authenticate themselves in a specific way, e.g. by logging in with a username and password that are assigned to her for this service only. In an 'identity silo' the storage of data, the IDM infrastructure, and the security level of the system are controlled on the level of the one specific service. Moreover, with identity silos every service has its own IDM procedures and architecture. When IDM silos are used, individuals usually need to cope with many different procedures for registration, identification and authentication (e.g. by remembering many login procedures). Because of this, the 'silo-model' can be burdensome for both users and organisations that rely on electronic identities. Moreover, the development and maintenance of different 'identity silos' may cost superfluous efforts. From a privacy perspective, 'identity silos' require users to continuously register themselves to new services, and to continuously identify and authenticate themselves. Because of this, personal information is probably stored on a multitude of locations, making it potentially difficult to update personal information or to remember where personal information is stored. Moreover, the need to re-authenticate oneself can lead to security issues like the reuse of (easy to guess) passwords and usernames for several services. Identity silos can lead to scattered, incorrect, inconsistent and incorrect identities of individuals.

A solution to the 'ad hoc' nature of the 'identity silos' is the centralised IDM model. Such a system relieves both the user and organisations from the many existing electronic identity 'one-offs' that resulted from a silo-approach.[81] The system deploys a central IDM model for several services that have a common group of users. It relies on one IDM architecture, an identity provider (IdP) 'in the middle', and central management of identity information. Because of this, there can exist a uniform security level. Moreover, maintenance of the system may be made more feasible because the control and management of identities is put at the disposal of the IdP. From a user perspective, the centralised IDM model is advantageous because the use of electronic identities can be made more convenient (e.g. through Single Sign On). However, having one identity provider –in this case one government agency- in the middle can make all actors involved (both individuals and relying organisations) vulnerable to the power of the central identity provider. Moreover, flaws in a centralised system can have far-reaching consequences ('all eggs are in one basket'). From a privacy perspective, data loss

[80] Cf. Olsen, T. et al., *Privacy - Identity Management*, available at <www.legal-ist.org>, last consulted 29 August 2008. Pato, J., *Identity management: Setting Context*, available at <http://www.hpl.hp.com/techreports/2003/HPL-2003-72.html>, last consulted 29 August 2008.

[81] Cameron, K., *The laws of identity*, available at <http://msdn.microsoft.com/en-us/library/ms996456.aspx>, last consulted 29 August 2008.

and identity fraud are substantial issues in centralised systems. Moreover, the use of personal data for unwanted purposes (profiling, function creep, social sorting) may be relatively high in a centralised system, as the IdP 'in the middle' has large amounts of personal data at his disposal, which may be linked, combined, or transferred to other contexts.

The federated IDM model can resolve some of the issues that are intrinsic to a centralised IDM model. Identity federation aims to make identities usable through different domains, whereas a centralised IDM model aims at managing identities centrally for a specific domain with common users. Moreover, the federated model –trusting on mutual agreements and standards- allows any number of IdPs to handle the authentication or even the exchange of identity attributes.[82] Hence, with a federated IDM model, one government organisation may accept a citizen for a service because this citizen has been previously authenticated for services in another (government or private) domain. With federated IDM in eGovernment the individual may potentially be able to use different identifiers or identities throughout government services, making it possible to separate contexts. In addition, the risk of linkability and mass loss of data may decrease if the federated system has several identity providers that can construct and issue identities, based on decentrally stored and managed personal data. Thus, a federated system can be more diverse and less dependent on one identity provider than the centralised IDM system. However, the model does rely heavily on mutual agreements and trust enhancing mechanisms between the identity providers, users, and relying parties that join the system. Because of this, an individual is still vulnerable to unreliable parties or insecure systems that are involved in a federated IDM system.

A development in the IDM landscape that can circumvent the vulnerability of the individual is the creation of 'user-centric IDM', which gives the citizen more control over the electronic identities used. In the government context this means that the citizen would be situated in the middle of the IDM process, by giving her control over the utilisation (and possibly also the construction)[83] of identities. In a user-centric system, government services that rely on authentication or identity information thus do not necessarily have to make use of locally stored information and neither will they have to communicate with other organisations that have this identity information at their disposal. Instead, government services that need identification and authentication could interact directly with the citizen to whom an eID relates. Subsequently, this citizen can prove identity-related claims by means of identities or attributes that were issued to her (e.g. by trusted parties) and are under her supervision. This makes the citizen more or less 'in control' of the electronic identities that others need to use as she can, facilitated by software and hardware put at her disposal, decide by herself if and which identities are utilised. In this way, the user can adjust the way she portrays herself to others and can control the kind of personal data that is used by services that rely on the use of eIDs (even though this would require some additional knowledge and effort concerning identity management at the user's end).

In theory, the user-centric IDM model approaches a privacy-friendly design the most because it is closely connected to the notion of informational control and self-determination, which are

[82] Olsen, T. et al., *Privacy - Identity Management*, available at <www.legal-ist.org>, last consulted 29 August 2008. Pato, J., *Identity management: Setting Context*, available at <http://www.hpl.hp.com/techreports/2003/HPL-2003-72.html>, last consulted 29 August 2008.

[83] For example, by means of composing credentials that are assigned by different 'credential providers' or 'authoritative parties'.

some of the core aspects of privacy.[84] Moreover, in a user-centric system, the individual can by herself determine the way she is portrayed to others and can autonomously decide when and which information is used for which purpose. However, chapter 3.1 described that "*IMS for user controlled context-dependent role and pseudonym management*" ('type 3 IMS') are likely to be difficult to apply for governmental institutions, as control over identity and identity information by these institutions in most cases is an important requirement. Hence, having user-centric IDM systems, even though privacy-friendly, will not always be feasible, even though some eGovernment initiatives indicate that there has been interest in user-centric IDM for some purposes.[85] In addition, IDM silos will not be feasible in an eGovernment context as well because this approach is difficult to align with the eGovernment objectives, such as there are efficiency, reducing administrative burdens, and reducing errors.[86] Because of this, centralised and federated (decentralised) IDM models are the kind of IDM systems that show most resemblance to the systems designed by Member States,[87] even though a clear line between the two models may be difficult to draw in practise.

4.2.2 Central vs. decentral IDM approaches in Member States

The IDM systems in Member States show some resemblance with either federal or central IDM systems. Their systems for example rely on the existence of one or several identity providers or can make use of central vs. decentral IDM architectures. Next to this, the country reports show that significant differences exist with regard to the identification and authentication of citizens (which varies from biometric authentication to PKI-based authentication).

In this section, we will mainly concentrate on parts of the Member States IDM systems which deal with the actual identity provision, data storage, and the flow of personal data. In short, this boils down to an assessment of the use of 1) data storage, 2) identifier policies and 3) identity data exchange. We consider these concepts to be relevant, especially in the light of the difficulties of legitimacy, proportionality, and transparency in the eGovernment IDM context, which were described in chapter 4.1.

Data storage

Electronic identities of citizens are constructed on demand of the citizen or on demand of other government services. Several eIDs of one citizen can exist, like a medical ID, a tax payer ID, or a social security ID. These different IDs are constructed from information which

---

[84] Cf. Fried, C., 'Privacy (A Moral Analysis)', *The Yale Law Journal*, vol. 77, issue 1, 1968, pp. 475-493; Westin, A., *Privacy and freedom*, Atheneum, New York, 1967; Stalder, F., "The failure of privacy enhancing technologies (pets) and the voiding of privacy', *Sociological Research Online*, vol. 7, issue 2, 2002, available at <www.socresonline.org.uk/7/2/stalder.html>, last consulted 29 August 2008.

[85] For example the initiative of the Dutch Commissioner Snellen, who advocated the development of 'digital lockers'. See Commissie Modernisering GBA [Commission Modernization Gemeentelijke Basisadministratie/Municipal Database Personal Records], *GBA in de toekomst. Gemeentelijke Basis Administratie persoonsgegevens als spil voor de toekomstige identiteits-infrastructuur* [GBA in the future. Municipal Database Personal Records as the pivot for future identity infrastructure], available at <www.minbzk.nl/aspx/download.aspx?file=/contents/pages/4985/eindrapport_gba_in_de_toekomst_3-01.pdf>, last consulted 29 August 2008.

[86] See also: SEC (2003) 1038, COM (2003) 567 final, adopted in Brussels, 26 July 2003, p. 8.

[87] Cf. IDABC, *Analysis and Assessment of similarities and differences – Impact on eID interoperability*, available at <http://ec.europa.eu/idabc/en/document/6484/5644>, last consulted 29 August 2008.

can be retrieved at a local database, but may also be retrieved from one central database or from other databases that are constructed for other government services.[88]

Some national IDM systems tend towards a centralised storage of specific personal data, which makes eID construction in government services dependant on this centrally stored information. For example, the NIR in the UK and the "key registers" in the Netherlands tend towards a centralised storage of some of the data relating to its citizens (even though other data repositories can still exist next to these central registers). The centralised model deserves attention in the field of privacy because data loss, identity fraud, contextuality of information, and profiling are possible issues here. Especially when a central register makes it possible to construct complete and usable electronic identities, data loss can lead to large scale identity fraud.

Identifier policy

When electronic identities are constructed (be it centrally or decentrally), these will need to be linked to a certain citizen, which requires eIDs to carry an identifier. In the design choice of an IDM system, Member States therefore have to choose an 'identifier policy'. With regard to identifiers, also a centralised approach exists next to a decentralised approach. For example, Member States can choose to use one central identifier for all electronic identities, but it is also possible to use a set of identifiers in an IDM scheme which can be utilised according the context or the sector an eID is used in.[89] Between these two approaches, there even exists a number model that combines the central and decentral identifier-approach. This model uses sectoral eIDs on a back-office level, whereas a single identifier is being used at the front.[90]

The choice for a central or a decentral identifier policy has privacy implications, because, when a central/single identifier is used, data and electronic identifiers can easily be linked throughout government contexts. Hence, the eID that was constructed for tax purposes may be linked to an eID used in the medical field. In this way, personal data can pop-up in undesired contexts. With the use of sectoral eIDs, this problem is less likely. A decentral identifier policy makes it more difficult to combine eIDs and identity information out of different contexts, which is only possible with the cooperation of, for example, trusted intermediaries that are necessary to transpose identifiers used in one context to the identifiers of another context.

There exist "a lot of divergent approaches towards the application of identifiers for persons in Member States".[91] Some countries use national identifiers whereas others use sectoral or contextual identifiers. For example, the Netherlands number model relies on the use of a central number (CSN) which is being used in all sectors. Some Member States oppose to the model of a central identifier, like Germany and Hungary.[92] A recent IDABC report indicates

---

[88] Opposed to the user-centric IDM, where information is stored at the user's end.
[89] Modinis IDM, *Modinis Study on Identity Management in eGovernment*, available at <www.cosic.esat.kuleuven.be/modinis-idm>, last consulted 29 August 2008.
[90] Cf. Commissie Van Thijn, *Persoonsnummerbeleid in het kader van identiteitsmanagement* [Personal number policy in the context of identity management], available at <www.ejure.nl/mode=display/downloads/dossier_id=187/id=47/Persoonsnummerbeleid.pdf>, last consulted 29 August 2008.
[91] Modinis IDM, *Modinis Study on Identity Management in eGovernment*, available at <www.cosic.esat.kuleuven.be/modinis-idm>, last consulted 29 August 2008, p. 9.
[92] IDABC, *Analysis and Assessment of similarities and differences – Impact on eID interoperability*, available at <http://ec.europa.eu/idabc/en/document/6484/5644>, last consulted 29 August 2008.

that "sector/application specific tokens are generally not considered to be a key part of a government's eIDM strategy".[93]

Data sharing

Decentral storage of data and the use of sectoral identifiers can create an IDM model that makes it easier to achieve privacy-friendliness than systems that make use of centralised storage and single-identifiers. But of course, in both systems security and trustworthiness of the institutions that process the data is still necessary. Moreover, it needs to be mentioned that when identity data is shared between different services, IDM systems still need to assess the format in which personal data is transferred, as privacy-friendliness can also be achieved by altering the format of data throughout contexts.

Several Member States rely on the 'authentic source principle'.[94] This principle addresses the need for one authentic source of each identity attribute. Authentic sources can realise the quality of data and can make IDM systems more efficient. However, it also means that these authentic sources form the foundation of electronic identities in many contexts. Bearing this in mind, it is important that the format of data is taken into account, and altered when necessary.

Identity information can exist in different forms. For example, when it is necessary to confirm a citizen's residence, a government service can make use of the full address of this citizen, whereas a confirmation by another government service (by means of a simple 'yes', this person lives in...), may also be sufficient. Member States therefore have to consider which format and what amount of data is necessary to prove the claims concerning a citizen. Grosso modo, three possibilities exist:

- government services have full access to other databases which makes it impossible to transpose the format of information in a privacy friendly-manner;
- government services need to request for identity information, for example at a trusted party having access to this database, but this information is not converted.
- government services need to request for identity information, which is converted in a privacy-friendly manner when this data is exchanged.

Data sharing, data exchange, and interoperability of data exchange are part of the pan-European eGovernment strategy. Hence, data sharing is inevitable and necessary, but can be executed in many different ways. On the basis of the country reports, it is difficult to assess how the actual data exchange takes place in Member States. However, with reusability of data and authentic sources as drivers behind several IDM initiatives, it is necessary to emphasize that data exchange shall occasionally be executed in a privacy-friendly manner instead of providing access to a database.

With the description of different IDM models, we do not attempt to prescribe an ideal privacy-friendly IDM model for eGovernment. Whether decentralised or centralised models are feasible depends on the specific aspects of the eGovernment context. For example, it would not be feasible to gather all data on the basis of inquiries that can be answered with only a 'yes' or a 'no'. However, for data that can be considered sensitive, such an approach

[93] IDABC, *Analysis and Assessment of similarities and differences – Impact on eID interoperability*, available at <http://ec.europa.eu/idabc/en/document/6484/5644>, last consulted 29 August 2008, p. 32.
[94] IDABC, *Analysis and Assessment of similarities and differences – Impact on eID interoperability*, available at <http://ec.europa.eu/idabc/en/document/6484/5644>, last consulted 29 August 2008, p.69-71.

may be suitable. Moreover, central management of identities may be necessary and useful for general personal data and is aligned with some objectives of eGovernment. However, what we do attempt to make clear is that a centralised approach to IDM management can, or should, be complemented with instruments that enhance the privacy of the citizen. Some of these instruments will be described in the following paragraphs.

4.2.3 General Organizational measures

Based on the European Data Protection Directive (95/46/EC) and the corresponding national data protection legislation general organisational measures are in place. A number of these measures ensue from the applicable European or national legislation. Additionally, other methods can be implemented to further strengthen a balanced approach towards fair identity management systems.

As mentioned earlier in this deliverable, the Directive, which has been transposed in national legislation, contains principles that lay the foundation for many of the organisational measures that have been put in place to safeguard the privacy requirements. More specifically the measures to ensure data quality, conservation and security can be referred to here. The supervisory agencies that have been set up to monitor the correct adherence to the legislative measures, which in, for example the Belgian situation, have led to the need of prior authorization by the data protection authority. Other important measures are taken in the carrying out of the transparency principles which have been described later on in this report.

Balancing the legal obligations of the government, and the privacy protection requirements of its citizens, is an ongoing challenge. One of the tools to support this effort is the Privacy Impact Assessment, described as a formal method by Roger Clarke in 1998.[95] A Privacy Impact Assessment (PIA) is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[96]

In the United States of America, the EGovernment Act of 2002 obliges government agencies to conduct a PIA whenever they want to acquire new electronic information systems or establish information collections that involve the use of personally identifiable information. The PIA must be shared with the Office of Management and Budget (OMB) when requesting new funding, and the PIA results must be made public if practically possible[97]

PIAs do not outline detailed questionnaires on how to assess the privacy impact of information systems. They rather suggest a number of issues that need to be addressed in the assessment process, thus leaving room for every federal agency to develop its own implementation to suit the specific circumstances of the agency in question. This results in a

[95] An updated version of the original publication is available at <http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html>, last consulted 22 September 2008.
[96] Office of Management and Budget, *OMB guidance for implementing the privacy provisions of the E-Government Act of 2002*, available at <http://www.whitehouse.gov/omb/memoranda/m03-22.html>, last consulted 17 August 2008.
[97] Holden, S.H. and Millett, L., 'Authentication, Privacy and the Federal E-Government', *The Information Society*, vol. 21, issue 5, 2005, pp. 367-377.

diverging body of PIA methods, but in general PIAs share a number of characteristics that are described below.

First, PIAs should be conducted early in the development process of new systems, when it is still possible to adapt the design in order to balance the privacy requirements with the functional system requirements. The consideration of privacy issues at the design stage is actually one of the overarching goals of PIAs: when the matter of privacy is only considered in later phases, costs of system adaptations may prove to be prohibitively expensive or even impossible. Second, the PIA should in principle be drafted by the people responsible for the business processes and supporting information systems. Although privacy specialists or system developers might review the PIA, process owners are in the optimal position to assess the privacy impact in the light of the organisational goals. Therefore, they should be able to consider process solutions and/or organisational adaptations that are less privacy-invasive, but are equally effective in attaining the organisational objectives. Finally, PIAs should also be conducted whenever organisational changes - either in the organisational, process or systems areas - are prepared: even apparently simple organisational restructurings may have grave privacy consequences if certain information systems or business processes are inadvertently brought together. A PIA can prove to be a powerful tool to highlight the potential risks before the actual implementation is carried out.

In eGovernment, authentication can be of major importance in the implementation of new initiatives. If this is the case, PIAs in their current form may prove to be too superficial, and the Privacy Analysis Framework For Authentication (PAFFA) could be employed.[98] Whereas PIAs are compulsory in many cases in the USA, PAFFA's are not, but the level of detail in PAFFA may prove to be a worthwhile investment in the assessment procedure, generating good insight in the design specifications and decisions of government IT innovations with a large authentication component.

PIAs have enjoyed a growing popularity in recent years, aided by their compulsory status in a number of countries.[99, 100, 101] Europe has been focussing on compliance checks with data protection legislation in place. Nevertheless the interest in PIAs is on the rise. This development is supported by the need to assess privacy impact of innovations in the public sector that go beyond the mere implementation of new information systems. Cases in point are mass transit systems and integrated health management systems that could benefit from an integrated assessment in an early development stage allowing for adaptations in business processes, and the type and extent of information to be stored.

4.2.4 Transparency enhancement – the state perspective

General requirements for transparency

From a state perspective it is most important that governmental processes are lawful, reliable and lead from the perspective of citizen concerned to comparable results in similar cases

[98] Kent, S.T. and Millett, L.I., *Who goes there? Authentication through the lens of privacy*, National Academy Press, Washington DC, 2003.
[99] Office of the New Zealand Privacy Commissioner, *Privacy Impact Assessment Handbook*, available at <http://www.privacy.org.nz/privacy-impact-assessment-handbook/>, last consulted 18 August 2008.
[100] Treasury Board of Canada Secretariat, *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*, available at <www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1_e.asp>, last consulted 18 August 2008.
[101] Office of the Privacy Commissioner of Australia, *Privacy Impact Assessment*, available at <http://www.privacy.gov.au/publications/pia06/index.html>, last consulted 18 August 2008.

within a procedure (fairness). Identity management is important in this context as it assures the authenticity of subjects of and actors in e-governmental processes and prepares the ground for administration internal quality assuring measures such as revision or auditing. Quality assuring measures are of especial importance in cases administrations use external service providers (outsourcing of governmental procedures and services). From the quality-assuring methods used, the requirements for transparency of procedures can be derived. Important methods and related requirements are mainly:

- Comparison of the processing of similar cases by governmental organisations to ensure fair processing;
  requirement: categorisation of cases and linking of individual cases to these categories; input, intermediary results and output of individual cases in one category also needs to be compared

- Auditing of procedures by governmental organisations;
  requirements: tasks in processes in the context of the procedure in question, roles and access rights of actors are described; the existing practice can be reviewed based on documentation and inspections; input, intermediary results and output of individual cases can be assessed to determine whether the processing is effective (if not efficient). These requirements are relevant as well in the context of internal audits with the aim of ensuring and improving internally the quality of governmental procedures as in the context of external audits where governmental organisations need to confirm a required level of quality to a superior public administration. Examples for internal audits are audits on a national governmental level carried out by the national boards of auditors, the audit of national governmental organisations by the European Court of Auditors is an example for an external audit

- Assessment of individual cases by governmental organisations;
  requirement: data of the individual (the data subject) processed in related procedures can be compared and checked for inconsistencies (caused on purpose, e.g. to commit fraud, or by accident); the implementation of this requirement needs to be in accordance with the finality principle (purpose binding principle)

- Fulfilling the request of individuals concerned (the data subjects) for information in the context of processing of their data e.g. in the context of data protection (transparency principle) or based on Freedom of Information Acts;
  requirement: tasks in the individual case, input, intermediary results, output and actors responsible for these tasks are documented

- Assessment of individual cases based on petitions by the individuals concerned (the data subjects) by an independent governmental organisation;
  requirement: tasks in the individual case, input, intermediary results, output and actors responsible for these tasks are documented

In the context of auditing the answer to the question: “Who did what in which case based on which roles and rights” is relevant. Audit logging and reports with respect to roles and rights in governmental systems and applications relying on identity management systems may provide important parts of the answer.

Levels of authentication and identification

Authentication in the context of governmental services requires different levels relating to different sets of rights in governmental systems and applications. As a result these levels

differ in the strength of authentication and the level of identification of citizens and governmental employees. At least the following levels clearly can be identified:

- Very high reliability of identity and authenticity of governmental employees in the context of processing highly sensitive data e.g. in secret services, military and police contexts
- High reliability of identity and authenticity of citizens and governmental employees in the context of processing sensitive data, e.g. special categories of personal data according to the Directive 95/46/EC
- Normal reliability of identity and/or authenticity of citizens and governmental employees in the context of processing personal data belonging to no special categories according to the Directive 95/46/EC
- No reliability in the identity and authenticity required as information or services are of a public nature. This typically is implemented using publications or public websites
- Special requirements mainly with respect to anonymity of citizens, e.g. in the context of certain steps in e-petitions and e-voting etc.

Having a close look at the last two categories of reliability, one can come to the conclusion that they are closely connected due to the fact that in cases where no authentication is required the implementation of the data minimisation principle may lead to the need to anonymise personal data. This extensively was discussed in the context of governmental websites and the storage and use of IP addresses of users e.g. in Germany.[102]

For the strength of authentication currently no common metric is available. Nevertheless strength of authentication is influenced by the following factors:

- Factors of authentication used; typically the factors knowledge, possession, biometric features and location at a given time can be differentiated.
- Ways of authentication; this describes whether the parties involved in a transaction authenticate on a comparable level. Today this is often not the case. An ATM for example authenticates to the user mainly by the way it looks; thus manipulation of the ATM to the user in many cases is not obvious
- Channels of communication of authentication information; this refers to different communicational channels used for the transfer of authentication information. A typical example is the use of mTANs for money transactions where in addition to the internet mobile phones are used to transfer a transaction number (TAN).

Strength of authentication will be further evaluated in the FIDIS deliverable D13.8 “Applicability of privacy models”.

4.2.5 Opacity enhancement – the state perspective

Opacity of citizens and governmental employees involved in governmental procedures may be required mainly for security reasons. In many countries freedom of information acts exist, allowing the citizen to take a look at governmental files concerning themselves. These rights are typically restricted, where either (1) the personal rights of other citizens involved in the

[102] See e.g. http://www.heise.de/newsticker/Zypries-droht-Haft-oder-Ordnungsgeld-beim-Speichern-von-IP-Adressen--/meldung/103440/

same procedure or (2) the rights of legal persons, for example with respect to business or trade secrets e.g. in the context of building applications, are at stake. Furthermore, restrictions are also needed, when (1) personal security of other citizens is involved e.g. in the context of witness protection programs or (2) state secrets and the personal security of people dealing with them are at stake. To achieve the required opacity typically data are anonymised, in many cases of printed documents by manually overwriting them.

In the literature (see references below) opacity of citizen also was discussed from a state perspective. In this context only a few applications were uncovered so far in which anonymity of authenticated citizens may play an important role. Examples are certain steps in e-voting and e-petitions.

But in addition the use of pseudonymised or anonymised data in governmental processes may have a value in certain steps by increasing quality with respect to fairness and objectivity or the implementing of data protection principles such as data minimisation.[103] In this context the use of pseudonymous credentials in e-government already was proposed in 2004.[104]

The use of governmental sectors and related identifiers for the citizens to enforce purpose binding clearly is state-of-the-art.[105] Differences can be observed in the way the borders of the sectors are enforced. Typical concepts are technical enforcement (e.g. in the Austrian citizen's card), organisational enforcement (e.g. in Switzerland by legislation on the use of ID numbers) or a combined approach (e.g. in Germany).

4.2.6 Transparency enhancement – the citizen's perspective

From a citizen's point of view a big advantage of democracy compared to other forms to organise a state is the possibility to be able to exercise influence on legislation. To be able to take an active role in democracies, the acting of the states needs to be transparent. This includes existing legislation and its implementation in governmental procedures and processes. With respect to procedures concerning themselves, citizens need the possibility to check whether they were carried out lawfully and fairly. Information needed in this context is: who processed which data how and when in the context of which administrative procedure? In some European member states Freedom of Information Acts provide a specific legal ground for this kind of transparency.

In traditional paper-based procedures steps of the processing and related data are documented in files. In electronic procedures applications and eIMS provide relevant information. In this context in addition to data stored in the application, log files are important for storing the information needed on data access and processing. In many cases the authentication of governmental officers in the context of applications is carried out based on an IMS. In these cases important information is to be found in the log files of the IMS.

---

[103] Riedl, R., *Anonymität im E-Government*, available at <http://www.ifi.unizh.ch/egov/E-Government-Anonymitaet.pdf>, 2004, last consulted 15 October 2008.
[104] See Auerbach, N., *Anonymous Digital Identity in e-Government*, 2004, available at <http://www.ifi.uzh.ch/archive/diss/Jahr_2004/thesis_auerbach.pdf>, last consulted 15 October 2008.
[105] Buitelaar, H. (ed.), *D13.3: Study on ID number policies*, *FIDIS deliverable*, 2007, available at <www.fidis.net>, last consulted 6 February 2008.

4.2.7 Opacity enhancement – the citizen's perspective

With respect to opacity the citizen's perspective in many cases seems to be individualistic. Brin analysed the reception of transparency and opacity enhancing tools by individuals. The following table summarises generally possible perspectives:

	Supporting tools	**Preventing tools**
Favorable from the personal perspective	Tools that help *ME* see what *OTHERS* are up to	Tools that prevent *OTHERS* from seeing what *I* am up to
Unfavorable from the personal perspective	Tools that help *OTHERS* see what *I* am up to	Tools that prevent *ME* from seeing what *OTHERS* are up to

Table 4.1: Categorization of tools concerning their effect on transparency[106]

Opacity is understood and required as a property to keep data in an understood and agreed communicational context (or as Nissenbaum[107] has described it: to keep data contextually integer). Contextual integrity of data is an important mechanism to protect the private sphere of individuals. But opacity also plays in important role as it may hinder feed back or punishment by society in case he or she has violated societal rules or laws. For that reason opacity of citizen is limited, e.g. in cases of criminal investigations.

In the context of governmental procedures roles and corresponding access rights in applications are an important instrument to implement opacity, i.e. to protect against unauthorised access. Again IMS play an important role, especially in those cases where authentication in applications is relying on them.

4.2.8 Conclusions

IMS may play an important role supporting the implementation of different opacity and transparency requirements both for public administrations and citizen. Many of these requirements can be fulfilled with basic functions of IMS such as:

- Providing the required reliability of authentication and identification
- Pseudonymous and/or anonymous authentication
- Audit logging based on a logging concept (which activity is to be logged how and stored for how long?), a revision proof logging infrastructure (referred to as syslogging infrastructure) and checks or evaluations on the content of audit logs.

The checks and evaluation procedures of audit logs may be supported by automated reporting tools. With respect to security related transparency requirements the Common Criteria (ISO/IEC 15408) provide relevant guidance.[108] Tools for implementing transparency and opacity in the context of IMS will be further elaborated in the FIDIS deliverable D16.3.

---

[106] Based on Brin, D., *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Addison-Wesley, Reading, 1998.
[107] Nissenbaum, H. F., *Privacy as Contextual Integrity*, 2004, available at <http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf>, last consulted 15 October 2008.
[108] See Meints, M. and Thomsen, S., 'Protokollierung in Sicherheitsstandards', *Datenschutz und Datensicherheit*, vol. 31, issue 10, 2007, pp. 749-751.

5 Summary and Conclusions

Part 1 of this document gives an overview which types of identity management are used in which way and to what purpose. Generally speaking, governmental IMS are used to identify and authenticate governmental officials and citizen in various governmental procedures. Typically governmental identity management is carried out in an organisation centric way, relying on centralised or distributed data repositories under the control of governmental administrations (type 1 identity management).

Reference is made to examples implemented in many European member states. This includes operational practice, especially

- Management of the life cycle of identities and ID documents
- Centralised and distributed identity management schemes
- IT-service or IT-operations management based on internationally established good-practice frameworks, namely IT Infrastructure Library (ITIL) and CobiT
- Information Security Management, in many cases referring to international standards such as the ISO 27000 series, CobiT or ISO/IEC 15408 Quality evaluation and management for identity management related processes
- Data protection management and related methods, especially the Privacy Impact Assessment (PIA)

In addition requirements for governmental IDM from the perspective of public administrations and citizens are listed. This covers

- Functional requirements such as the reliability between identity related information (attributers) and a physical person, data quality etc.
- Data protection requirements
- Security requirements and
- Requirements regarding transparency and opacity of governmental procedures relying on IMS from the perspective of governmental administrations and citizens

These requirements will be used in Deliverable 16.3 for the analysis of existing technologies in the context of governmental IMS.

Many of the requirements described seem to be concurring; this is most obvious with requirements regarding transparency and opacity. A balancing process does not only need to take these different targets into consideration, but also their different weighting by the parties involved – in this case governmental organisations and citizens. In the next chapter an overview on selected European governments with respect to their e-government and identity management strategy will be given. This also will give an insight how the results of this described balancing process may look like.

PART II – Country reports and EU policy

In this part a description is given of the situation with respect to the state of development of eGovernment in six European countries. These countries are the United Kingdom, The Netherlands, Germany, Austria, Switzerland and Belgium. They show interesting emphases in their development, often caused by their state structure. As a matter of course, special attention is given in these decriptions to their efforts to protect the privacy interests of their citizens. What can be learned from these developments for the possibilities of privacy friendly eGovernment? The initiatives the EU itself takes for its own organisation as well at a pan-European level is also scrutinised.

In the context of the i2010 program the European Commission carried out an EU e-government benchmark survey annually since 2000.[109] The survey investigated in 2007 whether 20 selected basic e-governmental services for citizen and enterprises are available and on which of five defined levels they are implemented. The services investigated were:

Citizens	**Businesses**
Income Taxes	Social Contribution for Employees
Job Search	Corporate Tax
Social Security Benefits	VAT
Personal Documents	Registration of a New Company
Car Registration	Submission of Data to the Statistical Office
Application for Building Permission	Custom Declaration
Declaration to the Police	Environment-related Permits
Public Libraries	Public Procurement
Birth and Marriage Certificates	
Enrolment in Higher Education	
Announcement of Moving	
Health-related Services	

Table II.1: 20 Public services evaluated in the EU eGovernment benchmark 2007

The five possible levels assigned to the implementation of e-government were in 2007:[110]

- Level 1: Information is given about the governmental service
- Level 2: Download form is available
- Level 3: Online dialog is possible
- Level 4: Complete transaction can be done online including the delivery of official documents

[109] See e.g. http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3634
[110] See http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf

- Level 5: Personalisation of the governmental services

It is hoped that the reference to the results of the benchmark will help in illustrating tendencies and make the content of the country reports more tangible for the reader. It should be noted that the benchmark is conducted every year and results sometimes change dramatically from year to year.

6 The EU perspective on eGovernment

6.1 The European understanding of eGovernment

Over the past decade, the European Union has increasingly promoted and supported the development of eGovernment. In its 2003 Communication, the Commission defines eGovernment as:

"*the use of information and communication technologies in public administration combined with organisational change and new skills in order to improve public services and democratic processes and strengthen support to public policies*."[111]

eGovernment is considered not only the way forward to realize better and more efficient administration, but also as a means for the public sector to maintain and strengthen "good governance"[112] in the information society. According to the same communication this requires:

- **An open and transparent public sector**, with governments that are understandable and accountable to the citizens, open to democratic involvement and scrutiny;
- A public service that is at the service of all, excluding no one from its services and respecting each person's individuality by providing **personalized services**;
- A productive public sector that delivers **maximum value for taxpayer's money** (cutting red tape, reducing errors and administrative burdens – both towards the citizen as well as civil servants).[113]

6.2 Implementation

The EU policy with regard to eGovernment emerged from a multitude of distinct initiatives and supporting programs, such as eTen, eEurope, IDABC, ePractice and ICT-PSP.[114] The most recent effort in consolidation took place in the "i2010 eGovernment Action Plan",[115] which sets forth not only the EU's priority objectives, but also outlines the "key enablers" to accelerate the implementation of its policy. Based on this text, the DG Information Society portal provides a diagram listing **5 priority objectives** in the area of eGovernment:

---

[111] European Commission Communication, 'The Role of eGovernment for Europe's future', SEC (2003) 1038, COM (2003) 567 final, adopted 26 July 2003, p. 7.
[112] See also European Commission Communication, 'European Governance – A White Paper', COM (2001) 428, adopted 25 July 2001.
[113] European Commission Communication, 'The Role of eGovernment for Europe's future', SEC (2003) 1038, COM (2003) 567 final, adopted in Brussels, 26 July 2003, p. 8.
[114] IDABC, *Harnessing ICT to improve public services*, Available at <http://ec.europa.eu/information_society/activities/egovernment/index_en.htm.>, last consulted at 30 August 2008.
[115] European Commission Communication, 'i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All', COM (2006) 173, adopted 25 March 2006.

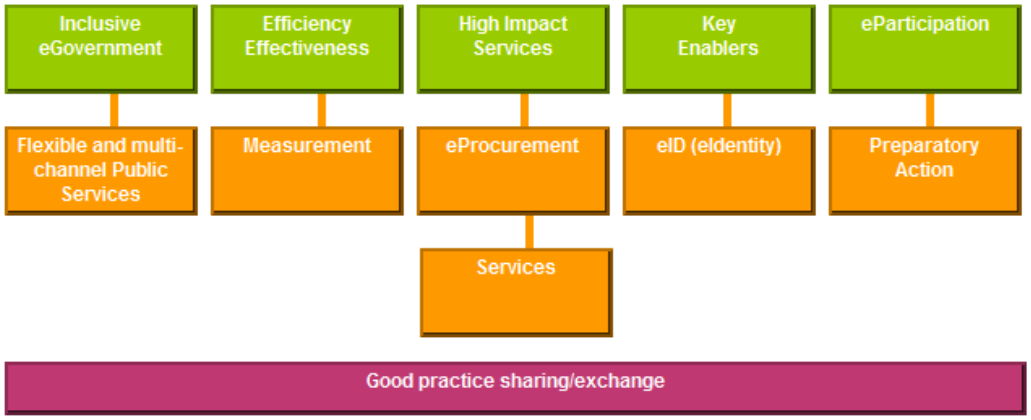

Figure 6.1: eGovernment Priority Objectives of the EU[116]

Since the EU's eGovernment policy is in fact scattered over a multitude of initiatives and programs, the entities charged with proper implementation of these initiatives are quite diverse as well.[117] It should also be noted that the approach for realizing these "priority objectives" varies significantly, ranging from stimulation to the adoption of regulatory instruments (mainly Directives and EC Decisions). In the following subsections, we shall elaborate further on those priorities and initiatives which either directly relate to eGovernment IdM, or clearly have implications thereon.

6.3 "High Impact Services": G2C and G2B.

Pursuant to the European initiatives, almost all Member States have established policies to stimulate the development of so-called "high impact services".[118] This notion refers to the fact that eGovernment has the potential to substantially change citizens' lives and the ways in which businesses interact with the Government.

Several high impact services can be pointed out, like for instance electronic tax declaration, enterprise registration, electronic invoicing, and the issuance of certificates and licences. High impact services can be detected both in services for citizens and businesses, and are present in all layers of eGovernment (information, interaction, and transaction). Moreover, high-impact services exist on a national and a European level.[119]

---

[116] IDABC, *Harnessing ICT to improve public services*, Available at <http://ec.europa.eu/information_society/activities/egovernment/index_en.htm.>, last consulted at 30 August 2008.

[117] European Commission Communication, 'The Role of eGovernment for Europe's future', SEC (2003) 1038, COM (2003) 567 final, adopted 26 July 2003, p. 7.

[118] European Commission, *eGovernment Progress in EU27+. Reaping the benefits*, available at <http://www.astic.es/eAdministracion/Documents/egovprogress7.pdf>, last consulted 30 August 2008.

[119] Impact services can for example be found on the IDABC website and in IDABC documents, e.g. in: IDABC, *Draft document as basis for EIF 2.0*, available at <http://ec.europa.eu/idabc/en/document/7728>, last consulted 30 August 2008.

6.3.1 Citizen services

In first instance, eGovernment can be used to provide citizens with greater access to information from public authorities. In 2000, the eEurope initiative identified four essential types of information to which Member States should ensure easy access:

- legal and administrative information;
- cultural information;
- environmental information; and
- real time traffic conditions and congestion data.[120]

By making information readily available, citizens could develop a better understanding as to where their taxes are spent and how decision-making is done. This in turn should lead to more transparent, accountable and open public institutions.[121]

A second priority lies in the advancement of direct communication between citizens and policy-makers. Through online forums, virtual discussion rooms and the like the Internet could be used to ensure consultation and feedback on major political initiatives. E-voting is also considered as a means for broad online consultation.[122]

A third type of high impact services, likely to bring the most change in the way citizens interact with the government, are the so-called transaction services. These services allow citizens for instance to apply for social benefits online (health, education, employment, etc.), file online tax declarations, or apply for permits, and thus demonstrate the highest degree of interactivity, with a clear desire to make these services "personalized". This personalized service delivery will increase the need for identification, authentication and authorisation of individuals and thus will create specific requirements in the field of IdM in eGovernment.

6.3.2 Business services

Towards businesses, the EU in first instance wishes to promote "single points of access" for administrative information and requirements.[123] Secondly, other information from the public sector should be made available online for re-use, in order to allow them to develop more attractive and competitive products.[124]

Similar to the high impact services for citizens, the EU also promotes transactional services for businesses, the most prominent example being eProcurement. The 2004 eProcurement Directives[125] put in place a framework for conducting public procurement electronically. Since then, Member States have committed themselves to giving all public administrations across Europe the capability of carrying out 100% of their procurement electronically (where

---

[120] European Commission Communication, 'An Information Society For All', 23 and 24 March 2000, p. 16.
[121] European Commission Communication, 'The Role of eGovernment for Europe's future', SEC (2003) 1038, COM (2003) 567 final, adopted in Brussels, 26 July 2003, p. 10.
[122] European Commission Communication, 'The Role of eGovernment for Europe's future', SEC (2003) 1038, COM (2003) 567 final, adopted in Brussels, 26 July 2003, p. 10.
[123] European Commission Communication, 'The Role of eGovernment for Europe's future', SEC (2003) 1038, COM (2003) 567 final, adopted in Brussels, 26 July 2003, p. 10.
[124] See also Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, O.J. L 345, 31 December 2003, p. 90 et seq.
[125] Directives 2004/18/EC and 2004/17/EC.

legally permissible) and to ensure that at least 50% of public procurement above the EU threshold is carried out electronically by 2010.[126]

In addition, the Services Directive can stimulate the use of electronic means for eGovernment services.[127] This Directive, which should be implemented by December 28, 2009 demands that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and **by electronic means**, through the relevant 'point of single contact'.[128]

6.3.3 Implementation at EU Level: The e-Commission

While the eEurope initiative called upon Member States to use the Internet to achieve better public service delivery, it also called upon the Commission for a similar commitment.[129] In 2001, the president of the EC issued a communication outlining the approach for implementing the "e-Commission".[130] The e-Commission services would also comprise three types: information services, interactive communication services and transaction services. The content of the information services were to be 'user-driven', 'coherent', 'thematic' and 'multimedia-based'.[131] As for communication services, three main sub-areas were envisioned: consultation and feedback mechanisms, e-mail contact points and interactive fora. For the transaction services, reference is primarily made to future practices of Member States, which would serve as "benchmarks" for implementing such services at Commission level.[132]

The Commission has since made significant progress in obtaining these objectives. An "Informatics Architecture" was defined (and recently updated) to render the hundreds of applications involved in Commission services coherent.[133] In the area of interactive policy making, the web portal "Your Voice in Europe" was introduced; which offers a 'single access point' to allow for interactive policy making.[134] The ePractice website is of course aimed at identifying and sharing best practices in Member States, among others in the field of eGovernment.[135]

As for transaction services, the Commission is working on an information system, common to the five DGs, which would ultimately allow proposals to be submitted electronically, the

[126] European Commission Communication, "i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All", COM (2006) 173, adopted 25 March 2006, p. 8.
[127] The Directive 2006/123/EC of the European Parliament and the Council of the European Union on services in the internal market.
[128] Art. 8 Directive 2006/123/EC.
[129] European Commission Communication, 'An Information Society For All', 23 and 24 March 2000, p. 16.
[130] European Commission Communication, 'Towards the e-Commission – Europa 2nd generation – Advanced Web Services to Citizens, business and other professional users', Brussels, 6 July 2001.
[131] European Commission Communication, 'Towards the e-Commission – Europa 2nd generation – Advanced Web Services to Citizens, business and other professional users', Brussels, 6 July 2001, p. 10.
[132] European Commission Communication, 'Towards the e-Commission – Europa 2nd generation – Advanced Web Services to Citizens, business and other professional users', Brussels, 6 July 2001, p. 13.
[133] See European Commission Communication, *The Commission Entreprise IT Architecture [CEAF] – version 1 explained*, available at <http://www.ec.europa.eu/dgs/informatics/ecomm/index_en.htm>, last consulted 30 August 2008.
[134] Visit http://ec.europa.eu/yourvoice
[135] Visit http://www.epractice.eu

evaluation of these proposals assisted by secure electronic means, and e-transactions throughout the lifetime of projects.[136]

6.4 "Key enablers": interoperability and electronic identity

For eGovernment services to come to full fruition, the development and implementation of such services needs to be facilitated by so-called 'key enablers'. Especially the interoperability of systems and electronic identities, and the use of Open Source Software (OSS) are considered key enablers for eGovernment.[137] The eGovernment Action Plan, which was already mentioned in paragraph 3.2 states:

"Further significant progress requires certain key enablers to be in place, particularly for high impact services to be effective. Among those, interoperable electronic identification management (eIDM) for access to public services, electronic document authentication and electronic archiving are considered critical key enablers."

The following paragraphs elaborate on key enablers, by describing pan-European eGovernment services (PEGS) and interoperability of electronic identity.

6.4.1 Development of pan-European eGovernment services (PEGS)

Offering more advanced services to citizens implies stronger co-operation and co-ordination among governmental bodies. Needless to say, the European vision for eGovernment did not merely envision advanced service delivery at the level of individual Member States. In 1999, the European Parliament and Council adopted two decisions with regards to trans-European networks for the electronic interchange of data between administrations (IDA).[138] As the decisions underlying the IDA framework expired in 2004, the follow-up IDABC programme was adopted by way of decision 2004/387/EC.[139] The latter decision embraces the notion of so-called 'pan-European' eGovernment services, which are defined as:

"*cross-border public sector information and interactive services, either sectoral or horizontal, i.e. of cross-sectoral nature, provided by European public administrations to European public administrations, businesses, including their associations, and citizens, including their associations, by means of interoperable trans-European telematic networks*" (Art 3(b)).

Pan-European eGovernment services permit citizens, businesses and public administrations to interact more efficiently with public administrations across borders. The delivery of such services requires interoperable information and communication systems between European

[136] European Commission Directorate-General for Informatics Communication, e-*Commission 2006-2010: enabling efficiency and transparency*, available at <http://www.ec.europa.eu/dgs/informatics/ecomm/index_en.htm>, last consulted 30 August 2008, p. 5.
[137] *Key enablers. The eGovernment Glue*, available at <http://ec.europa.eu/information_society/activities/egovernment/policy/key_enablers/index_en.htm>, last consulted 30 August 2008.
[138] Decisions 1719/1999/EC and 1720/1999/EC.
[139] Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public adminsitrations, businesses and citizens (IDABC), O.J. L 181 (corrig.), p. 25-35, art. 3 (b).

public administrations, as well as interoperable administrative front and back office processes.[140] The main objectives of the IDABC programme are therefore defined as:

- enabling efficient, effective and secure interchange of information between public administrations at all appropriate levels, as well as between public administrations and Community institutions or other entities where appropriate;
- facilitating the delivery of services to businesses and citizens, taking into account their needs;
- supporting the Community decision-making process and facilitating communication between Community institutions by developing a strategic framework at the pan-European level;
- achieving interoperability, both within and across different policy areas and, where appropriate, with businesses and citizens, notably on the basis of a European Interoperability Framework (EIF);
- contributing to the efforts of Member State public administrations and the Community in terms of streamlined operations, prompter implementation, security, efficiency, transparency, service culture and responsiveness;
- promoting the spread of good practice and encouraging the development of innovative telematic solutions in public administrations.[141]

Pan-European eGovernment services are to be developed in the context of specific projects of common interest and specific horizontal measures.[142] These projects and measures are defined in Annex I and II of the IDABC decision respectively. The "projects of common interest" correspond with EU policy domains such as competition, agriculture, education, culture, public health, tourism, environment, etc. The so-called "horizontal measures" however take on a broader dimension. They are intended to establish or enhance the underlying 'infrastructure services' which will enable the desired level of interoperability across specific sectors or policy domains. Some of the infrastructure services enumerated in annex II of the IDABC decision include: a secure and reliable communication platform for the interchange of data between public administrations, a system for the management of dataflows inter-linked with different workflows, model requirements for the management of electronic records in public administrations, and a metadata framework for public sector information in pan-European applications. Moreover, one of the infrastructure services mentioned in this Annex II concerns "identification, authorisation, authentication and non-repudiation services for projects of common interest". Furthermore, horizontal measures also include strategic and other support activities.

It bears noting that the services developed under the IDA/IDABC programmes also appear to have a purpose beyond service delivery: according to recital (28) such services should also be usable "in the framework of the common foreign and security policy and police and judicial cooperation in criminal matters, in accordance with Titles V and VI of the Treaty European Union".

[140] Decision 2004/387/EC, recital 14.
[141] Decision 2004/387/EC, art. 2, paragraph 2.
[142] Decision 2004/387/EC, recital 26.

The IDABC's European Interoperability Framework, which supports the European Union's strategy of providing pan-European, user-centred eGovernment services, facilitates the interoperability of services and systems between public administrations, and between administrations and the public (citizens, businesses).[143] The Framework, which comprises a set of standards, principles, and recommendations, is currently, being evaluated. A draft document for a new Framework has been provided on July 15, 2008. The revised Framework will be part of a more structured approach to interoperability and will operate jointly with the European Interoperability Strategy (EIS), the European Interoperability Architecture Guidelines (EIAG), and the European Interoperability (EIIS) Infrastructure Services[144]. Reasons for updating the EIF are, amongst others, the progress made by Member States in the field of electronic Identity Management.[145] According to the draft of the second version of the European Interoperability Framework, eID will be "one of the first and most important cases in which EU-wide interoperability is used and demonstrated on a practical basis".[146]

6.4.2 Electronic Identity Management and Interoperability: the EU perspective

Interoperability can be composed out of three dimensions: social and political (informal), formal, and technical.[147] In combination with data sharing, interoperability can be considered a critical feature for international electronic networks and electronic delivery of government services.[148]

To achieve 'true' and improved interoperability, government officials should consider interoperability in its broad view,[149] because eGovernment initiatives are in fact also of a political nature. Hence, ensuring trust and security and special attention to the use of identification and authentication are of importance as well. Interoperability therefore includes being able to identify the actors and organisational processes involved in the delivery of specific (pan-European) eGovernment services to individuals.

For digital interaction to develop, identity is a vital concept as this makes it possible to offer services, adjusted to specific individuals or businesses. However, identity in a digital context lacks traditional trust tokens and cannot rely on face-to-face contact. This makes security, reliability, trust, and privacy protection factors that influence the design of IdM systems. Subsequently, these factors also have an effect on IdM interoperability.[150] Until recently,

---

[143] IDABC, *European interoperability framework for pan_european egovernment services*. *Version 1.0*, available at < http://ec.europa.eu/idabc/servlets/Doc?id=19529>, last consulted 30 August 2008.
[144] IDABC, Draft document as basis for eif 2.0, available at < http://ec.europa.eu/idabc/servlets/Doc?id=31508>, last consulted 30 August 2008, p. 3.
[145] IDABC, Draft document as basis for eif 2.0, available at < http://ec.europa.eu/idabc/servlets/Doc?id=31508>, last consulted 30 August 2008, p. 69.
[146] IDABC, Draft document as basis for eif 2.0, available at < http://ec.europa.eu/idabc/servlets/Doc?id=31508>, last consulted 30 August 2008, p. 76.
[147]Backhouse, J. (ed.), *D4.1: Structured account of approaches on interoperability, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 30 August 2008, p. 40.
[148] Moen, W.E., 'Information technology standards: A component of federal information policy', *Government Information Quarterly*, vol. 11, issue 4, 1994, pp. 357-371, Backhouse, J. (ed.), *D4.1: Structured account of approaches on interoperability, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 30 August 2008, p. 19.
[149] Backhouse, J. (ed.), *D4.1: Structured account of approaches on interoperability, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 30 August 2008, p. 21.
[150] Cf. IDABC, *Analysis and Assessment of similarities and differences – Impact on eID interoperability*, available at <http://ec.europa.eu/idabc/en/document/6484/5644>, last consulted 30 August 2008, p. 89.

however, they have especially been handled on the level of the EU Member States which has resulted in different IdM design choices, like the use of one single identifier for all public services vs. systems in which every sector uses its own identifier.[151] Furthermore, the different national eID management systems may vary in their storage of identifiers and credentials (e.g. storage on smart cards vs. central databases), and can differ with regard to the authentication methods (e.g. systems that rely on passwords/usernames versus fingerprint-based systems).[152]

Variation of eIDM systems in Europe is considered to be a barrier for the take-up of ICTs in eGovernment and the competitive position of Europe, as they cannot effectively reduce administrative burdens.[153] Moreover, the European Union fosters the principles of the free movement of goods, persons, services, and capital. ICTs and eID management should facilitate the materialisation of such an internal market, but the current differences between eID systems of Member States rather seem to raise new barriers.[154]

EIDs which are portable, interoperable, and meet common standards, have the potential to support mobility and a flexible labour market.[155] Since the 2005 Manchester Declaration,[156] the implementation of electronic identity is recognised as one of the key enablers in eGovernment.[157] This is, subsequently, elaborated further in the i2010 eGovernment Action Plan:[158] *"By 2010 European citizens and businesses will be able to benefit from secure and convenient electronic means, issued at local, regional and national levels, and complying with data protection regulations, to identify themselves to public services in their own* ***or in any other*** *Member State…(emp. added)".*

The i2010 eGovernment Action Plan acknowledges that EU countries already implement eIDM systems and therefore aims to respect different national approaches whilst stipulating, however, that this should not create a barrier to the use of public services across borders. The Action Plan mentions the need for regulatory measures for the development of electronic identification and authentication for public services, and also notes that the Commission will pay attention to eIDM interoperability and mutual recognition (for example, in the follow up to the e-Signatures Directive). The Action Plan provides some necessary steps for achieving eIDM interoperability, comprising: a roadmap for a European eIDM framework, common eIDM specifications, large scale pilots, a review of the eSignatures directive, and a review of the uptake of the eIDM framework.

---

[151] Hayat, A., *A pan european interoperable electronic identity management system*, available at < http://www.iaik.tugraz.at/RESEARCH/publications/theses/Hayat.pdf>, last consulted 30 August 2008.
[152] An extensive description can be found in: Hayat, A., *A pan european interoperable electronic identity management system*, available at < http://www.iaik.tugraz.at/RESEARCH/publications/theses/Hayat.pdf>, last consulted 30 August 2008.
[153] European Commission Communication. 'Working together for growth and jobs. A new start for the lisbon strategy', COM (2005) 24.
[154] Which is, amongst others, indicated by Art 8. 2006/123/EC.
[155] Ministerial eGovernment Conference. (2005). *Ministerial declaration*. Manchester, UK; 4th Ministerial eGovernment Conference. (2007). *Ministerial declaration*. Lisbon, Portugal.
[156] Ministerial eGovernment Conference. (2005). *Ministerial declaration*. Manchester, UK.
[157] European Commission, *eGovernment Progress in EU27+. Reaping the benefits*, available at <http://www.astic.es/eAdministracion/Documents/egovprogress7.pdf>, last consulted 30 August 2008.
[158] European Commission Communication, 'i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All', COM (2006) 173, adopted 25 March 2006.

The Signpost Paper[159] and the eIDM Roadmap[160] elaborate on the targets for eGovernment electronic identification and authentication in Europe. Key ideas in these documents are the distinction between identity cards and electronic identification, respect for a high level of data protection, and importance of personal control and/or stewardship over personal data. Moreover, according to these documents a **federated and multilevel** model must be used for pan-European eIDM systems and, without an explicit mandate for the EC in the field of identification issues, a **'framework'-approach** must be considered, based on policies and mutual recognition of national electronic identities. Hence, an EU-level eID infrastructure is not considered necessary. In addition, a pan-European eIDM system needs to rely on **authentic sources**, should embrace a **context/sector based approach**, and needs to enable **private sector uptake.**[161]

The European eID framework needs to serve as a quality mark, which can guide users regarding conformance to the framework and the level of authentication provided. It can take away the burden of using specific cards and methods of authentication per transaction type. In addition, the eIDM Roadmap pays attention to the policy objective of 'leaving no citizens behind',[162] by addressing the possibilities of intermediaries management and delegation.

The eIDM Roadmap notes that the principle of subsidiarity needs to be taken into account. It does not aim at imposing any technical, organisational or legal infrastructural choices on Member States. However, it does mention six minimal requirements (e.g. usability, privacy, security), which need to ensure that the user is at the centre of developments in the field of pan-European eID. Moreover, it states that consistency of identifiers is important and that Member States must issue the means for electronic authentication and identification as well as competence and mandate management.

In practice, several European projects contribute to the implementation of the targets described in the eIDM Roadmap. Examples are the Modinis-IDM study, which contributes to the filling-in of several actions stated in the Roadmap.[163] In addition, the project 'eID Interoperability for PEGS' aims to solve technical issues about the pan-European identity management interoperability challenge. The eTEN European Community programme and IDABC/ICT-PSP studies provide input for the filling-in of the eIDM roadmap. Furthermore, a broad range of EU-funded projects related to electronic Identity Management can provide input for the Roadmap. Examples of such projects are FIDIS, PRIME, GUIDE, eESC, the Porvoo-group, and eEpoch. Next to these projects, there exists an eGovernment sub-group which reports the i2010 High Level Group on the implementation of the i2010 eGovernment Action Plan. Finally, on May 30 2008, a large scale project (LSP) was launched in which the

---

[159] eGovernment Unit, *Signposts towards egovernment 2010*, available at <http://ec.europa.eu/information_society/activities/ict_psp/documents/signposts2005.pdf>, last consulted 30 August 2008.
[160] eGovernment Unit, *A roadmap for a pan-european eIDM framework by 2010*, version 1.0, available at <http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf>, last consulted 30 August 2008.
[161] eGovernment Unit, *A roadmap for a pan-european eIDM framework by 2010*, version 1.0, available at <http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf>, last consulted 30 August 2008.
[162] Cf. paragraph 3.2 on implementation.
[163] Modinis IDM, *About Modinis IDM*, available at <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi>, last consulted 30 August 2008.

European Commission, 13 EU Member States, and Iceland will work together to enable different national electronic identity schemes to be recognised across national borders.[164]

[164] This large scale project is called 'Secure idenTity acrOss boRders linKed'(STORK). For more information see http://www.eid-stork.eu/.

7 Switzerland

7.1 General Framework / General Set-up

To understand the settings of the Swiss eGovernment strategy one must understand the Swiss political structure to some degree. The Swiss political system is decomposed into three levels which are: federal level, cantonal level, and communal level. Many important subjects are regulated on the cantonal level, and not on the federal one. Among others these are: taxes (taxes are regulated on the federal level, too), public education, health care, and more. This has had a strong impact on the formulation and the start of eGovernment initiatives.

Swiss federal administration started formulating an eGovernment initiative in the year 2002. In Eidgenössisches Finanzdepartement EFD (2002), the so-called *Die eGovernment-Strategie des Bundes* is described. First strategic goals have been defined, and the first actions have been planned. The document defines the general settings for an eGovernment framework for the first time for the Swiss federal level. In particular, it sets up the framework for cooperation between the three political levels in Switzerland, the roles of the different federal departments and offices. The document and its resulting actions laid the basis for the formation of organisations like e-geo.ch,[165] eCH,[166] and other non-profit organisations.

The period from 2002 to 2006 can be regarded as the period of orientation. A few concrete initiatives have been undertaken. Some are still on-going, and some have even been cancelled (e.g., Swisskey, an organisation for the provisioning of X.509 certificates under private law). Other important issues have either not yet been addressed, or have been postponed, such as the provision of a unique personal identifier for citizens.[167, 168] In summary, not much progress has been made during that period. The net result is the very bad ranking in comparison with other EU countries.[169] The findings of the benchmark reported for Switzerland are:

- Full online availability: Only 21% (EU27+: 58%) of the monitored public services are fully online available.
- Online sophistication: The Online sophistication of public services scores 60% (EU27+: 76%).
- Pro-active means: None of the Swiss public services reaches a 100% “stage 5” level.
- User centricity: Switzerland scores only 2% (EU27+: 19%) with respect to the user centricity criterion.
- National portal: Out of the 20 public services identified as crucial, Switzerland has a score of 75% (EU27+: also 75%).

Otherwise, Switzerland is one of the top countries in using ICT.

---

[165] See www.e-geo.ch
[166] See www.ech.ch
[167] In 2007, a unique person identifier for jobholders only has been introduced. See: http://www.avs-ai.ch/Home-D/allgemeines/nnahv/neueahvnummer.pdf
[168] In 2009, the so-called “Versichertenkarte” (a chip card with a unique identifier representing its holder) shall be introduced. See: http://www.bag.admin.ch/themen/krankenversicherung/04108/04109/index.html
[169] Online Availability of Public Services: http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf

In Eidgenössisches Finanzdepartement EFD (2007), Swiss federal public administration defined a new, common strategy involving also the cantonal political level, economy, and interested organisations. A new, much wider accepted approach has been defined whose corner stones are explained in the remaining part of this section.

7.2 Goals

For Switzerland having a modern service-oriented and information-oriented economy, it is of upmost importance to have an efficient, secure, and highly-reliable ICT-based communication capability with the public administration. It is expected that the provision of eGovernment solutions provides more value for the economy and the citizens compared to the "classical" public administration. The provision of eGovernment solutions enables an efficient, innovative, and demand-oriented economy- and living-space.

Within the Swiss eGovernment strategy, the following goals are defined, in the order of their significance:

- This first goal addresses business to government transactions (B2G). In Informatikstrategieorgan Bund ISB (2006), the goal is stated as follows:

  "The Swiss economy shall be able to perform ICT-based transactions with the public administration on the federal, on the cantonal, and possibly, on the communal level. The Swiss economy has a high demand for ICT-based services of the public administration. If available, the Swiss economy expects a substantial reduction of its non-value adding workload. The expected raise of the efficiency of Swiss enterprises is of utmost importance for the Swiss economy space." (Translated by the contributor.)

- The second goal addresses the transactions between public administrations on any of the three political levels (federal, cantonal, communal) (G2G). In Informatikstrategieorgan Bund ISB (2006), the goal is stated as follows:

  "Swiss public administrations shall be able to perform their services in an ICT-based manner, incorporating as many departments as necessary on any political level (federal, cantonal, and communal). The efficiency of the administrations' services shall be improved, and the services shall be more flexible." (Translated by the contributor.)

- The third goal addresses the transactions between the citizens and the public administration (C2G). In Informatikstrategieorgan Bund ISB (2006), the goal is stated as follows:

  "Swiss citizens shall profit from the improved services of the public administrations where they can expect the highest benefit, for example, where the traditional provision of a service involves many and intensive citizen / administration contacts. The provision of much simpler, flexible, and secure access to administrations' public services plays a central role." (Translated by the contributor.)

According to the plans expressed in Eidgenössisches Finanzdepartement EFD (2007) the goals shall be measured and evaluated in the year 2011.

7.3 The Maxims

As stated in Eidgenössisches Finanzdepartement EFD (2007), the Swiss maxims are based on seven principles:

- Orienting on efficiency and business processes

  Instead of the provision of less coordinated, expensive, and isolated eGovernment solutions, common solutions shall be sought that include all political levels. In addition, these solutions shall optimize the common understanding of services and processes.

- Focus and priority

  The eGovernment implementations shall be geared towards a few selected main themes which are of utmost interest for the demands of the economy and the citizens. EGovernment implementations shall not be driven by technology.

- Transparency and commitment

  Responsibility and decision processes shall be clearly defined. Transparently managed and periodically updated planning instruments shall enable the tracking of the activities.

- Innovation thanks to federalism

  The potential of innovative administrations shall be exploited. At the same time, a common approach and well-defined organisational structure shall guarantee the superior control.

- Cost reduction due to reusability and open standards

  Investments shall be optimised thanks to the principle “develop once – reuse many times”, open standards, and mutual exchange.

- Barrier-free access

  The compliance of approved standards shall guarantee the barrier-free access for e-government solutions to everyone, especially for elder people and handicapped.

- Instruments for decision makers

  Concrete measures for the realisation for, and control of eGovernment solutions shall enable the political decision makers to fulfil their responsibilities.

7.4 The Strategic Plans

The Swiss eGovernment strategy shall be realised through concrete projects. Some of these projects are already initialised, and some must still be negotiated. The most important measure, therefore, is the catalogue of prioritised projects. The catalogue shall periodically be updated.

As stated in Eidgenössisches Finanzdepartement EFD (2007), the items of the catalogue can be grouped as follows:

- *Priority of services*. From the set of public services, a subset of services shall be selected which have received a high priority. The priority shall be determined by the

cost/benefit ratio as perceived by the target audiences, given that theses services will be ICT-based;

- *Provision of prerequisites*. Legal, procedural, organisational, and/or technical prerequisites must be satisfied for the provision of prioritized public, ICT-based services. Processes must be optimised, and the infrastructure must be provided in a central or common manner.

The services listed in the catalogue are grouped. One group of services lists one of the following two options:

- The service does imperatively require a coordination between the different political levels and organisations in Switzerland; or
- The service can be realised decentralised, perhaps accompanied by the mutual exchange of experiences.

The other group of services lists the preconditions that must be met, and whether or not a Swiss-wide acclamation vote must be carried out.

7.5 Procedures and Steps

The transparency and progress for eGovernment persons in charge on all federal levels shall be achieved thanks to the provision of planning and controlling measures. In particular, the indication of deadlines and milestones are considered of upmost importance. Putting together the key data allows the evaluation of the progress in terms of the planned goals and deadlines, and allows positioning Switzerland within the international eGovernment context.

An evaluation shall be carried out after four years, that is, during the year 2011.

7.6 Organisation and Finance

The organisation of the roles between federal and cantonal instances and the funding for the eGovernment activities is defined in the Framework Agreement (2007) between the federation and the cantons.

The Framework Agreement (2007) defines the duration of the cooperation, the way how the federation and the cantons have to cooperate, the reusability of results by expressing the right to use, the obligation to use international and national standards,[170] the application of the recommendations of the "Schweizerische Informatikkonferenz" (SIK),[171] the privacy protection and security, and the evaluation of the provision of the jurisdiction.

The Framework Agreement (2007) defines the establishment of a controlling board ("Steuerungsausschuss").[172] The duties and competences of the controlling board are, among others:

- The definition and updating of the prioritised catalogue.

[170] See www.ech.ch
[171] See www.sik.ch
[172] The current constitution of the controlling board can be found at: http://www.isb.admin.ch/themen/egovernment/00068/00764/.

- The definition of the leadership organisation for the realisation of prioritised projects.
- The controlling of the prosecution of the strategy and of the ongoing projects.
- The reporting of the ongoing activities to the Swiss Federal Council.

The Framework Agreement (2007) defines a council of experts ("Expertenrat")[173] consisting of nine persons. The duties and competences of the council of experts are:

- The validation of the technical aspects of the ongoing projects and reports its findings to the controlling board.
- The provision of an advisory service for the controlling board.

The Framework Agreement (2007) defines also the establishment of an office for eGovernment.

The sponsoring of projects and their funding is defined on a pre-project basis, and must be negotiated individually. The organisation in charge may define special agreements if required.

7.7 Catalogue of Prioritised Projects

In Steuerungsausschuss E-Gov Schweiz (2007) a catalogue of prioritised tasks is given. It must be noted that the tables below lists federal initiatives only. Cantonal initiatives, if they exist, are not listed in this survey.

Notice that activities in the context of eHealth are outside the scope of the Steuerungsausschuss E-Gov Schweiz. eHealth activities in Switzerland are summarized in the next section.

Title / Name	**Organisation in charge**
Corporate foundation and mutation notification	Staatssekretariat für Wirtschaft (www.seco.admin.ch)
Wage date communication from companies to government and assurances	Swissdec (www.swissdec.ch)
Transactions among Swiss compensation offices	eAHV (www.eahv-iv.ch)
Custom clearance	Eidgenössische Zollverwaltung (www.ezv.admin.ch)
Public call for bids	Undefined
Building permits	Undefined
Ordering and delivery of certified register digests	Bundesamt für Justiz (www.bj.admin.ch)
Notification of change of address	Schweizerischer Verband der Einwohnerkontrolle (www.einwohnerkontrolle.ch)

[173] The current constitution of the controlling board can be found at: http://www.isb.admin.ch/themen/egovernment/00068/00764/.

E-voting	Schweizerische Bundeskanzlei (www.bk.admin.ch)
Access to geographical base data	e-geo.ch (www.e-geo.ch)
Filing of data for statistic offices	Undefined

Table 7.1: Summary of tasks that imperatively require the coordination of different political levels and organisations

Title / Name	**Organisation in charge**
Filing of VAT clearance	Eidgenössische Steuerverwaltung (www.estv.admin.ch)
Tax declarations	Schweizerische Steuerkonferenz (www.steuerkonferenz.ch)
Treatment of filing extension for tax declarations	Schweizerische Steuerkonferenz (www.steuerkonferenz.ch)
Registrations/deregistration of vehicles	Vereinigung der Strassenverkehrsämter (www.asa.ch)
Application and payment of parking permissions	Undefined
Lost and found service	Undefined
Access to legal data	Undefined

Table 7.2: Summary of tasks that require no coordination among different political levels and/or organisations

Title / Name	**Organisation in charge**
Established project organization for eGovernment	Office for eGovernment (www.isb.admin.ch/themen/egovernment)
Provision of a legal basis	Undefined
Inventory of public services	Schweizerische Bundeskanzlei (www.bk.admin.ch)
Unique personal identifier (UPI)	Undefined
Organization unique identifier (OUI)	Bundesamt für Statistik (www.statistik.admin.ch)
EGovernment architecture	Informatikstrategieorgan Bund (www.isb.admin.ch)
Standardisation of personal data	eCH (www.ech.ch)
Standardisation of organisation and salary data	Swissdec (www.swissdec.ch)
Harmonisation of registers	Bundesamt für Statistik (www.statistik.admin.ch)

National infrastructure for geographical data	e-geo.ch (www.e-geo.ch)
Swiss standard for the exchange of files and records	eCH (www.ech.ch)

Table 7.3: Summary of the provision of a general framework and standards.

Title / Name	**Organisation in charge**
Access to public services (portals)	Schweizerische Bundeskanzlei (www.bk.admin.ch)
Directory service for Swiss authorities	Schweizerische Bundeskanzlei (www.bk.admin.ch)
Service for e-forms	Schweizerische Bundeskanzlei (www.bk.admin.ch)
Service for the exchange of e-data	Undefined[174]
Service for the authentication and authorisation	Undefined
Service for certificates	Undefined
E-billing and e-payment	Undefined
Service for the long-term data storage	Undefined
Service for e-receipts	Bundesamt für Justiz (www.bj.admin.ch)
Integrated network support for all administration levels	Undefined

Table 7.4: Summary of the provision of prerequisites and services.

7.8 eHealth Strategy

On June 27 2007 the Federal Council has adopted the national strategy "eHealth" Switzerland submitted by the Federal Office of Public Health. The objective of the strategy is to deliver by 2015, with the means of the new technologies, better and efficient health services in Switzerland.

7.8.1 Goals

The goals of the Swiss eHealth strategy are the provision of

- affordable,
- efficient,
- safe, and
- high-quality

[174] An event bus has already been deployed in Switzerland.

health services. To achieve these goals, the confederation and cantons expressed their will to jointly achieve these goals in signing a Framework Agreement for eHealth (2007).

7.8.2 The Strategy

The Swiss eHealth strategy is defined in Strategie eHealth "Schweiz" (2007). The strategy can be summarized as follows:

- It first defines a set of areas of activities.
- These areas of activities are:
  - Electronic patient record
  - On-line services
  - Additional activities for realisation of the above two areas of activities.

A set of sub goals have been defined. The sub goals for the electronic patient record are:

- The definition of relevant Swiss standards (2008)
- The introduction of the health insurance card (2009)
- The introduction of prototype services on the cantonal level (since 2009)
- Reliable authentication and digital signature of service providers (2010)
- Reliable authentication for all service users, with an option for digital signatures (2012)
- Secure exchange of medical data between service providers and service users (2012)
- Free access of service users to their medical data (2015)

The sub goals for the on-line services are:

- The approval of quality standards (2009)
- The establishment of a eHealth portal with limited set of services (2010)
- The establishment of the secure, reliable access of citizens to their patient records (2015)

The sub goals for the additional activities are:

- Framework agreement between the confederation and the cantons, establishment of a coordination board (2007)
- Identification of the roles of the actors and their processes (2007)
- Clarification of the legislative needs (2008)
- Definition of a process of the national eHealth architecture (2008)
- Conditions for the public-private partnerships (2008)
- Prototype trials (2008)
- Transfer of research results of foreign countries (2008)
- Definition of new educational programs (2009)

- Definition of new educational programs (2013)

7.8.3 Assignment of Projects, Data Security and Privacy

To achieve the above goals, a set of projects have been defined. These are listed in Aufträge eHealth (2008). In these projects, aspects such as data security, protection of the privacy, and more, have to be investigated. Details remain to be seen.

7.9 Identity Management

In Switzerland, one kind of identity management is approached by the accreditation of several independent Swiss bodies which are entitled to issue and manage qualified certificates.

On the other hand, a new social security number, the so-called AHVN13 number shall be introduced during 2009. This replaces the existing AHV number whose range would otherwise be exhausted in the near future (see also section 7.10.2 later on).

7.9.1 Identities in Terms of Certificates

There is a register of Swiss bodies having been certified to issue qualified certificates. To quote:[175]

This register lists the Swiss bodies which are entitled to issue and administer qualified electronic certificates in accordance with the "Bundesgesetz vom 19. Dezember 2003 über die elektronische Signatur (ZertES, SR 943.03)," in accordance with the "Verordnung vom 3. Dezember 2004 über die elektronische Signatur (VZertES, SR 943.032)" and the "Technische und administrative Vorschriften des BAKOM vom 6. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1)". The standards ETSI TS 101.456 (Europe) and ANSI X9.79 (USA, Canada) may also serve as a basis for the certification of a Public Key Infrastructure (PKI) respectively a Certification Service Provider (CSP).

At the time of writing there are four Swiss bodies entitled to issue and manage electronic certificates (see table 6.5).

	Name	**Address**	**URL**
1	Swisscom AG	Alte Tiefenaustrasse 6 3050 Bern SWITZERLAND	http://www.swisscom.com/solutions/ http://www.swissdigicert.ch/
2	QuoVadis Trustlink Schweiz AG	Teufenerstrasse 11 9000 St. Gallen SWITZERLAND	http://www.quovadis.ch/
3	SwissSign AG	Beethovenstrasse 49 8002 Zürich SWITZERLAND	http://www.swisssign.com/
4	Bundesamt für Informatik und	Monbijoustrasse 74 3003 Bern	http://www.pki.admin.ch/

[175] See Hägler, S., *Public Key Infrastructure (PKI)*, available at <http://www.seco.admin.ch/sas/00229/00251/index.html>, last consulted 9 May 2008.

	Telekommunikation BIT	SWITZERLAND	

Table 7.5: Summary of Swiss bodies entitled to issue and manage electronic certificates

The legal basis for the issuing, management, and revoking of certificates is laid down in the act ZertES (2003), the ordinance VZertES (2004), and the prescription "Technische und administrative Vorschriften des BAKOM vom 6. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1)".

7.9.2 Citizen / Governmental Transactions

Currently, the contributor does not know of any C2G transaction based on certificates.

7.9.3 Business / Governmental Transactions

Certificate-based transactions take place in the area of cargo processing. The declaration of the import and export of goods and services is signed electronically and sent to the custom.[176]

7.10 National Registers, Universal Person Identifiers, Legal Basis

In parallel to the activities related to certificates and digital signatures, a universal person identifier has been defined.

7.10.1 Status

There are many registers for various kinds of data such as registers for persons, registers for the civil status of persons, commercial registers, criminal records, tax registers, and registers for buildings, to name a few. And many of these registers are maintained simultaneously on different political levels, that is, communities, cantons, and the confederation. Typical examples are the registers for persons.

One of the main drivers for the introduction of a Universal Person Identifier (UPI) in Switzerland is the intention to harmonize the person registers. As person registers are maintained at several places on different levels, they are fully decentralized.[177]

Political forces in Switzerland lead to the insight to restrict the UPI to persons only. That means that the UPI shall not be used in other registers such as the criminal records, or the tax registers.

The goals of the harmonization of the person registers are:

- simplifying the gathering of statistical data
- smooth exchange of register data
- the possibility of relating data within different registries
- forming a basis for the proliferation of true eGovernment application (e.g., an on-line portal)

[176] For more information, see http://www.ezv.admin.ch/themen/00476/00494/index.html
[177] The first effective need for a harmonization of the person registers is the census of population to be performed in 2010.

7.10.2 Result

The harmonization of the person registers affords the following achievements:

- A replacement of the existing AHV number whose range would otherwise be exhausted in the near future
- The definition of a Universal Person Identifier, the so-called AHVN13 number[178]
- The AHVN13 number will also be used for the "Krankenversicherungskarte" (health insurance card)
- Certain standardized information is kept in every person register
- The provision of the highly-secured data exchange platform Sedex (secure data exchange)[179]

The AHVN13 number has the following properties:

- it has the format 756.2335.6981.52
    - the first three digits is the country code, 756 for Switzerland
    - the next nine digits (2335.6981.5) denote the unique identifier of a person being registered in Switzerland; not particular meaning is encoded
    - the last digit (2) is the error checking number
- there is no particular meaning encoded
- it is never reused
- once assigned to a person, that person's number never changes

7.10.3 Legal Basis

The legal basis for the harmonization of the person registers is the act RHG (2006) and the ordinance RHV (2007).

The act defines the types of registers the law applies to, and the minimal content of the information about a person of an entry in the registers. It defines also some rules for the use of the data: its preparation for statistical purposes, its use for statistical purposes, and the publication of statistics based on the data. The act states that Swiss federal government must define which data can be used for what purposes. The act defines also rules to protect data from third parties. No details are given, however.

The ordinance RHV (2007) states more precisely the use of data, and the protection of data. For example, the details of data protection on transmission are defined, and how the protection must occur. It states the duties for federal, cantonal, and communal offices.

The ordinance RHV (2007) does not rule the details of the privacy of persons. However, it refers to the "Datenschutzgesetz" DSG (1992) whenever appropriate.

[178] AHV stands for the Swiss social security insurance.
[179] See http://www.bfs.admin.ch/bfs/portal/de/index/news/00/00/sedex.html. Sedex is based on OSCI, see http://www1.osci.de/.

7.11 Privacy Policy Statements in the Framework Agreement

To quote the Framework Agreement (2007):

"The Framework Agreement (2007) defines the duration of the cooperation, the way the federation and the cantons have to cooperate, the reusability of results by expressing the right to use, the obligation to use international and national (www.ech.ch) standards, the application of the recommendations of the "Schweizerische Informatikkonferenz" (SIK, www.sik.ch), the privacy protection and security, and the evaluation of the provision of the jurisdiction."

The Framework Agreement (2007) does not itself state the privacy protection. In that sense, the corresponding statement in the above quote is misleading. With respect to privacy, the Framework Agreement (2007) refers to the "Datenschutzgesetz" DSG (1992).

7.12 Data Security and Privacy

The act "Datenschutzgesetz" DSG (1992) regulates the collecting, protecting, processing, and disseminating of personal data of natural and legal persons. The act explicitly declares that personal data is only allowed to be processed by legitimate entities. Entities processing personal data have the responsibility, by law, to ensure the correctness of that data.

The act also regulates the security of personal data. It says that "sensitive" personal data must be protected from preventing unauthorized processing and manipulation. The act defines exhaustively the kind of "sensitive" data.

The right of access to personal data is regulated, too. Citizens have the right to receive information on the collected data by the owner of the data. An interesting aspect is that eHealth data can be communicated from the data owner to the citizen via a third party, that is, a physician. The act also regulates that the right of access can be restricted; however, the cases of application of this restriction are defined exhaustively.

To guarantee quality standards of collecting, processing, storing, and evaluating personal data, data owners may certify themselves. The act defines the role of a data protection officer who maintains an index of certified data repositories.

Personal data is not allowed to be manipulated inappropriately. The act regulates the legal claims citizens have regarding their personal data.

The act also regulates the rules applicable for the collecting, protecting, processing, and disseminating of personal data by the federal administration. For the administrations of cantons, the corresponding cantonal laws apply, if available. If not, then the federal law applies. The act regulates the treatment, by federal administration, of personal data for statistical, research, and planning purposes.

7.13 Relationship with the EU Initiative "i2010"

There is almost no information in official documents from Swiss government regarding the EU initiative "i2010". In Eidgenössisches Finanzdepartement EFD (2007), it is stated that the goal of the Swiss eGovernment strategy is to stand up to the EU initiative. How this shall be achieved remains to be seen.

Recall that the EU initiative "i2010" has the following directions of impact:[180]

- To create a single European information space.
- To strengthen innovation and investment in ICT research.
- To support inclusion, better public services and quality of life through the use of ICT.

Consequently, the concrete actions undertaken within the EU are both, much broader and much deeper. In contrast, the few Swiss actions seem to be more piecemeal. How the Swiss puzzle will have to be composed, and how the composition fits into the EU framework, remains to be seen.

[180] For more information see: http://ec.europa.eu/information_society/eeurope/i2010/

8 United Kingdom

8.1 What is the UK current policy and position?

8.1.1 eGovernment Interoperability Framework (eGIF)

In the UK the Government is developing the eGovernment Interoperability Framework (eGIF) which is at the heart of its strategy for ensuring that IT supports the business transformation of Government. This transformation is about delivering better, more efficient public services. The eGovernment Unit contributes to this through frameworks such as the eGIF and also by supporting joined-up service delivery, sharing best practice and placing the citizen at the centre of its focus.

The report "e-Government Interoperability Framework, Version 6.1" describing the eGIF was published by the eGovernment Unit of the Cabinet Office in March 2005. The following sections 8.1.1 to 8.1.4 are taken from the report and reproduced below with the kind permission of the publishers.

Better public services tailored to the needs of the citizen and business, require the seamless flow of information across Government. The eGIF sets out the Government's technical policies and specifications for achieving interoperability and Information and Communication Technology (ICT) systems coherence across the public sector. The eGIF defines the essential prerequisites for joined-up and web-enabled Government.

Adherence to the eGIF policies and specifications is mandatory. They set the underlying infrastructure, freeing up public sector organisations so that they can concentrate on serving the customer through building value-added information and services. It will be for the organisations themselves to consider how their business processes can become more effective by taking advantage of the opportunities provided by increased interoperability.

The main thrust of the eGIF is to adopt secure Internet and World Wide Web specifications for all Government systems. There is a strategic decision to adopt XML and XSL[181] as the core standards for data integration and management. This includes the definition and central provision of XML schemas for use throughout the public sector. The eGIF only adopts specifications that are well supported in the market place. It is a pragmatic strategy that aims to reduce cost and risk for Government systems while aligning them to the global Internet revolution.

The eGIF also sets out policies for establishing and implementing metadata[182] across the public sector. The eGovernment Metadata Standard (eGMS) will help citizens find Government information and resources more easily.

Stipulating policies and specifications is not enough in itself. Successful implementation will mean the provision of support, best-practice guidance, toolkits and centrally agreed schemas. To provide this, the Government has launched the GovTalk website. This is a Cabinet Office-led, joint Government and industry facility for generating and agreeing XML schemas for use throughout the public sector. GovTalk is also used for wide consultation on a number of other eGovernment frameworks and documents and provides best-practice guidance, Frequently

[181] Mark up languages used in systems development.
[182] Metadata are the terms used to describe a data schema for implementation. Having common metadata for different databases implies that they will be more interoperable at the semantic level.

Asked Questions (FAQs), and advice on training and toolkits, and outlines the management processes.

The aims of the eGIF will not be achieved overnight. The strategy needs to be managed as a long-term, ongoing initiative and must therefore be supported by robust processes. These processes, including the roles and responsibilities of key stakeholders, committees, management and working groups, are outlined in the report.

It is also essential to ensure that the eGIF remains up to date, aligned to the requirements of all stakeholders and able to embrace the potential of new technology and market developments. The eGIF introduces an Internet-based change- management process which has been designed to engage and serve the stakeholder community in a dynamic way and bring in innovations from industry on a global basis.

8.1.2 Key policies

These are the key policy decisions that have shaped the eGIF:

- alignment with the Internet: the universal adoption of common specifications used on the Internet and World Wide Web for all public sector information systems
- adoption of XML as the primary standard for data integration and data management for all public sector systems
- adoption of the browser as the key interface: all public sector information systems are to be accessible through browser-based technology; other interfaces are permitted but only in addition to browser-based ones
- the addition of metadata to Government information resources
- the development and adoption of the eGMS, based on the international Dublin Core model (ISO 15836)
- adherence to the eGIF is mandated throughout the public sector
- secure interfaces between Government information systems and intermediaries providing eGovernment services shall conform to the standards in the eGIF. Interfaces between intermediaries and the public are outside the scope of the eGIF.

The selection of eGIF specifications has been driven by:

- interoperability – only specifications that are relevant to systems' interconnectivity, data integration, e-services access and content management metadata are specified
- market support – the specifications selected are widely supported by the market, and are likely to reduce the cost and risk of Government information systems
- scalability – specifications selected have the capacity to be scaled to satisfy changed demands made on the system, such as changes in data volumes, number of transactions or number of users
- openness – the specifications are documented and available to the public
- international standards – preference will be given to standards with the broadest remit, so appropriate international standards will take preference over EU standards, and EU standards will take preference over UK standards.

8.1.3 Scope

The eGIF covers the exchange of information between Government systems and the interactions between:

- UK Government and citizens
- UK Government and intermediaries
- UK Government and businesses (worldwide)
- UK Government organisations
- UK Government and other Governments (UK/EC, UK/US, etc.).

Government information systems will be designed to meet UK legislation and to support channels that provide accessibility for disabled people, members of ethnic minorities and those at risk of social/digital exclusion.

8.1.4 Management processes

The eGovernment Unit in the Cabinet Office is the lead authority for implementing and maintaining this framework, in collaboration with departments, local authorities and other public sector bodies.

The eGIF is based on Government working in open partnership with industry and has been developed through close working with its industry partners. It proposes joint working and development of the policies and specifications for interoperability, relying heavily on industry worldwide to comment and to provide innovative solutions.

8.2 Identity Cards Act 2006

The Act is to make provision for a national scheme of registration of individuals and for the issue of cards capable of being used for identifying registered individuals; to make it an offence for a person to be in possession or control of an identity document to which he/she is not entitled, or of apparatus, articles or materials for making false identity documents; to amend the Consular Fees Act 1980; to make provision facilitating the verification of information provided with an application for a passport; and for connected purposes.

8.2.1 The National Identity Register

The Act states that a register of individuals (to be known as "the National Identity Register") will be established and maintained by the Government. The objectives of the Register will be confined to the statutory purposes which are to facilitate, by the maintenance of a secure reliable record of registrable facts about individuals in the UK. It will provide:

- a convenient method for such individuals to prove registrable facts about themselves to others who reasonably require proof; and
- a secure and reliable method for registrable facts about such individuals to be ascertained or verified wherever that is necessary in the public interest, such as national security or the prevention or detection of crime

The National Identity Register will contain personal information such as:

- name

- address
- gender
- date and place of birth
- immigration status
- fingerprints
- iris patterns
- facial image

It will not include sensitive personal information such as:

- ethnic origin
- medical records
- tax records
- religious beliefs

The Identity Cards Act 2006 states that the NIR can be linked to other databases. However, experts have previously called into doubt the security of such a scheme, as it will be a tempting target for hackers who could attack the interface between the various databases.

8.2.2 National Identity Scheme

The National Identity Scheme is envisaged to be an easy-to-use and extremely secure system of personal identification for adults living in the UK. Its cornerstone is the introduction of national ID cards for all UK residents over the age of 16, which is discussed later in this report.

Each ID card will be unique and will combine the cardholder's biometric data with their checked and confirmed identity details, called a 'biographical footprint'. These identity details and the biometrics will be stored on the National Identity Register.[183] Basic identity information will also be held in a chip on the ID card itself.

This technology aims to bring many benefits, including increased protection against identity theft or fraud.

Through the scheme, which will be run by the Identity and Passport Service (IPS), accredited organisations will be able – with the individual's permission – to use the ID card and the NIR to check their identity.

It is a requirement of the Identity Cards Act that a National Identity Scheme Commissioner will be appointed to keep under review the Act and supervise its operation. At the present time (November 2008) this officer has not been appointed.

8.2.3 What public issues have emerged?

The UK government proposal for introducing a national ID card has sparked a fierce public debate over the recent years. The proposal, unprecedented of its kind in scale and complexity,

[183] Identity and Passport Service, *What is the National Identity Scheme*, available at <http://www.ips.gov.uk/identity/scheme-what-run.asp#nir>, last consulted 30 August 2008.

has been the subject of much controversy and vigorous criticisms pertaining to many of its aspects. Although some commentators, such as the Information Commissioner, view the concept of a national identity system as acceptable, they argue against the current proposals of the UK government and contend alternative methods of identity management had not been fully explored. This section provides a brief overview of the issues and debates concerning the ID card scheme as voiced by politicians, campaigners, researchers, and citizens of the UK.

8.2.4 Objectives of the identity card scheme

Debate over the need, purpose and benefit of a national identification scheme continues to take place in the UK. While the debate was often framed in terms of the Identity Card Bill (now Act), the card itself is not necessarily at the heart of the proposal. While the Act contained only a few clauses about the card, the main purpose was to introduce a database – a National Identity Register (NIR). The identifying information stored on the NIR and how it could be increased, along with the scope of data sharing, were the most important aspects of the debate.[184]

A broad set of benefits is claimed by the UK government for the ID card scheme, amongst them, protection against identity theft and fraud, prevention of organized crime and terrorism, combat illegal working and reduce illegal immigration to the UK, and, allow the police more quickly to identify suspects and people they arrest.[185] The critics of the Act, however, held that many of these public interest objectives would be more effectively achieved by other means.

Crime prevention for example, identity theft and identity fraud in particular, may be better addressed by giving individuals greater control over the disclosure of their own personal information, while a card system such as the one proposed in the Act may even lead to a greater incidence of identity fraud. Similarly, prevention of terrorism may be more effectively managed through strengthened border patrols and increased presence at borders, or allocating adequate resources for conventional police intelligence work.[186] In sum, the extent to which the supposed benefits offered by a national identity scheme can stand up to real scrutiny has been challenged.

8.2.5 Privacy and Data Sharing

The proposed use of the system for a variety of purposes, and access to it from a large number of private and public sector organisations suggests increased level of interoperability – to broaden significantly the scope for what is referred to as 'data sharing'. Data sharing in this context covers disclosures of personal data among agencies and includes the transfer of complete databases as well as information from individuals' records. The term also refers to the addition or substitution of data from one database to another and is widespread in the private and public sectors.[187]

---

[184] Crossman, G., 'The ID Problem', in Birch, D.G.W., *Digital Identity Management: perspectives on the technological business and social implications*, pp. 175-183, Gower Publishing Limited, Hampshire, 2007.
[185] Identity and Passport Service, *Benefits to the Society*, available at <http://www.ips.gov.uk/identity/benefits-society.asp>, last consulted 30 August 2008.
[186] LSE Department of Information Systems, *The Identity project. An assessment of the UK Identity Cards Bill and its implications*, available at <http://identityproject.lse.ac.uk/identityreport.pdf>, last consulted 30 August 2008.
[187] P., Raab, C. and Bellamy, C., 'Joined-up government and privacy in the UK: Managing tensions between data protection and social policy', *Public Administration*, Vol. 83, Issue 1, 2005, pp. 111–133.

Legal analysis of the ID card scheme, particularly the NIR, raises concerns about compliance with data protection principles under the Data Protection Act 1998 (DPA). The first five principles –that information be fairly and lawfully processed, that it be processed for limited purposes, that it be adequate, relevant and not excessive, that it be adequate and that it be kept no longer than necessary- are seen to sit uncomfortably with legislation envisaging an information free-for-all.[188]

8.2.6 Cost

A main issue associated with the ID scheme in the UK concerns its anticipated costs. The LSE Identity Project report provides a detailed analysis of this issue, which is summarised in table 1 below. It is estimated that the likely cost of the ten-year rollout of the proposed identity cards scheme will be between £10.6 billion and £19.2 billion, with a median of £14.5 billion. This figure does not include public or private sector integration costs, nor does it take into account possible cost overruns. Any system that supports critical security functions must be robust and resilient to malicious attacks. Because of its size and complexity, the identity system will require security measures at a scale that will result in substantially higher implementation and operational costs than has been estimated.

	Low	**Median**	**High**
Issuing Identity Cards Over a 10-Year Period	814	1015	1216
Passports (Based on Passport Service Figures)	3936	3936	4065
Readers for Public Sector (As Specified in the Bill)	291	306	317
National Identity Register	1559	2169	2910
Managing the National Identity Register	2261	3658	5341
Staff Costs Over a 10-Year Period	1719	3368	5308
Miscellaneous	22	64	117
TOTAL	10602	14516	19274

Table 8.1: The National Identity Scheme – Projected Costs (All figures £'m)[189]

On the issue of cost, public debate revolves around the accuracy of the figures provided by the government as well as questions to the extent to which the proposal is cost effective. On the first account, it is argued that estimates made by the government are unreasonably low and are in any case notoriously unreliable. Estimates on government IT schemes rarely match final costs as evident in the case of the computerized system of the NHS which currently on

[188] Crossman, G., 'The ID Problem', in Birch, D.G.W., *Digital Identity Management: perspectives on the technological business and social implications*, pp. 175-183, Gower Publishing Limited, Hampshire, 2007.
[189] LSE Department of Information Systems, *The Identity project. An assessment of the UK Identity Cards Bill and its implications*, available at <http://identityproject.lse.ac.uk/identityreport.pdf>, last consulted 30 August 2008.

one estimate faces costs of approximately £30 billion, as compared to the government estimate of £6 billion.[190] Furthermore, commentators have challenged the cost benefit offered in the current government proposal of the identity card scheme. The profound implications of the proposal in terms of public cost requires justification on the part of the government to establish cost-effectiveness.

8.2.7 Technology

The technology envisaged for this scheme is, to a large extent, untested and unreliable. Critics of the UK ID Card Bill repeatedly called attention to the fact that no scheme on this scale has been undertaken anywhere in the world, thus highlighting the risks attached. Smaller and less ambitious systems have encountered substantial technological and operational problems that are likely to be magnified in a large-scale, national system. The use of biometrics gives rise to particular concern because this technology has never been used at such a scale[191]. System architecture emerges as a key issue, with debates around the proposed central database. Issues of data integrity also emerged in this context. Crossman argues that inaccuracies in the proposed database and its impact give citizens much to fear.[192] The impact of inaccuracies will depend on the extent to which information is disseminated and the amount of auditing performed. As ever-greater reliance is placed on digital identity information passing between public bodies without the input of the subject, the scope for contamination by inaccurate information increases. With as yet little auditing proposed, it is inevitable that many people will be unaware that incorrect identifying information about them is being passed between public bodies.[193]

8.2.8 User acceptance

An appropriate identity system for the UK would be one based on a foundation of public trust and user demand rather than one based on enforcement through criminal and civil penalties. The goal of public trust would be made possible, in part, through the use of reliable and secure technologies and the creation of a more flexible "citizen-centred" model. [194] Indeed, citizen perceptions – their fears and expectations - hold important implications for any future attempts at implementing eID cards, as these perceptions may well be translated into subsequent behaviours, namely, resistance to use misuse, or non-use. A pioneering study looking systematically at citizens' attitude toward eID has been published as part of the EU Future of Identity in the Information Society (FIDIS) research project.[195] Preliminary findings point to the strong, negative attitudes held by UK citizens. Areas of concern that

---

[190] Crossman, G., 'The ID Problem', in Birch, D.G.W., *Digital Identity Management: perspectives on the technological business and social implications*, pp. 175-183, Gower Publishing Limited, Hampshire, 2007.
[191] LSE Department of Information Systems, *The Identity project. An assessment of the UK Identity Cards Bill and its implications*, available at <http://identityproject.lse.ac.uk/identityreport.pdf>, last consulted 30 August 2008.
[192] Crossman, G., 'The ID Problem', in Birch, D.G.W., *Digital Identity Management: perspectives on the technological business and social implications*, pp. 175-183, Gower Publishing Limited, Hampshire, 2007.
[193] Crossman, G., 'The ID Problem', in Birch, D.G.W., *Digital Identity Management: perspectives on the technological business and social implications*, pp. 175-183, Gower Publishing Limited, Hampshire, 2007, p. 179.
[194] LSE Department of Information Systems, *The Identity project. An assessment of the UK Identity Cards Bill and its implications*, available at <http://identityproject.lse.ac.uk/identityreport.pdf>, last consulted 30 August 2008.
[195] Backhouse, J. and Halperin, R. (eds.), *D4.4: Survey on Citizen's trust in ID systems and authorities, FIDIS deliverable*, 2007, available at <www.fidis.net>, last consulted 30 August 2008.

warrant attention include low level of institutional trust and severe criticism of the authorities as regards their competence and integrity.[196]

8.3 How are issues being addressed?

8.3.1 Identity fraud

Identity fraud is the fastest growing crime in the UK and putting the personal details of millions of individuals onto Government databases puts them at risk of identity fraud. Individuals' identities are widely scattered in both digital and paper files on Government databases including:

- NHS medical records database

  A £12billion NHS system is being created to hold the medical records of 50m patients.

- DNA database

  The largest in the world, it holds details of 4.25m people and is growing at a rate of 30,000 a month.

- Police records

  The police national computer holds 96m pieces of information, including criminal records and details of arrest

- DVLA database

  Holds the names, addresses, driving license and vehicle details of 42m drivers

- HMRC

  Her Majesty's Revenue and Customs holds the names and addresses of 6m people who make tax credit claims and also stores the names, addresses and National Insurance and salary details of the 30.5m people who pay income tax as well as the details of those who receive child benefit.

- Passport database

  Holds the names, dates of birth, passport and immigration details of 45m UK citizens[197]

Security of an individual's personal details is paramount because with a few key bits of information such as a social security number, billing name and address, mother's maiden name, identity thieves can easily appropriate identities and open credit card accounts, make purchases and apply for loans. Unlike other crimes, the victims typically are unaware until well after the crime has been committed.

In the UK the Government has introduced the Manual of Protective Security (MPS), which all Government departments are required to follow. Any sensitive data must be securely stored and very tight controls should be in place to ensure that those able to access information have

[196] Backhouse, J. and Halperin, R. (eds.), *D4.4: Survey on Citizen's trust in ID systems and authorities, FIDIS deliverable*, 2007, available at <www.fidis.net>, last consulted 30 August 2008.
[197] Blakely, R., 'Where the government holds your details', The Sunday Times, November 25, 2007.

been security vetted; sensitive data should be encrypted when in transit. It will be a criminal offence to make unauthorized disclosures from the database. The MPS is the Cabinet Office document that governs sensitive data. The manual, which is not available to the public, states that departments should classify the impact of losing information on a scale from zero (low) to six (high).

8.3.2 Biometrics issues

The UK is considering plans to create a national "biometrics" database of everyone's unique markers, such as fingerprints and facial characteristics as a defense against crime, but critics say that it could not guarantee security and could make matters worse. Academic research in North America has shown that it is possible to "reverse engineer" finger prints from mathematical biometric data.[198]

8.3.3 Trust in eGovernment

Trust is a reliance relationship between different parties or identities. A trusted party is assumed to be both willing and able to fulfill promises, agreements, policies and laws. One of the problems Governments face concerning identity management is that of trust between the state and the citizen. It is paramount that the personal information of the citizen will be kept secure and confidential by the state, at all times. In the UK the privacy aspects of eGovernment service provision are covered in the Trust Charter for electronic service delivery (e-Trust Charter). There are existing statutory requirements relating to the protection of personal data and communications under the Data Protection Act and the Human Rights Act as well as other pieces of legislation.

It is envisaged that trusted identities will play an important role in the application of identity management systems.

However, it must be noted that in the UK over the last year there have been many careless and inexcusable breaches of people's personal information by Government departments, banks, retailers and other organizations.[199]

8.3.4 Citizen safeguards

The eGovernment's strategy revolves around key transformations focusing on the needs of the citizen and to build service delivery around what the citizen wants. Citizens need to feel involved with developments and to have on-line access to their records and data held by Government. The Varney Report (Service Transformation – 2006) may be summarised as follows:

- Clear statements of intent
- Acknowledge the importance of ensuring citizen confidence
- Respond to the need and concerns of the citizen

---

[198] Cf e.g. Heath, N., *ID card will drown in a billion mismatches,* <http://www.silicon.com/publicsector/0,3800010403,39294213,00.htm> , last consulted 5 November 2008. Simon Davies published an article on November 25, 2007 with reference to a LSE report on the question whether biometrics is the answer. <http://www.timesonline.co.uk/tol/news/politics/article2937058.ece>, last consulted 5 November 2008.

[199] Espiner, T., The worst IT security incidents of 2007, available at <http://resources.zdnet.co.uk/articles/features/0,1000002000,39290745,00.htm>, last consulted 30 August 2008.

- Ensure the citizen is protected by:
    - Rigorous auditing
    - Technical protections
- Provide transparency
- A governance framework of the highest standard should be put in place

9 Netherlands

Over the past few years the Dutch government has introduced several initiatives which are together considered to constitute the electronic government.[200] Although not all initiatives have been fully introduced yet, many of them are likely to have a significant impact on identity management in Dutch eGovernment and are therefore worth discussing.

eGovernment, as a policy objective, has enjoyed much attention by the Dutch government since the 1990's. In an attempt to demonstrate the complexity of the Dutch eGovernment policy, we will first list some of the historical benchmarks in the development of eGovernment in the Netherlands. Subsequently, some emerging issues will be addressed, by indicating their legal implications. Finally some successful examples of eGovernment scenarios will be cited.

9.1 Historical benchmarks

It is worth elaborating how the relevant policies and legal measures, taken by the Dutch government have been evolving during the past years. One of the first initiatives in the field of administration was the Government Information (public Access) Act in 1991, which entitled Dutch citizens the right to get information related to an administrative matter if it is contained in documents held by the public authorities or companies carrying out work on behalf of a public authority.[201] With regard to the electronic administration, first the '1994 National Action Programme on Electronic Highways´ was introduced. With this initiative the Dutch government started its first ICT policy. Even though the purpose of the National Action Programme was to stimulate the development of 'electronic highways', it did not as yet address the provision of online public services.

Moreover, even though further initiatives and policies in the Dutch legislative system have appeared – often going hand in hand with the relevant EU regulations such as the Personal Data Protection Act[202] from 2000 implementing Directive 95/46/EC[203] – there still does not exist an overall regulatory framework for the eGovernment issues in the Netherlands at the moment of this writing.

An important regulatory development in eGoverment policy having implications on identity management is the Act on Electronic Government Communications, which was enacted on

---

[200] Holvast, J., 'Elektronische overheid' [Electronic government], in Berkvens, J.M.A. and Prins, J.E.J., *Privacyregulering in theorie en praktijk* [Privacy regulation in theory and practice], pp. 105-124, Kluwer, Deventer, 2007, p.110.

[201] *Wet openbaarheid van bestuur* [Government Information (Public Access) Act], 31 October 1991, available at <wetten.overheid.nl> (Dutch) and <www.minbzk.nl/contents/pages/5306/public_access_government_info_10-91.pdf> (English), last consulted 5 February 2008.

[202] *Wet bescherming persoonsgegevens* [Personal Data Protection Act], 6 July 2000, available at <wetten.overheid.nl> (Dutch) and <http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml> (English), last consulted 5 February 2008.

[203] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281*, 23/11/1995, pp. 31-50.

the 1st July 2004. Significant remaining (legal) challenges in the field of eGovernment measures include:[204]

- Privacy

  It is noted that data protection is a core question, since most eGovernment services require personal data processing. In order to avoid problems, such as time and money-consuming technical, organizational and policy adjustments, at a later stage, data protection regulations must be taken into account and implemented in eGovernment services right from the start.

- Dematerialization of government communications

  The regulatory framework should be constantly revised, as much as the legal status of electronic communications must be harmonised gradually with technological evolution. Technical rules that affect eGovernment related laws and boil down to technical specifics have to be monitored periodically, in order to best match cross-cutting latest technological standards with relevant regulations, e.g. the position of electronic signatures in the legal system.

- Confidentiality and reliability of eGovernment communications

  Information security remains a focal point in eGovernment-related policies due to the sensitivity and vulnerability that technological facilities for data-processing incorporate. The infringement of rights relevant to personal data-protection might occur if the proper functioning of technological security systems is problematic, e.g. personal data and information becomes available for unauthorised players as well.

- Efficient eGovernment communications and service provision

  The Citizen Service Number will in view of the criticism of the Dutch Data Protection Authority and the Council of State persist as an issue of further attention. The same is true for the way in which the government deals or, rather, does not deal (timely) with e-mail communications by citizens. Efficiency can be effective only if the government practices what it preaches.

- Interoperability of eGovernment data exchange

  Interoperability as regards data exchange is of growing importance both on the European and on the national level. On the European level, interoperability is a core feature that helps out public administration between the national and European level with the purpose of creating a pan-European eGovernment network. At the same time eGovernment processing on the national level remains relevant to develop digital co-operation further within the national public sector.

- Access to and re-use of public sector information

  The debate on the modernization of the Government Information (Public Access) Act 1991 as a consequence of, amongst others, ICT developments, and the introduction of a constitutional right of access to public-sector information as well as an accompanying obligation concerning accessibility of fundamental public-sector information is still unsettled.

---

[204] Hof, S. van der, 'The status of e-government in the Netherlands', in Prins, J.E.J., *Designing e-government*, pp. 245-261, Kluwer Law International, Alphen aan den Rijn, 2007, pp. 258-261.

9.2 eGovernment policy and achievements

Looking at Dutch eGovernment from the policy perspective, the following developments can be discerned. In the first place there has been a development in the Dutch government's approach towards citizens. A shift has occurred from a reactive attitude towards a more proactive and customer-oriented policy.[205] This shift entails a government that actively approaches citizens and automatically applies regulations that apply to specific citizens. In this context privacy concerns emerge since offering such proactive service implies that the government needs even more personal information on citizens at her disposal. Moreover, this information will be used to establish profiles as to be able to offer the correct and desired services.

9.2.1 Personal Internet Page

A second development is to give the citizens more control over their own data. To this end steps have been taken to introduce a Personal Internet Page, currently known as 'MijnOverheid.nl' (MyGovernment.nl). Through this internet page, which has already been introduced on a small scale for testing purposes and will be fully adopted in 2009, citizens can have dealings with the government whenever and wherever they want. They can access and exchange information and keep up to date on pending procedures.[206] Specific services offered by MijnOverheid.nl are the following. In first place there is the Berichtenbox, in which citizens will receive messages from the government, for example that their passport is about to expire. Furthermore, an overview of all products and services offered by the Dutch government is provided. Citizens can search for specific services or products, find a description of each and see which public body is in charge. In addition, MijnOverheid.nl gives access to personal data so that the citizen can see certain processing operations that have been performed upon their personal data. The website will use for this purpose information from the Landelijk Raadpleegbare Deelverzameling, which offers a selection from the Gemeentelijke Basisadministratie Persoonsgegevens (GBA, [Municipal Database Personal Records]): personal data, address, residence and nationality. However, in the course of 2008 MijnOverheid.nl will switch to GBA-Verstrekkingen so that additional information will be provided: information on parents and children, history, source documents and information on the consultation of personal data by others.[207] Future versions will also offer information regarding car, house, work and income. Finally, MijnOverheid.nl will enable citizens to carry out and remain informed on their current business with the government, for example filing a tax declaration, applying for a building permit and following the progress of the application procedure.[208]

MijnOverheid.nl is a portal to all government websites which citizens access by logging on with their BSN (citizen service number, see below) and DigiD (digital identity, see below).

---

[205] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Rapport Voorbij het loket, over de mogelijkheden en onmogelijkheden van pro-actieve dienstverlening voor de Nederlandse overheidsorganisaties [Report Past the counter, on the possibilities and impossibilities of proactive services for the Dutch government organisations], Den Haag, maart 1999, available at <www.minbzk.nl>, last consulted 5 February 2008.

[206] Voortgangsrapportage Elektronische Overheid mei 2007 [Progress Report Electronic Government May 2007] , available at <www.e-overheid.nl/atlas/planning/>, last consulted 5 February 2008.

[207] http://nvvb.gemeenteweb.nl

[208] www.mijnoverheid.nl

Until recently citizens would have to log on separately each time they wanted a service from a different government website. However, the project Single Sign On has been initiated to change this and make MijnOverheid.nl more user-friendly. As a consequence citizens will only need to log on once, when entering MijnOverheid.nl, and will then be able to freely use all services without having to log on again.[209]

9.2.2 Companies website

For companies the website 'Antwoord voor Bedrijven' (answer for companies) has been developed. This website is a national online service counter for business use. On this internet page the central government[210] aspires to unite all the information companies need in one place. The website aims at answering all questions that entrepreneurs may want to ask the government. To this end it offers a search function and the possibility to send an e-mail to or chat with the people in charge of the website. The latter will either answer the question themselves or refer to the public body that can answer the question. The focus of 'Antwoord voor Bedrijven' is to provide information such as relevant legislation, regulations, subsidies, licences and requirements. In the future the website will, like MijnOverheid.nl, also offer the possibility to do business with the government. Companies will then for example be able to apply online for licences.[211]

9.2.3 Identification solutions

Identity number

In order for a service as MijnOverheid.nl to work effectively, electronic identification and authentication procedures must be in place. The electronic identification process has been facilitated by the introduction of the Burgerservicenummer (BSN, citizen service number) in late 2007. The BSN is a single unique number to be used in the contacts between citizens and the Dutch government. The BSN replaces the two numbers formerly used, namely the administration number and the social-fiscal number. There is an ongoing discussion as to whether, and to what extent the BSN might be used by entities other than government institutions. However, it seems inevitable that the BSN will be used by others like private companies. The likeliness of an extensive use of the BSN attributes to the fear of increased identity fraud. Since the BSN will serve more purposes than the two numbers it replaces and combines both in one number, it has a heightened attractiveness to fraud. Moreover, the consequences of identity fraud will be more substantial because the BSN is applied in more contexts. Another concern with regard to the BSN is that it will be used for profiling purposes.[212]

The BSN will be used to link all personal data of citizens to one unique number so as to facilitate a more efficient and reliable data exchange and a better service for citizens. Behind the BSN there is a whole system of (technical) services that takes care of generating, distributing, managing and consulting the BSN. This system includes access to identifying data in underlying registrations, such as the GBA (key register of Persons), and the registers

---

[209] www.mijnoverheid.nl; www.e-overheid.nl; www.bkwi.nl

[210] In close cooperation with ministries, other central government institutions, executive institutions, provinces and municipalities.

[211] www.e-overheid.nl; www.antwoordvoorbedrijven.nl; www.bedrijvenloket.nl; www.minez.nl.

[212] Holvast, J., 'Elektronische overheid' [Electronic government], in Berkvens, J.M.A. and Prins, J.E.J., *Privacyregulering in theorie en praktijk* [Privacy regulation in theory and practice], pp. 105-124, Kluwer, Deventer, 2007, pp. 113-116; www.burgerservicenummer.nl.

for ID cards, which can be used for the verification of a person's identity. The BSN system offers all BSN users the possibility to check whether an identity document is valid and whether a certain number is indeed a BSN. In addition to government organisations, certain authorised users can also retrieve the identifying data belonging to a certain BSN, find out which BSN belongs to certain identifying data and check whether a BSN and certain identifying data belong together.[213]

Key registers

The key register of persons mentioned earlier, is one of several key registers that together constitute one of the basic facilities of the electronic information structure considered necessary for eGovernment. The government needs enormous amounts of information to fulfil her tasks and she has gathered all this information in thousands of different systems. To relieve the administrative burden for the government, to enhance efficiency and to facilitate customer-oriented services the key registers have been introduced. In the key registers all information that belongs to one topic is gathered together. The different key registers have also been linked. Consequently, government organisations can easily access the data they need and citizens do not need to repeatedly give the same information.[214] So far the Dutch government has implemented ten key registers, such as: persons,[215] business and legal persons,[216] buildings,[217] topography,[218] addresses,[219] land registry,[220] vehicles,[221] incomes.[222]

9.2.4 eAuthentication

DigiD

To provide for a uniform electronic authentication procedure among several government organizations, the Dutch government has developed three products/services for e-authentication. The first service is 'DigiD' (digital identity), which offers citizens and companies the possibility to access several online government services using only one username and password. Access to DigiD can be obtained through an application in which the citizen provides some personal data, in the near future including the BSN. After checking the data the citizen will receive by post a password that can be used once as activation.

---

[213] Matrix.e-overheid.nl; on the BSN see also Buitelaar, H. (ed.), *D13.3: Study on ID number policies, FIDIS deliverable*, 2007, available at <www.fidis.net>, last consulted 6 February 2008.
[214] www.e-overheid.nl
[215] Contains personal data of all inhabitants, e.g. name, address, data of birth, gender.
[216] Contains information on all Dutch companies and legal persons, e.g. company name, address, type of company, personal addresses of owner, partner, director, commissioner, authorized agent, data of branches, official receiver in case of bankruptcy.
[217] Contains information on all premises on Dutch territory (and also information on the so called *verblijfsobjecten*, the places destined for premises that are not permanently connected to the ground and the parts of water destined for permanent placement of vessels), e.g. the purpose of the premises (inhabitation, recreation, office, industrial, etc.), location (co-ordinates), size, status (e.g. realised, in use, out of use).
[218] Contains all topographical maps of the Netherlands providing detailed descriptions of all geo-objects on these maps, e.g. for a road the type of road, number of lanes, type of road surface, road number, road name, etc.
[219] Contains the addresses of all premises from the key register of buildings. This register has a central place in the system of key registers because it enables through addresses the connection of persons, businesses and buildings.
[220] Contains a registration of each parcel in the Netherlands, for each parcel it contains information on location, surface and some legal data, such as the owner of the parcel.
[221] Contains information on the license number, the vehicle and personal data of the owner of the vehicle.
[222] Contains the year income of citizens, identifying data regarding the citizen (including the Burgerservicenummer) and information regarding the status and source of the authentic data.

Subsequently the citizen can choose a username and password. Both are checked each transaction. The levels of security offered by DigiD will be low, medium and high. However, currently only the low protection level is available. For higher security levels the electronic signature in combination with the Public Key Infrastructure can be used (see below).[223]

eNik

As part of the DigiD process for e-authentication, the eNik (elektronische Nederlandse identiteitskaart; electronic Dutch identity card) is being developed. The eNik will have a chip containing biometric data and an electronic signature. Furthermore the eNik allows for the encryption of messages and digital identification and authentication. The eNik's chip will contain the BSN, three private keys and biometric data. In addition it will also contain three certificates that comply with PKIoverheid (PKIgovernment, see below). To be able to use all functions of the eNik, the end users need a card reader and the necessary software. Also services providers need the necessary software so as to be able to verify identities and digital certificates. To electronically verify identity the functions of the eNik will become part of DigiD. The combination with the eNik offers a higher authentication security level than the sole use of DigiD. When an eNik is issued activation data will also be issued so as to be able to use the electronic functions of the card. These activation data will consist of PIN and PUK codes.[224] So far the eNik has not been introduced yet and due to delays in the project it is uncertain when the introduction will take place.[225]

PKI

PKIoverheid (Public Key Infrastructure government) is the third service for e-authentication. The PKI for the government enables safe electronic communication with and between public bodies by providing means of electronically signing and encrypting messages. To this end the PKI uses certificates which offer a high level of security. Within DigiD the certificates of PKIoverheid are the most reliable means of authentication. PKIoverheid is based on European standards and the Wet elektronische handtekeningen (Electronic Signatures Act).[226]

Biometric data

As mentioned above, the eNik will contain biometric data. However, the use of biometrics for identity documents is not new in the Netherlands. Following Council Regulation No 2252/2004[227] the Dutch government introduced in august 2006 the Dutch identity card and passport with a chip for storage of facial images. In 2009 storage of fingerprints will follow.[228] The Dutch government's position concerning the use of biometrics can be called positive, notwithstanding the existing criticisms with regards to its consequences for the protection of privacy and personal data.

---

[223] Holvast, J., 'Elektronische overheid' [Electronic government], in Berkvens, J.M.A. and Prins, J.E.J., *Privacyregulering in theorie en praktijk* [Privacy regulation in theory and practice], pp. 105-124, Kluwer, Deventer, 2007, p. 120.

[224] www.e-overheid.nl; a PIN code is a Personal Identification Number used for authentication so as to gain access to the electronic functions of the eNik; a PUK code is a Personal Unblocking Key that can be used to unblock the card after wrongfully entering the PIN code more times than allowed.

[225] *Voortgangsrapportage e-overheid oktober 2007* [Progress Report egovernment October 2007], available at <www.e-overheid.nl/data/files/architectuur/VR6okt2007.pdf>, last consulted 6 February 2008.

[226] www.e-overheid.nl; www.pkioverheid.nl

[227] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *Official Journal L 385*, 29/12/2004, pp. 1-6.

[228] www.minbzk.nl/onderwerpen/persoonsgegevens-en/reisdocumenten/veelgestelde-vragen

9.2.5 eGovernment scenarios

eCitizen Programme

One of the primary goals of the Dutch eGovernment policy is to improve information exchange, service delivery and interactive participation. The government seeks to realize this by introducing a 'new partnership' between citizen and government, whereby more responsibility and choice will be given to citizens. Acting in line with this consideration one of the most recent eGovernment achievements of the Dutch government has even won the European eDemocracy Award 2007 at the Global eDemocracy Forum, held in October in Paris.[229] This policy document is the eCitizen Charter, which was introduced in 2005.[230]

The Charter can be regarded as the first integrated attempt at combining the rights, obligations and roles of citizenship in relation to governance in the Netherlands. The eCitizen Charter is based on research into existing quality systems and several surveys of citizen's expectations. Moreover, as far as the Dutch cabinet is concerned, the required empowerment is being supported by ICTs in order to help citizens as much as possible to accomplish their new role. It is deliberately written from the citizens' perspective and it consists of 10 quality requirements for digital contacts and each requirement is formulated as a right of a citizen and a corresponding duty of government. The Dutch National Ombudsman has declared to adopt the charter as part of his evaluation principles. The charter is a collection of guiding principles in the Netherlands Government Reference Architecture (NORA). Thus it creates the basis for national interoperability standards in eGovernment matters. Since the joint declaration on April 18th 2006 the government holds the eCitizen Charter as the guiding principles for citizen centred government. The 2006 OECD-peer review recommended to integrate the charter in national policy. As a consequence the charter was adopted by the Dutch Standardisation Council as the national standard for public service delivery.

The specific requirements of the eCitizen Charter are as follows:

- Choice of Channel

  The Choice of Channel (digital or not) principle is often used by commercial service providers like banks and insurance companies who understood what their customers expect. They changed their policy by having persuaded their clients to shift to internet banking. Likewise government bodies seem to introduce smart ways of channel management.

- Transparent Public Sector

  It often happens that citizens get lost in the administrative system. Internet enables government to work virtually together with the public, provided that politicians and officials are ready to change from a supply to a demand orientation. An example of helping people to find their ways in the digital public administration is the Fully Integrated National Database (called FIND), which is a catalogue of public services, giving descriptions and access to all of the existing 2500 products of national, regional and local government.

- Overview of Rights and Duties

---

[229] www.burger.overheid.nl/service_menu/english

[230] ECOTEC and Tavistock Institute, *A Handbook for Citizen-centric eGovernment, version 2.1*, December 2007, available at <www.ccegov.eu/downloads/Handbook_Final_031207.pdf>, last consulted 5 February 2008, pp. 73-76.

Each citizen is supposed to know the law, but usually it is not easy to be sure what the duties and rights of a citizen are. Therefore lots of citizens do not get what they are entitled to. In an area like social security there exists a jungle of regulations and institutions in which people got lost. Digital government helps to introduce a personalised internet page: "MyGovernment.nl". Surveys state that people in the Netherlands are happy about the system.[231]

- Personalised Information

  Since 2007, the ordinary method of official publication in the Netherlands is the digital way. The central portal www.overheid.nl provides access to all government agencies and their services. Beyond the distribution of digitally published original documents, eGovernment facilitates a shift from a supply driven way of information provision to a demand oriented method.

- Convenient Services

  EGovernment services have the positive effect of combining data and converting many separate databases into a so-called authentic e-registers, thus making it no longer necessary to fill in forms. An important prerequisite is that procedures are transparent and people can easily find out what data is stored by government, and for what purpose.

- Comprehensive Procedures

  It is often the case that administrative procedures are not comprehensible or unnecessarily complicated. Therefore, by providing insight into the electronic version of administration, government might enable better understanding and gain in credibility. When the full process is transparant, it does not seem to take as much time as when government functions are a pure black box.

- Trust and Reliability

  By changing the tradition of getting into touch with government and it becoming increasingly of a virtual nature implies, that we become more and more dependent on the availability and continuity of electronic networks. While public authorities are usally responsible for infrastructure, this responsibility is not common as far as the digital highway is concerned. Continuity and trust are crucial to be assured.

- Considerate Administration

  A citizen-conscious electronic administration means not only that citizens have the right to be taken seriously; customer friendliness contributes a lot towards improving performance. Even though, putting the perspective of a customer first is still a major culture change for the public sector. Because government lacks the discipline of the market which forces business to act when circumstances change, other incentives are necessary. The digital complaints procedure which lowers barriers compared to submitting complaints in writing and the quality charters are the most promising instrument.

- Accountability and Benchmarking

---

[231] Burger@Overheid.nl, *Workbook eCitizen Charter*, available at <www.burger.overheid.nl/files/workbook_ecc_english.pdf>, last consulted 5 February 2008, p. 10.

After privatisation, many collective services (job search, health care, energy supply, etc.) experience that market mechanism only functions for them when people have the information to make choices themselves. Thus public feedback mechanisms need to be introduced, in order to be accountable to people. School report cards serve as an example to help parents to select education institutions. Nowadays this is done in the Netherlands to support the major privatising operation of health insurance and care.

- Engagement and Empowerment

  EGovernment is not only useful to improve service delivery, reduce administrative burdens and enhance internal efficiency, but is promising as regards matters of involvement and participation. Methods which improve service delivery can be of help to promote empowerment. The success of the Voting Assistant (www.stemwijzer.nl) helps voters to compare the election programmes of political parties and make a well founded choice. [232]

9.2.6 eGovernment in practice: one-stop-shop for Hotel Restaurant Café licenses in Amsterdam

Europe's remarkable economic growth is facing diverse societal problems, including high unemployment rates. By decreasing the barriers and administrative obstacles for people in order to set up SMEs, the project of Café licences in Amsterdam (HoReCa Project) seeks to stimulate economic growth. The project aims to create new jobs and to increase social inclusion in line with the goals set by the Lisbon Agenda and by the European regional policy. Moreover, the project also contributes to the i2010 eGovernment Agenda and to EC programmes.

Reduction of administrative burdens and costs are important aspects to consider. This is also the purpose of making (local) licenses and dispensations simpler. The example of the city of Amsterdam also highlights the exigency of process simplification. Therefore municipality of Amsterdam aims to develop its service provision by the help of approaching citizens and businesses at the same time. Hence the city can be regarded as a pioneer example with an influence on the national level by changing contextual conditions, in cooperation with four Dutch Ministries.

In general local eGovernment policy is divided in two main parts: 1) Service provision, and 2) Rules and Regulations. The first deals with building-up multiple channels and the second deals with legal simplifications. Moreover, it is aimed at implementing these simplifications through the channels. Since these channels are needed throughout the country, the local initiative of Amsterdam can influence the national legal level as well.

Dutch national law and relevant policy already requires municipalities to streamline their administrative procedures in order to make co-ordinated, composite and coherent decisions on licences and procedures. The project of Amsterdam seems to contribute successfully to the implementation of this policy and it can give an insight into the work of the national government by providing a good practice.

Technically the HoReCa project meets all the required standards formulated by the national agency of electronic authorities EGEM. Moreover the success of it appears to be impressive,

[232] Burger@Overheid.nl, *Workbook eCitizen Charter*, available at <www.burger.overheid.nl/files/workbook_ecc_english.pdf>, last consulted 5 February 2008, pp. 6-25.

since the national ICT agency, ICTU, has taken formally the commitment to transfer the Amsterdam system also to other local governments.[233]

[233] www.amsterdam.nl/horeca; www.epractice.eu/cases/horeca1.

10 Belgium

10.1 Introduction

Belgium is one of the best broadband-connected countries in Europe, but has not yet matched this with equally high levels of service, usage and skills.[234] However, introducing secure and easy-to-use eID solutions opens the door to new business opportunities, advances the internal market and facilitates the free movement of citizens. Having such a system facilitates public service delivery in areas such as procurement, social security, taxation and health. It also delivers benefits like convenience, time and cost savings, reduced fraud, simplified procedures, and enhanced privacy.[235] In Belgium identification of the citizen is primarily based on his national registry number.

10.2 The Belgian general trends with regard to ID numbers[236]

In the Belgian eGovernment there is a globally unique identifier. Identification is necessary in different contexts:

- the National Registry Number ("Rijksregisternummer");
- the ID card number;[237]
- the Social Security Card number;
- the INSZ number;
- the Crossroads Bank for Social Security number;
- the Fiscal number;
- the eGovernment registration number;
- the enterprise number.

The data exchange is built on globally unique identifiers which allow identification and data linkage across contexts.[238]

---

[234] European Commission, *i2010 Annual Report 2007 Belgium*, available at <http://ec.europa.eu/information_society/eeurope/i2010/docs/annual_report/2007/country_factsheets/2007_factsheet_be.pdf>, last consulted 31 August 2008.
[235] European Commission, *eGovernment Progress in EU27+. Reaping the benefits*, available at <http://www.astic.es/eAdministracion/Documents/egovprogress7.pdf>, last consulted 31 August 2008, 18/3.
[236] Buitelaar, H. (ed.), *D13.3: Study on ID number policies, FIDIS deliverable*, 2007, available at <www.fidis.net>, last consulted 6 February 2008, p. 54-69.
[237] See Dumortier, J. and Graux, H., *eID Interoperability for PEGS. National Profile Belgium*, available at <http://ec.europa.eu/idabc/servlets/Doc?id=31520>, last consulted 31 August 2008, pp. 14-16; Alsemoy, B. van and Cock, D. de, 'Due processing of personal data in eGovernment?', *Datenschutz und Datensicherheit*, vol. 32, issue 3, 2008, pp. 178-183; Cock, D. de, *Belgian eID card technical overview*, available at <http://homes.esat.kuleuven.be/~decockd/site/EidCards/belpic/mySlides/belgian.eid.card.technical.overview.pdf>, last consulted 31 August 2008.
[238] Koops, B.J., Buitelaar, H. and Lips, M. (eds.), *D5.4: Anonymity in electronic government: a case-study analysis of governments' identity knowledge, FIDIS deliverable*, 2007, available at <www.fidis.net>, last consulted 29 August 2008, p. 58, nr. 6.8.

As far as possible reference will be made of the sophistication stage reached, with reference to the maximum stage possible for the service. The information is based on the enhanced methodology used to assess the level of online availability and sophistication of the services according to the European annual report on benchmarking the supply of online public services.[239]

10.3 The eGovernment achievements

The OECD Peer Review[240] underlines that in Belgium the full online availability of services for businesses and citizens was 50% in 2006 and 60% in 2007. It is a bit more than 80 % in 2007. Concerning the online sophistication of basic public services for businesses Belgium ranks among the leaders. This ranking gives an overall view of the position of Belgium amongst other European countries.

	2003	2004	2005	2006	EU25	Rank
eGovernment Indicators						
% basic public services for citizens fully available online	16.7	16.7		18.2	36.8	21
% basic public services for enterprises fully available online	62.5	62.5		87.5	67.8	3
% of population using e-Government services			18.2	30.2	23.8	11
of which for returning filled in forms			4.4	7.4	8.1	12
% of enterprises using e-Government services		60.0	61.5	59.3	63.7	20
of which for returning filled in forms	24.7	26.1	33.4	36.6	44.8	21

Table 10.1: eGovernment position Belgium[241]

In services for enterprises Belgium belongs to the top of Europe. Use by citizens of available services however seems good but enterprise use is below average.

10.3.1 The NRN

Belgian municipalities maintain the civil status register, the birth register and the population register. The latter consists of 3 sub-registers:[242]

- The (core) 'population register': data about Belgians, foreigners with a permanent residence permit, gypsies, commercial travelers and homeless people who have a reference address;
- The foreigners register: data about foreigners with a temporary residence permit, also called 'bis-register';
- The waiting register: data about candidate refugees, also called 'ter-register'.

---

[239] Capgemini, *The user challenge. Benchmarking the supply of online public services*, available at <http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf>, last consulted 31 August 2008.
[240] Leyman, F., *OECD Peer Review eGovernment BELGIUM*, available at <http://www.oecd.org/dataoecd/43/13/40305982.pdf>, last consulted 31 August 2008. See also Capgemini, *The user challenge. Benchmarking the supply of online public services*, available at < http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf>, last consulted 31 August 2008, p. 31.
[241] Published in European Commission, *i2010 Annual Report 2007 Belgium*, available at <http://ec.europa.eu/information_society/eeurope/i2010/docs/annual_report/2007/country_factsheets/2007_factsheet_be.pdf>, last consulted 31 August 2008.
[242] Art. 19 Act 19 July 1991.

Municipalities issue cards to Belgians and foreigners that are authorized to reside in Belgium. Non-nationals receive residence cards (called "blue cards")[243] and identity cards (called "yellow cards")[244] with, largely, the same data. Persons in the waiting registers are issued "white cards".[245]

The municipalities are responsible for keeping the population registers up to date.

The National Registry is an information processing system responsible for the intake, storage and communication of information regarding the identification of natural persons.[246] It officially exists since 1983. It evolved from an internal tool to a major tool of the eGovernment.

The decision to introduce the electronic identity card for every citizen older than 12 has been taken in July 2001. Completion of the roll-out is expected by early 2009.Deployment started in the second half of 2003. Since late 2006 an eID is possible for children under 12. It is necessary for traveling abroad and is valid for European countries and some not-European countries. The card contains a chip and a pin code. Thanks to this the children can safely chat on Internet. It also can be used as access for the library, as annual subscription for the swimming pool, for the subscription at school or as a member card in a sports club. Moreover the card is also an extra protection in case of emergencies: the parents can add to the card maximum five telephone numbers that can be contacted in case of emergency.

One of the main principles of the Belgian eGovernment is that every entity has one and only one identification number that remains stable over time.[247] The identification also is exhaustive (every entity has an identification key). It is a unique number.

The Law of 25 March 2003[248] created a legitimacy ground to some entities to process the National Registry Number identifier to exchange data about registered entities within the whole Belgian public sector context. The purpose is to:

- facilitate the exchange of information between administrations;
- enable the automated updating of the databases;
- rationalizing the communal management of the population registries;
- simplify some administrative formalities.

In February 2008 the Council of Ministers accepted the proposition to introduce an electronic foreigners card. A pilot project has been effectuated in three communes (Antwerp, Tubeke

---

[243] See Vlaams Minderhedencentrum, *Oude Bijlage 8/9 - Verblijfskaart van een onderdaan van een lidstaat der EEG*, available at <http://www.vmc.be/vreemdelingenrecht/wegwijs.aspx?id=770>, last consulted 31 August 2008.
[244] See Vlaams Minderhedencentrum, *Oude Bijlage 7 - Identiteitskaart voor Vreemdeling*, available at <http://www.vmc.be/vreemdelingenrecht/wegwijs.aspx?id=723>, last consulted 31 August 2008.
[245] See Vlaams Minderhedencentrum, *Oude bijlage 6 - Bewijs van Inschrijving in het Vreemdelingenregister*, available at <http://www.vmc.be/vreemdelingenrecht/wegwijs.aspx?id=712>, last consulted 31 August 2008.
[246] Art. 1 Act 8 August 1983.
[247] Deprest, J. and Robben, F., *eGovernment: the approach of the Belgian federal administration*, available at <http://www.ksz-bcss.fgov.be/documentation/fr/documentation/Presse/2003%20-%20E-government%20paper%20v%201.0.pdf>, last consulted 31 August 2008, p. 21.
[248] Law of 25 March 2003 modifying the law of 8 August 1983 and the law of 19 July 1991 concerning the population registers and the identity cards and the modification of the law of 8 August 1983, Belgian State Gazette, 28 March 2003.

and Uccle).[249] In this way they would, just as Belgians, with their eID card also have access to authentification, identification and electronic signature and access to Tax-on-Web, … In the future links with the SIS-card[250], the labour card and the identity card will be possible. For foreigners the number used is the same as the one employed in the social security sector (also known as the "INSZ").

The eID makes it possible to sign electronic documents and e-mails, to access safe chat rooms for children, to access container parks, to log in in the computer of the employer. Official documents can be ordered with the eID. The eID can be used as library card, as access for lockers, for the reservation of a hotel room.

There already is a long debate concerning the usage of single national identification numbers.[251] It is clear that the NRN was not intended for use outside the governmental context.

10.3.2 Biometric passports

In November 2004, Belgium was the first country in the world to start issuing electronic passports complying with the recommendations of the International Civil Aviation Organization (ICAO). These passports feature a contactless microchip storing personal identification data and biometric information (facial image of the holder). Fingerprints were due to be added at a later stage.

10.3.3 Digital certificates

The so-called "commercial certification authorities certificates" can be used in a number of eGovernment applications as an alternative to eID card signatures**.**

As of April 2007, the federal government had recognized three private certification authorities complying with the required standards regarding qualified certificates defined in the Belgian e-Signatures Act. Their certificates can be used for certain eGovernment applications, tax and social security eServices in particular.

Like the eID, these digital certificates contain certain identity data, the public key connected with the certificate holder, the public key usage, the validity of the certificate and the category of certificate. They can be issued to both natural persons and legal entities.

10.3.4 Municipal population register

In addition to the basic NRN the population register also contains passport details (with passport number, number of the Belgian ID card, number and date of issuance of the Social Security Card and pseudonyms). Only the general data protection rules apply to these identifiers.[252]

---

[249] See http://www.eid.belgium.be/. In the press (Gazet van Antwerpen, 10th July 2008) has been mentioned that the first electronic card has been transferred to a foreigner by the local authority of Retie.
[250] Cf section 10.3.6 below.
[251] Buitelaar, H. (ed.), *D13.3: Study on ID number policies, FIDIS deliverable*, 2007, available at <www.fidis.net>, last consulted 6 February 2008, o.c., p. 58.
[252] Buitelaar, H. (ed.), *D13.3: Study on ID number policies, FIDIS deliverable*, 2007, available at <www.fidis.net>, last consulted 6 February 2008, o.c., p. 61.

10.3.5 ID number for social security

In the Belgian social security system 2000 social security offices are responsible for the delivery of Belgian social security. More than 10.000.000 socially insured persons and 200.000 employers are frequently in contact with those offices to claim their entitlements, provide information and pay their contributions.

The actual situation is as follows:

- social insured persons and their employers have to declare electronically to only one address (start and end of employment relationship, three monthly declaration about income, social risk)
- the Crossroads Bank for Social Security manages and uses a reference directory

Some categories of persons that are relevant for social security, fiscal and other purposes are not included in the NRN and the Population Registry. Article 8 of the Crossroads Bank for Social Security Act of 15 January 1990, as amended by the law of 16 January 2003, stipulates that for social security purposes the identification number of the Crossroads Bank itself can be used.

The INSZ number consists of 11 digits: 6 for the date of birth, the 3 following for the serial number of the registration and the last 2 for the verification number.

The usage is free. It falls under two different usage regimes: the one concerning the NRN and the general data protection law.

10.3.6 The SIS-card

The SIS-card has a bank card format, similar to the generic eID card but without a photo of the bearer. It is mandatory. It is issued by any insurance fund to any person subject to Belgian health care regime, starting at birth (for employees, the self employed, unemployed, children, public officials) and regardless of nationality. The card contains the following information: the national register number, last name and two first names, date of birth, gender, SIS-card number, and expiry date of the card. The card is used by health professionals to verify the public medical insurance status. This requires a specific reader, only issued to mandated persons and organizations and a specific card (the SAM card) to decrypt the information stored on SIS cards. There is no need for a PIN-code since the information can only be read through the specific readers in combination with a SAM card.

10.3.7 The Crossroads Bank for Social Security (CBSS)

The CBSS was created in 1995 to improve the efficiency of the social security. It is not an official register in the strict sense, but a reference repertory in the form of a relational database. It refers to the authentic source, but doesn't contain data. Information exchanges between the databases of social security organizations are only possible after obtaining an appropriate mandate to do so by law, or by the sector committee of social security, a committee within the Belgian Privacy Commission.

10.3.8 BIS-register of the Crossroads bank for Social Security

It is created for those who are not entered in the National Register, but are subject to Belgian social security regulations. It contains: the Crossroads bank number, first and last name(s), place and date of birth, gender, nationality, official address and invoicing address, place and date of death, marital status.

In practice: Social security benefits

- Unemployment benefits[253]

  The Central Government (Federal), Federal Department Social Security is responsible for these data. Enrolment must be done in person with the organisms in charge of managing unemployment benefits payments: either the public body CAPAC-HVW (Auxiliary Fund for the Payment of Unemployment Benefits, or the accredited trade-unions (CSC-ACV, FGTB-ABVV and CGSLB-ACLVB). These organizations' websites provide enrolment forms for downloading.

  The sophistication stage is 4/5 (Average sophistication level of procedures related to social security benefits).

- Child allowances[254]

  These data fall under the responsibility of the Central Government (Federal), Federal Department Social Security, National Office for Family Allowances for Employed Workers (ONAFTS-RKW). This service is fully automated in Belgium.

  The allowed sophistication stage is 4/5 (Average sophistication level of procedures related to social security benefits).

- Medical costs (reimbursement or direct settlement)[255]

  The Central Government (Federal), Federal Department Social Security, National Institute of Medical and Invalidity Insurance (RIZIV-INAMI) is responsible**.** The website of the National Institute of Medical and Invalidity Insurance (RIZIV-INAMI) provides information about the reimbursement of medical costs. Belgium has been one of the first countries to introduce a smart social insurance card (SIS card). This card enables direct settlement of certain medical costs, while other costs are reimbursed through mandatory/complementary private social insurances. These social insurances have their own websites, some of which offer e-Services. The scheme is administered by the Crossroads Bank for Social Security (http://www.ksz-bcss.fgov.be/).

  The Sophistication stage is 4/5 (Average sophistication level of procedures related to social security benefits).

- Student grants[256]

  These data fall under the responsibility of the Community/Regional Government: Government of Flanders, Government of the French Community, Government of the German-speaking Community. The scholarships website of the Flanders Community offers information and downloadable forms, while the other websites provide information only. The Flemish Digital application form has been extended to secondary education in August 2007.

  The Sophistication stage is 4/5 (Average sophistication level of procedures related to social security benefits).

---

[253] https://www.socialsecurity.be/
[254] http://www.rkw.be/
[255] http://inami.fgov.be/
[256] See http://www.ond.vlaanderen.be/studietoelagen/ (Flanders); http://www.cfwb.be/allocations-etudes/ (French-speaking community); http://www.dglive.be/desktopdefault.aspx/tabid-126/601_read-4810/ (German-speaking community).

10.3.9 Limosa-project[257]

This project registers foreign enterprises and foreign workers who are temporarily professionally active in Belgium, and are not included in other registers. The employer or organization that sends somebody to Belgium or the person himself if he is self-employed must declare. The person receives a username and password after an electronic registration process. He must electronically declare the activity. Then a so called Limosa-1-certificate is issued electronically. This certificate must be printed out and always carried by the foreign worker. The Belgian client must check this certificate. A first version of the electronic system Limosa, aimed at monitoring and controlling all forms of foreign occupation of workers in Belgium, is live.

10.4 The fiscal number

Description

The Belgian Ministry of Finances (SPF Finances) makes a new range of services available online at Tax-on-Web[258] in order to help citizens complete their tax returns. The services, which can only be accessed by users who have registered for an eID card or token, allow users to find details of their outstanding tax liabilities, backtrack over their past tax history, build up a preference list, and keep an eye on the progress of their tax return as it is processed. Tax-on-web allows Belgian residents to file their tax returns online. The applications enable taxpayers to calculate the amount of their income tax, validate and save their data online, submit their returns electronically, and get a receipt from the Tax Administration. The online help system assists them in going through the different steps of the process.

The sophistication stage[259] is 5/5.

Properties

All taxable persons are assigned a fiscal ID number (art. 314 §1 Belgian Income Tax Code). For natural persons this number corresponds to the NRN. For legal persons a fiscal ID number is assigned. It is their VAT number, consisting of the country code BE plus a string of 9 numbers between 0 and 9. Other persons that are not registered in the NR receive a separate ID number, built according to the same rules as for the Crossroads Bank.

Usage

It can be used for identification purposes of a number of internal and external relations the Fiscal administration has with other entities.

10.5 The Enterprise number

The Crossroads Bank for Enterprises provides access to information held in the National Register of legal persons, the trade register, VAT registers and social security registers. The information in these registers is maintained by the institutions that were competent. Access is

[257] See www.limosa.be
[258] www.ccff02.minfin.fgov.be/taxonweb/
[259] Capgemini, *The user challenge. Benchmarking the supply of online public services*, available at <http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf>, last consulted 31 August 2008.

only possible with an appropriate mandate to do so by law,[260] or by the sector committee within the Belgian Privacy Commission.[261] The so called enterprise counters[262] register the entities. Since 2003 only one body is appointed to be responsible for a single collection of basic identification data concerning the company, its registration in the Crossroads Bank for Enterprises and the subsequent updates. Each company and plant receives a single identification number. Generally following data are gathered: the name, place of establishment, legal form (in case of legal persons), legal status (e.g. normal, bankruptcy, …), date of establishment, management and proxies, economical activity by NACE-code, certain financial information, local establishments and any other legally identification data and/or permits.

10.6 Services for enterprises[263]

- ***Social contribution for employees:*** Belgian companies or their representatives can carry out eighteen electronic transactions from application to application or online via the social security portal. Since 1 January 2003 all Belgian employers must submit their quarterly declaration of wages and working times electronically to the National Office for Social Security. All authorized social security institutions can access the submitted data. The Central Government (Federal), Federal Department Social Security is Responsible.

  The sophistication stage is 4/4.

- ***Corporate tax: declaration, notification:***[264] It concerns information and 'intelligent' forms that can be digitally signed and submitted electronically. The Central Government (Federal), Federal Department Finance is responsible.

  The sophistication stage is 4/4.

- ***VAT: declaration, notification:***[265] InterVAT[266] enables electronic submission of VAT declarations. Another application called EdiVAT[267] allows submission based on the EDI (Electronic Data Interchange). It belongs to the responsibility of the Central Government (Federal), Federal Department Finance.

  The sophistication stage is 4/4.

- ***Registration of a new company:***[268] Since July 2003 the Commerce Registry administered by the Federal Department Justice has been replaced by a Crossroads Bank for Enterprises and a series of 10 Enterprise Counters providing one-sop shop services for businesses. These Enterprise Counters are administered by accredited

[260] Law of 16 January 2003 establishing a Crossroads Bank of Enterprises, modernizing the trade register, establishing accredited enterprise counters. See http://mineco.fgov.be/enterprises/crossroads.bank/pdf/law.BCE-KBO.nl.001.pdf.
[261] See http://www.privacycommission.be/nl/sectoral_committees/central_enterprise_database/
[262] Ondernemingsloket/guichet d'entreprise.
[263] https://www.socialsecurity.be/
[264] http://www.minfin.fgov.be/
[265] http://www.minfin.fgov.be/portail1/fr/intervat/welcomeintervatfr.html
[266] http://www.minfin.fgov.be/portail1/fr/intervat/welcomeintervatfr.html
[267] http://minfin.fgov.be/portail1/fr/edivat/edivatfr.html
[268] http://mineco.fgov.be/enterprises/crossroads_bank/home_fr.htm

private organizations. Most of them make it possible to register a business online. Since 1 June 2006, a company can be created within 3 days (instead of 67 days originally) thanks to the electronic registration desk through which the data required for the company registration can be electronically exchanged at the notary's. The Central Government (Federal), Federal Department Economy, SMEs, Self-employed and Energy, Crossroads Bank for Enterprises is responsible.

The sophistication stage is 4/4.

- ***Submission of data to statistical offices:***[269] Data concerning company revenues already declared to the tax administration do not need to be re-submitted separately to the Statistics Division. Likewise, data related to employees already submitted to Social Security and/or Employment administrations are automatically submitted for statistical purposes. The Central Government (Federal), Federal Department Economy, SMEs, Self-employed and Energy, Statistics Division is responsible.

  The sophistication stage is 5/5.

- ***Customs declarations:***[270] Since 4 February 2008 the web-based application "Paperless Customs and Excise" (PDLA) is operational. It replaced the previous electronic customs declaration system SADBEL (*Système Automatisé de Dédouanement pour la Belgique et le Luxembourg*). PDLA allows for the electronic introduction and processing of customs and excise declarations. The electronic filing of customs declarations will become mandatory in July 2009. Moreover, the Customs and Excise Administration has also developed a web-based application called WEB - N.C.T.S. for managing transit operations, based on the EU's New Computerised Transit System (NCTS). It belongs to the **r**esponsibility of the Central Government (Federal), Federal Department Finance, Customs and Excise Administration.

  The sophistication stage is 4/4.

- ***Environment-related permits (incl. reporting):***[271] Regional websites provide information and online forms for permit requests. Applications are handled by municipalities. It falls under the **r**esponsibility of the Regional Government and Local Government (Communes).

  The sophistication stage is 2/5.

10.7 Public procurement[272]

The Belgian public procurement portal brings together links to: (1) the Joint Electronic Public Procurement (JEPP) portal[273] which allows for the electronic notification and dissemination of federal public calls for tender; (2) the e-Tendering platform,[274] which provides economic operators with the tools and services for the automated, safe and transparent submission,

[269] http://www.statbel.fgov.be/
[270] http://plda.fgov.be/
[271] http://www.vmm.be/(Flanders);http://environnement.wallonie.be/(Wallonia);http://www.ibgebim.be/(Brussels Region)
[272] http://www.publicprocurement.be/portal/page/portal/pubproc
[273] www.jepp.be
[274] https://eten.publicprocurement.be

signing and encryption of tender documents, and (3) the e-Catalogue platform,[275] which offers a collaborative environment for companies to upload their catalogues and manage their dossiers while furthermore enabling the reception of electronic orders and the modification of orders' status. In March 2008 the implementation of the last two platforms has been started.[276] These data belong to the responsibility of the Central Government (Federal), Federal e-Procurement Service within the Federal Department Staff and Organization, Directorate of the Official Journal (Belgian Moniteur), Bulletin of Adjudications (BDA). It provides links to portals and platforms which currently cover three of the various phases of the procurement process, namely; e-Notification, e-Tendering and e-Catalogue.

The sophistication stage is 4/4.

- Federal e-Catalogue platform:[277] Also undergoing a pilot implementation phase**,** the e-Catalogue platform[278] offers a collaborative environment for companies to upload their catalogues and manage their dossiers while furthermore enabling the reception of electronic orders and the modification of orders status. On this platform, public officers can consult catalogues and place purchase orders. They can moreover follow up the order status and create an acceptance report. Lastly, the application provides the necessary tools for supporting the management of a dossier covering the visualization and modification, as well some management activities relating to the catalogues. More information on the platform can be viewed at the relevant case page of the e-Practice portal: http://www.epractice.eu/cases/2581.
- Regional e-Tendering portal of the Walloon region and the French-speaking Community:[279]
  Some regional, community and local authorities have developed their own e-Tendering portals. For instance, the Walloon region and the French-speaking Community share the same portal.

10.8 Certificates (birth and marriage): request and delivery[280]

Requests of certificates are handled by individual municipalities (communes). The federal portal Belgium.be provides access to general information on the procedures related to obtaining these certificates. In the Brussels Region, a secure electronic counter system named IRISbox[281] and featuring the use of digital signatures enables citizens to securely request and pay for civil certificates online (birth, marriage, death, residence, nationality, etc.). Payment is made for a set of 10 certificates at once. The system is provided by the Brussels Regional Informatics Center (BRIC) and is currently used by 5 of the 19 municipalities of the Brussels Region. The **r**esponsibility belongs to Local Government (Communes) - in partnership with the regional government for the Brussels region.

---

[275] https://ecat.publicprocurement.be
[276] Sophistication ratings quoted in Capgemini, *The user challenge. Benchmarking the supply of online public services*, available at <http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf>, last consulted 31 August 2008.
[277] https://ecat.publicprocurement.be/
[278] https://ecat.publicprocurement.be
[279] http://marchespublics.wallonie.be/fr/index.html
[280] http://www.belgium.be; http://www.bruxelles.irisnet.be/
[281] http://www.bruxelles.irisnet.be/fr/servicesl/services/irisbox/irisbox_c.shtml

The sophistication stage is 4/4.

10.9 Annexes

10.9.1 Annex I: legislation

The Legal framework

- There is currently no overall eGovernment legislation in Belgium. The main legal framework for eID cards can be found in
  - the Law of 19 July 1991 regarding the population registers and identity cards, which is the basic legal source;[282]
  - the Law of 25 March 2003[283] modifying the law of 8 August 1983 establishing a National Register of natural persons and the Law of 19 July 1991 regarding the population registers and identity cards and modifying the law of 8 August 1983 establishing a National Register of natural persons, modernizing the existing registers;
  - the Royal Decree of 25 March 2003[284] on identity cards, introducing the basic provisions with regard to the eID card;
  - the Royal Decree of 5 June 2004[285] establishing a system of rights of access to and correction of the information which is electronically stored on the identity card and of the information stored in the population registers or in the National Register of natural persons;
  - the Royal Decree of 1 September 2004[286] related to the general introduction of the electronic identity card, through which the roll-out was extended outside of pilot communes.
- The main legal frameworks for the Crossroads Banks is laid down in
  - the Law of 16 January 2003 establishing a Crossroads Bank of Enterprises, modernizing the trade register, establishing accredited enterprise counters and pertaining to diverse other provisions';[287]
  - the Law of 15 January 1990 establishing and organizing a Crossroads Bank of social security.[288]
- Concerning electronic signatures and certification service providers the legal framework can be found in:
  - Law on the use of Electronic Signature in Judicial and Extra-Judicial Proceedings[289]

[282] O.J., 3 September 1991.
[283] O.J., 28 March 2003.
[284] O.J., 28 March 2003.
[285] O.J., 21 June 2004.
[286] O.J., 15 September 2004.
[287] O.J., 25 February 2003.
[288] O.J., 22 February 1990; err. O.J., 2 June 1990 and 2 October 1990.

This law of 20 October 2000 introduced the use of the electronic signature within judicial and extra-judicial proceedings. It has been the first law to address the eSignature issue.

- Law laying down a legal framework for electronic signatures and certification services[290]

  The so-called "e-Signature Act" Law of 9 July 2001 establishes certain rules with regard to the legal framework for electronic signatures and certification service providers.[291] This decree transposes into Belgian Law the Directive 1999/93/EC[292] of 13 December 1999 on a Community framework for electronic signatures. It gives legal value to electronic signatures and electronically signed documents while setting up a legal framework for certification services. It furthermore literally translates the definitions of advanced and "qualified" electronic signature that are laid down in this directive. In accordance with the directive, the act foresees that the use of electronic signatures in the public sector may be subjected to additional requirements, provided that such requirements are objective, transparent, proportionate and non-discriminatory. Also, they may only relate to the specific characteristics of the application concerned and may not constitute an obstacle to cross-border services for citizens in the EU.

  It is worth mentioning that at regional level in Wallonia, a law on electronic forms signed with the eID card and two related decrees have been adopted in December 2006 by the Walloon Parliament and in July 2007 by the Walloon Government respectively.These decrees give the same legal value to electronic forms as that of paper forms. The user will fill in an electronic form and sign it with its eID. The Walloon Region is the first authority in Belgium to propose this possibility.

  Moreover, the legal framework for the use of electronic identity cards is set in a series of Royal and Ministerial Decrees: Royal Decree of 25 March 2003 on the legal framework of electronic ID cards; Ministerial Decree of 26 March 2003 on the format of electronic ID cards; Royal Decree of 1 September 2004 on the generalization of electronic ID cards; and Royal Decree of 18 October 2006 on the eID document for Belgian children under 12.

- Law on the right of access to administrative documents[293]

  The right of access to documents held by the public sector is guaranteed by Article 32 of the Belgian Constitution, which was amended in 1993 to provide everyone with a right to consult any administrative document and have a copy made, except in the cases and conditions stipulated by the laws, decrees, or rulings referred to in Article 134.39.

  This constitutional right is implemented at federal level by the 1994 law on the right of access to administrative documents held by federal public authorities. The text allows individuals to ask in writing for access to any document held by federal authorities and

[289] http://mineco.fgov.be/information_society/e-signatures/law_e_signature_001.pdf
[290] http://mineco.fgov.be/information_society/e-signatures/law_e_signature_002.pdf
[291] O.J., 29 September 2001.
[292] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML
[293] http://www.mumm.ac.be/Downloads/bmdc_LOI-WET_11_04_1994.pdf

can include documents in judicial files. The law also includes a right to have the document explained.

Government agencies must respond immediately, or within thirty days if the request is delayed or rejected. Each decision must include information on the process of appealing and name the civil servant handing the dossier.

A law of 1997 provides for the same kind of transparency obligations for provinces and municipalities. Furthermore, the Flanders region/community, the French community and the Brussels region have also adopted their own legal acts on the right of access to administrative documents.

- Data Protection/Privacy Legislation: Law on the protection of private life with regard to the processing of personal data[294]

  The so-called "Privacy Law" of December 1992 is intended to protect citizens against the abusive use of personal data. The law defines the rights and duties of both the data subject and the processor. Moreover it provides a legal basis for the creation of an independent body in charge of overseeing its respect, namely the Commission for the Protection of Privacy.[295]

  Since its promulgation this law has undergone major modifications. It has been notably modified in 1998 in order to transpose the EU Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC).[296] The Privacy law was last amended in 2003 to take into account the fast developments occurring within the Information Society. The status, composition and competences of the Commission for the Protection of Privacy have been modified in accordance with the new requirements. This law is now available in its 'consolidated version' dated of August 2007.

- e-Commerce Legislation

  Two laws on certain legal aspects of information society services were adopted on 11 March 2003 and published in the Belgian Official Journal on 17 March 2003. Both texts define the essential concepts underpinning electronic commerce. Among others, they lay down information and transparency requirements with particular regard to consumers while regulating advertisement on networks (including spamming), removing obstacles to the conclusion of contracts by electronic means as well as determining the responsibilities and duties of intermediaries (site hosts, access providers, etc).

  Those 'e-Commerce laws' transposed the EU Directive on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (the so-called "e-Commerce Directive" - 2000/31/EC)[297] into Belgian Law.

- e-Communications Legislation: Law on electronic communications

[294] http://www.privacycommission.be/fr/static/pdf/wetgeving/loi_vie_privee.pdf
[295] http://www.privacycommission.be/fr/commission/
[296] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
[297] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML

The law on electronic communications was adopted on 13 June 2005 and published in the Belgian Official Journal on 20 June 2005. It was intended to transpose the EU regulatory framework for electronic communications[298] into Belgian law.

Since several anomalies were retrospectively found out in this law, the Belgian Council of Ministers approved on 14 July 2006 a draft law (*"avant-projet de loi")* in order to correct the identified deficiencies.

In addition, a specific law containing provisions relating to spamming[299] was adopted on 24 August 2005[300] so as to transpose the related article of the EU Directive 2002/58/EC[301] on privacy and electronic communications (the so-called 'e-Privacy Directive').

- e-Procurement Legislation
  - Law on public procurement and several public works contracts, public supply contracts and public service contracts[302]

    This law of 15 June 2006 was modified on 12 January 2007 and published in the Belgian Moniteur of 15 February 2007.
  - Law on the acceptance of bids, information to candidates and principals as well as time limits with regard to public procurement and several public works contracts, public supply contracts[303]

    This law of 16 June 2006 was modified on 12 January 2007 and published in the Belgian Moniteur of 15 February 2007.

  Although they are not yet in force, these two laws form the new public procurement legal framework of Belgium. They transpose into Belgian Law the EU Directives on public procurement, namely: the Directive coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors (2004/17/EC)[304] and the Directive on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts (2004/18/EC).[305]

  They grant electronic means of procurement with the same legal value as that of traditional means. In addition, they define new concepts based on the above mentioned public procurement directives, namely the electronic auctions and the dynamic purchasing system.
- Re-use of Public Sector Information (PSI)

[298] http://ec.europa.eu/information_society/topics/telecoms/regulatory/new_rf/index_en.htm
[299] http://www.droit-technologie.org/legislation-212/loi-sur-les-services-financiers-a-distance-et-sur-le-spamming.html
[300] O.J., 31 August 2005.
[301] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
[302] http://reflex.raadvst-consetat.be/refLex/pdf/Mbbs/2007/02/15/103089.pdf
[303] http://reflex.raadvst-consetat.be/refLex/pdf/Mbbs/2007/02/15/103090.pdf
[304] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0017:EN:HTML
[305] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0018:EN:HTML

- Law transposing the directive 2003/98/EC on the re-use of public sector information[306]

  This law of 7 March 2007[307] adopted at federal level transposes into Belgian law the general principles governing the re-use of public sector information in line with the provisions of the relevant EU Directive 2003/98/EC.[308]

- Royal Decree establishing the procedures and time limits for the handling of requests for public sector information re-use[309]

  This Royal Decree of 29 October 2007[310] regulates formal aspects related to the procedure and timelines for handling public sector information re-use requests.

- The eGovernment policy co-ordination is governed by formal agreements[311] among all governments. The regional and community governments had to equally transpose the Directive on the re-use of public sector information. Flanders, the Brussels region and two Communities (French and German-speaking) have also their own legal texts (decree) which are greatly inspired from the relevant federal legislation.

  The implementation has a decentralized approach, but with co-ordinated planning and programme management and permanent co-operation between government levels and government bodies.

  Because there are five different levels in Belgium (federal, community, regional, provincial and municipality) integration was necessary. Otherwise, citizens and companies don't know which authority to address with which question. In March 2001[312] a co-operation agreement has been concluded between the federal State and the communities and regions with regard to constructing and operating a common E-platform. It has been signed by the Federal State, Flemish Community, French Community, German-speaking Community, Flemish Region, Walloon Region, Region of Brussels-Capital, Flemish Community Commission, French Community Commission and Common Community Commission. There also was the intention to involve provinces and municipalities. A second co-operation agreement has been launched in 2005.[313] Principles concerning an integrated eGovernment can be found in an intergovernmental co-operation agreement of 28 August 2006[314] (B.S. 19.10.06).

  The aim of the co-operation agreement is to use information and communications technology to transmit information to all citizens, companies and other organizations and authorities in a user-friendly way. It also is to offer the opportunity to carry out electronic transactions with the authorities in a trusted, secured environment. The co-operation consists of the building, co-ordinating and operating an integrated E-platform. This is an electronic platform facilitating rapid, direct communications

[306] http://www.kafka.be/doc/1194970906-4682.pdf
[307] O.J., 19 April 2007.
[308] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0098:EN:HTML
[309] http://www.kafka.be/doc/1194970926-9944.pdf
[310] O.J., 6 November 2007.
[311] See http://www.belgium.be/eportal/application?pageid=contentPage&docId=20434.
[312] O.J., 8 March 2001.
[313] See : http://www.corve.be/overegov/regelgeving/beleid_samenwerkingsakkoord.php
[314] O.J., 19 October 2006.

between government and citizens, companies and other organizations, as well as among the parties themselves.

Moreover an integrated middleware environment is in development for the organization of the exchange of structured electronic messages between three types of components: portals, websites and back-end information systems. They can receive and send electronic messages from and to the integrated middleware environment, either directly or indirectly through their own middleware environment.[315]

Similar infrastructure elements are implemented at regional level. For instance, in February 2006, the Coordination Cell for Flemish eGovernment (CORVE) launched VKBO-GO, the online application of the Flemish Crossroads Bank for Enterprises**.** Users of this application can consult the Flemish Crossroads Bank for Enterprises, which contain authentic data on Belgian enterprises. More and more public servants, as well as local governments, use the VKBO-GO. It is expected that this usage will increase even more as the use of this authentic data results in a considerable reduction of the administrative burden for enterprises, thus facilitating the simplification of governmental processes.

10.9.2 Annex II: various services

Car registration (new, used, imported cars)[316]

The service has been fully integrated through the WebDIV[317] application that allows insurance companies and car dealers to register cars online. The information requested for the registration of a vehicle actually consists of four number items on the basis of which all other information is available.

This matter falls under the responsibility of the Central Government (Federal), Federal Department Mobility and Transport, Vehicles Registration Directorate

The Sophistication stage is 4/4.

Personal documents: passport and driver's licence

- Passport[318]

  The Central Government (Federal), Federal Department Foreign Affairs is responsible. It only concerns information. Passport applications are handled by local authorities (communes) according to their own processes.

  The sophistication stage is 1-2/4 (Average sophistication level of procedures related to personal documents)

- Driver's licence[319]

[315] Deprest, J. and Robben, F., *eGovernment: the approach of the Belgian federal administration*, available at <http://www.ksz-bcss.fgov.be/documentation/fr/documentation/Presse/2003%20-%20E-government%20paper%20v%201.0.pdf>, last consulted 31 August 2008, p. 43.
[316] http://www.leaseconnect.be/
[317] http://www.leaseconnect.be/licenseplatesFR.asp
[318] http://www.diplomatie.be/fr/travel/passports.asp
[319] http://www.diplomatie.be/fr/travel/passports.asp

The Central Government (Federal), Federal Department Mobility and Transport is responsible. It only concerns information. Driving licence applications and renewals are handled by local authorities (communes) according to their own processes.

The sophistication stage is 1-2/4 (Average sophistication level of procedures related to personal documents)

Registration of lease contracts

The lessor must register all the lease contracts in a delay of 2 months after signature. This is possible via www.myrent.be. He can use a digital qualified certificate or his eID.

E-cops

This is an online point for declaration of criminality on internet. It is an initiative of the Federal Computer Crime Unit of the Federal judicial Police.

Police-on-web[320]

As of June 2007, Belgian citizens can report a number of crimes to the police online 24 hours a day through the new Police-on-Web[321] service. Via Police-on-web everybody can declare a crime (e.g. theft, vandalism, …). Belgian citizens can report a number of crimes to the police online 24 hours a day through the Police-on-Web[322] service. To register an e-Complaint, people need to use their eID card or token. The declaration is done with the electronic Identity card. Any violent or dangerous crime requiring an immediate police response should be reported to the police in the traditional way.

This topic falls under the responsibility of the Central Government (Federal), Federal and Local Police.

The sophistication stage[323] is 3/3.

De Lijn (subscriptions)

De Lijn is the bus and tramway firm in Flanders. With the electronic Identity card, a device (card reader) and a certificate on the computer a subscription can be ordered. The Flemish public transport company De Lijn implements its electronic sales point. Travellers with an eID card and card reader can buy their season ticket from home via the website. Through the Flemish Government's MAGDA platform for data exchange, the web application retrieves the necessary data on the family composition details of the traveller.

Agriculture electronic service desk

In August 2007 has been presented the Agriculture electronic service desk. Farmers only need to register their farming parcels once, resulting in a considerable administrative burden reduction. The exchange of this data is made possible by the MAGDA platform of CORVE.

Small and Middle sized Enterprises test

---

[320] https://www.epol.be/eloket/

[321] http://www.belgium.be/eportal/application?origin=onlineServicesHome.jsp&event=bea.portal.framework.internal.refresh&pageid=contentPage&docId=44611.0; www.belgium.be/

[322] https://www.epol.be/eloket/

[323] Sophistication ratings quoted in Capgemini, *The user challenge. Benchmarking the supply of online public services*, available at <http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf>, last consulted 31 August 2008.

The DG Research of the European Commission proposes on its website[324] the SME test developed by the Walloon Region; this test allows an enterprise to know if it is considered as an SME by Europe and Member states. This test is proposed to the European enterprises willing to participate in a research program.

Employment : 'first job' card[325]

Since 1 April 2007, young Belgian jobseekers, under the age of 26, holding an eID card are able to apply online for a 'first job' card[326] from the National Employment Office.[327] 'First job' card holders are eligible for an initial employment contract which allows them to find work more easily in Belgium. Within 24 hours, the card is completed and sent by email in PDF format. 'First job' card holders are eligible for an initial employment contract, or CPE, which allows them to find work more easily in Belgium. Employers are legally obliged to engage a quota of young people on such CPE contracts. As the young worker usually has fewer formal qualifications, the employer receives a reduction in employers' contributions in return for taking them on. There are greater employers' reductions for those taking on youngsters without training, with special needs, or those who come from outside the European Union. From now on, youngsters will be able to apply for their cards on the National Employment Office website. They fill in an on-line form with details of their qualifications and whether they are registered as job-seekers. They are also asked whether they have special needs, or whether they are from abroad. Within 24 hours, the CPE card is completed and sent by email and PDF format. It can then be sent to an unlimited number of potential employers.

In order to apply, young people will need an electronic identity card or a citizen's card, available from the Belgian national website.[328] For those without computer access, paper forms are still available.

Employment: Job search services by labour offices[329]

The websites of the Regional Employment Offices allow users to post their CVs online, browse and search job ads, obtain information about companies/organizations that recruit and about professional training programs. All three websites furthermore provide a link to a specific application, namely the 'Front Office Employment',[330] which allows the job seeker (in particular the unemployed persons) to know which financial support he/she is entitled to receive in order to help him/her to find a job, and employers to look for which subsidies (or financial help) a company can receive when hiring specific categories of people. This application integrates an overview of all employment stimulating measures in a particular situation, the prior conditions to qualify for these measures and the application procedure to benefit from them. It belongs to the responsibility of the Regional Government, Regional Employment Offices.

The sophistication stage is 4/4.

---

[324] http://ec.europa.eu/research/sme-techweb/index_en.cfm
[325] http://www.epractice.eu/document/64.
[326] European Communities, *BE: Young job-seekers aided by on-line 'first job' cards*, available at <http://www.epractice.eu/document/64>, last consulted 31 August 2008.
[327] http://www.onem.be/
[328] http://www.belgium.be
[329] http://www.leforem.be/ (Wallonia); http://www.vdab.be/ (Flanders); http://www.actiris.be (Brussels region).
[330] www.autravail.be in France and www.aandeslag.be in Netherlands.

Public libraries (availability of catalogues, search tools)[331]

It concerns Information and online catalogue for Flanders and German-speaking libraries, and information only for French-speaking community libraries. An online common catalogue of the Federal Departments Libraries is available on the Federal Portal Belgium.be.[332] The responsibility belongs to the Central Government, Community/Regional Government.

The sophistication stage is 3-4/5.

Enrolment in higher education/university[333]

The Community Government is responsible**.** It only concerns information.

The sophistication stage is considered to be 1-2/4.

Announcement of moving (change of address)[334]

The federal portal provides information on change of address notification. Notifications are handled by individual communes. Since the end of May 2004, citizens can e-Notify their change of address to the commune provided the local authority in question is accessible via the Internet. The local Government, the Municipalities are responsible.

The sophistication stage is 2/4.

Health related services (interactive advice on the availability of services in different hospitals; appointments for hospitals)[335]

Be-Health is an integrated platform aimed at delivering all health and healthcare-related information and services online through a single portal. It provides among others health-related information and advice for citizens, secure electronic communication between health professionals as well as among citizens and healthcare institutions/ organizations, and collects health-related data (e.g. spending, statistics, etc.). This platform makes extensive use of eGovernment infrastructure services (e.g. federal intranet, eID card). The Central Government (Federal Department Health, Food Security and Environment) and Regional Government is responsible.

The sophistication stage is 1/4.

Application for building permission

Each region has its own legislation regarding building permission. Applications are managed by individual local authorities (communes) according to their own processes. The **r**esponsibility belongs to the Regional and Local Government, Municipalities

The sophistication stage is 2/4.

---

[331] http://www.bibliotheek.be/ (Flanders); http://www.cfwb.be/biblio/ (French Community); http://www.mediadg.be/ (German-speaking community); http://www.bib.belgium.be/Search.aspx?lang=0 (Federal Department Libraries).
[332] http://www.bib.belgium.be/
[333] http://www.ond.vlaanderen.be/hogeronderwijs/ (Flanders); http://www.enseignement.be/ (French Community); http://www.dglive.be/ (German speaking community).
[334] http://www.belgium.be
[335] https://www.behealth.be/

11 Germany

Since the start of the new millennium the Federal Government in Germany has started several initiatives which are considered to constitute the eGovernment. Many of these initiatives have raised new issues concerning identity management and are therefore worth discussing. However, the political debate about identity management is still in an early stage. This can be deduced from the fact that there are neither concrete plans for a comprehensive and integrated system for facilitating identity management nor the legal, technical and organizational preconditions for developing such a system in the near future. At present, the basic policy aims at digitizing the existing means for the definition, authentication and administration of identities of German citizens, i.e. the registers of residence and the personal documents.

11.1 Background

Germany is a federal republic made up, subsequent to its reunification in 1990, of 16 states (*Bundesländer*). These states have their own legislative and executive bodies. Within the federal system, the municipalities (*Städte, Gemeinden, Kreise*) are the lowest level in the three tier administrative structure after the federal government and the states.

Due to the Federalism Reform Agreement between the Federal Government and the 16 State Prime Ministers the legislative authority for civil registration has been shifted from the state to the federal level. Thus identity management is now increasingly developed and co-ordinated by the federal government, which has to seek agreement with the state governments and municipalities, as they still have the authority for technical and organisational implementation of the law and the responsibility for identity management solutions in the context of their legal obligations (e.g. parts of the social insurance system).

11.2 eGovernment initiatives

One of the first German eGovernment initiaitives was the 'BundOnline 2005'[336] programme which commenced in 2000 and came to an end, as planned, in December 2005. The result of this programme was that 440 of the Federal Government's administrative services were made available online. In September 2006 the Federal Government adopted the new programme 'E-Government 2.0'.[337] This programme aims to define the major strategic objectives concerning eGovernment action plan as part of the European Union's i2010 initiative.[338] The objectives concern the identification and communication in the area of eGovernment. Furthermore, they intend to enhance the federal eGovernment services in terms of quantity and quality, and to establish electronic collaboration between the public administration and the business community utilising common business process chains. In addition to the latter, there is also the 'Deutschland Online'[339] initiative, which has been adopted by the Federal Government, states and municipalities. This initiative provides the framework for cooperation and

[336] http://www.bundonline2005.de/
[337] http://www.staat-modern.de/Anlage/original_1070438/E-Governemt-2.0-Das-Programm-desBundes.pdf
[338] http://europa.eu.int/information_society/eeurope/i2010/index_en.htm
[339] http://www.deutschland-online.de/

coordination between all administrative layers. To cope with this interoperability challenge a number of standards for data exchange were developed and co-ordinated by the OSCI-Leitstelle.[340] Examples for these standards are OSCI v2.0 for governmental web-services and XMeld for the transfer of citizen's register's data (see paragraph 1.1.3).

However, these initatives so far have put Germany already forward in the context of eGovernment. In the i2010 benchmark carried out in 2007 Germany is ranked on position 10 regarding the sophistication of online services and position 8 regarding the availability of online services.[341]

11.3 Identity resources

Most relevant for the issue of eIDM are the citizens' registers of residence (*Melderegister)*, the civil status registers (*Personenstandsregister*) and the business register (*Unternehmensregister*). For German citizens the citizens' register and the civil status register are root registers. Every identity established in the context of e-government refers to these registers. These registers are run on the municipality level.

In Germany every citizen aged 16 or older is obliged to have an Identity Card (*Personalausweis*). This identity is renewed typically after 10 years; as a result national identity-card-numbers are not permanent, as they change with every newly issued Identity Card. The e-passport is an optional document for international travel purposes. It is valid for 10 years, after which a new passport with a new passport number is issued. The passport number also is stored in the citizens register. Both documents are issued based on national standards by the municipalities.

Besides the mandatory Identity Card, there are several sector-specific and also mandatory identity resources, in particular a social security number and a federal tax number. These numbers are issued for every citizen and do not change during the life. The tax number also is stored in the citizens register, so sectors are not separated in any case. These numbers are issued directly by or by order of federal offices responsible for the corresponding sectors.

For sector specific purposes there are additional registers in Germany. They e.g. refer to the work of social services, the car registration office, secret services and the police. They are set up and run based on sector specific legislation. In many cases they are also based on the citizens register, as they take over citizens register's data either directly or indirectly via the national Identity Card. These additional registers are run mainly on the federal and the federal state's level.

11.3.1 Identity Card

The Identity Card is issued by the municipality of the residence of the holder, but they are centrally produced by the Federal Printing Office. The document number is a unique serial number, which in fact constitutes a unique personal identity number. However, in Germany there is no unique personal identity number as a central identity resource. This is due to the

[340] http://www1.osci.de/sixcms/detail.php?id=1181
[341] Statistisches Bundesamt Deutschland, *Statistisches Jahrbuch 2008,* 2008, available at <http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Publikationen/Querschnittsveroeffentlichungen/StatistischesJahrbuch/JahrbuchDownload,templateId=renderPrint.psml>, last consulted 6 October 2008.

census decision (*Volkszählungsurteil*) of the Federal Constitutional Court (*Bundesverfassungsgericht*) of 1984 and its interpretation by the Federal Parliament (*Deutscher Bundestag*) that according to this sentence the constitution does not allow a unique personal identity number. Instead, natural persons are identified by a combination of attributes such as first and family name and date and place of birth.

Furthermore, according to § 3 Identity Card Act, it is explicitly forbidden to use this document number for accessing personal data in files or for linking data in different files. The special machine-readable code is technically not suited for online authentication. But this will change, when the present paperbased ID card will be substituted by a digital ID card from 2008 or 2009 onwards.

11.3.2 Passport

As in the rest of the European Union, the paper-based passports in Germany are gradually being exchanged for a new digital passport (Elektronischer Reisepass, ePass). In accordance with European Directive 2252/2004 it contains an RFID chip with digital personal data, a digital photo of the face of the owner and from 2007 on also two digitized finger prints of the owner. The new passport is not intended for use in electronic communication beyond border control. It however sets standards for the use of biometric identifiers.

Both the old as the new passports carry a serial document number, which, as aforementioned, may not be used for the access to or the linking of personal data.

11.3.3 Sector specific identifiers

In horizontally defined sectors of government such as tax administration, there are sector-specific IDs such as the number for the German pension insurance fund (*Sozialversicherungsnummer*), the health insurance number, ID for draftees or the recently introduced federal Tax ID (*Steuernummer*).

11.3.4 Citizens registers of residence

The civil registers of residence (*Melderegister*) in Germany are maintained by the local municipalities.

The Federal Ministry of the Interior is at present preparing a Federal Registration Act (*Bundesmeldegesetz*), which will be added to the state law (*Melderechtsrahmengesetz*) as the primary source for the regulation of data processing. According to this new legislation, expected for 2009, in addition to the citizens' registers of residence an integrated copy register is planned on the federal level as a new standardised and centrally available source of registration data for federal offices.

The shift of the legislative authority for civil registers to the federal level will probably lead to a federal central register, which will be fed from local registers. It is envisaged that this central register could play an important role in the identification processes with many other government entities at all levels. However this is still disputed, as a federal law need also to be approved by the federal states in the Federal Council of Germany. For that reason, the Federal Registration Act is being coordinated with the federal states and they currently have much input.

State law on civil registers of residence may allow the collection of additional data and procedural provisions. Most states allow the registration authorities to assign reference

numbers in the register. These may only be used for special purposes and not as unique personal IDs.

The Federal Directive for the interchange of registration data (*Bundesmeldedatenübermittlungsverordnung*), based on the Citizens Registration Frame Act has recently been revised and a data exchange format (XMeld) has been made mandatory for all registration offices. They may keep their different software systems, but by adding a special interface these have to be able to import and export data according to the XMeld standard.

If the Act leads to a central register, then the most of the direct interchange of register data between the local registers will become obsolete. But it is most likely that XMeld will still be used for interchange between central and local registers and the interchange with third parties.

11.3.5 Civil status registers

The registration data of residence and the data on the civil status are not stored together, although the local authorities are responsible for both. Normally the city's registrar in the civil status office (*Standesamt*) is responsible for recording births, marriages and deaths. For data interchange between offices, a combination of the following attributes is used: name of office, name of civil status register (*Personenstandsbuch*) and entry number.

At present, paper as storage medium is used for register entries. However, in February 2007 the Personal Status Law (*Personenstandsgesetz*) was passed. This law allows data storage in electronic form in civil status registers (*Personenstandsregister*) as of January 2009.

11.3.6 Business registers

There are several registers of companies. Most important are the Commercial Registers (*Handelsregister*). Responsible for those registers are the Local Courts (*Amtsgerichte*). The data of the Commercial Register is stored and administered in electronic form. As a complement, the Companies Register (*Unternehmensregister*) was introduced in 2007 providing additional information, which has to be published in the Official Federal Gazette. The database is run by a private entity, the Publisher of the Federal Gazette (*Bundesanzeiger Verlag*). As a link between companies information from "Bundesanzeiger" and "Handelsregister" an internal identifier is used (*UnternehmensID*). Recently first steps have been made to set up IDs for companies across sectors using the Business Identification Number and the Turnover Tax Identification Number.

11.3.7 Digital signatures

Regarding digital signatures, Germany was the first member state in the European Union to pass legislation in 1997, which has since been adapted to the European directive in 2001. However, even on the level of qualified signatures German signature cards are on purpose not suited for reliable identification because they only contain first name and family name of the holder and no additional relevant attributes such as the date of birth.

11.4 Policies

Currently there are no eID cards in use in Germany. The Federal Government passed an eCard strategy in a cabinet decision on 9th March 2005. This decision mainly concerns the electronic passport (*ePass*), the electronic health card and the electronic identity card (*ePA*).

11.4.1 eHealth Card

The Federal Ministry of Health (*Bundesministerium für Gesundheit)* is responsible for the electronic health card. To identify the patient, the card shall be provided with a photo. Optionally, an electronic signature shall also be possible. The electronic health card is intended to facilitate processes in the health system and to make the patient data digitally available to the physician.

The general concept of the German e-health card was already introduced and described in the FIDIS Deliverable D 4.2 "Set of requirements for interoperability of Identity Management Systems" in chapter 12.6 in 2005.[342] Meanwhile the project has made significant progress. The technical specifications are finalised, prototypes for the field testing are available and the 3rd phase of the tests (10.000 participants in seven regions in Germany) is in progress.[343] Data Protection Commissioners were involved in the concept and testing phase and approved the security and data protection concept of the e-health card.[344]

The intensive testing already shows its value. With respect to usability the current concepts obviously has limitation. Elderly users of the e-health card are obviously not always able to handle the 6 digits long PIN appropriately. For this reason parts of the testing were remedied in one of the test regions.[345] Currently a working group organised by the gematik,[346] the organisation responsible for the standardisation and technical concept, is looking for alternative implementations.

11.4.2 eID Card

The eID Card (*elektronischer Personalausweis*), planned for being issued from 2008/2009 onwards, shall replace the traditional paper-based identity card (*Personalausweis*). The eID Card will become a universal token for authentication and identification on the Internet for eGovernment and eBusiness services.[347] For this purpose, features for electronic authentication and for digital signatures will be implemented. The chip[348] on the card will contain the same information which is printed on the card today.

A special emphasis in this concept is put on security and data protection aspects of the authentication functionality. Terminals or online service providers need a certificate to be able to access the authentication information on the eID. An access control scheme restricts the access to that information on the eID that is needed for the purpose of the service offered. In addition the eID holder is technically able to restrict the access rights of the service provider further.[349]

---

[342] See http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.2.set_of_requirements.pdf
[343] See http://www.die-gesundheitskarte.de/index.html
[344] See e.g. http://www.gesundheitskarte-sh.de/, message from January 18th 2008.
[345] http://www.gesundheitskarte-sh.de/, message from April 11th 2008.
[346] See http://www.gematik.de/(S(jzfz2p45ynakhs55rrz4ndys))/Homepage.Gematik
[347] http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen,did=60006.html
[348] The chip will be wireless and store additional electronic data such as a digital biometric picture of the face and the digital images of the two index fingers. Basis Access Control (BAC) and Extended Access Control (EAC) are supported as access control mechanisms.
[349] The technical concept is in accordance with the ICAO standards for Machine Readable Travel Documents (MRTD), the technical directive TR-03110 for Advanced Security Mechanisms for MRTDs and the standards of CEN/TC224WG15 covering identification card systems, especially the European Citizen Card (Bender, J. et al.., 'Sicherheitsmechanismen für kontaktlose Chips im Deutschen elektronischen Personalausweis' Safety mechanisms for contactless Chips in German electronic Identity Card], *Datenschutz und Datensicherheit,*

As the card shall be used for authentication in the private sector as well, and because in different contexts different parts of the total data are necessary, there will be a function to allow the holder to control which data can be read in a specific situation. For example, when an age control is required, only the data from the age field can be read.

11.4.3 Citizens' portals

In the context of the European Directive 2006/123/EC[350] simplifications to access markets in European member countries for service providers are to be implemented by end of 2009. One important aspect is the creation of "points of single contact".[351] In the context of a federated governmental administration this requires adjustment of the corresponding legislation and the setup of a technical infrastructure to facilitate cross-administration workflows.

In the context of the initiative "Deutschland Online" (Germany Online) the planning phase for the implementation of the legal grounds (responsibility for the pilot: Federal State of Schleswig.-Holstein) and technical infrastructure (responsibility for the pilot: Federal State of Baden-Württemberg) started in November 2007.[352] Meanwhile a number of workshops were carried out and work on a so called blue print, a description of the model for the steps and components required to implement the directive, is in progress. It is planned to finalise the blue print by mid of 2008.[353]

To enable the delivery of official documents a technical infrastructure is needed to meet security requirements with respect to confidentiality, authenticity and non-repudiation. The technical concept for such an infrastructure currently is developed in the context of the project citizen's portals.[354] The concept is open for the implementation by different internet service providers. Core element of the concept is a mail account of an identified citizen. This account can be used for the transfer and delivery of official documents and authentication in the context of governmental services. The authentication functionality is meant as a pre-step for the online authentication function to be implemented in the national eID card.

According to the E-Government 2.0 Programme the portals will integrate identity data of citizens and provide authentication services. Furthermore, they shall enable secure and anonymous online communication and serve as a safe storage place for important documents.

11.4.4 Governmental Gateways[355]

Web portals for governmental services in Germany already were developed in the late 1990s. Originally they started as pure information platforms and offered no interactive services or transactions to the citizen. To facilitate transactions a middleware is required, connecting web

---

volume 32, issue 3, 2008, pp. 173-177). Thus the concept also includes the use of the eID Card as Machine Readable Travel Document (MRTD).

[350] See http://www.entemp.ie/trade/marketaccess/singlemarket/07serv005.pdf

[351] See Art. 6 Directive 2006/123/EC

[352] See http://www.deutschland-online.de/DOL_Internet/broker.jsp?uMen=ea920482-4b88-e011-4fbf-1b1ac0c2f214

[353] See http://www.deutschland-online.de/DOL_Internet/broker.jsp?uMen=58c105dd-ba3e-a511-4fbf-1b1ac0c2f214

[354] Stach, H., 'Mit Bürgerportalen für einfach sichere, vertrauliche und verbindliche elektronische Kommunikation', *Datenschutz und Datensicherheit*, volume 32, issue 3, 2008, pp. 184-188.

[355] The difference between citizens' portals and governmental gateways is that the latter is a middleware for governmental applications (see the section 'Governmental gateways'), while the citizens' portals are the front end layer towards citizens.

portals with governmental procedures and related applications. This middleware typically is called a government gateway.[356] In the early 2000s the first government gateways were introduced. One of the first federal states establishing one was the Federal State of Hamburg in 2003.[357] Originally the gateway connected an authentication and payment infrastructure with an online access to the citizen's register in Hamburg. Now the Hamburg Gateway is an one-stop access point to a wide range of online services and offers a central authentification for registered citizens. It was taken up in the EU Good Practice Framework Database for e-government in 2006.[358] The technological platform of this gateway is now multi-client capable[359] and also used by other federal states such as Schleswig-Holstein.

11.5 Legal Framework

Data Protection

For data processing by public authorities, the Federal Data Protection Act (*Bundesdatenschutzgesetz*) stipulates the following principles: legal reservation, limitation of use to specific circumstances and data reduction and data economy. This means that it has to be guaranteed that only data are collected or used, which are necessary and which are permitted by the law.

Signature Act

In Germany, regulations on electronic signatures are mainly to be found in the Signature Act (SigG dated 16 May 2001, BGBl. I dated 21 May 2001, p. 876).The federal and state administrative procedure law stipulates that, in administrative procedures, the written form can be replaced by qualified electronic signatures according to the signature act (e.g., § 3a subsection 2 of the Federal Administrative Procedures Act).

Other important legal provisions with regard to identity management:

- Design and use of identity card and passport are regulated in the Identity Card Act and the Passport Act. If these documents are to be designed differently, for example, in order to be able to use them for electronic communication, these acts will have to be changed correspondingly.
- The authorities responsible for the identity cards (the citizen's registration offices at the municipality level) keep records on identity cards (§ 2a of the Identity Card Act). Among others, these local registers issue the identity cards and verify their authenticity. A nation-wide data file will not be established.
- The passport register is regulated parallelly (§ 21 Passport Act). The passport register is kept by the passport authorities (again the citizen's registration offices at the municipality level) who issue passports and verify their authenticity, the identity of the person who owns the passport or for whom it has been issued, and who executes passport law.

[356] See e.g. http://userp.uni-koblenz.de/~egov/wiki/de/index.php?title=GovernmentGateway
[357] See http://www.dataport.de/dataport/themen/e-government/governmentgateway/start.html
[358] See http://www.epractice.eu/index.php?page=gpcase.list&cntr=9&domain=5957&topic=0&srchbx=Hamburg&go.x=22&go.y=5
[359] The gateway is run by one operator (computer centre Dataport) on a shared physical infrastructure.

- The civil status registers are regulated by the Personal Status Law, which now also allows the electronic storage of these data.
- The statutory basis for commercial registers and company registers are laid down in § 8 and § 8b of the Commercial Code (Handelsgesetzbuch).

11.6 Interoperability

As described in section 1.1.3, interoperability between the local registers has been achieved by making the data exchange format X-Meld mandatory.

Further questions of interoperability mainly concern transborder usage. As there are no concrete technical specifications available, interoperability on the different levels cannot yet be assessed. However, in presentations of the plans and in EU working groups, people responsible for this project in the Federal Ministry of the Interior (*Bundesministerium des Innern*) stress that technical specifications will be in line with CEN and ISO standards and that they aim for pan-European interoperability on the application layer as well. The BMI takes part in the ad hoc group for eIdentity within the eGovernment Expert Group. The Procurement Office within the Federal Ministry of the Interior participates in a pilot application for interoperability in transborder e-procurement within the GUIDE project. Further, the Ministry is considering joining the consortium for the Large-Scale Pilot for interoperable eIDM.

The goals are in line with the eIDM roadmap, which aims for a federated structure with mutual recognition of the different technical systems.

12 Austria

Austria can be considered as one of the leading countries in the European Union when it comes to eGovernment initiatives. Since 2002 Austria is developing its e-Government strategy in two directions:[360]

- Building up online procedures to address the citizens
- Setting up internal methods and electronic procedures within government

To facilitate this in Austria a number of laws were enacted and modernised. This includes:[361]

- E-Government Act (see paragraph 12.5.1.)
- Electronic Signature Act
- Law on general governmental Procedures
- Official Documents Delivery Act including
  - Decree for the Delivery of official Documents in public Services
  - Decree for the Delivery of Forms in public Services
- Citizen's Register Act
- Act on governmental Sectors[362]
- Law on additional Registers [363]
- Law for the Use of Electronic Signatures in public Administrations
- An eGovernment modernisation Act of 2007, including a number of changes in the laws and acts mentioned above

On a technical level infrastructural core components were set up which are increasingly available now. These core components include: [364]

- Setup of an authentication infrastructure (citizen and administration cards, linked to citizen's registers and governmental directory services)
- Setup of an electronic communication infrastructure, electronic governmental procedures and related supporting services such as a time stamp service; in future the integration of traditional communication channels such as voice in electronic procedures is planned
- Setup of electronic payment systems

---

[360] See http://www.cio.gv.at/egovernment/strategy/
[361] See http://www.digitales.oesterreich.gv.at/site/5238/default.aspx
[362] In this act 26 governmental sectors and nine sector spanning activities are defined and named. The concept of these sectors plays a relevant role in the concept of authentication of citizen, see FIDIS Deliverable D3.6 "Study on ID Documents", chapter 5.5.
[363] This registers allow the integration of foreigners in the Austrian citizen's card concept and thus the authentication for certain governmental services.
[364] See http://www.digitales.oesterreich.gv.at/site/5240/default.aspx

- Setup and operation of an electronic signature scheme as well for the private as the public sector
- Setup of a trust seal for eGovernmental procedures; currently this seal has been issued for 21 governmental agencies and their services[365] and 28 commercial infrastructure or module providers[366]
- Security infrastructure[367]

This progressive approach has led to among others a comprehensive identity management initiative referred to as Citizen Card (Bürgerkarte), a project that was launched by the Austrian Federal Government and which is facilitated with the abovementioned eGovernment Act (E-Government Gesetz).

12.1 Background

Austria is a federal republic. Legislative and executive powers are divided between the Federal Parliament resp. Government and the nine Provincial Parliaments resp. Governments (Länder). At federal level, legislative power is held by a bicameral Federal Parliament (National Council and Federal Council). Executive power is held by the Federal Government, led by the Federal Chancellor, answerable to the National Council.

An ICT Strategy Unit has been installed at the Federal Chancellery. This group is responsible for the eGovernment Act and the Signature Act. Coordination on the federal level and with provinces, municipalities and local authorities is carried out by the ICT Board. The ICT Board is composed of the Chief Information Officers of all the federal ministries and their deputies. A Federal CIO is installed that chairs the ICT Board. An e-Cooperation Board allocates responsibility for the preparation of implementation projects and coordinates the implementation projects of the participating organisations (ICT Board, eGovernment working groups of the provinces and the public-administration bodies responsible for ICT). The two bodies ICT Board and e-Cooperation Board are coordinated by the ICT strategy platform "Digital Austria" which is led by the Federal CIO.

In short, the Federal eGovernment initiatives are coordinated by the ICT Board. While the regional and the local eGovernment is under the responsibility of the authorities in the provinces, cities and municipalities.

A reference server[368] has been set up by the provinces, which acts as a platform for communication between all levels of administration, on which proposals for working methods and concepts, contributions to discussions and conventions decided between the federal government and the provinces, are published.

IT activities at both provincial and federal level are coordinated in various working groups and priorities are set jointly in order to ensure an effective implementation of eGovernment. Working groups focusing on specific needs act together with the ICT Board to support the coordinating activities. This means that concepts and projects are agreed before decisions are

[365] See http://www.digitales.oesterreich.gv.at/site/5292/default.aspx#a13
[366] See http://www.digitales.oesterreich.gv.at/site/5282/default.aspx
[367] See http://www.cio.gv.at/securenetworks/
[368] http://reference.e-government.gv.at

adopted across all levels of administration. In this way, differences of opinion on an expert level can be avoided.

12.2 eGovernment initiatives

In the past Austria has taken decisive action to implement the eGovernment project swiftly and efficiently. In May 2003, the Austrian Federal Government launched an eGovernment initiative to coordinate all eGovernment activities in Austria. Two cross-departmental coordination bodies (ICT Board and e-Cooperation Board) were set up. At the same time, stock was taken of all ongoing activities and a roadmap was agreed. The obligations of the ICT Board and the e-Cooperation Board are coordinated by the ICT strategy platform. The joint presidency of these bodies by the federal CIO ensures a coordinated approach with no overlapping.

12.3 Identifiers

Registration of residents used to be on the local level, in many cases based on paper registers. The Central Register of Residents (CRR, Zentrales Melderegister) went operational on 1st March 2002 – the day when the new Registration Act (Meldegesetz) went into force. The CRR was based on data from a census that has been carried out in 2001. Note, that Austria has no obligation to carry or possess any official identity card.

Apart from the registration of residents, some sectoral or application-specific identity management systems and identifiers have grown over time.

For natural persons, the most widespread system providing unique identifiers used to be the health insurance and social security system. In conventional proceedings the social security number legally got used in a few other sectors, such as inter alia taxes, scholarships (Studienbeihilfe), tracking education (Bildungsevidenz), or building and loan association (Bausparen).

For legal persons and self-employed natural persons the tax number is used. The tax number is assigned by the tax authorities on request. Another tax identifier is the VAT number (Umsatzsteuer-Identifikationsnummer, UID). Further traditional unique identifiers for legal persons are the identifiers of legal persons in the Register of Company Names (Firmenbuch, Firmenbuchnummer) or the Central Register of Associations (Zentrales Vereinsregister, ZVR-Nummer).

12.4 Identity resources

12.4.1 Base Registers

For natural persons Austria maintains two registers: the Central Register of Residents[369] (CRR) and the Supplementary Register for Natural Persons (SrnP).

[369] http://zmr.bmi.gv.at

The CRR is operated by the Federal Ministry of Interior and it stores resident data and identity data. The identity data consists of name, gender, nationality, place and date of birth, and travel document data (type, number, issuing state and authority) for foreigners. The residence data is the entity's address, type of residence (main or second residence), the date of registration or deregistration and the name of the house owner or leaseholder. Moreover, a unique identifier CRR-number (ZMR-Zahl) is stored.

The SRnP holds – upon request by the entity concerned – natural persons that are not required to be registered in the CRR (e.g. expatriates, foreigners with no residence in Austria). The source PIN Register Authority is responsible for the SRnP, it recourses to the services of the Federal Ministry of Interior. The unique identifier's format is the same as the CRR-number. The record and the identifier can be transferred from the SRnP to the CRR to maintain unique identification, e.g. in cases where expatriates return to Austria, foreigners take residence in Austria, or vice versa.

For legal persons Austria maintains three registers: the Register of Company Names,[370]

the Central Register of Associations[371] and a Supplementary Register of Other Data Subjects[372].

The Register of Company Names is a public trade register under the responsibility of the Federal Ministry of Justice with a 6-digit identifier. The Central Register of Associations is maintained by the Federal Ministry of Interior and uses the 'ZVR-Nummer' as an identifier. Entities not covered by registers mentioned before can apply for being registered in a further supplementary register. Examples for such entities are churches, public authorities, foundations, municipalities, etc. The register is maintained by the sourcePIN Register Authority that recourses to services of the Federal Ministry of Finance.

Legal persons use the identifier (Firmenbuchnummer or ZVR-Nummer) in their communications both in conventional paper communication (e.g. letterheads), or in their electronic presence (e.g. an obligation to present the Firmenbuchnummer and the VAT number exists under the eCommerce Act).

For natural persons, however, the identifiers are under specific data protection constraints. The sourcePIN Register Authority plays an important role.

12.4.2 SourcePin Register Authority

The duties of the sourcePIN Register Authority are taken care of by the Data Protection Commission. The main responsibilities are to implement the citizen card concept and the cooperation with its service providers.

The sourcePIN is a unique identifier that is derived from base register identifiers for natural persons, i.e. the CRR-number or the SRnP-number. The sourcePINs are only stored in a so-called identity link (*Personenbindung*) in the citizen card. The identity link is a data structure that is created by the sourcePIN Register Authority during the issuance process of citizen cards. A signature of the sourcePIN Register Authority attests the link between the unique identifier 'sourcePIN' and an electronic signature provided to the entity by the citizen card issuer. The identity also holds the name and data of birth. These data are frequently needed in

[370] http://www.justiz.gv.at/firmenbuch
[371] http://zvr.bmi.gv.at
[372] http://www.ersb.gv.at/

official proceedings and intelligent forms can be pre-filled with the name and data of birth. The sourcePIN may only be stored in the identity link in the citizen card, thus is under sole control of the citizen.

12.4.3 Sector-specific identification

The Austrian concept refers to identifiers as personal identification numbers (PINs). The eIDM model implemented using the citizen cards are sector-specific PINs that are derived from the sourcePINs. Using cryptographic one-way functions the sector-specific identifiers are calculated so that the citizen is uniquely identified in one sector, but identifiers in different sectors cannot be unlawfully cross-related.

The Sector Delineation Regulation (*E-Government-Bereichsabgrenzungsverordnung - E-Gov-BerAbgrV*) defines 26 sectors of state activities so that within each sector using the same identifier no data protection issue is caused. Examples for such sectors are taxes, health or sports.

The eIDM model is open for the private sector. Companies can use the citizen card to derive private sector-specific PINs that are unique within their sphere, but cannot be cross-linked with identifiers of other entities. In this case the company's identifier is used as a delineator during the cryptographic calculations of the PINs instead of the governmental sector number described above.

12.4.4 Citizen cards

The citizen's card facilitates a sector specific authentication of Austrian citizens and registered foreigners. The technical background of the citizen's card has been described in the FIDIS deliverable D3.6 "Study on ID Documents" in chapter 5.5.

The notion citizen card does not stand for a specific card that is the same for each citizen, such as, e.g., a passport. The citizen card is rather technology-neutral concept that allows designing secure electronic public administration services for various different solutions. Therefore, several citizen cards are available, such as bank cards, the Austrian health-insurance card or mobile phones, which can be used as a two-factor authentication solution. In short, the citizen card concept defines minimal requirements that are necessary to carry out electronic administrative procedures securely. Major requirements that an eID token needs to fulfil are electronic signatures and storage of the identity link or electronic mandates. Quality criteria are defined such as security requirements for the electronic signatures,[373] or the interface between Web-applications and the citizen card.[374]

The citizen's card can be used together with a reader infrastructure supported by the government (e.g. certain types of card reader), and a governmental security and communicational software component installed on the local computer of the user. The Austrian citizen's card is recognised as one of the most privacy preserving implementations of national eIDs so far,[375] due to the technical enforcement of the borders between

[373] Qualified signatures fulfil the requirements. For an interim period until end of 2007 other electronic signatures referred to as "administrative signatures" are admissible

[374] Technical details are available at http://www.buergerkarte.at/en/technik/index.html

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

governmental sectors. Nevertheless, as (1) the SAML-based authentication scheme, (2) the governmental sectors, and (3) hard- and software components facilitating generating and transporting authentication information are predefined (selected) by the Austrian government, the identity of Austrian citizens in this context is managed by the Austrian state.

In 2006 and 2007[376] Austria performed best in this benchmark compared to the other 26 European Countries covered with a score of 99%, followed by Malta and Slovenia with 96%.

12.5 Legal Framework

12.5.1 eGovernment legislation

Entering into force on 1 March 2004, the eGovernment Act was a milestone achievement. Austria was one of the first EU Member States to adopt comprehensive legislation on eGovernment. It serves as the legal basis for the instruments used to provide a system of eGovernment and for closer cooperation between all authorities providing eGovernment services. Regarding the identity management aspects the law defines the citizen card concept and its use in the public sector using sector-specific PINs and in the private sector using private sector-specific PINs. The eGovernment Act has been lastly amended at the end of 2007, and it is complemented by the Administrative Signature Regulation (16 April 2004), the Sector Classification Regulation (16 July 2004), the SourcePIN Register Regulation (3 March 2005) and the Supplementary Register Regulation (2 August 2005), each of which defines in more detail some provisions of the eGovernment Act and facilitates its implementation.

12.5.2 eSignatures/eIdentity legislation

The Electronic Signature Act (Signaturgesetz; SigG) was passed by Parliament on 14 June 1999 and came into force on 1 January 2000, making Austria the first EU Member State to implement Directive 1999/93/EC on a Community framework for electronic signatures.

The Act legally recognizes electronic signatures satisfying certain security requirements and provides some evidential value to less secure electronic signatures. Electronic signatures are defined for natural persons only. It is complemented by the Austrian Signature Ordinance which has been lastly amended on 1 January 2005 (Federal Law Gazette part II No. 527/2004). The conditions for the use of electronic signatures in the public sector, as well as for the use of Citizen Cards and sector-specific personal identifiers are regulated by the E-Government Act.

12.6 Interoperability

Austria has considered access for non-nationals and interoperability in the design of the eIDM system from the beginning. Three options exist, depending on the residence of the entity and whether a foreign eID token is used:

- Non-national with residence in Austria; Austrian eID
  In this case, the entity is usually registered in the Central Register of Residents[377]. An

http://www.austria.gv.at/DesktopDefault.aspx?TabID=4951&Alias=bka&infodate=19.12.2005 and http://www.ptapde.gr/news/PR_e-PRODAT_20051215.pdf.

[376] See http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf

Austrian eID can be activated. In practise, if having a residence in Austria the entity is likely to already possess a health insurance card[378], a bank card or an Austrian mobile phone that can be activated as citizen card. If not, an SSCD that can be activated as citizen card can be purchased by the certification service provider A-Trust.

- No residence in Austria; Austrian eID
  In the case of non-nationals that do not have a residence in Austria or that do not fall under registration obligation, the entity can enrol to the Supplementary Register for Natural Persons. An Austrian eID can be activated then, such as an SSCD of the certification service provider A-Trust[379].

- Using foreign eID tokens
  A non-national may use his home-country's eID. At least smart card like foreign eID solutions can be integrated into Austrian citizen card concept the same way as the different Austrian smart cards (bank card, health insurance card, student cards, etc.). From a technical point of view, the integration into the Austrian eID middleware 'citizen card environment' has already been done for eID cards from Belgium, Estonia, Finland, and Italy. From the legal point of view, a regulation will clearly define which foreign eID cards are accepted.

[377] If the entity has a residence in Austria but no registration obligation, such as under privileges and immunities of international organisations, the case of an entity with no residence in Austria applies.
[378] If working in Austria or if for other reasons falling under Austrian compulsory health insurance
[379] Enrolment to the SRnP or registration of the qualified certificate requires showing identity documents, i.e. in practice personal presence in Austria at least once.

13 Summary and Conclusions

The investigated European member countries show similar targets with respect to governmental IMS: Creation of one (or more) reliable identity management schemes that serves identifying citizen in the real and the electronic world. Typically these identity management schemas show a similar structure: in addition to an identity card (ID or eID) a register with reference data is kept. The investigated European countries also have a strategy how to deal with these registers. In most cases a number of existing registers kept by different governmental agencies is linked either (a) by introducing a unique identifier (The Netherlands, Switzerland), or (b) by linking them in a defined way (Austria, Belgium, Germany). However, as historic starting points (e.g. no establishes ID card and citizen's register schema in U.K. in difference to the other investigated EU member countries), governmental structures (federal vs. centralistic) and the number of citizens differ widely, the implementation of these concepts shows significant differences. While in U.K. a national (e)ID document still is in preparation, in Belgium an eID was introduced already since 2004 and in 2009 all citizen will have such an eID.

For the "real" (physical) world in addition to the electronic passport typically traditional paper based documents or identity cards (credit card format plastic cards) are used. In general national ID cards are used for more purposes than identifying citizen in the context of governmental procedures. Traditionally they are already used as travel documents in the Schengen countries and for authentication purposes in the private sector. In the last years a trend can be observed to introduce biometrics to strengthen the binding between card and card holder in the physical world (U.K., Germany). In this context the ICAO standards seem to play an increasing role to guarantee compatibility with electronic passports.

For the electronic world electronic signature schemes are available in most of the investigated countries for many years now. However, not in all cases they are designed to fulfil authentication requirements (e.g. in Austria, Germany), mainly because the required information is not stored in the citizen's certificates and/or the enrolment does not cover these information. In these cases an additional authentication scheme for citizens is introduced in citizen cards (Austria) or will be part of the planned future national identity card (Germany).

In the political debate also security seems to play an important role – frequently prevention of "identity theft" is one of the security targets of national eID schemes. However, security of the corresponding registers is not part of the public debate equally, possibly except in U.K. because of a number of recent security problems concerning various governmental databases.

From a data protection point of view the Austrian concept to enforce technically the borders between defined governmental sectors is most notably. However, apart from the health sector there seems to be no common understanding and definition of governmental sectors to date. Some of the investigated e-government concepts try to avoid different sectors and explicitly aim at linking them via a unique identifier (The Netherland, Switzerland). In Switzerland a privacy debate has started, as this identifier obviously seems to be attractive for uses apart from the intended purpose, especially in the private sector.

A more homogenous understanding of governmental sectors which should be principally separated could be as well a strong data protection driver as an important interoperability driver because of homogenised legal backgrounds for data access and exchange. If such an understanding can not be reached interoperability may put privacy and security of European

citizen at risk, as data intended to be used in a specific sector in the home country of a citizen may be used in many more sectors in other countries where they stay as guests. In this way measures designed to prevent or hamper 'identity theft' or violation of purpose binding may be disabled through the back door in other countries.

An important aspect of the Austrian concept is that for the purpose of authentication SAML-certificates are used, while most of the other European member states use X.509v3 certificates. A middleware concept similar to government gateways developed in Germany could be an approach for a solution, as this technology supports the connection of different IMS, as long as privacy and security policies are compatible.

The European Union has started a number of initiatives to promote an inclusive e-government in the member countries. Main objective of these activities are:

- Inclusiveness
- Efficiency and effectiveness of e-governmental services
- Promotion of high impact services
- Promotion of key enabler, especially eIDs
- E-participation

In addition in the context of the i2010 initiative an e-government benchmark has been carried out since 2000. The results indicate that there are significant qualitative differences in the implementation of e-government throughout Europe. Given this and the significant differences found in the analysed concepts in the country reports there still seems a lot of work to do.

14 Bibliography

ADAPID Project Group, *Requirement Study*, available at <https://www.cosic.esat.kuleuven.be/adapid/docs/adapid-d2.pdf>, last consulted 15 October 2008.

Alsenoy, B. van and Cock, D. de, 'Due processing of personal data in eGovernment? A case study of the Belgian electronic identity card', *Datenschutz und Datensicherheit*, vol. 32, issue 3, 2008, pp. 178-183.

Auerbach, N., "Anonymous Digital Identity in e-Government", Dissertation, Zürich, June 2004. Download: http://www.ifi.uzh.ch/archive/diss/Jahr_2004/thesis_auerbach.pdf

Backhouse, J. (ed.), *D4.1: Structured account of approaches on interoperability, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 30 August 2008.

Backhouse, J. and Halperin, R. (eds.), *D4.4: Survey on Citizen's trust in ID systems and authorities, FIDIS deliverable*, 2007, available at <www.fidis.net>, last consulted 30 August 2008.

Backhouse, J. and Vanfleteren, M. (eds.), *D4.2: Set of requirements for interoperability of Identity Management Systems, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 31 August 2008.

Bauer, M., Meints, M. and Hansen, M. (eds.), *D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 29 August 2008.

Bender, J. et al., 'Sicherheitsmechanismen für kontaktlose Chips im Deutschen elektronischen Personalausweis' [Safety mechanisms for contactless Chips in German electronic Identity Card], *Datenschutz und Datensicherheit*, volume 32, issue 3, 2008.

Berkvens, J.M.A. and Prins, J.E.J., *Privacyregulering in theorie en praktijk* [Privacy regulation in theory and practice], pp. 105-124, Kluwer, Deventer, 2007.

Birch, D.G.W., *Digital Identity Management: perspectives on the technological business and social implications*, Gower Publishing Limited, Hampshire, 2007.

Blakely, R., 'Where the government holds your details', *The Sunday Times*, November 25, 2007.

Bot, D. de, *Verwerking van Persoonsgegevens* [Processing of Personal Data], Kluwer, Antwerpen, 2001.

Brin, D., *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Addison-Wesley, Reading, 1998.

British Office for Government Commerce (OGC), *ITIL*, available at <http://www.ogc.gov.uk/guidance_itil.asp>, last consulted 15 October 2008.

Buitelaar, H. (ed.), *D13.3: Study on ID number policies, FIDIS deliverable*, 2007, available at <www.fidis.net>, last consulted 6 February 2008.

Bullesbach, A., Prins, C. and Poullet, Y., *Concise European IT Law*, Kluwer Law International, Alphen aan de Rijn, 2006.

Burger@Overheid.nl, *Workbook eCitizen Charter*, available at <www.burger.overheid.nl/files/workbook_ecc_english.pdf>, last consulted 5 February 2008.

Bygrave, L.A., 'Core principles of data protection', *Privacy Law and Policy Reporter*, vol. 7, issue 9, 2001.

Cameron, K., *The laws of identity*, available at <http://msdn.microsoft.com/en-us/library/ms996456.aspx>, last consulted 29 August 2008.

Cap Gemini, *The user challenge. Benchmarking the supply of online public services*, available at < http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf>, last consulted at 30 August 2008.

Cock, D. de, *Belgian eID card technical overview*, available at <http://homes.esat.kuleuven.be/~decockd/site/EidCards/belpic/mySlides/belgian.eid.card.technical.overview.pdf>, last consulted 31 August 2008.

Commissie Modernisering GBA, *GBA in de toekomst. Gemeentelijke Basis Administratie persoonsgegevens als spil voor de toekomstige identiteits-infrastructuur* [GBA in the future. Municipal Database Personal Records as the pivot for future identity infrastructure], available

at<www.minbzk.nl/px/download.aspx?file=/contents/pages/4985/eindrapport_gba_in_de_toekomst_3-01.pdf>, last consulted 29 August 2008.

Commissie Van Thijn, *Persoonsnummerbeleid in het kader van identiteitsmanagement* [Personal number policy in the context of identity management], available at <www.ejure.nl/mode=display/downloads/dossier_id=187/id=47/Persoonsnummerbeleid.pdf>, last consulted 29 August 2008.

Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, available at <www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm>, last consulted at 29 August 2008.

Cuijpers, C.M.K.C., *Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn* [Privacy law or private law? A private law alternative for the implementation of the European Privacy Directive], Wolf Legal Publishers, Nijmegen, 2005.

Deprest, J. and Robben, F., *eGovernment: the approach of the Belgian federal administration*, available at <http://www.ksz-bcss.fgov.be/documentation/fr/documentation/Presse/2003%20-%20E-government%20paper%20v%201.0.pdf>, last consulted 31 August 2008.

Dobler, D.W. and Burt, D.N., *Purchasing and Supply Management*, McGraw Hill, New York, 1996.

Dutton, W. et al., 'The cyber trust tension in e-government: Balancing identity, privacy, security', *Information Polity*, vol. 10, issue 1-2, 2005, pp. 13-23.

Dumortier, J. and Graux, H., *eID Interoperability for PEGS. National Profile Belgium*, available at <http://ec.europa.eu/idabc/servlets/Doc?id=31520>, last consulted 31 August 2008.

ECOTEC and Tavistock Institute, *A Handbook for Citizen-centric eGovernment, version 2.1*, December 2007, available at <www.ccegov.eu/downloads/Handbook_Final_031207.pdf>, last consulted 5 February 2008.

eGovernment Unit, *A roadmap for a pan-european eIDM framework by 2010,* version 1.0, available at <http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf>, last consulted 30 August 2008.

eGovernment Unit, *Signposts towards egovernment 2010*, available at <http://ec.europa.eu/information_society/activities/ict_psp/documents/signposts2005.pdf>, last consulted 30 August 2008.

Espiner, T., The worst IT security incidents of 2007, available at <http://resources.zdnet.co.uk/articles/features/0,1000002000,39290745,00.htm>, last consulted 30 August 2008.

European Commission, 'European Governance – A White Paper', COM (2001) 428, adopted 25 July 2001.

European Commission, *eGovernment Progress in EU27+. Reaping the benefits*, available at <http://www.astic.es/eAdministracion/Documents/egovprogress7.pdf>, last consulted 30 August 2008.

European Commission Communication, 'An Information Society For All', 23 and 24 March 2000.

European Commission Communication, 'First report on the implementation of the data protection directive' (95/46/ec) (No. COM(2003) 265 final), Brussels.

European Commission Communication, 'i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All', COM (2006) 173, adopted 25 March 2006.

European Commission Communication, 'The Commission Entreprise IT Architecture [CEAF] – version 1 explained', available at <http://www.ec.europa.eu/dgs/informatics/ecomm/index_en.htm>, last consulted 30 August 2008.

European Commission Communication, 'The Role of eGovernment for Europe's future', SEC (2003) 1038, COM (2003) 567 final, adopted 26 July 2003.

European Commission Communication, 'Towards the e-Commission – Europa 2nd generation – Advanced Web Services to Citizens, business and other professional users', Brussels, 6 July 2001.

European Commission Communication. 'Working together for growth and jobs. A new start for the lisbon strategy', COM (2005) 24.

European Commission Directorate-General for Informatics Communication, e-*Commission 2006-2010: enabling efficiency and transparency*, available at <http://www.ec.europa.eu/dgs/informatics/ecomm/index_en.htm>, last consulted 30 August 2008.

European Communities, *BE: Young job-seekers aided by on-line 'first job'cards*, available at <http://www.epractice.eu/document/64>, last consulted 31 August 2008.

Fried, C., 'Privacy (A Moral Analysis)', *The Yale Law Journal*, vol. 77, issue 1, 1968.

Gasson, M., Meints, M. and Warwick, K. (eds.), *D3.2: A study on PKI and biometrics, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 29 August 2008.

Gutwirth, S.L., 'Biometrics between opacity and transparency', *Annals of the Italian National Institute of Health (Ann Ist Super Sanita)*, vol. 43a, issue 1, 2007, pp. 61-65.

Hayat, A., *A pan european interoperable electronic identity management system*, available at < http://www.iaik.tugraz.at/RESEARCH/publications/theses/Hayat.pdf>, last consulted 30 August 2008.

Hägler, S., *Public Key Infrastructure (PKI)*, available at <http://www.seco.admin.ch/sas/00229/00251/index.html>, last consulted 9 May 2008.

Heath, N., *ID card will drown in a billion mismatches*,

<http://www.silicon.com/publicsector/0,3800010403,39294213,00.htm>, last consulted 5 November 2008.

Holden, S.H. and Millett, L., 'Authentication, Privacy and the Federal E-Government', *The Information Society*, vol. 21, issue 5, 2005.

IDABC, *Analysis and Assessment of similarities and differences – Impact on eID interoperability*, available at <http://ec.europa.eu/idabc/en/document/6484/5644>, last consulted 29 August 2008.

IDABC, Draft document as basis for eif 2.0, available at < http://ec.europa.eu/idabc/servlets/Doc?id=31508>, last consulted 30 August 2008.

IDABC, *European interoperability framework for pan_european egovernment services. Version 1.0*, available at < http://ec.europa.eu/idabc/servlets/Doc?id=19529>, last consulted 30 August 2008.

IDABC, *Harnessing ICT to improve public services*, Available at <http://ec.europa.eu/information_society/activities/egovernment/index_en.htm.>, last consulted 30 August 2008.

Identity and Passport Service, *What is the National Identity Scheme*, available at <http://www.ips.gov.uk/identity/scheme-what-run.asp#nir>, last consulted 30 August 2008.

International Telecommunication Union - Telecommunication Standardization Sector. Focus Group on Identity Management. Report on Identity Management Framework for Global Interoperability.

Introna, L.D., 'Privacy and the computer: Why we need privacy in the information society', *Metaphilosophy*, vol. 28, issue 3, 1997, pp. 259-275.

Kent, S.T. and Millett, L.I., *Who goes there? Authentication through the lens of privacy*, National Academy Press, Washington DC, 2003.

Kindt, E., 'Belgische Kruispuntbank bekroond door de Verenigde Naties met 'Public Service Award', *Computerrecht*, 2006.

Kosta, E. and Dumortier, J., 'The Data Retention Directive and the principles of European Data protection legislation', *Medien und Recht International*, issue 3, 2007.

Kosta, E. et al., *Requirements for privacy enhancing tools*, 2008, available at <www.prime-project.eu>, last consulted 15 October 2008.

Koops, B.J., Buitelaar, H. and Lips, M. (eds.), *D5.4: Anonymity in electronic government: a case-study analysis of governments' identity knowledge, FIDIS deliverable*, 2007, available at <www.fidis.net>, last consulted 29 August 2008.

Kuner, C., *European Data Protection Law. Corporate compliance and regulation*, Oxford University Press, London, 2007.

Leyman, F., *OECD Peer Review eGovernment BELGIUM*, available at <http://www.oecd.org/dataoecd/43/13/40305982.pdf>, last consulted 31 August 2008.

Kent, S.T. and Millett, L. I. (eds.), *Who goes there?: Authentication through the lens of privacy*, The National Academies Press, Washington DC, 2003.

Leenes, R. (ed.), *D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research, FIDIS deliverable*, 2006, available at <www.fidis.net>, last consulted 29 August 2008.

LSE Department of Information Systems, *The Identity project. An assessment of the UK Identity Cards Bill and its implications*, available at <http://identityproject.lse.ac.uk/identityreport.pdf>, last consulted 30 August 2008.

Meints, M. and Thomsen, S., 'Protokollierung in Sicherheitsstandards', *Datenschutz und Datensicherheit*, vol. 31, issue 10, 2007.

Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997.

Ministerial eGovernment Conference. (2005). *Ministerial declaration*. Manchester, UK; 4th Ministerial eGovernment Conference. (2007). *Ministerial declaration*. Lisbon, Portugal.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *Rapport Voorbij het loket, over de mogelijkheden en onmogelijkheden van pro-actieve dienstverlening voor de Nederlandse overheidsorganisaties* [Report Past the counter, on the possibilities and impossibilities of proactive services for the Dutch government organisations], Den Haag, maart 1999, available at <www.minbzk.nl>, last consulted 5 February 2008.

Modinis IDM, *Modinis Study on Identity Management in eGovernment*, available at <www.cosic.esat.kuleuven.be/modinis-idm>, last consulted 29 August 2008.

Modinis IDM Study Team, *Common Terminological Framework for Interoperability Electronic Identity Management. Version 2.01*, available at <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc>, last consulted 29 August 2008.

Moen, W.E., 'Information technology standards: A component of federal information policy', *Government Information Quarterly*, vol. 11, issue 4, 1994, pp. 357-371.

Nabeth, T. and Hildebrandt, M., (eds.), *D2.1: Inventory of topics and clusters, FIDIS deliverable*, 2005, available at <www.fidis.net>, last consulted 29 August 2008.

Nabeth, T. et al, *D2.3: Models, Fidis deliverable, 2005*, available at <www.fidis.net>, last consulted 29 October 2008.

Nissenbaum, H. F., *Privacy as Contextual Integrity*, 2004, available at <http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf>, last consulted 15 October 2008.

OASIS Provisioning Services Technical Committee, *SPML FAQ*, available at <http://www.openspml.org/spml_faq.html.> last consulted at 29 August 2008.

OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at org >, last consulted at 29 August 2008.

Office of Management and Budget, *OMB guidance for implementing the privacy provisions of the E-Government Act of 2002*, available at <http://www.whitehouse.gov/omb/memoranda/m03-22.html>, last consulted 17 August 2008.

Office of the New Zealand Privacy Commissioner, *Privacy Impact Assessment Handbook*, available at <http://www.privacy.org.nz/privacy-impact-assessment-handbook/>, last consulted 18 August 2008.

Olsen, T. et al., *Privacy - Identity Management*, available at <www.legal-ist.org>, last consulted 29 August 2008.

Pato, J., *Identity management: Setting Context*, available at <http://www.hpl.hp.com/techreports/2003/HPL-2003-72.html>, last consulted 29 August 2008.

Papakonstantinou, V., 'A data protection approach to data matching operations among public bodies', *International Journal of Law and Information Technology*, vol. 9, issue 1, 2001.

Prins, J.E.J., *Designing e-government*, pp. 245-261, Kluwer Law International, Alphen aan den Rijn, 2007.

Raab, C. and Bellamy, C., 'Joined-up government and privacy in the UK: Managing tensions between data protection and social policy', *Public Administration*, Vol. 83, Issue 1, 2005.

Reed, A., *The definite guide to identity management*, 2002, available at <http://www.realtimepublishers.com>, last consulted 15 October 2008.

Reisen, A., "Digitale Identität im Scheckkartenformat", *Datenschutz und Datensicherheit* 3/2008, pp. 164-167, Wiesbaden 2008.

Riedl, R., *Anonymität im E-Government*, available at <http://www.ifi.unizh.ch/egov/E-Government-Anonymitaet.pdf>, 2004, last consulted 15 October 2008.

Robben, F., *1st Modinis Workshop on Identity Management in EGovernment*, 2005, available at http://www.law.kuleuven.ac.be/icri/frobben/presentations/20050504.ppt>, last consulted at 29 March 2008.

Samoy, I.,'"What's in a name?" Het "in naam van-vereiste" bij de vertegenwoordiging vier jaar na Schoordijk' [What's in a name? The "in name of requirement" in representations four your after Schoordijk], *Tijdschrift voor Privaatrecht*, vol. 41, issue 1, 2004, pp. 563-576.

Schneier, B., *Applied Cryptography*, Addison-Wesley, New York, 1996.

Slone, S. (ed.), *Identity Management. A white paper*, 2004, available at <http://www.opengroup.org/online>, last consulted 29 March 2008.

Stach, H., 'Mit Bürgerportalen für einfach sichere, vertrauliche und verbindliche elektronische Kommunikation', *Datenschutz und Datensicherheit*, volume 32, issue 3, 2008.

Stalder, F., 'The failure of privacy enhancing technologies (pets) and the voiding of privacy', *Sociological Research Online*, vol. 7, issue 2, 2002, available at <www.socresonline.org.uk/7/2/stalder.html>, last consulted 29 August 2008.

Statistisches Bundesamt Deutschland, *Statistisches Jahrbuch 2008*, 2008, available at <http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Publikationen/QuerschnittsveroeffentlichungenStatistischesJahrbuch/JahrbuchDownload,templateId=renderPrint.psml>, last consulted 6 October 2008.

Treasury Board of Canada Secretariat, *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*, available at <www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1_e.asp>, last consulted 18 August 2008.

US American Information Systems and Audit Control Association (ISACA), *CobiT*, available at <http://www.isaca.org>, last consulted 15 October 2008.

Vlaams Minderhedencentrum, *Oude bijlage 6 - Bewijs van Inschrijving in het Vreemdelingenregister*, available at <http://www.vmc.be/vreemdelingenrecht/wegwijs.aspx?id=712>, last consulted 31 August 2008.

Vlaams Minderhedencentrum, *Oude Bijlage 7 - Identiteitskaart voor Vreemdeling*, available at <http://www.vmc.be/vreemdelingenrecht/wegwijs.aspx?id=723>, last consulted 31 August 2008.

Vlaams Minderhedencentrum, *Oude Bijlage 8/9 - Verblijfskaart van een onderdaan van een lidstaat der EEG*, available at <http://www.vmc.be/vreemdelingenrecht/wegwijs.aspx?id=770>, last consulted 31 August 2008.

Voortgangsrapportage Elektronische Overheid mei 2007 [Progress Report Electronic Government May 2007] , available at <www.e-overheid.nl/atlas/planning/>, last consulted 5 February 2008.

Webopedia, *Provisioning*, available at <http://www.webopedia.com/TERM/P/provisioning.html>, last consulted 29 August 2008.

Westin, A., *Privacy and freedom*, Atheneum, New York, 1967.

Wikipedia, *GovernmentGateway*, available at <http://userp.uni-koblenz.de/~egov/wiki/de/index.php?title=GovernmentGateway>, last consulted 31 August 2008.