# FIDIS

Future of Identity in the Information Society

| | |
|---|---|
| Title: | "D3.17: Identity Management Systems – recent developments" |
| Author: | WP3 |
| Editors: | Martin Meints (ICPP, Germany), |
| | Harald Zwingelberg (ICPP, Germany) |
| Reviewers: | Jozef Vyskoc (VaF, Slovakia), |
| | Vashek Matyas (MU, Czech Republic) |
| Identifier: | D3.17 |
| Type: | [Report] |
| Version: | 1.0 |
| Date: | Monday, 10 August 2009 |
| Status: | [Final] |
| Class: | [Public] |
| File: | fidis-wp3-del3.17_Identity_Management_Systems-recent_developments.doc |


***Summary***

This document describes and analyses developments and trends on the market for IMS in the recent years including current standardisation efforts. Use cases describe such new types of IMS. Trends in the development of new IMS gave an initiative to revise the typology for IMS developed within FIDIS.


# 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 (JWG)*** | 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** | 28.10.08 | • Initial draft (Martin Meints, ICPP) |
| **0.2** | 02.02.09 | • Contributions of ICPP, TUD and KU integrated |
| **0.3** | 09.02.09 | • Contribution of KULeuven integrated, chapter 4 created and structured |
| **0.4** | 20.02.09 | • Contribution KULeuven updated, chapter 5.1 and 5.2 integrated |
| **0.5** | 06.03.09 | • Chapter 5.3 integrated |
| **0.6** | 8.05.09 | • Draft version for EC Review.<br>• Integration of Executive Summary, |
| **0.7** | 08.05.09 | • adding missing parts |
| **0.8** | 17.06.09 | • Internal Review |
| **0.9** | 01.07.09 | • Integrate Review Comments |
| **1.0** | 10.08.09 | • Second internal Review<br>• Integration of Review Comments<br>• Final Editing (Harald Zwingelberg, Marit Hansen, ICPP) |

# Foreword

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

| *Chapter* | *Contributor(s)* |
|---|---|
| **1 (Executive Summary)** | Harald Zwingelberg (ICPP), all authors |
| **2 (Introduction)** | Martin Meints (ICPP), all authors |
| **3 (Developments in and Trends for IMS** | 3.1, 3.4 Martin Meints (ICPP)<br>3.2 Hans Hedbom (KU)<br>3.3 Denis Royer, Shuzhe Yang (JWG) |
| **4 (Use Cases)** | 4.1, 4.2 Stefanie Pötzsch (TUD)<br>4.3 Harald Zwingelberg (ICPP)<br>4.4 Brendan Van Alsenoy (KULeuven)<br>4.5 Harald Zwingelberg (ICPP) |
| **5 (Proposal for a revised typology of IMS** | 5.1, 5,2 Martin Meints (ICPP)<br>5.3 Denis Royer (JWG)<br>5.4 Harald Zwingelberg (ICPP) |
| **6 Summary and Conclusions** | Martin Meints (ICPP), Harald Zwingelberg (ICPP), all authors |

# Table of Contents

# 1 Executive Summary

In the course of the FIDIS project a selection of Identity Management Systems (IMS) was documented in a database[4] and their development was observed. Within FIDIS Deliverable D3.1 a typology for IMS was developed. This typology contains three basic types of IMS differentiated by the aspect of control, and methods used for the identity management:

Type 1: IMS for account management, implementing authentication and authorisation
Type 2: IMS for profiling of user data by an organisation
Type 3: IMS for user-controlled context-dependent role and pseudonym management.

Since 2005 when the first FIDIS report on IMS was published the market of IMS has rapidly developed. In this document these developments were analysed and three relevant trends were observed:

- A concentration of products in the market, especially for type 1 IMS, while at the same time tools for user control were integrated in large identity management frameworks.
- Social networks became an important group of IMS in recent years, fascinating many users. Social networks are also a hybrid type of identity management systems, combining type 2 IMS (financing the platform through targeted advertisements) and type 3 IMS (self edited user profiles).
- The market of type 3 identity management tools and systems still remains very fragmented and driven rather by open source initiatives than by commercial players.

The increasing number of hybrid types of IMS observed in the market has shown the limitations of the initial typology. Proposals for a revised typology are derived in Chapter 5 of this report. It is shown how these approaches can describe the properties of IMS with differing degrees of user centricity and the properties of social networks.

Looking at the standardisation efforts in the IMS sector there seem to be two clear trends. One trend is the drive for federation and interoperability, mainly pushed by the Liberty Alliance and OASIS. The efforts in the standardisation of web services' have matured quite well primarily through the work of Liberty Alliance but also through the OASIS work. Concerning federation standards for the general information system sector and the telecom sector the current and planned work in ITU-T and ISO/IEC seems to be promising. A big issue within the federation area seems to be the interoperability and harmonisation of the different federation standards and solutions.

The second trend is the drift from standards for organisation centric IMS towards a more deliberate suit of standards trying to find a reasonable balance between customers needs for security and privacy and the organisation or business needs for security and information.

[4] The FIDIS database on identity management systems (IMS database) is publicly available at http://imsdb.fidis.net/.

IMS become more and more complex and integrated solutions rather than simple out-of-the-box products. This makes the decision for the introduction of a new generation of IMS increasingly difficult, especially in the context of Enterprise Identity Management Systems (EIMS). In this deliverable a research approach aiming at a decision support framework, based on the balance scorecard approach, is presented (section 3.3.2). Based on initial key performance indicators in four relevant dimensions a framework for an organisation specific decision scorecard can be developed.

Chapter 4 is dedicated to use cases from (1) commercial IMS, (2) research approaches, (3) the Open Source community and (4) governmental solutions. Microsoft CardSpace, the integrated PRIME prototype and OpenID demonstrate the increasing role of user centricity, user control and privacy enhancement within in the first three sectors named. The use case describing efforts in the public sector addresses the projects and solutions developed within the various Belgian e-Government initiatives (section 4.4) and shows inter alia an eID solution that is still mainly controlled by the state and shows privacy enhancement mainly by enhancing transparency of the eID's usage to the citizen.

Finally we see a current development in the market that user centricity and control is increasingly recognized an integral part of many IMS and IMS-related standards by the relevant bodies. However, the implementation of these improvements is often lagging behind while commercial vendors or governments apply centralistic IMS. This leaves room for further research addressing information security and privacy aspects of IMS, especially in the mentioned areas of application.

# 2 Introduction

In the course of the FIDIS project a selection of Identity Management Systems (IMS) was documented in a database[5] and their development was observed. Another FIDIS research result was the development of a typology for IMS. This typology contains three basic types of IMS (Bauer, Meints, Hansen 2005). In this model the aspect of control (control by an organisation or the user concerned), and methods used for the identity management (central account management, profiling techniques or user-centric methods) were covered:

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.

Since 2005 when the first FIDIS report on IMS was published the market of IMS has further developed rapidly. In this document these developments will be analysed and future trends derived from the developments observed. Clearly the focus of FIDIS research was put on user controlled and user centric IMS. However, this analysis also takes external sources into consideration to cover relevant trends in other types of IMS.

This document is structured as follows: Chapter 3 gives an overview on trends observed on the market of IMS, research results concerning IMS and IMS related standardisation. To further explain relevant trends, chapter 4 presents commercial, research, Open Source and governmental use cases of IMS. In chapter 5 approaches for new typologies of IMS are proposed and discussed. This document closes with chapter 6 containing a summary and the conclusions.

[5] The FIDIS database on identity management systems (IMS database) is publicly available at http://imsdb.fidis.net/.

# 3 Developments in and Trends for IMS

## 3.1 Market Trends

For almost four years a selection of IMS has been documented in the FIDIS IMS database[6] and the records in this database have been updated regularly. Taking external studies (e.g., Hansen et al. 2003) into consideration, trends can be followed over an even longer period. These developments were summarised in Bauer, Meints, Hansen (2005). In this document an update of trends observed since 2005 will be given. However, in the IMS database a focus was put on user controlled and user centric IMS. For this reason the observations of the market for type 1 and 2 IMS shows significant gaps. Concerning type 1 IMS these gaps are partly filled in section 3.3.1 by analysing information from FIDIS-external sources, and for federation frameworks in the FIDIS Deliverable D3.12 (Prien and Leenes 2009).

The most obvious trend is further product integration, a trend also observed already in the past. This trend can be observed as well in the context of type 1 as type 3 IMS. One example for product integration in the context of type 1 IMS were numerous products that were bought in 2004 to 2007 by Oracle and subsequently integrated in Oracle's identity management solution "Oracle Identity Management". In the context of type 3 IMS this trend also was observed. Examples are the integration of Sxip[7] into OpenID (version 2.0) and the integration of originally separate tools into web browsers as Add-ons (the integration of skipper as Add-on in Firefox[8] is an example for this type of integration).

Another important trend observed is that the number of IMS of a hybrid type increases. This trend originally was fuelled by the failure of the Microsoft Passport concept. The new strategy followed by a number of manufacturers and vendors of originally quite pure type 1 IMS was described by Kim Cameron in his so-called "Laws of Identity", published in 2005 (Cameron 2005). Following the FIDIS IMS typology, we now can observe that properties of type 1 and type 3 IMS are increasingly combined in numerous products. On one hand originally type 1 focused directory services get improved by integrating credential systems and the addition of connectors to identity meta-frameworks. Examples for this are the integration of UProve in the Microsoft Passport concept and Idemix in the IBM Tivoli identity manager.

At the same time a number of federation frameworks (see also Prien and Leenes 2009) and identity meta-frameworks became available, driven by large manufacturers (Identity Metasystem[9], Microsoft; Liberty Alliance[10], SUN and others; Higgins[11], IBM, Novell and others), but also by the Open Source community (OpenID[12]). These meta-frameworks mainly contain a suite of protocols to connect (a) a number of repositories (type 1 IMS), (b) numerous service providers and in some cases (c) client-site identity management frontends. For example Microsoft's Passport and IBM's Tivoli identity manager support the connection to identity meta-frameworks, in particular the Microsoft identity meta-system (see also chapter 4.1) and Higgins. As a result users can choose among a number of identity providers,

[6] See http://imsdb.fidis.net/ (last accessed 10 August, 2009)
[7] See http://www.sxip.com/background (last accessed 10 August, 2009)
[8] See http://www.sxip.com/blog (last accessed 10 August, 2009)
[9] See http://www.identityblog.com/stories/2005/07/05/IdentityMetasystem.htm (last accessed 10 August, 2009)
[10] See http://www.projectliberty.org/ (last accessed 10 August, 2009)
[11] See http://www.eclipse.org/higgins/ (last accessed 10 August, 2009)
[12] See http://openid.net/ (last accessed 10 August, 2009)

context specific (partial), verifiable identities and can select them in specified communicational context via own frontends (e.g., CardSpace). This type of integrated type 1 and 3 identity management solutions also were discussed under the term of user centric IMS.

Still, identities "self declared" and shaped by users play a significant role on the market of identity management components or systems in various services. They are mainly established where a link to the physical identity for the service provider from an economic perspective does not matter, as identification of users can be done effectively enough by other means, mainly profiling carried out based on the users' web-behaviour or the content they provide to the service provider. Examples for the implementation of this identity management can be found in web mailers and numerous social networks, which are mainly financed by advertisements targeted to certain user groups based on profiles.

Social networks became an important group of IMS in recent years, addressing various groups in the population such as pupils in school, students and business professionals. They are also a hybrid type of identity management systems, combining type 2 IMS as their economic core (financing the platform through targeted advertisements) and type 3 IMS (self edited user profiles). In social networks personal data entered by the users to maintain their profiles and communication carried out via the platforms provided by the operators of the social networks, e.g., fora and mail interfaces, is analysed to build up profiles.

Webs of trust based, e.g., on mashed personal networks and reputation systems did not become the core component of independent identity management systems, though approaches were made in this direction (e.g., with LOAF and Sxip network). Nevertheless these identity management methods are well established as integral identity management instrument in various platforms such as social networks (personal networks and recommendations in LinkedIn[13]) or auction platforms (e.g., vendors in eBay[14]).

The market of type 3 identity management tools and systems still seems to be very fragmented and only to a limited extent driven by commercial players. Mostly tools are still developed in the Open Source community and the research community. Obviously browsers developed by the Open Source community, especially Mozilla Firefox, became an established platform for the integration of type 3 identity management tools. Available examples include:

- Password generator, password safes, (single) sign-on tools and form fillers, partially as enhanced Add-ons.
- Anonymization services (Tor[15], AN.ON[16] and JonDonym[17]).
- Cookie managers.
- Tools to detect pixel embedded from a remote HTTP server into the website visited, used to transfer user data to this remote server (e.g., Ccounterpixel[18]).
- History management tools (e.g., iJournal further developed in the context of MozPETs).

[13] See http://www.LinkedIn.com/ (last accessed 10 August, 2009)
[14] See http://www.ebay.com/ (last accessed 10 August, 2009)
[15] See http://www.torproject.org/ (last accessed 10 August, 2009)
[16] See http://www.anon-online.de/ (last accessed 10 August, 2009)
[17] See http://www.jondos.de/ (last accessed 10 August, 2009)
[18] https://addons.mozilla.org/en-US/firefox/addon/5414 (last accessed 10 August, 2009)

In the context of profiling (type 2 IMS) an increased use for marketing and advertising was observed, while Ambient Intelligence (and thus unobtrusive identification by the environment using, e.g., type 2 IMS) mostly still is a vision rather than a reality. Since the late 1980s Privacy Preserving Data Mining (PPDM) was developed, and still is an area of research. However, PPDM was applied in few projects so far only and integration of PPDM methods and algorithms in data mining work benches takes place very slowly so far (see also Custer 2009, chapter 4.1).

In the context of governmental IMS still quite pure type 1 IMS are used, mainly focussing on directory services and Public Key Infrastructure (PKI). Important aspects of the use of IMS in this domain are describes by Buitelaar, Meints and Van Alsenoy (2008) and Buitelaar, Kindt and Meints (2009). From a privacy point of view the most important difference to user centric architectures discussed above is that eIDs referring to the described centralised IMS allow the linking of every authentication and transaction of the users. Only one successful approach to limit this linkability has been implemented so far by technical enforcement of governmental sectors in the context of the Austrian citizen card.

Governmental IMS typically are quite large. They may be embedded in a hierarchical and governmental organisation spanning procedures. Use of intermediaries, service portals and federation are commonly relevant requirements governmental IMS need to fulfil. Relevant aspects in this domain will be also described in the use case of the Belgian eID in chapter 4.4.

## 3.2 Standardisation Relating to IMS

This section tries to give an overview of the standardisation efforts within the IMS area. The focus of the section is on what we believe to be the more influential standardisation bodies and the more generally applicable standards within the web services, general information systems and telecom area. Thus, what might be called product standards or open software efforts like OpenID[19], Higgins[20] and LiD[21] are not discussed.

### 3.2.1 Introduction

In 1984 the Study Group VII of ITU-T (by that time called CCITT) raised Question 35 and begun the work on an enormous task: to create a global distributed structured source of information on organizations, objects and people. At around the same time ISO was realizing the need for a directory service for the OSI framework. The initiating spark for both organizations was the need to be able to rapidly find contact information (e-mail addresses, computer addresses) in a more and more interconnected world and in order to do that an electronically accessible, structured, and searchable database was needed. The two efforts where joined in 1986 and the results of the combined efforts was the X.500 standardisation suit (Chadwick 1996). In a sense this can be seen as one of the first standardisation efforts of a construct that we today maybe would refer to as an Identity management system since the purpose of the directory was to globally and to some extent uniquely name an object of interest (including organizations and people) and associate attributes with those named entries. As with many of the OSI protocols the X.500 protocols have not been widely implemented and supported possibly because they are large and cumbersome to implement

[19] http://openid.net/ (last accessed 10 August, 2009)
[20] http://www.eclipse.org/higgins/ (last accessed 10 August, 2009)
[21] http://lid.netmesh.org/wiki/Main_Page (last accessed 10 August, 2009)

and possibly in this case because it envisioned one worldwide large distributed directory (the ISO/IEC 9594 actually refers to it as The Directory) under the control of countries and multilateral organizations. Despite of this some of the standards within the suite survived and are now frequently used either directly or in simplified versions, e.g., the X.509 certificate standard (Cooper et al. 2008) or the LDAP directory access protocol (Semersheim 2006) and to some extent the Web has taken over some of the roles that the directory was supposed to have. From a privacy perspective, however, the X.500 series leaves a lot to be desired. It is very organization centric in its views and it is doubtful if privacy issues were at all taken into consideration in the development process, e.g., the first version ('88) had no access control at all and the whole idea of the directory is to facilitate linking rather than avoiding it.

### 3.2.2 Liberty Alliance and OASIS

In the late 1990 the web was grooving faster and faster and becoming more and more commercialized. The business needs and informational possibilities of the web lead to that a number of proprietary or simple ad hoc IMS where created to facilitate authentication and information retrieval at different web sites. The fact that these systems could not interact easily with each other, even if they used the same standardized authentication mechanism and a need to simplify the authentication process for the users implied a need for interoperability and federation. As a result of this Liberty Alliance[22] was formed by around 30 partners in 2001 with the specified purpose of "establish open standards, guidelines and best practices for identity management." This is, among other things, done by building "open standard-based specifications for federated identity and identity-based Web services"[23]. In 2002 Liberty Alliance presented their first standard Liberty Alliance ID-FF (Identity Federation Framework) (Liberty Alliance 2002) followed in 2003 by Liberty Alliance ID-WSF (Identity Web Services Framework) (Liberty Alliance 2003). Today Liberty Alliance has released a number of different standards, white papers and best practice recommendation relating to the Web identity management area and according to their own figures more than 80 products have past conformance testing[24]. The specifications produced by Liberty Alliance tries to balance the consumers need for privacy by the business need for security and information and it is an expressed view from the Alliance that the privacy and security of the user's personal information is extremely important. Thus the specification includes mechanisms for policies, notice and consent as well as user controlled ways of relaying assertions between services and identity providers. There are also mechanisms to facilitate anonymous and pseudonymous assertions. However, since the specification only covers the interface and interaction between the different components in the framework, the actual centricity and privacy properties of the deployed product or service is highly dependent on the actual implementation and how the questions of storage, audit, obligations and policies are handled.

OASIS[25] (Organization for the Advancement of Structured Information Standards) started in 1993 as SGML Open but changed their name in 1998. They primarily produce standards within the XML and Web services area. Regarding the IMS area the OASIS efforts can be largely divided into two branches. One is the Security Assertion Markup Language (SAML) (OASIS 2008) area. The other is the parts of the WS-* standards that have a connection to

[22] http://www.projectliberty.org/ (last accessed 10 August, 2009)
[23] http://www.projectliberty.org/liberty/about (last accessed 10 August, 2009)
[24] http://www.projectliberty.org/liberty/about/history (last accessed 10 August, 2009)
[25] http://www.oasis-open.org/ (last accessed 10 August, 2009)

IMS (OASIS 2006, 2007 and 2009). The work on SAML started in late 2000 while the WS-* work is of later date. SAML is an XML based framework that is currently in version 2.0. The purpose of the framework is to communicate user authentication, entitlement, and attribute information. There has been an influence from groups outside OASIS regarding SAML, e.g., Liberty Alliances ID-FF is now incorporated in the SAML 2.0 standard.

The WS-* security protocol family is tied to the SOAP protocol. It consists of a number of standards. However, the standards most interesting from an IMS standpoint are WS-Security (OASIS 2006), WS-Trust (OASIS 2007) and WS-Federation (OASIS 2009). The basic standard WS-Security specifies how to secure SOAP messages. It also introduces the concept of security tokens in the SOAP world. WS-Trust builds on WS-Security and specifies a framework for requesting and issuing security tokens as well as specifications for validating claims and broker trust relationships. Finally, WS-Federation extends WS-Trust and specifies mechanisms for identity federation between security domains. WS-Federation is still under development and is currently in Committee Draft status.

As with the Liberty Alliance specifications the OASIS standards do contain mechanisms and recommendations to address privacy issues. They also share the same open structure as the Liberty Alliance standards which mean that the actual deployment will give the centricity and privacy properties of the implementation. However, at a glance the OASIS standards seems to be somewhat more service provider centric than the Liberty Alliance standards but since WS-Federation is still under development this might change in the final standard.

### 3.2.3 ISO and ITU-T

Within ISO/IEC Joint Technical Committee 1 (JTC 1) Sub Committee 27 (SC 27)[26] is responsible for standardizing general security issues relating to information systems. When ISO/IEC JTC 1 SC 27 realized that standardisation efforts were needed in the identity and privacy area, Working Group 5 (WG 5) was formed to address issues related to identity management, privacy technology and biometrics. From an ISO perspective the group is quite young and all of its standardisation efforts are still work in progress. Within the IMS area three standards are currently under development: “24760 – A Framework for Identity Management”, “29146 – A Framework for Access Management” and “29155 – Entity authentication assurance”. The two latest standards are currently in very early stages of development so it is difficult to provide any evaluation at this point in time. However, WG 5 has a mixture of experts ranging from vendors to privacy commissioners and tries to create liaisons with a number of external organisations within the area, among them Liberty Alliance and FIDIS.

Unlike the previously mentioned standard efforts the ISO/IEC JTC 1 SC 27/WG 5 tries to take a unified view on the IMS question i.e. not only making standards for federation and interoperability but also aspects of the IMS itself. This is evident in 24760 where the focus is to provide a framework for the definition of identity and the secure, reliable, and privacy friendly management of identity information. Since the standards are still under development it is hard to make a judgment on the final result but we know, through FIDIS liaison with WG 5, that the privacy community has an influence on the standards and that suggestions and

26 http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306 (last accessed 10 August, 2009)

comments from that side are taken seriously and discussed and incorporated if deemed relevant.

ITU-T[27] is more recently getting into the IMS standardisation area. In 2007 it created a Focus Group on Identity Management[28]. The purpose of the focus group was too "facilitate the development of a generic Identity Management framework". The group produced a number of documents among them "Report on Requirements for Global Interoperable Identity Management" and "Report on Identity Management Framework for Global Interoperability"[29]. These documents are very operator (or network) centric in their views on identity management. However, they have been heavily commented by ISO/IEC JTC 1 SC 27/WG 5 through their liaison with ITU-T and to the extent that these comments are taken into consideration in upcoming work they might help to balance the view in the ongoing ITU-T standardisation work on identity management. The work of the focus group has resulted in the creation of a Joint Coordination activity for Identity Management within ITU-T[30] and harmonization and cooperation efforts in the area of entity authentication assurance with ISO/IEC JTC 1 SC 27/WG 5 and Liberty Alliance. So far no finalized standards have been released as a result of this process and since we have a very limited insight into the ongoing work within the Joint Coordination activity it is quite hard to make an assessment of the final results.

### 3.2.4 Trends

Looking at the standardisation efforts in the IMS sector, two clear trends appear. One trend is the drive for federation and interoperability. On the web services side federation standardisation has reached quite far primarily through the work of Liberty Alliance but also through the OASIS work. The effect of the federation efforts is that it in a sense has created interoperability between different authentication mechanisms and processes. However, as far as we know, we have yet to see federation standards for the general information system sector and the telecom sector that goes beyond mere roaming agreements. Hopefully this can be achieved through the current and planned work in ITU-T and ISO/IEC. The next big issue within the federation area seems to be the interoperability and harmonisation of the different federation standards and solutions. The Liberty Alliance initiated Project Concordia[31] and the ITU-T focus group on IdM are efforts that are trying to address these areas.

The other trend is the drift from an organization centric approach towards a more balanced view trying to find a reasonable trade off between customers need for security and privacy and the organisation or business need for security and information at least regarding the standardisation efforts within the web services community and ISO. The notable exception to this trend, at least judging by the documents presented so far (see, e.g., the Focus Group reports[32]), is the ITU-T work that still, in our view, have a predominantly operator (or network) centric view. Hopefully this view will change though in the finished standards through the influence of inputs from other standardisation organisations.

---

[27] http://www.itu.int/ITU-T/ (last accessed 10 August, 2009)
[28] http://www.itu.int/ITU-T/studygroups/com17/fgidm/ (last accessed 10 August, 2009)
[29] Available at: http://www.itu.int/ITU-T/studygroups/com17/fgidm/ (last accessed 10 August, 2009)
[30] http://www.itu.int/ITU-T/jca/idm/ (last accessed 10 August, 2009)
[31] http://projectconcordia.org/ (last accessed 10 August, 2009)
[32] Available at: http://www.itu.int/ITU-T/studygroups/com17/fgidm/ (last accessed 10 August, 2009)

Further, one can conclude from the standard documents that all of them assume as its basic setting what we have called a type 1 IMS. However, some of the specifications, notably Liberty Alliance and to some extent OASIS, do include functionality and profiles that could be used to facilitate type 3 IMS.

## 3.3 Selected Results in IMS-Related Research

This section focuses gives an overview in IMS related research, being in the scope of this deliverable. The first part is dedicated to the development of a timeline, incorporating current developments in the field of IMS. The second part is focussing on the decision support for introducing (enterprise) IMS into organisations and approaches on how to support the decision making process.

### 3.3.1 Timeline of the Development of IMS

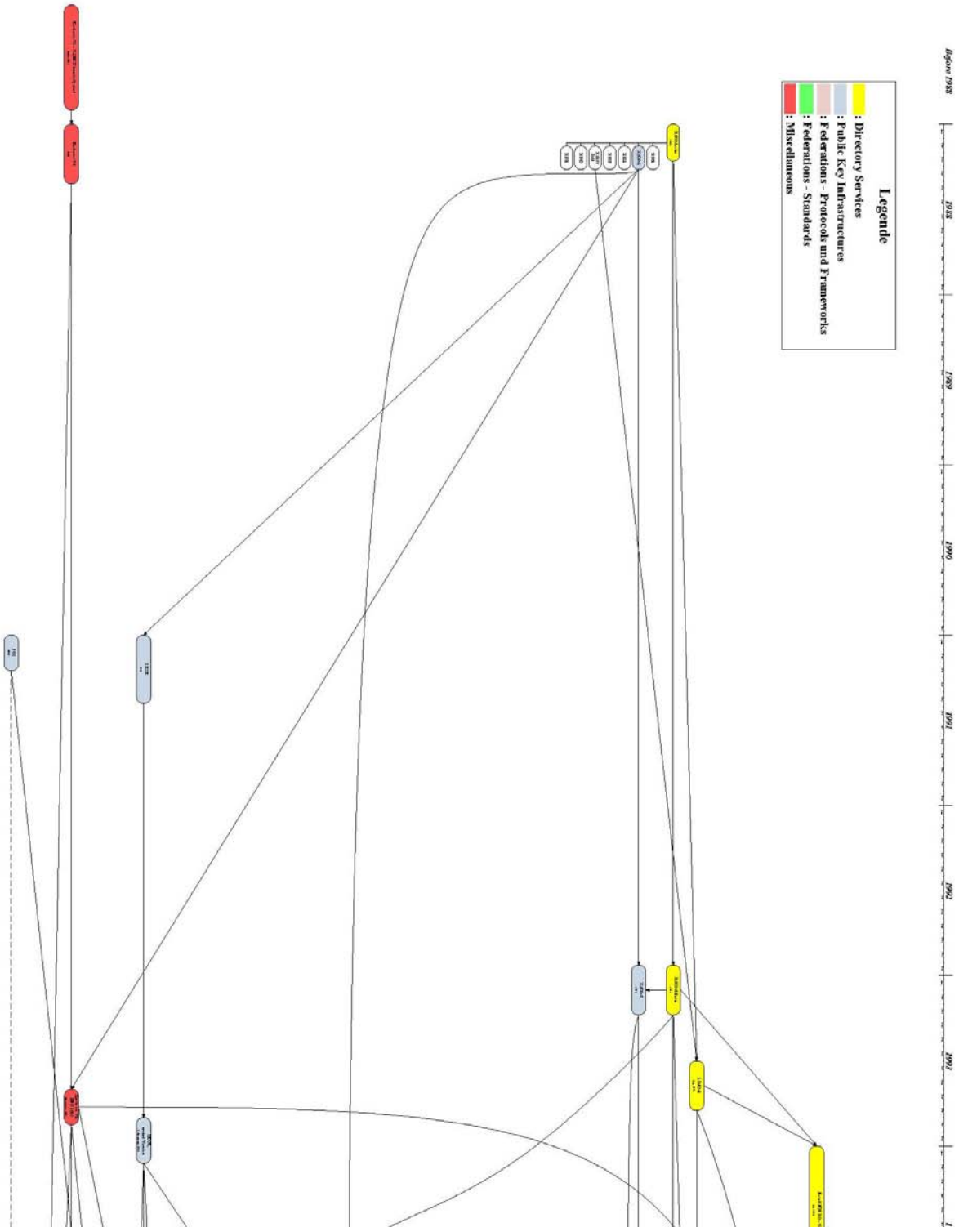
The importance of IMS is undoubted today. Emerging from approaches, such as X.500, the related technologies have emerged at a "good pace". Especially focus and functionality of IMS have developed considerably, not taking into consideration the plethora of application scenarios, those technologies are used in.

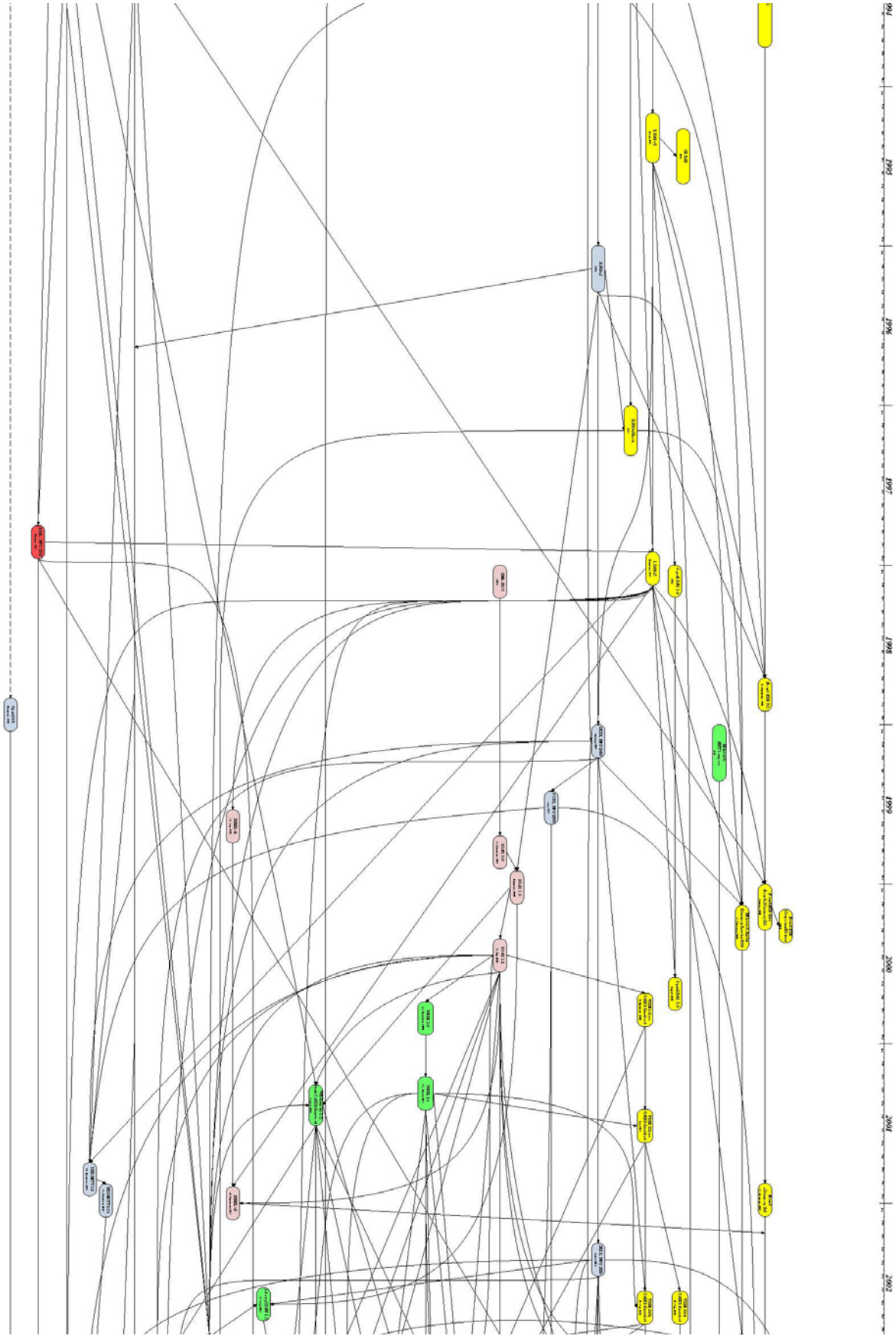
However, the evolution and the development of identity management systems and the related technologies over the past few years is a field not (yet) fully analysed. Especially the different paths that technologies took over time are of interest. Accordingly, we started to collect the different IMS technologies, capturing their development over the past few years, in order to derive a timeline of IMS. The resulting timeline itself is especially focussing on the area of directory services, PKI, federative systems and standards, and miscellaneous aspects in the field.

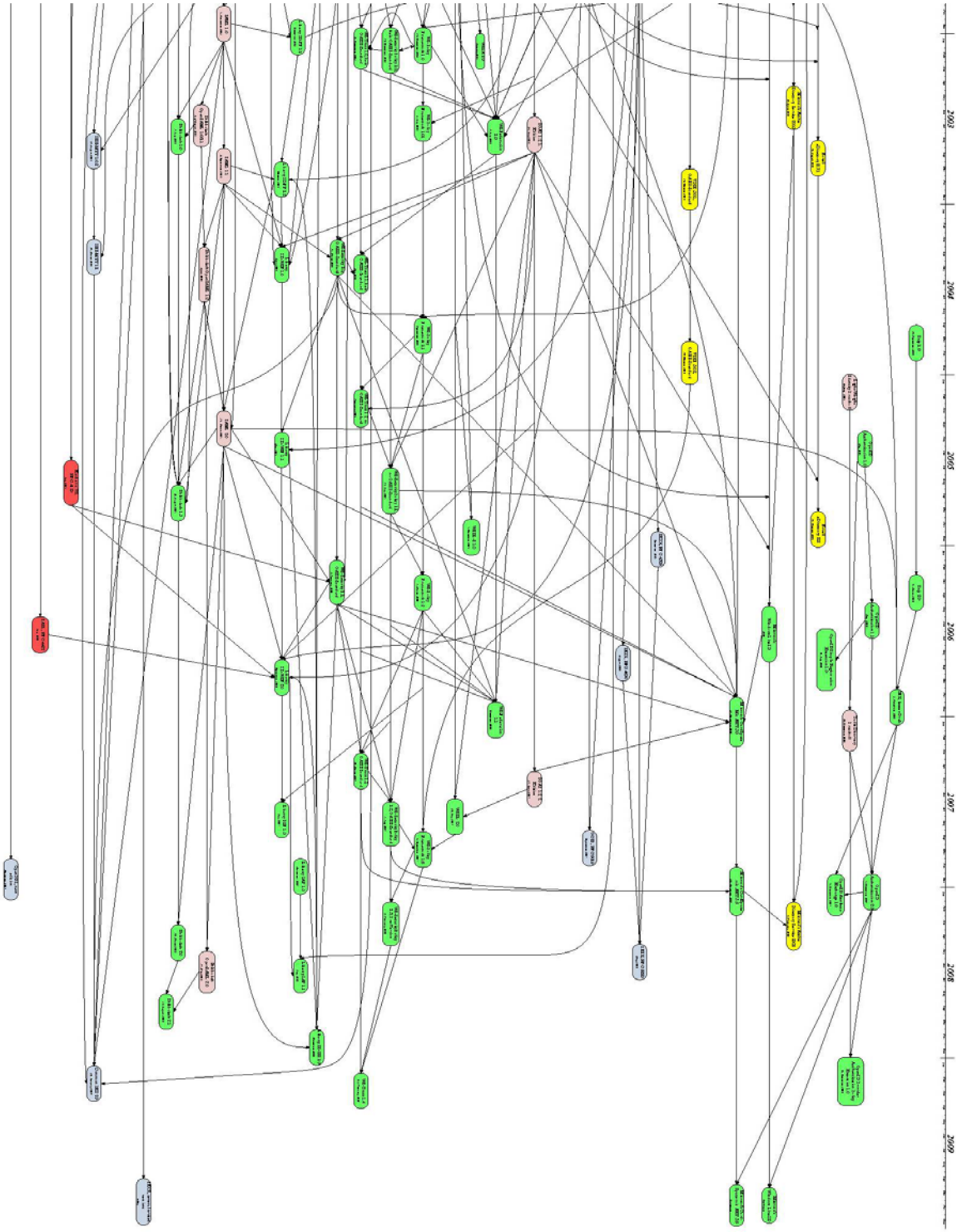
The resulting timeline starts from the directory services related to the X.500 series, spreading into the various technologies being around. Due to the numerous data samples we could acquire, the timeline basically focuses more on core technologies, than on specific products. However, future extension could also take specific IMS products and application fields into consideration. The next three pages are dedicated to the timeline itself.

While current developments in IMS seem to look stable and straight-forward, the future developments of IMS will be challenging. Especially aspects such as cloud computing will bring new aspects into the market, which need to be accommodated. Accordingly, the future investigation and observation in the market seems necessary to further track these developments.

**Figure 1 Timeline on the Development of IMS by Shuzhe Yang (JWG):**


Legende
: Directory Services
: Public Key Infrastructures
: Federations - Protocols und Frameworks
: Federations - Standards
: Miscellaneous
Before 1988
1988
1989
1990
1991
1992
1993





### 3.3.2 Decision Support for the Introduction of Enterprise IMS

Identity Management can be found in a variety of today's organisational processes. Being costly when introduced into an organisation, adequate assessments of the costs, benefits, and the organisational settings are required. Today's methods for the evaluation and decision support of new IT (including IMS) are typically based on single dimensions (e.g., financial or technology aspects). The origin of discussion of the evaluation of IT investments goes back to the late 1980s and it has consequently been addressed ever since and several methods and frameworks have been presented for assessing the economic impacts and the value of IT (security) investments (cf. Walter and Spitta 2004). Prominent examples are the commonly used *return on investment* (ROI) or the *return on security investments* (ROSI). A selected literature sample and a summary of its findings in this domain can be found in Royer and Meints (2009).

Whereas several different approaches have been proposed to evaluate IT and IT security investments, further difficulties can be observed with regard to evaluation methods, metrics, and data collection.

The evaluation methods based on financial measures are not well-suited for IT security investments as they do not reflect the wide range of potential benefits, such as intangible aspects (Magnusson et al. 2007, pp. 26; Martinsons et al. 1999, pp. 72) and the interconnectedness of the different aspects. An example is the achievement of being compliant to relevant laws and regulations by executing an IMS project.

The metrics used are often single-dimensional, only looking from a specific point of view, such as financial aspects. One example for this is the return on security investments, which is limited to the monetarisation of IT security investments (e.g., by analysing productivity losses associated with security breaches). As a result, decisions are made on a limited amount of information, which could lead to suboptimal results, as only a narrow and incomplete picture of the impact of IT security investments is considered.

So, while currently accepted methods try to tackle the stated additional problems of IT (security) investments, there is no approach (yet) capable of integrating all the aspects into one approach. Thus, extended metrics and adequate methods seem necessary in order to evaluate the potential return on IMS and ultimately to support the decision making process. Therefore, we argue that there is no decision support approach yet, which is capable of supporting decision makers when investing in IMS projects. As shown, this is due to the facts that:

- IMS projects have a high level of complexity with regard to the operational and organisational structure. In order to get *the big picture*, further aspects of the *(E)IMS* introduction need to be observed.
- The presented approaches are too narrow in scope and focus on single dimensions (e.g., financial measures or technical issues).
- Moreover, no approach is yet capable of capturing the potential benefits resulting from increased effectiveness through the introduction of IMS, which may occur in different aspects.

However, an approach based on the balanced scorecard (BSC) concept (cf. Kaplan and Norton 1996), combined with the aspects described by other evaluation methods seems appropriate in order to embrace the presented challenges of *(E)IMS* introductions in general.

Such an approach would allow executives to overcome complex decision-making situations by bridging the gap between the different impacting fields and decision parameters.

During the early 1990s, Kaplan and Norton introduced the BSC concept as a performance measurement system for organisations, addressing shortcomings of traditional performance measurement systems (Kaplan and Norton 1996). Arguing that financial accounting measures are too narrow in scope, the BSC does not rely only on financial outcomes (Martinsons et al. 1999, p. 72), but is supplemented with additional organisational measures that complement past and future performance indicators in a holistic way (Martinsons et al. 1999, p. 73).

The resulting scorecard translates additional measures into four perspectives: financial, customer, internal business processes, and learning & growth (Kaplan and Norton 1996). The perspectives are derived from the visions & strategies of an organisation. Also, they represent the three major stakeholder groups of an organisation: shareholders, customers, and employees. The term ³balanced² reflects the intent to maintain a balance between the perspectives and their contained performance indicators, i.e., the balance is kept between short- and long-term objectives, lagging and leading indicators, and financial and non-financial measures. Further research extended the BSC concept by forming causal chains and causal networks among the perspectives¹ indicators, also referred to as strategic maps (Kaplan and Norton 2004, pp. 55).

In summary, the integration of the BSC¹s perspectives allows for a more comprehensive view on the organisation itself (e.g., history and trends). Also, the BSC enables an active management of an organisation down to the project level, helping to act in the best long-term interests (Martinsons et al. 1999, p. 73; Jonen et al. 2004, pp. 196).

In order to build a decision support framework for the introduction of EIMS, substantial modifications to the original perspectives of the BSC concept are necessary. This is due to the fact that the derived framework is going to be used for *decision making (E)IMS Decision Matrix (E/IMS)*. Here, we derived four perspectives and corresponding indicators for an EDM – namely: financial/monetary, security/risk/compliance, business process, and supporting processes/infrastructure.:

- ***Financial/Monetary Perspective:*** This perspective includes factors such as the financial information and the costs associated with an *(E)IMS* project (TCO, LCC, etc.). This helps to give an overview of all the (prospective) cash in- and out-flows.
- ***Business Process View:*** Analysing the business processes, this perspectives looks into the core processes of an organisation. By evaluating the integration of the Enterprise IdM and the IS in an organisation the prospects of higher efficiency and productivity could be made measurable.
- ***Security, Risk, and Compliance:*** This perspective of the BSC deals with the associated risks and the security management of *(E)IMS* projects. Here, factors resulting from compliance, such as data protection, SOX and others, data security (e.g., roles, access permissions), and security standards (if required) play a major role for the evaluation.
- ***Supporting Processes:*** The last perspective evaluates the supporting processes in an organisation (such as HR, IT, organisational Management) that are not directly adding value. For the impact of EIdM, this perspective offers the possibility to assess the alignment and the targeted achievement of supporting and business processes.

Moreover, the perspectives can be further classified into two superordinate objectives: the business objectives (financial/budget and business processes) and the objectives driven by compliance (compliance objectives: security/risk-management and supporting processes). By using the BSC approach, these two objectives can be brought together in a coherent and comprehensive way to facilitate the decision making process (Royer and Meints 2009). The resulting EDM based on the four perspectives is presented in the following Figure 2:

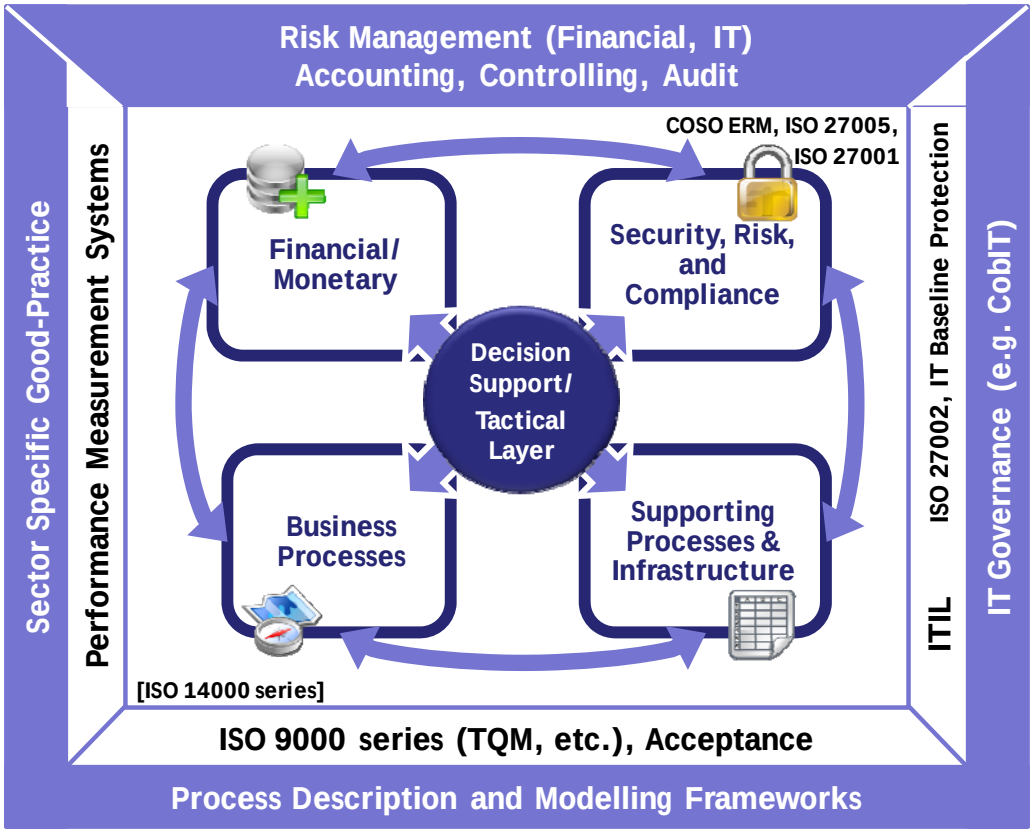



**Figure 2 Initial design of the derived Enterprise IdM Decision Matrix (EDM), incorporating the relevant standards and best-practice frameworks**

Each of the perspective should be translated into corresponding metrics and decision parameters that reflect the goals of the introduction of EIMS into organisations. Examples are already presented by Royer and Meints (2009) and an expert study conducted in 2008.[33] To this regard, such a framework – once being implemented – can help to manage complexity in a more transparent way for the decision makers in an organisation. This is due to the fact that they get broader view on the "big-picture" than just using single-scale indicators (e.g., ROI, ROSI).

[33] This study was conducted among 11 experts (users, vendors, and integrators) in the domain of enterprise IdM, especially focusing on the decision parameters and their linkages. The interviews used semi-structured interview guidelines. The results were aggregated, using the qualitative content analysis as described by Miles and Huberman (1994). The complete results of the expert study have been finalised and are currently in the publication/review process.

## 3.4 Summary and Preliminary Conclusions

From the trends described and analysed the following conclusions can be drawn:

- On the market of IMS the following important trends were observed:
  - Market concentration as well in the area of type 1 as type 3 IMS
  - Development and deployment of federation frameworks
  - Development of concepts and technical frameworks for user centric IMS
  - Deployment of governmental IMS infrastructures, mainly on the user side based on citizen cards and central repositories for the verification of certificates (in most cases using PKI)
- Due to the rapidly increased number of hybrid IMS on the market, the typology proposed in 2005 is not suitable to describe clusters of IMS on the current market, while the properties described by these types still play an important role. As a consequence of this observation a proposal for a revised typology will be proposed and discussed in this deliverable (chapter 5).
- Research directed at support for the decision and introduction of IMS in organisations so far was focused on single dimensions such as technical integration or financial aspects. In this deliverable the proposal of a multi-dimensional decision framework based on the balanced scorecard approach is presented.
- In standardisation of IMS mainly two trends can be observed: Standardisation aims at (a) promotion of federation and interoperability and (b) development of approaches balancing security needs of organisations and privacy needs of individuals. The latter also supports further development and market penetration of user-centric IMS.

# 4 Use Cases

This chapter exemplifies current IMS with different origins describing their respective features, architecture, and workflow with several use cases. Section 4.1 outlines Windows CardSpace, the commercial IMS solution in the portfolio of the Microsoft Cooperation. In section 4.2 the solution developed within the EC-research project PRIME is presented. Within the Open Source realm the OpenID has been developed. It will be described in section 4.3. Finally the Belgian e-Government exemplifies an IMS developed and deployed in the governmental domain (section 4.4).

## *4.1 Commercial Solution: Windows CardSpace*

Windows CardSpace is part of the .NET Framework of Microsoft and relies on an analogy with various kinds of cards that people are familiar with, e.g., bank cards or member cards.

### 4.1.1 Architectural Overview

In general there are three different parties, which are relevant in the architecture of Windows CardSpace (Cameron and Jones 2006):

1. The *user*, who holds several information cards, which contain several pieces of identity information about her.
2. *Relying parties*, e.g., websites, services or companies that request and accept the information cards as security tokens.
3. *Identity providers* who are asserting the information cards as security tokens about the user.

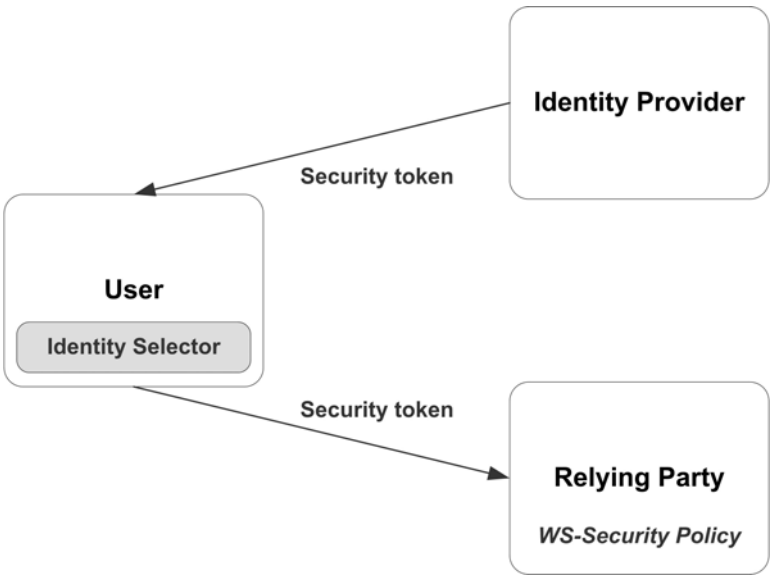



**Figure 3 Windows CardSpace Architecture**

Relying parties in their role as interaction partners of the user have to specify which identity providers as issuers of the information cards they trust. A relying party's policy is generally

described using *WS-SecurityPolicy*, that policy is retrieved using WSMetadataExchange, a *security token* is acquired using WS-Trust, and that token is conveyed to the relying party using WS-Security.

On user's side the so-called *identity selector* provides a graphical user interface and enables the user to choose an information card among her portfolio of different information cards (Cameron, Jones 2006).

### 4.1.2 Digital Identities in CardSpace

In CardSpace a digital identity consists of a set of pieces of information about the user, so-called claims. These claims are carried in the security tokens and are represented as information cards. CardSpace distinguishes between two basic types of information cards: personal cards and managed cards. *Personal cards* can hold varying personal data, e.g., name, e-mail address, date of birth, or similar. This information is encrypted locally and may be sent to relying parties if necessary. However, the user decides which data should be revealed to the respective relying party. Personal cards are also called self-issued cards since the user has also the role of an identity provider in this case. The second type of cards is called *managed cards*. These represent information (e.g., credit card information) provided by other organisations which act as identity providers and maintain the actual data in their systems, while the user's local managed card contains a link to these data (Microsoft Corporation 2008b).

CardSpace allows the user to define any number of personal cards or acquire managed cards. Each card in consists of

1. a unique ID,
2. time and date of creation,
3. a claim about a set of personal data (*security token*), e.g., name and e-mail address, that form a digital identity of the user,
4. digital signature of the identity provider.

The user chooses from her set of cards (digital identities) which data should be revealed to the respective relying party. Thus, relying parties can have varying knowledge of the user's identity.

### 4.1.3 Handling of the Identity Information

The user decides how many and which of her cards should be transmitted to the relying parties. Besides necessary data, which is requested by the relying party, optional information can be included. Based on a privacy policy that relying parties should publish, users may decide to interact with that relying party and to release personal information via cards. There are no rules for format or content of such a privacy policy (Microsoft Corporation 2007).

In order to specify requirements from the relying party concerning acceptable authentication mechanisms like, e.g., trusted identity providers, type of security tokens, etc., user's device retrieves a relying party's *security policy*. The identity selector matches the requirements from the relying party with the user's information cards in order to find those cards, which meet the security policy (Alrodhan and Mitchell 2007).

### 4.1.4 Workflow

If a user for example wants to communicate with a website that allows for login by managed information cards, the process of authentication with CardSpace proceeds as follows (Microsoft Corporation 2008a):

1. The user tries to access a protected resource of the website as the relying party.
2. The relying party communicates to the user's client, which security token would be required.
3. The identity selector filters the users' information cards and finds those that would fulfil the relying party's requirements. The user selects one of those cards, e.g., a managed card. The selected card does not contain personal data, but specifies which identity provider possesses the required information.
4. The requirements from the relying party are passed further to the identity provider, who generates a respective security token and sends it back to the user's client.
5. After the user gives her consent, the security token is released to the relying party.
6. Based on the personal information included in the security token, the relying party grants the user access to the resource.

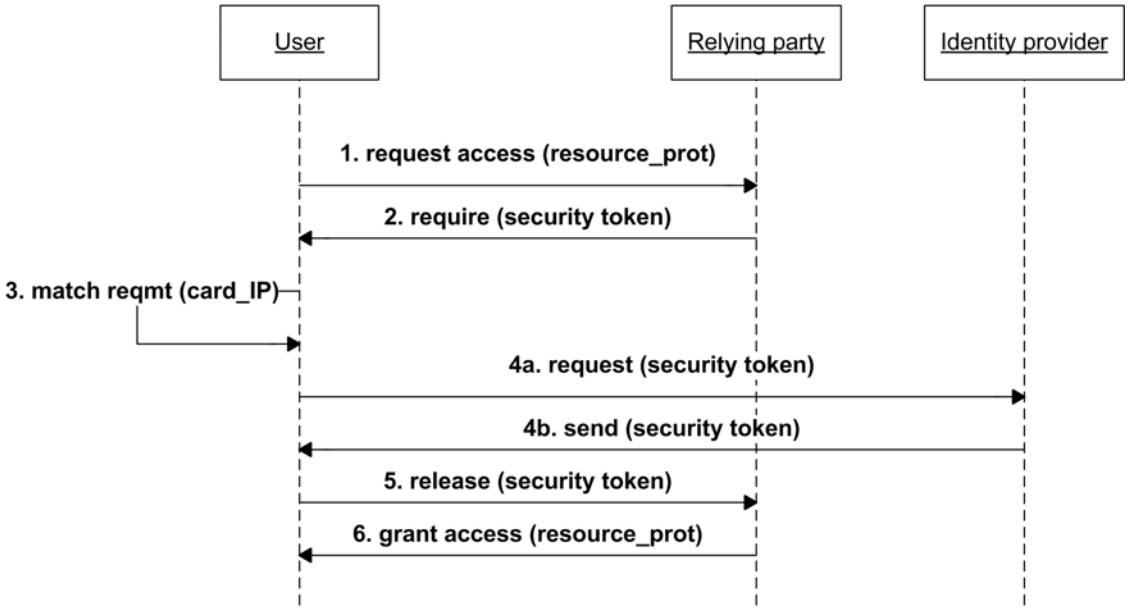



**Figure 4 Authentication process using CardSpace**

The policy of the website that specifies the required security token (step 2) can be expressed by simply using HTML. Websites do not necessarily need to implement any of the WS-*specifications in order to act as relying parties.

### 4.1.5 Client-Based vs. Server-Based Storage of Personal Data

Contrary to its predecessor Microsoft .NET Passport, CardSpace does not store personal information on a central server. Some data are being encrypted and held client-side, while other data remains on the servers of identity providers. This arrangement defines the de-centralised nature of the CardSpace system.

### 4.1.6 Comprehensive Overview

A comprehensive overview about CardSpace is given in the following. The structure is chosen based on the FIDIS Database on IMS (FIDIS 2008).

#### 4.1.6.1 Manufacturer

Microsoft

#### 4.1.6.2 Type of the IMS / Class of the IMS

User centric identity management

Product is functionally focused on identity management

#### 4.1.6.3 References for the IMS

http://www.microsoft.com/net/WindowsCardSpace.aspx (last accessed 10 August, 2009)

#### 4.1.6.4 Open/Closed IMS?


#### 4.1.6.5 State of IMS Deployment


#### 4.1.6.6 Distribution of the IMS

(CardSpace is included with Windows Vista)

#### 4.1.6.7 Geographic Scope


#### 4.1.6.8 Hard- and software Requirements of the IMS

.NET Framework 3.0 or higher;

Internet Explorer 7.0 or other browser with identity selector plugin

#### 4.1.6.9 Installed Base of the IMS (Userbase)

n/a

#### 4.1.6.10 Interoperability and supported Standards

WS-*specifications,

LDAP, Kerberos,

X.509, SAML

#### 4.1.6.11 Server-side Components

n/a

#### 4.1.6.12 Client-side Components

Identity selector

#### 4.1.6.13 Description of Functionality / Features (Client and Server)

Identity management, single-sign on, authentication

#### 4.1.6.14 Main Functionality

Identity meta system

#### 4.1.6.15 Purchase Costs in EUR

n/a (shipped as part of Windows Vista)

#### 4.1.6.16 Flow Charts of the IMS

See Figure 5

#### 4.1.6.17 Screenshots of the IMS

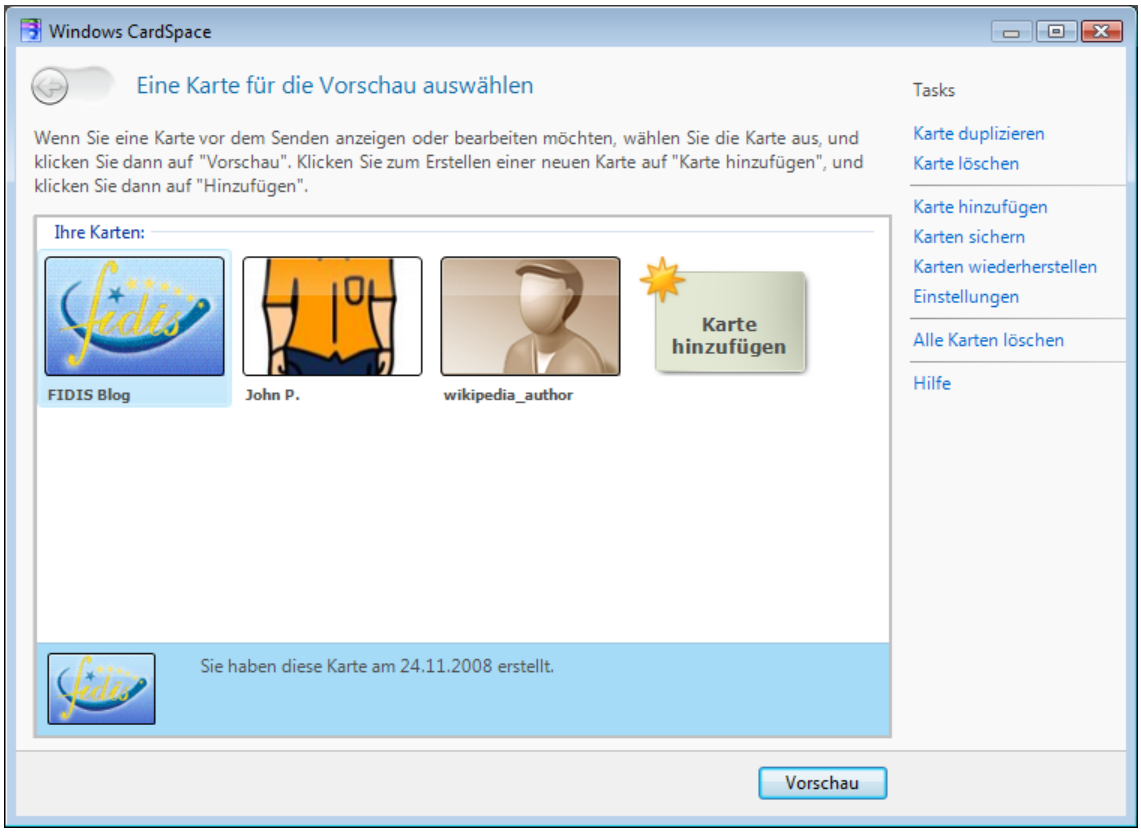



**Figure 5 Screenshot Windows CardSpace User Interface**

## 4.2 Research Solutions: PRIME System

Within the European project PRIME (Privacy and Identity Management for Europe) a privacy enhancing identity management system was developed as a general proof of concept. This PRIME prototype is a client-server system containing different functional modules to provide privacy functionalities and control over personal data items used in different online scenarios to users.

### 4.2.1 Architecture

The PRIME system is a data and metadata processing system supporting users in making decisions by suggesting choices and in using cryptographic methods to protect their statements and validate those of others. In order to suggest choices, rules (called *policies*) and knowledge containing past and present facts (called *decision context*) need to be considered.

The client side of the PRIME system is composed of three major parts:

1. the PRIME core,
2. the PRIME Console, and
3. the PRIME-enabled application.

The *PRIME core* represents the lowest layer, where data is stored and the privacy protocols are running. The *Console* enables the user to access and manage her personal data that is stored in the PRIME core. The *application layer* contains the common client application enhanced by a component called PRIME middleware. The middleware allows for communication between the common client application and the PRIME core. All applications, even the Console, have to obtain authorisation in order to access the PRIME core. External applications could adapt the console look and feel, and functionality as needed.

The server side of the PRIME system principally contains the PRIME core and an application part. The PRIME Administration Console is enhanced by services side management functionality to manage obligations, for instance. It also integrates a middleware layer that could act as an interface for external applications to access the PRIME core functionality.

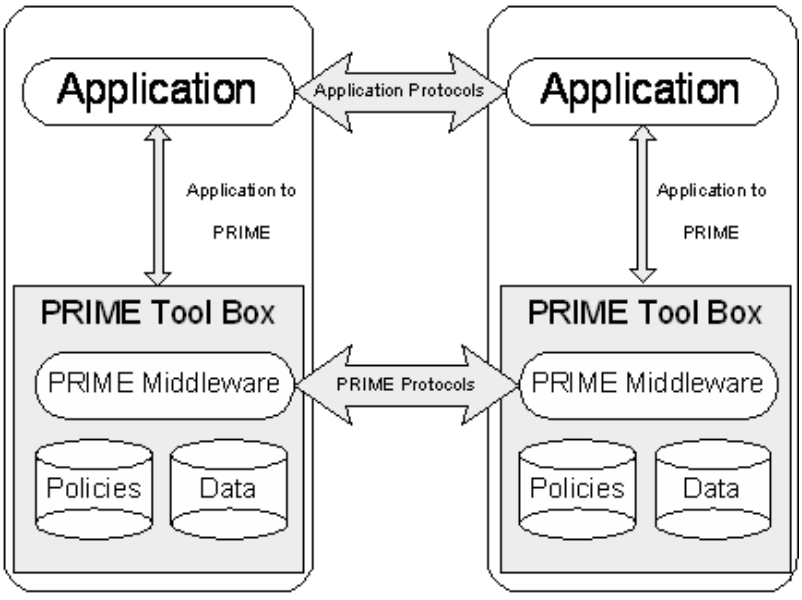



**Figure 6 PRIME Architecture**

Further, there could be third party components assisting the service or client side in verifying addresses, issuing, managing, of validating credentials and certificates etc.

All these parts are connected via an anonymized and encrypted network connection, using Tor (Tor 2008) and further cryptographic functionality.

The privacy functionality is contained in the so-called *PRIME Toolbox*. It holds modules dealing with re-identification, self-identification, authentication, authorisation and policy enforcement (Bergmann 2007).

### 4.2.2 Digital Identities in PRIME

The *PRIME Identity Manager* (see Figure 6) allows the user to administer her personal data within PRIME and to configure various settings concerning his digital identities. These setting's are called *Preference Sets* (short form: *Presets)* for version 2, respectively *Privacy Preferences* (short form: *PrivPrefs*) for version 3 of the prototype (Bergmann et al. 2008). These Presets or PrivPrefs represent a user's digital identities in the system.

The usual process of user's management and usage of her digital identities is handled dynamically by the so-called „Send Personal Data?" – Dialogue. This module intercepts the data flow of a common application and directs it to the PRIME system. PRIME then requests user's input for the handling of the disclosure of her personal data and redirects data to the application accordingly. Thereby the user has the option to choose data for transfer to the transaction partner, e.g., pseudonyms, credentials etc. The user also provides her informed consent via the „Send Personal Data?" – Dialogue.

### 4.2.3 Handling of the Identity Information

In PRIME users state their preferences concerning the handling of their personal data by defining Presets (and choosing PrivPrefs in version 3, respectively). Service providers submit templates for *data handling policies* bound to each requested personal data items. Before a user discloses personal data, both the user and the service provider agree on those data handling policies.

The negotiation process starts with the data handling preferences of the user and the template for the data handling policy presented by the service provider. Preferences set by a user are enforced by comparing each request for personal data by a service provider against the user's statement. Only if the negotiation process succeeds, i.e., there are no conflicts during the comparison or there is an explicit consent of the user, requested personal data is revealed under the agreed policy. The service provider guarantees for enforcement of the data handling policy (Casassa Mont et al. 2007; PRIME 2008a).

### 4.2.4 Workflow

Assuming that both, the user's device and the service provider have installed the PRIME middleware, authentication of the user takes place as follows (Casassa Mont et al. 2007, pp. 64):

1. The user browses to the Web site of a service provider and wants to get access to a protected resource.
2. In this case, when personal information from a user is required, the PRIME middleware of the service provider sends a request for an identifier of the user (e.g., pseudonym) to the PRIME middleware on the user's device.

3. On the user's device a pseudonym is generated and sent back to the service provider, who checks whether data about this pseudonym is already available in the database and if authentication based on these data is possible.
4. If this check fails, further information is requested from the user. For each piece of requested data the service provider submits data handling policies that describe the purpose of the data collection (e.g., payment) and related obligations (e.g., deletion of data after defined period of time).
5. The user device checks if the provided data handling policies from the service provider match the user's preferences and, after positive matching, the requested personal data is sent to the PRIME middleware of the service provider and passed on to the application.
6. Now the user can be authenticated and access to the restricted resource is granted. The PRIME middleware is responsible for enforcing data handling policies, e.g., deleting the data item after a fixed period of time.

### 4.2.5 Client-Based vs. Server-Based Storage of Personal Data

In PRIME, personal data of users including credentials issued by distinct authorities are stored on client-side. Thus, the user is in control of her data, but always needs access to her client device which is running the PRIME middleware in order to use the identity management service.

### 4.2.6 Comprehensive Overview

In the following a comprehensive overview about the PRIME system is given.

#### 4.2.6.1 Manufacturer

Project PRIME – Privacy and Identity Management for Europe

https://www.prime-project.eu/ (last accessed 10 August, 2009)

#### 4.2.6.2 Type of the IMS / Class of the IMS

User centric identity management

Product is functionally focused on identity management

#### 4.2.6.3 References for the IMS

https://www.prime-project.eu/ (last accessed 10 August, 2009)

#### 4.2.6.4 Open/Closed IMS?


#### 4.2.6.5 State of IMS Deployment


#### 4.2.6.6 Distribution of the IMS

The PRIME Prototype is not available yet. However, major parts of it should be published under a free licence in the near future and will then be publicly

available (cf. PRIME successor project PrimeLife: http://www.primelife.eu/ (last accessed 10 August, 2009)).

#### 4.2.6.7 Geographic Scope

IMS EUROPEAN

#### 4.2.6.8 Hard- and Software Requirements of the IMS

512 MB RAM, recommended 1 GB,

1 GHz CPU (Intel or AMD), higher recommended,

500 MB, recommended 1GB HDD space,

Java SE 1.5.0 (is included in the installation package),

Mozilla Firefox 1.5 (is included in the installation package), Mozilla Suite, Mozilla 1.7.X or higher,

Microsoft Windows XP SP2, Microsoft Windows 2000, (Debian Linux, Kernel 2.6 or Apple Mac OS X work with limitations).

#### 4.2.6.9 Installed Base of the IMS (Userbase)

n/a

#### 4.2.6.10 Interoperability and supported Standards

To use the PRIME at its full extent, both communication partners need to have the PRIME software installed.

#### 4.2.6.11 Server-side Components

PRIME core, PRIME-enabled application including PRIME middleware

#### 4.2.6.12 Client-side Components

PRIME core, PRIME Console, PRIME-enabled application including PRIME middleware

#### 4.2.6.13 Description of Functionality / Features (Client and Server)

Identity management, authentication, authorisation, policy management, form filling

#### 4.2.6.14 Main Functionality

Identity management

#### 4.2.6.15 Purchase Costs in EUR

0

#### 4.2.6.16 Flow Charts of the IMS

Online (requires flash plugin):

http://blues.inf.tu-dresden.de/prime/AdvTv3/AdvTv3/Content/Prototypes/Integrated%20Prototype/prime.html

#### 4.2.6.17 Screenshots of the IMS

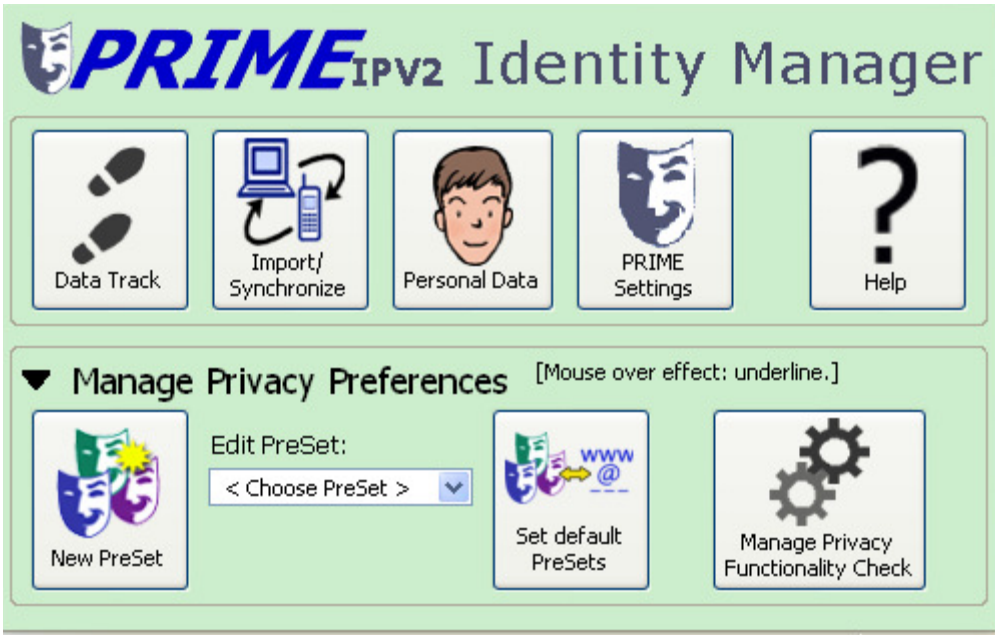



**Figure 7 User Interface of the Prime Identity Manager**

#### 4.2.6.18 General Comments

Even if a web application does not support PRIME, users can still experience some PRIME functionality by activating the FormFiller, which is realised as Browser PlugIn for Mozilla Firefox. However, PRIME-specific server-side features are not available in this mode, e.g., negotiation and enforcement of privacy policies. User's personal data is no longer protected by PRIME during and after transmission from PRIME enabled client-side to non PRIME enabled server-side.

## *4.3 Open Source Solution: OpenID*

OpenID is a protocol for a user-centric authentication and access control, enabling the individuals to identify themselves with different parties and services by proving to be in control over a specific resource on the web. Providing single-sign-on functionality it reduces the need to remember many varying logins with different services. The system is open in the sense that the standard is public as well as software implementations are released as open source. OpenID is based solely on established existing technologies such as URI, HTTP(S) requests, SSL or the Diffie-Hellmann method on key agreements. Excluded from the specification is the question, how the user identifies himself with the identity provider.

OpenID is broadly spread on the web and has supporters in both, the realm of major labels such as IBM, Microsoft, Google, AOL or Yahoo! as well as open source initiatives and smaller web services.

### 4.3.1 Architectural Overview

In the basic setting three parties are involved in the application of OpenID:

1. the *user* asserting a certain identity to a service provider, website, etc.,
2. the OpenID provider is a *identity provider* offering a service for users to register a URL as an OpenID,
3. the *relying party* which is the service provider that wants to verify the users assertion about his identity.

The user asserts his identity to a relying party by providing an identifier. This can either be a URL of a website under the user's control or the URL of an identity provider's website. Since the introduction of OpenID Authentication 2.0 also Extensible Resource Identifier (XRI) may be used.

### 4.3.2 Enrolment Phase

Before OpenID can be applied the user has to get one or more OpenID identifier. This may be done by registering with an identity provider or by inserting the necessary code in a self-owned website.

The OpenID then needs to be registered with the sites it is supposed to be used on. This may either work by simply logging in with the relying party using the OpenID. Many relying parties will, however, require that the user identifies oneself with the attributes known to the service, especially the username stipulated at the initial registration with the site. Once the OpenID is linked to this account with the relying party, the OpenID account can be used for login with the respective relying party.

Depending on the identity provider and the features offered, an OpenID may offer several enhanced ways to manage ones identities. When logging in with a relying party for the first time the user gets the opportunity to specify which personal data deposited with the OpenID provider shall be shared with the relying party. Some providers enable the users to create personas encompassing predefined sets of identity information for selected uses, e.g., for business, private and blogging purposes. However, the attribute exchange is not part of the actual OpenID specification which encompasses only the authentication procedure in relation with the relying party but object of the OpenID Attribute Exchange specification.[34]

### 4.3.3 Login Process

The actual login process with a relying party is kept easy for the user. After the user presents his OpenID into the relying parties login page he will be referred to the OpenID provider where he then proofs his identity. The user is then referred back to the relying party's site, being logged in already.

The detailed process encompasses seven steps:[35]

1. The user initiates authentication by presenting his identifier (URL, XRI) in the OpenID login form on the relying party's website.
2. The provided OpenID is parsed to discover the URL under which the identity provider accepts the protocol messages and the supported protocol version. Additionally it may

[34] See for details on the OpenID Attribute Exchange Specification which is currently available in version 1.0: http://openid.net/specs/openid-attribute-exchange-1_0.html (last accessed 10 August, 2009)
[35] For the detailed technical specification see: http://openid.net/specs/openid-authentication-2_0.html (last accessed 10 August, 2009)

be necessary to extract a claimed identifier when the user asserts to control a certain identifier at the providers endpoint (e.g., a pseudonym or username).
If the provided identifier is an XRI normalisation of the format will be done during this phase.

3. In an optional step the relying party and the identity provider may establish an association applying the Diffie-Hellmann method to agree on a shared secret. The secret will be used to verify subsequent messages from the OpenID provider to the relying party, removing the need for subsequent direct requests after each authentication request.
4. The user is redirected by the relying party to the specified OpenID provider with an authentication request.
5. The OpenID provider verifies that the user is allowed to perform an OpenID authentication. The manner in which this may happen is not object of the OpenID specification.
6. The OpenID provider redirects the user's user-agent to the relying party including a statement whether the authentication was successful or failed.
7. The relying parties verifies the information received by using the shared key established in step 3 or by another direct request with the OpenID provider.

The steps are illustrated in the following figure:

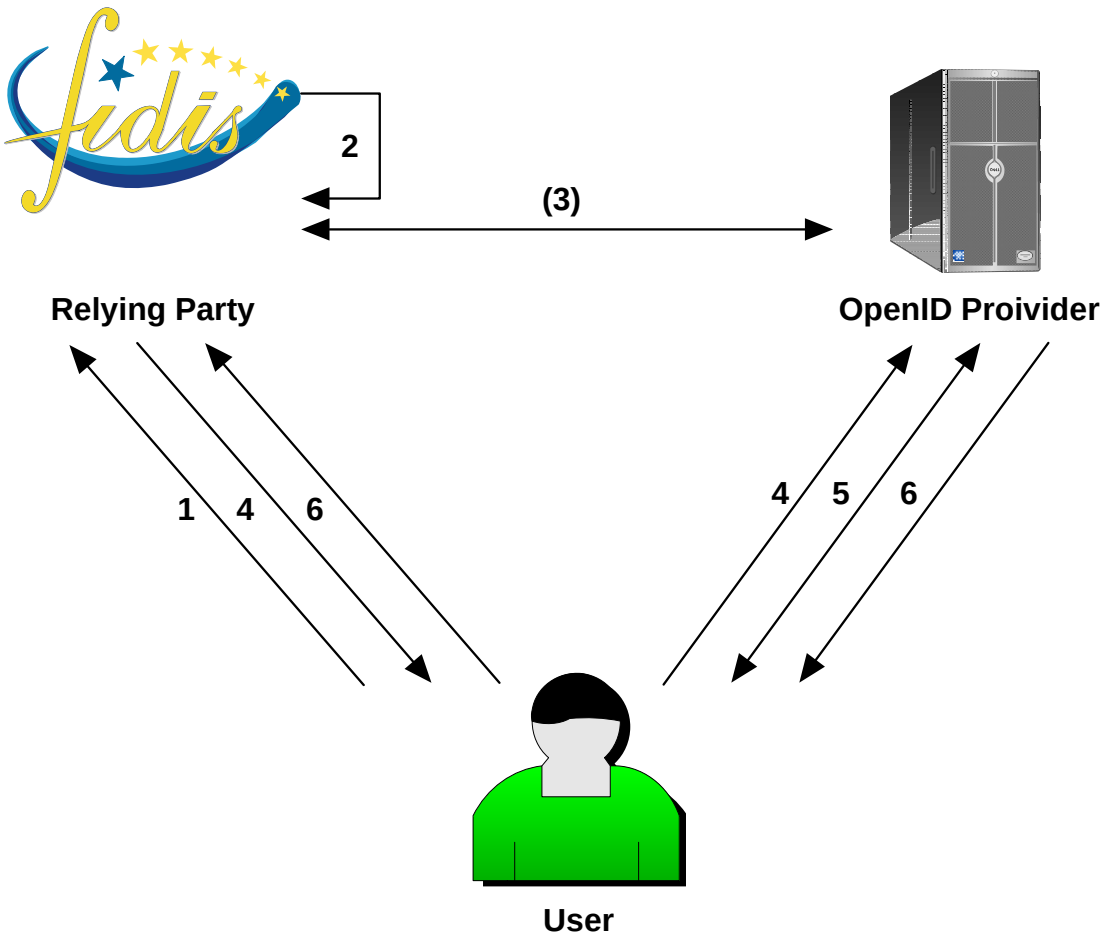



**Figure 8 OpenID Architecture with the FIDIS website as an example for a relying party**

### 4.3.4 Known Issues

Known issues with OpenID include several challenges related to security and privacy when applied in particular by inexperienced users. OpenID authentications are valuable target for phishing attacks as a stolen OpenID offers access to numerous services the user has subscribed to and thus is perfect loot for spammers and may provide a good basis for further ID-theft. For this a malicious website only needs to redirect the user to the phishing website or, more perky, simply ask for the URL and the corresponding password and inexperienced users will likely provide username and password.[36] But as users are likely to assign the same login and password for many websites, enabling a single malicious website to access the other services as well, OpenID does not raise the threat level much for these users. And the issue of authentication is explicitly taken out from the scope of the specification (see step 5). The OpenID providers can apply any means to strengthen security by replacing the simple authentication via password with, for example, one-time passwords sent via a separate

[36] Examples taken from Slot, *Beginner's guide to OpenID phishing*, download: http://marcoslot.net/apps/openid/ (last accessed 10 August, 2009) For a video demonstration of a phishing attempt see Kim Cameron, http://www.identityblog.com/wp-content/images/2008/02/OpenID/Normal/OpenIDPhish.html (last accessed 10 August, 2009)

communication channel such as SMS. The identification of the user with the OpenID provider could also be coupled with other more secure systems of identification such as hardware tokens and biometrics[37], or by providing an information card[38] from CardSpace. With these measures taken there is nothing to harvest for phishers but a cryptographic token or an unusable one-time password. This, however, shows that the phishing problem is not OpenID immanent but depending on the security measures taken by the OpenID provider and the awareness of the user.

As the system does not provide rules for the security of the identification process the user's choice of the OpenID provider is essential for the overall security of the system. Seeking for security policies the author examined the websites for enrolment and creating accounts of various OpenID providers seeking for statements on security measures taken or advice for secure handling of credentials.[39] For this purpose accounts were registered with ten OpenID providers. During the process further information about possible security issues were sought by cursory looking over the content of the registration pages and security and privacy-related links were followed. As expected the providers that rely on a password for the authentication process only do not provide much information on security issues or possible countermeasures. Some providers stipulate the user's obligation to keep the password secret within their general terms and conditions. One of them at least pointed the user's attention to the issue of phishing and indicated the necessity to check the link of the OpenID page before filling the password.

Those providers who offer security enhancing measures also inform about possible threats and how their system intends to prevent this kind of abuse. However, additional and effective counter measurements against phishing attacks were taken primarily by less known providers specialised in identity management and secure authentication. On the opposite the websites with the highest popularity and the most users seemed to be rather cautious not to frighten off users with modifications of the accustomed processes.

As secure authentication is not part of the OpenID specification and not all OpenID providers care for such measures the user must consider his need for security and advanced identity management. He is then enabled to choose a provider that is trustworthy enough for the purposes the OpenID will be applied. Another issue to mind is to pick a provider that is well established already and thus likely to exist for a longer period of time. Finally the chosen OpenID may reveal the pseudonym used for the provider's website or allow third persons to draw conclusions about the user's public profile. So one should also consider picking an identity used for business purposes with a serious appearing provider.

### 4.3.5 Conclusion

The OpenID specification provides for an identification procedure to be used as single-sign-on across the boundaries of services and is based on decentralised identity providers. It does

[37] This approach is used by the AXSionics AXS Card. A field test of the card being applied to an authentication within the OpenID framework has been done within the FIDIDS project. For details see the upcoming FIDIS Deliverable D3.14 and http://www.axsionics.ch/tce/frame/data/8ba8758dafcd968a98959eb686ce71c4b39692cf9696927189a875d3b2a786d0929692718cbe758fb5bd8a8a.pdf (last accessed 10 August, 2009).

[38] For an example of the combination of OpenID with Microsoft Identity Cards see video by Kim Cameron at: http://www.identityblog.com/wp-content/images/2008/02/OpenID/Normal/OpenIDPhish.html (last accessed 10 August, 2009)

[39] Status as of March 2009.

not provide for a trust network nor does it intend to do so. The user needs to trust the identity provider he confides his personal data to or may become his own OpenID provider. Precautions against phishing and other attacks must be taken by the provider and on the user's side.

## 4.4 E-Government Solutions: Developments and Trends in Belgian e-Government

Under this section, we will describe the major initiatives that have been taken in recent years to advance Belgian e-Government identity management. From the start, Belgian e-Government strategies have been aimed at achieving back-office integration and developing user-centric services. Due to a complex federal structure, many of the actual solutions have been developed autonomously by each of the Belgian governments. While collaboration has occurred for certain projects, a single nation-wide approach to integrated service delivery has not yet been formally established.[40]

Our focus shall lie on the actions undertaken at the federal level to facilitate information exchange and extend user- and access management. We shall attempt to document their current status and outline expected future developments.

### 4.4.1 Deployment of Common Authentication Means

Although this development is not entirely novel, a brief reference needs to be made to the mechanisms that have been put in place for entity authentication. The Belgian electronic identity (eID) card may be considered as the primary means of authentication for citizens and business representatives. The federal government also provides two other authentication mechanisms, namely a conventional username/password combination and the so-called 'federal token'.[41] All three authentication mechanisms are available for take-up by entities from other government levels.[42] Corresponding to these authentication mechanisms are four assurance levels:

- level 0: no verification of user identity;
- level 1: verification through username/password;
- level 2: verification through combination of username/password and federal token;
- level 3: verification through electronic identity card.[43]

It is expected that by the end of 2009, over 8 million Belgians (roughly 80% of the population) will possess an eID card. It is yet to be seen how this will influence the further

---

[40] See also OECD e-Government Studies, *OECD e-Government Studies – Belgium*, 2008, available through http://www.fedict.belgium.be/nl/downloads (last accessed 10 August, 2009), p. 115 et seq.

[41] A federal token is a medium strength authentication mechanism, consisting of 24 codes, each 6 characters long, which can be used together with a username/password combination.

[42] J. Deprest and F. Robben, 'eGovernment: the approach of the Belgian federal administration', 2003, available at http://www.ksz-bcss.fgov.be/documentation/fr/documentation/Presse/2003%20-%20E-government%20paper%20v%201.0.pdf (last accessed 10 August, 2009), p. 12.

[43] These assurance levels are determined largely by the level of security provided by the authentication mechanism itself, but of course also by the registration process preceding them. See also J. Dumortier and H. Graux, 'eID interoperability for PEGS – National Profile Belgium', report for the IDABC study on European eGovernment Services, November 2007, p. 20, available at http://ec.europa.eu/idabc/servlets/Doc?id=31520 (last accessed 10 August, 2009).

use of the two other authentication mechanisms. It appears as if these alternative authentication mechanisms were introduced based on eInclusion considerations (to bridge the time gap during which not all Belgian citizens, and particularly civil servants, have an eID card at their disposal) and for applications warranting a lower authentication assurance level.[44]

For more detailed information on the Belgian electronic identity card see FIDIS deliverable 3.6.[45] For the purpose of completeness, we note that an eID card for foreigners as well as a Kids-ID has been introduced.

### 4.4.2 Use of Intermediaries

Early on, e-Government architects realized that transforming resources and applications into functional products for end-users generally requires putting in place additional building blocks and services. Use of intermediaries was recommended to reduce the potential burden on individual service providers. These intermediaries would become part of a common framework, which could be then leveraged by individual entities when developing applications.[46]

#### 4.4.2.1 Universal Messaging Engine

The Universal Messaging Engine (UME) is a message-oriented middleware offered by FedICT[47] which enables the exchange of structured messages between government applications. The main added value of the UME lies in the fact that the applications connected to it no longer need to establish point-to-point communications with each other, but can communicate through an intermediary entity. The UME is currently in its second version.

The UME is often described as an electronic messaging service.[48] Its main function is to route requests and replies from one application to another. The sender of each request (client application) must specify the intended recipient of the request (data provider application). The UME ensures that the request arrives at the designated recipient, but provides no assurance as to whether the recipient will provide the desired response. The UME does not concern itself in any way with the content of the messages it delivers.

---

[44] B. Van Alsenoy and D. De Cock, 'Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card', *Datenschutz und Datensicherheit*, March 2008, pp. 178-179.

[45] More information can also be found in D. De Cock, K. Wouters and B. Preneel, 'Introduction to the Belgian eID card – Belpic', in *Public Key Infrastructure*, 2004, Lecture Notes in Computer Science Book Series, http://www.eid.belgium.be/ (last accessed 10 August, 2009) and at http://www.godot.be/ (last accessed 10 August, 2009).

[46] FedICT, 'e-Gov Architecture – Architectural Blueprint', not dated, available at http://www.fedict.belgium.be/nl/downloads (last accessed 10 August, 2009), pp. 2-11. See also J. Deprest and F. Robben, 'eGovernment: the approach of the Belgian federal administration', 2003, available at http://www.ksz-bcss.fgov.be/documentation/fr/documentation/Presse/2003%20-%20E-government%20paper%20v%201.0.pdf (last accessed 10 August, 2009), p. 9 et seq..

[47] FedICT is the Belgian Federal Public Service Department for Information and Communication Technologies (http://www.fedict.belgium.be/ (last accessed 10 August, 2009)).

[48] FedICT, 'De Universal Messaging Engine Versie 2', p. 7, published online at: http://www.belgium.be/eportal/ShowDoc/fed_ict/imported_content/pdf/FunctUME225022002.pdf?contentHome=entapp.BEA_personalization.eGovWebCacheDocumentManager.nl#search=%22UME%20directory%22, 25 February, 2002 (last accessed 20 June, 2006). Not online anymore; related: http://www.fedict.belgium.be/fr/binaries/UME-CASE_tcm166-9091.pdf (last accessed 10 August, 2009).

While the UME can authenticate the application that issues a request,[49] it does not authenticate individual end users. The responsibility of user authentication lies entirely upon the application which provides the interface to the UME.[50] The actual verification is often provided by a third entity, the Federal Authentication Service (FAS).

A prominent example of an application providing an interface to the UME is Digiflow.[51] Digiflow is accessible through the federal portal website, and in principle every UME message can be processed via Digiflow.[52] Civil servants initiating a request will first be redirected to the Federal Authentication Service, where they will be requested to authenticate themselves using one of the accepted authentication mechanisms (either username-password in combination with a federal token or the electronic identity card).[53] Once it has verified the user's identity[54], the Federal Authentication Service will create a SAML assertion which is forwarded to Digiflow through the user's browser.[55] The Federal Authentication Service is currently in the process of being upgraded to SAML v2.0.

The UME performs some, albeit relatively limited, role with regards to the authorization of requests. The UME manages a so-called 'authorization directory', which specifies which application may direct which type of requests to which data providers. The access control performed by the UME is limited in the sense that it does not verify the privileges of the end user before forwarding a request. Once the UME decides to forward a request, the application on the side of the data provider will have to evaluate whether or not the requesting entity is authorized. The main responsibility for authorization management therefore lies on the side of data providers themselves.[56] Every data provider determines its own method for doing so (e.g., through its own authorization tables for individual users or through role-based approach).

The UME has been in use since 2001, but it is likely that its role will soon be taken over by the Federal Service Bus.

#### 4.4.2.2 Federal Service Bus

The Federal Service Bus (FSB) is the successor to the UME. The goal of this intermediary is to provide more advanced services to end users and to evolve fully towards a service-oriented architecture (SOA).[57]

---

[49] Application authentication can be performed through mutual SSL authentication.
[50] FedICT, 'De Universal Messaging Engine Versie 2', *o.c.*, p. 2.
[51] http://www.fedweb.belgium.be/nl/online_diensten/online_digiflow.jsp (last accessed 10 August, 2009).
[52] http://www.belgif.be/index.php/Digiflow (last accessed 10 August, 2009).
[53] FedICT, 'Gebruikershandleiding Digiflow 2.5.', (Digiflow User Manual), version 5, February 2008, available online: http://www.fedweb.belgium.be/nl/binaries/2009-02-06%20-%20Gebruikershandleiding%20Digiflow%202.5%20-%20NL_tcm120-39856.pdf (last accessed 10 August, 2009). The appropriate assurance level and corresponding authentication mechanism is determined by each data provider. There are in fact four assurance levels used in Belgian e-Government: see section 4.4.1.
[54] This is done through by initiating either an OCSP (eID card) or LDAP (federal token).
[55] See also K. Van Asch, 'The Federal Authentication Service', 2008, http://www.cevi-users.be/new/tmp/fedict.pdf (last accessed 10 August, 2009).
[56] Every data provider is also charged with managing that part of the UME's authorization directory which relates to its services.
[57] http://fedict.newlink.be/nwsl_archive.aspx?nwsl_id=11&email=&item=67&inum=4&lng=1 (last accessed 10 August, 2009)

The FSB is said to be an Enterprise Service Bus (ESB), operating according to the so-called VETRO (Validate, Enrich, Transform, Route, Operate) integration pattern. Enrichment involves adding additional data to a message to make it more meaningful and useful to a target service or application.[58] Transformation converts messages to a specific format, thus facilitating semantic interoperability.[59] Thus, contrary to the UME, the FSB can perform operations upon the content of messages when appropriate. Another reason why the FSB is considered more 'intelligent' than the UME is due to its orchestration capabilities. Orchestration makes it possible to introduce business logic into the order in which services are executed.[60]

The FSB will also contain a central registry in which available services are published, a repository with service documentation, and a service test environment.[61] The registry of services will reduce the burden on individual applications connected to the FSB, as they will in principle no longer need to specify the intended recipient of their request (but can simply select the service they wish to use).

The FSB will standardize web services not only for users within the public administration, but also for external users (citizens and companies). These web services are based on the WS-Security standard.[62]

The FSB remains an application-to-application network. Just as the UME, the FSB will not provide its own user interface, and the burden of individual user authentication will remain with applications providing the interface to the FSB (e.g., Digiflow). It is likely that many of these applications will continue to make use of the Federal Authentication Service to verify the identity of end users (see 4.4.2.1).

The authentication of applications is more advanced under the FSB than under its predecessor. The FSB is able to make use of the Belgian Government Certification Authority[63] to generate an application-certificate for each client or data provider application with whom it interacts. In principle every application that wishes to make use of the FSB will be required to present its application-certificate.

The FSB plays a similar role with regards to the authorization as the UME, but its authorization directory refers to services instead of messages. The main responsibility for authorization management consequently remains on the side of the data providers.

FedICT has recently announced that the FSB is being finalized. The UME and FSB currently co-exist but it is expected that the FSB will fully replace the UME. [64]

---

[58] D. Chappell, 'Enterprise Service Bus', 2004, O'Reilly Media, p. 199.
[59] *Ibid*, p. 200.
[60] FedICT, 'e-Gov Architecture – Architectural Blueprint', not dated, published at http://www.fedict.belgium.be/nl/downloads (last accessed 10 August, 2009), 13.
[61] http://www.belgif.be/index.php/FSB (last accessed 10 August, 2009)
[62] See http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf (last accessed 10 August, 2009) for more information.
[63] For more information on the Belgian Government CA and its place in the CA structure see D. De Cock, K. Wouters and B. Preneel, 'Introduction to the Belgian eID card – Belpic', in *Public Key Infrastructure*, 2004, Lecture Notes in Computer Science Book Series.
[64] ePractice, 'eGovernment Factsheet – Belgium – National Infrastructure', 14 February, 2007, last edited on 5 May, 2009, available online: http://www.epractice.eu/en/document/288183 (last accessed 10 August, 2009).

#### 4.4.2.3 Crossroads Bank for Social Security

The Crossroads Bank for Social Security (CBSS) was created in 1990, and has since fulfilled a leading role in the stimulation and co-ordination of e-Government in Belgium.[65] Although the CBSS has already been operational for a long time, it is still worth briefly mentioning its core functionalities to better understand the role of intermediaries in Belgian e-Government identity management.

In addition to co-ordinating and facilitating electronic data exchange among actors of the social sector, the CBSS has the task of actually organizing these data exchanges. To this end, the CBSS is manages a so-called 'reference directory', which displays the following[66]:

- which persons/companies have files at which entity of the social sector for which periods of time, and in which capacity they are registered ('directory of persons');
- which information/services are available at which entities of the social sector ('data availability table');
- what kind of information/service can be accessed, in what situation and for what period of time ('access authorization table');
- which users/applications wish to receive which services automatically.

This reference directory is used to[67]:

- route data requests to entities that can supply the requested data;
- transmit data automatically where appropriate (e.g., change in address);
- to perform access control.

The CBSS can make use of the services provided by the UME or FSB when exchanging data with government administrations, but this is not always the case. For instance, the CBSS has a direct connection to the National Registry.

The reference directory of the CBSS does not contain any of the actual data to which it refers itself, but it does contain the necessary 'pointers' which allow locating and retrieving the information.[68] All personal data is referenced using the 'INSZ-number' of the person to whom the data refers, which is either the National Registry Number (for all persons who are

---

[65] D. De Bot, ''Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart als belangrijkste juridische bouwstenen', Brugge, Vandenbroele, 2005, p. 77.

[66] Crossroads Bank for Social Security, 'e-Government Program of the Belgian Social Sector', December 2008, published at http://www.ksz.fgov.be/documentation/En/CBSS_2008.pdf (last accessed 10 August, 2009), p. 5; F. Robben and P. Maes, 'De Kruispuntbank van de Sociale Zekerheid als motor van E-Government in de sociale sector', 2006, available at http://www.ksz-bcss.fgov.be/documentation/nl/documentation/Pers/De_KSZ_in_2006.pdf (last accessed 10 August, 2009), p. 7 and http://www.ksz-bcss.fgov.be/nl/fluxdonnees/fluxdonnees_2.htm (last accessed 10 August, 2009).

[67] *Ibid*, p. 5 and Crossroadsbank for Social Security, 'E-Government in the Belgian social security sector – Belgian Best Practices', 2003, available at http://www.ksz-bcss.fgov.be/en/como/brochure%20definitief.pdf (last accessed 10 August, 2009), p. 12.

[68] J. Dumortier and H. Graux, 'eID interoperability for PEGS – National Profile Belgium', report for the IDABC study on European eGovernment Services, November 2007, p. 17-18, available online: http://ec.europa.eu/idabc/servlets/Doc?id=31520 (last accessed 10 August, 2009). Note that the reference directory of the CBSS does not always point to the actual information, but may also simply refer to other (more 'local') reference directories (which in turn lead to the actual information).

registered there), or an identification number provided by the Crossroads Bank itself.[69] In addition to its reference directory the CBSS does collect and maintain certain identity information itself (e.g., its own repository of identity data contained in the National Register and a Register with similar identity data for persons not listed in the National Register, but who do enjoy social security in Belgium).[70]

The authorization of users by is said to be based on a 'generic Policy Enforcement Model', which operates complementary to the earlier mentioned access authorization table.[71] Requests for access or to perform a particular action first arrive at the Policy Enforcement Point (PEP) of the data or service provider. This request, together with the relevant information concerning the request (identification of the user, requested information, context) is forwarded to the Policy Decision Point (PDP). The PDP is the logical entity which will determine whether or not the user is authorized to perform the requested action. The PDP bases its decision on the policy rules made available by the Policy Administration Point (PAP), which stipulate under which conditions authorization may be granted. In order to establish whether these conditions are met, the PDP most likely needs additional information (e.g., relating to the capacity or role in which the user has been registered or a personal attribute of that user). This information is obtained from/through one or more Policy Information Points (PIP). Once the Policy Decision Point has evaluated the applicable policy rules and relevant policy information, it forwards its ruling back to the Policy Enforcement Point.

The CBSS offers a wide variety of services, including 42 transaction services.[72] For each of these services the CBSS specifies the required assurance level and corresponding authentication mechanism (username-password w/token, eID card). To gain access to services provided to institutions and groups, it is required that the user has been registered as a member of that particular organization or group by its local administrator. Specific capacities or mandates of individual users can be verified through authentic sources. Both the use of delegated administration and authentic sources will be discussed in greater detail under the following sections.

Finally, we note that practically all individuals with social security in Belgium are issued a social identity card (the 'SIS'-card).[73] The primary purpose of this card is to ensure that each individual is identified properly when interacting with entities of the social sector (through his/her INSZ number).[74] The card's chip also contains additional information, such as social

---

[69] See also H. Buitelaar (ed.), 'FIDIS D13.3: Study on ID number policies', September 2007, p. 63 et seq..

[70] Art. 4 of the Law of 15 January 1990 creating and Organizing a Crossroads Bank for Social Security (Belgian Official Journal, 22 February 1990). See also http://www.ksz-bcss.fgov.be/Nl/fluxdonnees/fluxdonnees_4.htm (last accessed 10 August, 2009).

[71] The description of the generic policy enforcement model provided here is based on the presentations of F. Robben, available at http://www.law.kuleuven.ac.be/icri/frobben/presentations.htm (last accessed 10 August, 2009), the documentation made available on the e-Health website (https://www.ehealth.fgov.be/ (last accessed 10 August, 2009)) and the OASIS standard XACML v2.0.

[72] See http://www.ksz-bcss.fgov.be/Nl/fluxdonnees/fluxdonnees_home.htm (last accessed 10 August, 2009) and http://www.ksz-bcss.fgov.be/Nl/bcssenbref/bcssenbref_1.htm (last accessed 10 August, 2009) .

[73] Art. 3 of the Royal Decree of 18 December 1996 prescribing measures for the introduction of a social identity card for all individuals with social security, Belgian Official Journal, 7 February 1997.

[74] F. Robben and P. Maes, 'De Kruispuntbank van de Sociale Zekerheid als motor van E-Government in de sociale sector', 2006, available at http://www.ksz-bcss.fgov.be/documentation/nl/documentation/Pers/De_KSZ_in_2006.pdf (last accessed 10 August, 2009), p. 15.

security status, health insurance fund registration number …[75] This information is encrypted and can only be decrypted by customized card readers in combination with a so-called Security Access Module (SAM) card.[76]

Policy makers have announced that for the majority of people the SIS-card will eventually be replaced by the eID card.[77] It is not envisaged that the data currently stored on the SIS-card will be stored in the eID card. Rather, access to this information will be provided through the CBSS and/or the recently launched e-Health platform.[78]

#### 4.4.2.4 E-Health[79]

The federal e-Health platform was launched in 2008, with the mission to support and facilitate electronic data exchange and service provisioning among all actors of the health care sector. Its assignments include, but are not limited to:

- specifying a basic architecture, and the technical norms and standards to be adhered to by participants;
- providing a platform for secure data exchange, and the basic services related thereto;
- managing and co-ordinating ICT-related aspects of data exchange from and to electronic health records, as well as electronic medical prescriptions;
- acting as a independent third party for the encoding and anonymization of health data for scientific research purposes or policy support.

In order to realize a platform for secure data exchange, the e-Health platform will provide several 'basic services'. A first of such services is an integrated system for user- and access management, to which we will return shortly. The e-Health platform will also provide services such as time-stamping, end-to-end encryption, and a secured electronic mailbox.

In addition to these 'basic' services, the e-Health platform will also provide a variety of 'value-added' services. Examples of such value-added services include: consultation of the insurance status of patients, transmission of electronic invoices from nurses to health insurance funds, cancer registration services, etc. This list is continuously being updated.

The purpose of the e-Health platform is not to store any medical data relating to patients, but to provide the platform which enables the exchange of such data among authorized actors. In the future, the e-Health platform will most likely also manage its own reference directory,

---

[75] Art. 2 of the Royal Decree of 18 December 1996 prescribing measures for the introduction of a social identity card for all individuals with social security, Belgian Official Journal, 7 February 1997.

[76] Rijksinstituut voor ziekte en invaliditeitsverzekering (RIZIV), 'Het gebruik van de SISkaart en van de SAMkaart', April 2003 (updated October 2004), available at http://www.riziv.fgov.be/care/nl/infos/sis-sam/pdf/sissam.pdf (last accessed 10 August, 2009), p. 11 et seq..

[77] Persbericht van de Ministerraad, 'Elektronische Identiteitskaart – omschakeling van de SIS-kaart naar de elektronische identiteitskaart', (Press communication by the Council of Ministers), 23 June 2006, available at http://www.presscenter.org/repository/news/514/nl/514c4600b477f9b727b51459cecfe286-nl.pdf (last accessed 10 August, 2009).

[78] See also Crossroads Bank for Social Security, 'e-Government Program of the Belgian Social Sector', December 2008, published at http://www.ksz.fgov.be/documentation/En/CBSS_2008.pdf (last accessed 10 August, 2009), p.16-17.

[79] This section is based on information obtained from the e-Health website (https://www.ehealth.fgov.be/ (last accessed 10 August, 2009)) and the Law of 21 August 2008 for the creation and organisation of the e-Health platform (Belgian Official Journal, 13 October 2008).

similar to that of the CBSS (indicating which data is available where, which entities have a 'relationship of care' with a particular patient, etc).

Individual users are authenticated by requiring them to use their eID card or their username and password in combination with their federal token. To gain access to services provided to institutions and groups, it is required that the user has been registered as a member of that particular organization or group by its local administrator. Specific capacities or mandates of individual users can be verified through authentic sources (see section 4.4.3). The authorization of users is based on the generic Policy Enforcement Model described earlier (see section 4.4.2.3).

We note that each data exchange over the platform is said to be logged by a 'Security Logging Module', specifying which entity has performed which action upon which personal data, at what time, and the application that was used to do so.

The e-Health platform is clearly being modelled after the architecture of the CBSS. Although it is said that the two networks, from a technical perspective, will operate independently of one another, the e-Health platform does and will probably continue to make use of several of the services provided by the CBSS.

### 4.4.3 Use of Authentic Sources

In the previous section we described the role of intermediaries for information exchange in Belgian e-Government. These intermediaries enable users to access what is commonly referred to as 'authentic sources'. An authentic source can be described as a data repository which has been recognized as being the most qualitative source of such information. Classic examples of authentic sources include the National Register and the Crossroads Bank for Enterprises.

One of the main principles of Belgian e-Government is that different governmental bodies should not be collecting the same information repeatedly from citizens and companies.[80] The information should be collected only once, be validated, and subsequently updated by one or more entities functionally responsible for managing this information. Once it has been validated, the information should be put at the disposal of all authorized users.[81] This notion of 'collect once, use many times' has been and continues to be an important driver for e-Government in Belgium.[82]

Authentic sources are also becoming an integral part of user- and access management in Belgian e-Government.[83] In practice, user privileges are often accorded because the entity in question displays certain characteristics (employee of a particular organisation or agency, the

---

[80] J. Deprest and F. Robben, 'eGovernment: the approach of the Belgian federal administration', 2003, available at http://www.ksz-bcss.fgov.be/documentation/fr/documentation/Presse/2003%20-%20E-government%20paper%20v%201.0.pdf (last accessed 10 August, 2009), p. 6.

[81] *Ibid*, p. 6.

[82] See also OECD e-Government Studies, OECD e-Government Studies – Belgium, 2008, available through http://www.fedict.belgium.be/nl/downloads (last accessed 10 August, 2009), p. 47.

[83] See F. Robben, 'Gebruikers- en toegangsbeheer: beschikbare diensten', presentation held at the E-Government Summit, Brussels, 8 November 2006, available at http://www.law.kuleuven.ac.be/icri/frobben/presentations.htm (last accessed 10 August, 2009). See also Belgian Privacy Commission, Recommendation nr. 01/2008 of 24 September 2008 concerning user- and access management in the governmental sector, 24 September 2008, p. 6, available at http://www.privacycommission.be/nl/docs/Commission/2008/aanbeveling_01_2008.pdf (last accessed 10 August, 2009).

quality of being a health professional, etc). By ensuring that the relevant characteristics can be verified through authentic sources, users' privileges may more easily be managed and kept up-to-date.[84] In 2007, FedICT reported to have implemented an authentic source for bailiffs, and to have obtained the approval to do the same for notaries.[85] The recently created e-Health platform also makes use of several authentic sources as part of its user- and access management (e.g., repositories listing health care providers and institutions).

Authentic sources have also been installed to maintain information on legal mandates. For several applications, citizens and companies have the ability to delegate privileges to third party service providers (e.g., accounting firms, social secretariats). We shall discuss how this system is organized in greater detail under the following section.

It has also been argued to further develop authentic sources of authorizations, specifying which actions may be performed under which conditions, and during which time-frame.[86]

To ensure proper implementation and use of authentic sources capabilities, it is also said that distributed user- and access management systems should be developed in accordance with the 'principle of Circles of Trust'[87]. It requires governmental agencies involved in a particular data exchange to make certain arrangements, among others with regard to which entities will be charged with performing authentication services, how the results thereof will be communicated in a secure manner, which entity will keep which logs, and the procedures which will enable full tracing of all processing activities.[88]

### 4.4.4 Delegated User and Access Management

In order for businesses or groups to be able to interact with the government in a digital environment, a system needs to be in place which allows them to identify the individuals within their organization that are authorized to act on their behalf.[89] A similar need arises when citizens or businesses wish to entrust the performance of certain legal actions with the administration to a third party (e.g., an accountant or social secretariat). To address these needs, the Belgian government has supplemented its identity management systems with two components: delegated administration and mandate registration.

---

[84] See also J.C. Buitelaer, M. Meints and E. Kindt (eds.), "FIDIS D16.3: Requirements for Privacy-Friendly Identity Management in eGovernment", 2009.

[85] FedICT, 'Activiteitenrapport 2007', published online at http://www.fedict.belgium.be/nl/binaries/Activiteitenrapport%20NL%2007_tcm167-22742.pdf (last accessed 10 August, 2009), p. 10.

[86] Belgian Privacy Commission, Recommendation nr. 01/2008 of 24 September 2008 concerning user- and access management in the governmental sector, 24 September 2008, p. 9 and F. Robben, 'Gebruikers- en toegangsbeheer: beschikbare diensten', presentation held at the E-Government Summit, Brussels, 8 November 2006.

[87] Belgian Privacy Commission, Recommendation nr. 01/2008 of 24 September 2008 concerning user- and access management in the governmental sector, 24 September 2008, p. 4.

[88] *Ibid*, p. 4.

[89] Crossroadsbank for Social Security, "Beschrijving van de component – Gebruikers- en Toegangsbeheer", ("Description of the component user- and access management"), not dated, available at http://www.ksz.fgov.be/documentation/nl/documentation/Pers/Bijlage_business_basisdiensten.pdf (last accessed 10 August, 2009).

#### 4.4.4.1 Delegated Administration

Delegated administration allows central IT administrators to selectively assign tasks and capabilities to remote ('local') administrators. In first instance delegated administration is used to decentralize user (de-)provisioning. Local administrators can generally create new users, provide them with the appropriate credentials, and decide which parts of an application they shall be authorized to use.[90]

This model was first implemented to manage the user privileges of civil servants, but has since been extended in order to allow private companies to express which of their employees are permitted to access one or more e-Government applications on their behalf.

A local administrator is designated by filling out a standard form, which must be signed by the legal representative of the organization. Once the form has been processed, the person designated as administrator will be issued a user ID and password, which allows him to register himself as such on the web portal of the Social Security[91]. This registration as local administrator has the result of including the administrator in the broader User Management for Enterprises system which is managed by the Crossroads Bank for Social Security.

The local administrator has the ability to create new users and is also charged with issuing passwords to members of his organization. He is also responsible for determining which applications are available to which user.[92] This model allows the government to centrally manage the authorization policies for its applications, whilst giving companies or groups the ability (and responsibility) to manage the user privileges of their individual employees or members.

#### 4.4.4.2 Mandate Registration

One of the first major accomplishments of the Belgian government in the area of 'high-impact services'[93] was the ability for citizens and businesses to file their tax declaration online (Tax-on-Web[94]). This application involves two types of delegation, namely delegated administration and agency. Whereas the former type of delegation is mainly technical in nature, the latter refers to a legal contract.[95]

When a citizen or business wishes to mandate an (external) accountant to file a tax declaration on its behalf, they shall need to complete a standardized form which serves as proof of the agency agreement between the accountant and her/his client. This form must be submitted to the relevant fiscal authorities, who will then register the mandate of the accountant.

---

[90] See also J.C. Buitelaar, M. Meints and B. Van Alsenoy (eds.), "FIDIS D16.1: Conceptual Framework for Identity Management in eGovernment", November 2008, p. 27 et seq.

[91] http://www.securitesociale.be/ (last accessed 10 August, 2009)

[92] The data repositories containing information as to which persons have been registered in which capacity by their local administrator essentially also act as an authentic source. If a user seeks to perform an action on behalf of an organization, the system will need to verify whether the user has in fact been registered by the local administrator of that organization in a capacity which authorizes him to perform the requested action.

[93] See http://ec.europa.eu/information_society/activities/egovernment/policy/impact/ (last accessed 10 August, 2009).

[94] http://www.taxonweb.be/ (last accessed 10 August, 2009)

[95] Note that the actions performed by local administrators can clearly also have legal implications, e.g., when he or an individual he provisioned submits a declaration on behalf of the organization. For this reason the local administrator is referenced in many documents as also being a 'mandate holder'. See, e.g., Crossroadsbank for Social Security, "Beschrijving van de component – Gebruikers- en Toegangsbeheer", ("Description of the component user- and access management"), p. 10.

In addition to being registered in a mandate repository, accountants themselves must also be registered in the User Management for Enterprises system by their local administrator.[96]

Since 2007 the mandates for Tax-on-Web are registered and managed through the MaGMa ('Generic Management of Mandates')-application (also operated by FedICT). This generic application allows civil servants, through a web-interface, to register, modify, consult and delete mandates that are relevant for a variety of e-Government services. Its purpose is to act as an authentic source of mandates towards other applications that need to rely upon this information.

A similar procedure has been implemented in a variety of sectors. For instance, employers have the possibility of mandating social secretariats to file reports with the social security administration on their behalf.[97] The recently launched e-Health platform also provides several delegation opportunities, e.g., for the registration of performances on behalf of medical professionals.[98]

### 4.4.5 Conclusion and Outlook

In 2003, an e-Government vision paper authored by representatives of FedICT and the CBSS stated that: 'In concrete terms, the co-operation between government levels in Belgium will lead to an ever expanding network of service integrators'.[99] It may be expected that the current approach will be extended to all sectors where advanced e-Government services shall be developed. The use of intermediaries and authentic sources will continue to play a major role in both service provisioning and user- and access management in Belgian e-Government. It remains to be seen how this architecture will be used when pan-European e-Government services are implemented on a larger scale.

## *4.5 Summary and Preliminary Conclusions*

The presented use cases exemplify the current state of the development within the field of IdM research in the sectors of commercial IMS deployment, open source initiatives developing protocol standards, governmental IMS solutions and user centric IdM solutions based on an EC-funded project.

In respect to the location where personal data is stored the systems vary and show a trend to authentic sources equally acting as a trust anchor for the retrieved information. While within the PRIME prototype all data is stored and managed locally by the user information that needs to be derived from third parties may be imported in the form of digital credentials. The governmental IMS system, as it is deployed in Belgium, bases on authentic sources for such data. Authentic sources are data repositories which have been recognized as being the most qualitative source for such information. Intermediaries provide a reference directory about

---

[96] This is necessary because individual accountants typically work for a larger legal entity, which in turn requires further (local) administration of user privileges.

[97] See Crossroadsbank for Social Security, 'E-Government binnen de sector van de sociale zekerheid – Aangifte van sociale risico's' ("E-Government in the social security sector – declaration of social risks"), not dated, available at www.vbo-feb.be/index.html?file=1583 (last accessed 10 August, 2009).

[98] See https://www.ehealth.fgov.be/binaries/website/nl/pdf/forms/formulaire_f3p_designation_mandataire_n.pdf (last accessed 10 August, 2009).

[99] J. Deprest and F. Robben, 'eGovernment: the approach of the Belgian federal administration', 2003, available at http://www.ksz-bcss.fgov.be/documentation/fr/documentation/Presse/2003%20-%20E-government%20paper%20v%201.0.pdf (last accessed 10 August, 2009), p. 47.

which information or service is available with which repository. Within the Microsoft CardSpace a dual approach has been chosen. So called personal cards are self-issued by the user, while managed cards link to data that is provided by organisations maintaining the actual data within their systems, e.g., credit card companies. OpenID provides a protocol for authentication and attribute exchange (optional). The specification for the authentication process described by OpenID does neither provide requirements in respect to the location where data is stored, as a user may choose an existing OpenID provider or set up her own infrastructure nor does it specify authentic sources. Future development will show, whether such systems will grow together once more governmental eID systems on national level evolve and how existing governmental and private IdM infrastructures may be incorporated in upcoming pan-European approaches.

# 5 Proposals for Revised Typologies of IMS

## 5.1 Typologies and Classifications of IMS – How and What for?

As pointed out by Bowker and Star (1999: 10) classification can be understood as a "spatial, temporal, or spatio-temporal segmentation of the world". Typically classifications aim at having the following, idealised properties that are difficult to implement (Bowker, Star 1999: 10):

1. Application of consistent and unique classification principles.
2. Use of categories that are mutually exclusive.
3. Completeness of the system.

They also point out that classifications are influenced by politics. Influences on the development may come from the social background of the authors, a purpose a classification is going to be used for, or semantic conflicts, e.g., arising from the need to design a classification that sounds "scientific" (Bowker, Star 1999: 66).

Looking into the typology of IMS proposed by Bauer, Meints and Hansen (2005) there clearly is a classification behind it. In this section a small analysis concerning this classification is carried out. The principles used for classification are:

- The control model used in the IMS (control by an organisation or the user concerned).
- The methods (or groups of technologies) used for the identity management (central account management, profiling techniques or user-centric methods).

Obviously these classifications principles are limited in uniqueness; for example control can be shared or distributed (e.g., federated), and profiling techniques today also may be used in the context of user centric methods (e.g., in history management functions). Possibly as a consequence the resulting categories are not mutually exclusive, as described in section 3.4. When the typology was developed, for example models for shared control were not broadly discussed, so the categories at that point in time were unique with respect to existing IMS. From today's point of view on the classification used one can conclude that the proposed typology is limited in its capacity to describe the current market of IMS.

However, the proposed typology never was meant to be understood as a classification. It was developed with the idea in mind to describe technical prototypes of IMS well understandable for the general public, while covering trends of the market at that time. So the classification scheme was largely influence by pragmatic considerations concerning the use of the typology. Meanwhile also parts of the pragmatic considerations have changed in the last four years, especially the market situation for IMS (see also Meints 2007 and 2008).

In the following section a approach to deal with this situation and to propose new typologies will be introduced. The approach is a modification of the IMS typology as already introduced.

## 5.2 The Clustering Approach

When further developing the original typology proposed by Bauer, Meints and Hansen (2005) one needs to take a look at its shortcomings. The most important shortcoming is (as already described) that IMS existing on the market increasingly show hybrid characteristics concerning the types. The reasons are:

- Shared or distributed control model.
- Application of two (or more) technical approaches (centralised account management, profiling and user centric methods).
- Two or more purposes for which the IMS are used; one example for this are social networks. From the point of view of the participants they are user centric and user controlled IMS, the operator of the social networking platform typically is making the turn around by targeted advertisements, based on profiling.

At least the first two aspects seem to be interlinked: certain technical approaches come along with a preferred control model. And in fact federation frameworks can be described as a combination of techniques for centralised account management and user centric identity management methods. The third reason for the shortcoming is not can not be dealt with in the original typology, as multiple purposes are not part of the classification behind it.

Bauer, Meints and Hansen (2005) already proposed a classification of IMS describing how relevant the identity management functionality is in the context of a product. For transparency reasons in the context of sets of classes we propose rearranging the numbering of the classes and adding one class as follows:

- Class 3: Identity management is main functionality (or economic core) of the product.
- Class 2: The product is no genuine IMS, but IMS functionality is relevant.
- Class 1: The focus of the product has nothing to do with identity management, nevertheless IMS functionality is included.
- Class 0: The corresponding type does not apply to the IMS.

A quite simple idea to deal with the described shortcoming is the combination of the typology and the classification. As a result every IMS is classified towards its type character. Every IMS is described through a set of three class values, relating to each of the three types. In the following table the IMS from the FIDIS IMS database[100] were investigated that are manufactured and used as IMS (resulting at least referring to one type in the class value 3). Theoretically 24 possible sets or clusters of class values are possible. The investigation shows that seven of them can be observed (sets of classes are grouped using one cluster number and the same background colour):

[100] See http://imsdb.fifid.net

| Cluster No. | IMS / class values | Type 1 | Type 2 | Type 3 |
|---|---|---|---|---|
| I | Visible Path | 0 | 0 | 3 |
| | Roboform | 0 | 0 | 3 |
| | Cockiepal | 0 | 0 | 3 |
| | KeyPass Password Safe | 0 | 0 | 3 |
| | Norton Password Manager | 0 | 0 | 3 |
| | LOAF | 0 | 0 | 3 |
| | CookieSwap | 0 | 0 | 3 |
| | MozPETs | 0 | 0 | 3 |
| | TOR | 0 | 0 | 3 |
| | Sxipper | 0 | 0 | 3 |
| II | Hushmail | 1 | 0 | 3 |
| | Jabber | 1 | 0 | 3 |
| | OpenPrivacy | 1 | 0 | 3 |
| | JAP / AN.ON | 1 | 0 | 3 |
| | Keygloo | 1 | 0 | 3 |
| | Entropy | 1 | 0 | 3 |
| III | Friendster | 1 | 3 | 2 |
| | Orkut | 1 | 3 | 2 |
| | Leverage Software | 1 | 3 | 2 |
| | LinkedIn | 1 | 3 | 2 |
| | Xing | 1 | 3 | 2 |
| | studiVZ | 1 | 3 | 2 |
| IV | Spamgourmet | 2 | 0 | 3 |
| | OpenID | 2 | 0 | 3 |
| | LID | 2 | 0 | 3 |
| V | Sxip Network | 2 | 1 | 3 |
| VI | Athens Identity Manager | 3 | 0 | 0 |
| | CaCert | 3 | 0 | 0 |
| | Shibboleth | 3 | 0 | 0 |
| | CIDAS | 3 | 0 | 0 |
| | Entegrity AssureAccess | 3 | 0 | 0 |
| | HiPath Sicurity Dirx | 3 | 0 | 0 |
| VII | Liberty Alliance | 3 | 0 | 2 |
| | CardSpace/Identity MetaFramework | 3 | 0 | 2 |

**Table 1: Sets of class values for selected IMS**

Even though many hybrid type IMS could be identified IMS of a single type seem to remain important on the market of IMS. In the database especially user controlled identity management tools (10 items in the database, cluster I, background colour green) and organisation-centric IMS solutions (6 items in the database, cluster VI, background colour purple) are two important groups. The remaining 19 IMS are of hybrid type, reflecting the fact that diversity of technology and distribution of control increases in the underlying identity management models.

While hybrid types evolve in recently developed areas such as web 2.0 some areas of application remain unchanged and require single type IMS such as profiling applications in the area of law enforcement or classical centralized account management functionalities for high security environments where access restriction and clear identification will remain necessary. The evolvement of hybrid types of IMS seems to reflect new demands on the market.

In this context it needs to be mentioned that user controlled IMS are understood as defined by Pfitzmann and Hansen (2008). In the majority of examples analysed in Table 1 user control is achieved by management of identity data stored locally on a computer under control of the user. In some cases management methods are transparent down to the code level. In difference to this approach user centric IMS include centrally managed components, so that transparency (notice) and / or choice of the user may be limited.

Two clusters (II and IV, background colours light blue and blue grey) show user centric IMS increasingly with a centralised component to implement a trust anchor. Neighbouring to these sets are identity management frameworks relying on a variety of strong centralised repositories and offering a client to select which of the centrally supported identities to use in which communicational context (cluster VII, background colour dark blue).

A cluster that currently is growing rapidly is composed of various social networking platforms, mainly relying on profile based advertisements in its economic core. The user's perception is of course different – for him social networks offer a platform to edit and maintain one's own profile, and, based on that profile, to get or keep in touch with others.

In the group of IMS analysed Sxip Network is rather exotic, combining a user controlled client with a centralised repository and server based profiles.

## 5.3 Typology Based on a New Classification

During the work on the classification of IMS, further discussion came up on an alternative approach to cluster the existing IMS. The attempt was made to define a set of categories that fulfil the requirements described in the introduction of this chapter (consistency, mutual exclusiveness, and completeness). Accordingly, the following three perspectives for a classification were derived. In addition metrics are suggested for these categories. Categories (perspectives) and the corresponding metrics are listed below:

- ***Control***: This perspective especially relates to the control of the data in an IMS. The metric we suggest covers the range from organisation centric to distributed systems for the control over the related ID data:
    - organisation centric, e.g., central storage of data with one controller,
    - federated systems, e.g., where data is shared or distributed over several systems and controllers,
    - distributed systems, e.g., data is stored on clients or with numerous controllers.
- ***Technology***: The second perspective focuses on the technical aspects. Here, a scale of four characteristics was chosen to segregate between the different ways how claims are handled in the system:
    - repository based systems,

- profile-based systems,
- reputation-based systems,
- self-declared systems.

- ***Process***: The last perspective of the categorisation relates to the focus of the IMS with regard to the procedural aspects and ranges ranging from centralistic infrastructures to processes with individual IMS:
  - infrastructure based solutions and monolithic approaches from one source, e.g., single sing-on, Active Directory,
  - hybrid systems,
  - process related IMS: Depending on each governmental or business process individual IMS are applied, e.g., one specialized IdM module with individual (partial) identities for the users per process or application.

## 5.4 Conclusion

The typology introduced in FIDIS deliverable D3.1 by Bauer, Meints and Hansen (2006) has been refined to overcome the identified limitations of this approach. The revised typology is able to reflect recent developments on the market of IMS. By including all three types of IMS into the analysis the recently evolving hybrid types of IMS can be described accurately. Also the view is broadened thus enabling an examination of the IMS's operators' economic interests as well as the involved technologies. The refined typology has been applied to a selection of IMS from the FIDIS database on IMS. It could also be shown that clusters of IMS with similar properties are formed allowing future research on such shared properties.

Further an alternative typology based on a new classification has been proposed. A detailed analysis and comparison of that classification system remains an area for future research work. It could in particular be interesting to investigate whether clusters formed under the proposed alternative classification will contain the same or similar elements as in the revised typology introduced in section 5.2 although the categories the classifications base on differ. It may be expected to find that entirely different types of IMS according to revised typology (e.g., III. social networks, VI. account management, see section 5.2) may mutually share the same value in the metric on one perspective, e.g., regarding organisation centric control, but show diversity in respect to another perspective such as the technology applied, e.g., repository versus profile based handling of claims.

Also the information value of the proposed classification remains area for future work, e.g., which conclusions in respect to possible benefits or threats for users may be drawn from the membership of an IdM in a certain group or cluster.

# 6 Summary and Conclusions

In this deliverable we observed and summarized findings on trends and developments of the IMS market, standardisation of IMS and in related research.

Based on the observation of products documented in the FIDIS IMS database a number of trends in the market of IMS were described:

- Further concentration of products in the market, especially type 1 IMS, while at the same time tools for user control are integrated in large identity management frameworks. As a result we increasingly observe type 1 IMS with a significant type 3 component. User centric components include the use of credentials (UProve, Idemix), and the possibility to use one identity, supported by an identity provider of the user's choice, enabled through the use of federation frameworks.
- Social networks became an important group of IMS in recent years, addressing various groups in the population such as pupils in school, students and business professionals. They are also a hybrid type of identity management systems, combining type 2 IMS (financing the platform through targeted advertisements) and type 3 IMS (self edited user profiles).
- The market of type 3 identity management tools and systems still remains very fragmented and to a low degree only driven by commercial players. Mostly tools are still developed in the Open Source community and the research community. Obviously browsers developed by the Open Source community, especially Mozilla Firefox, became an established platform for the integration of type 3 identity management tools.

Looking at the standardisation efforts in the IMS sector, there seem to be two clear trends. One trend is a movement towards federation and interoperability, mainly driven by the Liberty Alliance and OASIS concerning the standardisation of web services federation standardisation has reached quite far primarily through the work of Liberty Alliance but also through the OASIS work. Concerning federation standards for the general information system sector and the telecom sector the current and planned work in ITU-T and ISO/IEC seems to be promising. A big issue within the federation area seems to be the interoperability and harmonisation of the different federation standards and solutions. The Liberty Alliance initiated Project Concordia and the ITU-T focus group on IdM are efforts that are trying to address these areas.

The second trend is the drift from standards for organization centric IMS towards a more balanced suit of standards trying to find a reasonable balance between customers needs for security and privacy and the organisation or business needs for security and information at least regarding the standardisation efforts within the web services community and ISO. These trends in standardisation go hand in hand with the trends observed on the market of IMS and indicate that these trends are expected to remain stable for the following years by manufacturers on the market. A time line visualising the past development is presented in this deliverable.

One drawback of the development of IMS that are more and more complex and integrated solutions rather than simple out-of-the-box products is that decision making for the introduction of a new generation of IMS is increasingly difficult, especially in the context of

EIMS. In this deliverable a research approach aiming at a decision support framework, based on the balance scorecard approach, is presented. Based on initial key performance indicators in four relevant dimensions a framework for an organisation specific decision scorecard can be developed. The four dimensions include (1) requirements from the core business processes, (2) requirements from supporting processes such as ICT management, (3) information security and compliance, and (4) financial aspects.

Chapter four is dedicated to use cases from (1) commercial IMS, (2) research approaches, (3) the Open Source community and (4) governmental solutions. Windows CardSpace, the integrated PRIME prototype and OpenID demonstrate the increasing role user centricity, user control and privacy enhancement play in the first three developing sectors.

The described use case of the Belgian e-Government approach shows a public eID solution that is still mainly controlled by the state and shows privacy enhancement mainly by enhancing transparency of the processes to the citizen. This use case also shows how eIDs and related repositories need to be embedded in quite complex e-governmental infrastructures to enable the use in various governmental sectors and related applications.

Finally, the typology of IMS introduced by Bauer, Meints and Hansen (2006) is discussed in the light of the results of this deliverable. The increasing number of hybrid types of IMS observed in the market shows the limitations of this approach. A proposal for a revised typology of IMS has been presented. The clustering approach is based on the typology introduced by Bauer, Meints and Hansen. The application of the proposed typology to selected IMS from the FIDIS IMS database shows that it is able to describe the properties relevant IMS on the market show today. By broadening the view to all three types of IMS it makes it possible to have a look not only at the technological architecture of an IMS but also the economic aspects and interest behind the upcoming systems and to properly model them. The typology thus is useful for the classification approaches concerning IMS with differing degrees of user centricity, and social networks that show a commercial, profiling driven backend property that is quite different from the impression the user controlled interface creates.

A positive conclusion that could not be drawn in this way back in 2005 by Bauer, Meints and Hansen is that increasing user centricity and control becomes an integral part of many IMS and IMS-related standards, especially in the context of web services. However, partly the implementation of these improvements is still lagging behind where centralistic vendors or states apply IMS, for understandable reasons lined out, e.g., by Buitelaar, Meints and Van Alsenoy (2008) and Buitelaar, Kindt and Meints (2009). There is still quite some room for research addressing information security and privacy aspects of IMS, especially in the mentioned areas of application.

# 7 Bibliography

Alrodhan, W., Mitchell, C., 'Addressing privacy issues in CardSpace', at Third International Symposium on Information Assurance and Security, 2007, pp. 285-291.

Bauer, M., Meints, M., and Hansen, M. (eds.), 'FIDIS Deliverable D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems', Frankfurt a.M., 2005, available online: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf (last accessed 10 August, 2009).

Belgian Privacy Commission, 'Recommendation nr. 01/2008 of 24 September 2008 concerning user- and access management in the governmental sector', 24 September 2008, p. 6, available online http://www.privacycommission.be/nl/docs/Commission/2008/aanbeveling_01_2008.pdf (last accessed 10 August, 2009).

Bergmann, M., Crane, St., Fischer-Hübner, S., Pettersson, J. S., 'Human-Computer Interaction', PRIME Book (version 1), 18 July 2008, pp. 357-388, to appear.

Bergmann, M., 'PRIME Public Deliverable D11.2.b: User-side IDM Integrated Prototype V2', 30 March 2007.

Bowker, G. C., Star, S. L., 'Sorting Things Out', MIT Press, Cambridge, Massachusetts, 1999.

Buitelaar, H., Kindt, E., Meints, M. (eds.), 'FIDIS Deliverable D16.3: Requirements for privacy-friendly identity management in e-government', to appear Frankfurt a.M., 2009.

Buitelaar, J. C., Meints, M., Van Alsenoy, B. (eds.), 'FIDIS Deliverable D16.1: Conceptual Framework for Identity Management in eGovernment', Frankfurt a.M., 2008. available online: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp16-del16.1-conceptual_framework_for_identity_management_in_egovernment.pdf (last accessed 10 August, 2009).

Cameron K., 'Laws of Identity', Kim Cameron's Identity Weblog, 2005, available online: http://www.identityblog.com/stories/2004/12/09/thelaws.html (last accessed 10 August, 2009).

Cameron, K., Jones, M. B., 'Design Rationale behind the Identity Metasystem Architecture', Microsoft Cooperation, January 2006, available online: http://research.microsoft.com/~mbj/papers/Identity_Metasystem_Design_Rationale.pdf (last accessed 10 August, 2009).

Casassa Mont, M., Crosta, St., Kriegelstein, T., Sommer, D., 'PRIME Architecture V2' Public Deliverable D14.2.c, 29. March 2007, available online: https://www.prime-project.eu/prime_products/reports/arch/pub_del_D14.2.c_ec_WP14.2_v1_Final.pdf (last accessed 10 August, 2009).

Chadwick, D. W., 'Understanding X.500 – The Directory', 1996, available online: http://sec.cs.kent.ac.uk/x500book/ (last accessed 10 August, 2009).

Chappell, D., 'Enterprise Service Bus', 2004, O'Reilly Media.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W., 'RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile', May 2008.

Crossroadsbank for Social Security, 'E-Government in the Belgian social security sector – Belgian Best Practices', 2003, available at http://www.ksz-bcss.fgov.be/en/como/brochure%20definitief.pdf (last accessed 10 August, 2009).

Crossroads Bank for Social Security, 'e-Government Program of the Belgian Social Sector', December 2008, available online: http://www.ksz.fgov.be/documentation/En/CBSS_2008.pdf (last accessed 10 August, 2009).

Crossroadsbank for Social Security, 'Beschrijving van de component – Gebruikers- en Toegangsbeheer', ('Description of the component user- and access management'), not dated, available online: http://www.ksz.fgov.be/documentation/nl/documentation/Pers/Bijlage_business_basisdiensten.pdf (last accessed 10 August, 2009).

Custers, B. (ed.), 'FIDIS Deliverable D7.16: Profiling in Financial Institutions', Frankfurt a.M. 2009, available online: http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp7-del7.16.Profiling_in_Financial_Institutions.pdf (last accessed 10 August, 2009).

De Bot, D., 'Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart als belangrijkste juridische bouwstenen', Brugge, Vandenbroele, 2005.

De Cock, D., Wouters, K., Preneel, B., 'Introduction to the Belgian eID card – Belpic', in Public Key Infrastructure, 2004, Lecture Notes in Computer Science Book Series.

Deprest, J., Robben, F., 'eGovernment: the approach of the Belgian federal administration', 2003, available online: http://www.ksz-bcss.fgov.be/documentation/fr/documentation/Presse/2003%20-%20E-government%20paper%20v%201.0.pdf (last accessed 10 August, 2009).

Dumortier, J., Graux, H., 'eID interoperability for PEGS – National Profile Belgium', report for the IDABC study on European eGovernment Services, 2007, p. 20, available online: http://ec.europa.eu/idabc/servlets/Doc?id=31520 (last accessed 10 August, 2009).

ePractice, 'eGovernment Factsheet – Belgium – National Infrastructure', 14 February, 2007, last edited on 5 May, 2009, available online: http://www.epractice.eu/en/document/288183 (last accessed 10 August, 2009).

FedICT, 'De Universal Messaging Engine Versie 2', p. 7, published online at: http://www.belgium.be/eportal/ShowDoc/fed_ict/imported_content/pdf/FunctUME225022002.pdf?contentHome=entapp.BEA_personalization.eGovWebCacheDocumentManager.nl#search=%22UME%20directory%22, 25 February, 2002 (last accessed 20 June, 2006). Not online anymore; related: http://www.fedict.belgium.be/fr/binaries/UME-CASE_tcm166-9091.pdf (last accessed 10 August, 2009).

FedICT, 'Activiteitenrapport 2007', available online: http://www.fedict.belgium.be/nl/binaries/Activiteitenrapport%20NL%2007_tcm167-22742.pdf (last accessed 10 August, 2009).

FedICT, 'Gebruikershandleiding Digiflow 2.5.', (Digiflow User Manual), version 5, February 2008, available online: http://www.fedweb.belgium.be/nl/binaries/2009-02-06%20-%20Gebruikershandleiding%20Digiflow%202.5%20-%20NL_tcm120-39856.pdf (last accessed 10 August, 2009).

FedICT, 'e-Gov Architecture – Architectural Blueprint', not dated, available online: http://www.fedict.belgium.be/nl/downloads (last accessed 10 August, 2009).

FIDIS Database on IMS, available online: http://www.fidis.net/no_cache/interactive/ims-db (last accessed 10 August, 2009).

Hansen, M., Krasemann, H., Krause, C., Rost, M., Genghini, R., 'Identity Management Systems (IMS): Identification and Comparison Study', Kiel, 2003, available online: https://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf (last accessed 10 August, 2009).

Jonen A., Lingnau, V., Müller, J., Müller, P., 'Balanced IT-Decision-Card: Ein Instrument für das Investitionscontrolling von IT-Projekten', in Wirtschaftsinformatik 46(3) pp. 196-203, 2004.

Kaplan, R. S., Norton, D. P., 'The Balanced Scorecard: Translating Strategy into Action', Boston, 1996.

Kaplan, R. S., Norton, D. P., 'Strategy Maps', Boston, 1996.

Liberty Alliance, 'Liberty Alliance ID-FF 1.2 Specifications', 2002 available online: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications (last accessed 10 August, 2009).

Liberty Alliance, 'Liberty Alliance ID-WSF 2.0 Specifications', 2003, available online: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_1_1_specifications (last accessed 10 August, 2009).

Martinsons, M., Davison, R., Tse, D., 'The balanced scorecard: A foundation for the strategic management of information systems', in Decision Support Systems, 25 (1), pp. 71-88, 1999.

Meints, M. (ed.), 'FIDIS Deliverable D3.11: Report on the Maintenance of the IMS Database', Frankfurt a.M. 2007 available online: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.11.report_ims_database.pdf (last accessed 10 August, 2009).

Meints, M. (ed.), 'FIDIS Deliverable D3.15: Report on the Maintenance of the IMS Database', Frankfurt a.M. 2008, available online: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.15_Report_on_the_Maintenance_of_the_IMS_Database.pdf (last accessed 10 August, 2009).

Microsoft Corporation, 'About Information Cards and Digital Identity', 2008, Microsoft Corporation, 2008, available online: http://msdn.microsoft.com/en-us/library/ms734655.aspx (last accessed 10 August, 2009).

Microsoft Corporation, 'Introducing Windows CardSpace', Microsoft Corporation, 2008, available online: http://msdn.microsoft.com/en-us/library/aa480189.aspx (last accessed 10 August, 2009).

Microsoft Corporation, 'Identity Selector Interoperability Profile V1.0', April 2007, Microsoft Corporation, 2007.

Miles, M. B., Huberman, A. M., 'Qualitative data analysis', 2nd ed. Sage, Thousand Oaks et al. 1994.

OASIS, 'Security Assertion Markup Language (SAML) V2.0 Technical Overview', Committee Draft 02, 25 March 2008, available online: http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf (last accessed 10 August, 2009).

OASIS, 'Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)', OASIS Standard Specification, 1 February, 2006, available online: http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf (last accessed 10 August, 2009).

OASIS, 'WS-Trust 1.3', OASIS Standard, 19 March, 2007, available online: http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf (last accessed 10 August, 2009).

OASIS 'Web Services Federation Language (WS-Federation) Version 1.2', Committee Draft 02, January 7, 2009, available online: http://www.oasis-open.org/committees/documents.php?wg_abbrev=wsfed (last accessed 10 August, 2009).

OECD e-Government Studies, 'OECD e-Government Studies – Belgium', 2008, available online: http://www.fedict.belgium.be/nl/downloads (last accessed 10 August, 2009).

Persbericht van de Ministerraad, 'Elektronische Identiteitskaart – omschakeling van de SIS-kaart naar de elektronische identiteitskaart', (Press communication by the Council of Ministers), 23 June 2006, available online: http://www.presscenter.org/repository/news/514/nl/514c4600b477f9b727b51459cecfe286-nl.pdf (last accessed 10 August, 2009).

Pfitzmann, A., Hansen, M., 'Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management', Dresden, 2008, available online: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf (last accessed 10 August, 2009).

Prien, B., Leenes, R. (eds.), 'FIDIS Deliverable D3.12: Federation – What's in it for Costomers and Consumers?', Frankfurt a.M. 2009, available online: http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp3-del3.12.Federated_Identity_Management.pdf (last accessed 10 August, 2009).

Rijksinstituut voor ziekte en invaliditeitsverzekering (RIZIV), 'Het gebruik van de SISkaart en van de SAMkaart', 2003 (updated October 2004), available online: http://www.riziv.fgov.be/care/nl/infos/sis-sam/pdf/sissam.pdf (last accessed 10 August, 2009).

Robben, F., 'eGovernment: the approach of the Belgian federal administration', 2003, available online: http://www.ksz-bcss.fgov.be/documentation/fr/documentation/Presse/2003%20-%20E-government%20paper%20v%201.0.pdf (last accessed 10 August, 2009).

Robben, F., Maes, P., 'De Kruispuntbank van de Sociale Zekerheid als motor van E-Government in de sociale sector', 2006, available online: http://www.ksz-

bcss.fgov.be/documentation/nl/documentation/Pers/De_KSZ_in_2006.pdf (last accessed 10 August, 2009).

Robben, F., 'Gebruikers- en toegangsbeheer: beschikbare diensten', presentation held at the E-Government Summit, Brussels, 8 November, 2006, available online: http://www.law.kuleuven.ac.be/icri/frobben/presentations.htm (last accessed 10 August, 2009).

Royer, D., Meints, M., 'Betriebliches Identitätsmanagement – Enterprise Identity Management – Towards a Decision Support Framework Based on the Balanced Scorecard Approach', in Wirtschaftsinformatik, 2009 pp. 284-294, available online: http://www.springerlink.com/content/t1m2186u41636qlx/ (last accessed 10 August, 2009).

Sermersheim, J., (Ed.), 'RFC 4511: Lightweight Directory Access Protocol (LDAP): The Protocol', 2006.

Tor Project, "Tor: anonymity online", The Tor Project, 2008, available online: http://www.torproject.org/ (last accessed 10 August, 2009).

Van Alsenoy, B., De Cock, D., 'Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card', in Datenschutz und Datensicherheit, March 2008.

Van Asch, K., 'The Federal Authentication Service', 2008, available online: http://www.cevi-users.be/new/tmp/fedict.pdf (last accessed 10 August, 2009).

Walter, S. G., Spitta, T., 'Approaches to the Ex-ante Evaluation of Investments into Information Systems', in Wirtschaftsinformatik 46 (2004) 3, pp. 171-180.

Websites for further reading on topics related to section 4.4 on e-Government solutions (last accessed 10 August, 2009):

http://www.ehealth.fgov.be/

http://www.eid.belgium.be/

http://www.fedict.belgium.be/

http://www.fedweb.belgium.be/

http://www.godot.be/

http://www.ksz-bcss.fgov.be/

http://www.law.kuleuven.ac.be/icri/frobben/presentations.htm

http://www.securitesociale.be/

http://www.taxonweb.be/

# 8 Annex

## 8.1 Abbreviations

| | |
|---|---|
| BSC | Balanced Scorecard |
| CBSS | [Belgian] Crossroads Bank for Social Security |
| EDM | Enterprise IdM Decision Matrix |
| eID | Electronic Identity |
| EIMS | Enterprise Identity Management Systems |
| ESB | [Belgian] Enterprise Service Bus |
| FAS | Federal Authentication Service |
| FedICT | Belgian Federal Public Service Department for Information and Communication Technologies |
| FIDIS | Future of Identity in the Information Society |
| FP6 | Sixth Framework Programme |
| FSB | [Belgian] Federal Service Bus |
| HTML | Hypertext Markup Language |
| ICT | Information and Communication Technology |
| ID | Identity |
| ID-FF | [Liberty Alliance] Identity Federation Framework |
| ID-WSF | [Liberty Alliance] Identity Web Services Framework |
| IdM | Identity Management |
| IEC | International Electrotechnical Commission |
| IMS | Identity Management Systems |
| ISO | International Organization for Standardization |
| ITU-T | Telecommunication Standardization Sector on behalf of the International Telecommunication Union (ITU) |
| JTC 1 | ISO/IEC Joint Technical Committee 1 |
| LCC | Life Cycle Costing |
| LDAP | Lightweight Directory Access Protocol |
| MaGMa | Belgian for: Generic Management of Mandates |
| n/a | not available |
| OASIS | Organization for the Advancement of Structured Information Standards |
| OpenID | open, decentralized standard for user authentication |

| | |
|---|---|
| OSI | Open Systems Interconnection |
| PAP | Policy Administration Point |
| PDP | Policy Decision Point |
| PEP | Policy Enforcement Point |
| PIP | Policy Information Point |
| PKI | Public Key Infrastructure |
| PPDM | Privacy Preserving Data Mining |
| PRIME | Privacy and Identity Management for Europe (FP6 project) |
| ROI | Return on Investment |
| ROSI | Return on Security Investment |
| SAM | Security Access Module |
| SAML | Security Assertion Markup Language |
| SC 27 | Sub Committee 27 (of ISO/IEC Joint Technical Committee 1) |
| SGML | Standard Generalized Markup Language |
| SIS | [Belgian] Social Identity Card |
| SOAP | Simple Objects Access Protocol |
| SOX | Sarbanes-Oxley Act |
| TCO | Total Cost of Ownership |
| UME | Universal Messaging Engine |
| URL | Uniform Resource Locator |
| VETRO | Validate, Enrich, Transform, Route, Operate |
| WG | Working Group |
| WS | Web Service |
| XML | Extensible Markup Language |
| XRI | Extensible Resource Identifier |

## 8.2 Index of Figures



## 8.3 Index of Tables