FIDIS

Future of Identity in the Information Society

Title:	"D4.2: Set of requirements for interoperability of Identity Management Systems"
Author:	WP4
Editors:	James Backhouse (LSE) Michael Vanfleteren (KU Leuven)
Reviewers:	Els Soenens (VUB, Belgium) Paolo Spagnoletti (Luiss University, Italy)
Identifier:	D4.2
Type:	[Deliverable]
Version:	1.1
Date:	Tuesday, 20 December 2005
Status:	[Final]
Class:	[Public]
File:	fidis-wp4-del4.2.Set_of_requirements.doc

Summary

This report highlights the spread of opinion amongst a group of European experts in application areas of identity management on the issue of interoperability of such systems. It builds from an earlier report that presented a literature review and an account of research in interoperability. It uses the three-part conceptual framework of technical, formal and informal dimensions through which to frame the questions posed and interpret the answers given. The 23 interviewees from 5 different European countries, while differing in detail, display a remarkable consensus on much of the issues. Application areas from which the experts are drawn cover egovernment, ehealth and ecommerce, and while, given their specific nature, there may be many points on which such areas diverge, the likelihood of interoperability is deemed to turn on a small number of key questions, mostly non-technical. Importance is given to building trust in the citizen and end-user through good communication, usability, compliance with data protection and privacy principles.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

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

Members of the FIDIS consortium

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

Versions

Version	*Date*	*Description (Editor)*
0.1	25.09.05	• Initial release based on editorial meeting with Michaël Vanfleteren (John Baptista)
0.2	05.10.05	• Added edited interviews and agreed structure of document (John Baptista)
0.3	15.10.05	• Added ecommerce chapter (Michael Vanfleteren)
0.4	17.10.05	• Final draft (John Baptista)
0.5	25.10.05	• Revised draft for editorial review (James Backhouse
0.6	07.11.05	• Changes made based on reviews (John Baptista)
1.0	11.11.05	• Final version (James Backhouse)
1.1	20.12.05	• Final delivery version

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)*
Introduction	James Backhouse (UK, LSE)
Background, methods and panel of interviewees	John Baptista (UK, LSE)
Themes addressed in the interviews	John Baptista (UK, LSE)
ecommerce	Michael Vanfleteren (KUL, Belgium)
egovernment	John Baptista (UK, LSE)
ehealth	John Baptista (UK, LSE)
Towards a set of requirements	James Backhouse (UK, LSE)
Conclusion	James Backhouse (UK, LSE)
Report 1: Marc Sel, ecommerce	Els Kindt (KUL, Belgium)
Report 2: Oliver Libon, egovernment	Michael Vanfleteren (KUL, Belgium)
Report 3: Paul Timmers, egovernment	Michael Vanfleteren (KUL, Belgium)
Report 4: Frank Robben, ehealth	Xavier Huysmans (KUL, Belgium)
Report 5: Bernd Burkert, ecommerce	Martin Meints (ICPP, Germany)
Report 6: Bettina Neke, ehealth/egovernment	Martin Meints (ICPP,Germany)
Report 7: Hannes Federrath, ecommerce	Andreas Westfeld and Sandra Steinbrecher (TUD, Germany)
Report 8: Gerhard Weck, ecommerce	Andreas Westfeld and Sandra Steinbrecher, (TUD, Germany)
Report 9: Bettina Müller, ehealth	Andreas Westfeld and Sandra Steinbrecher, (TUD, Germany)
Report 10: Rüdiger Dierstein, ehealth	Andreas Westfeld and Sandra Steinbrecher (TUD, Germany)
Report 19: Herbert Leitold, ecommerce	Stephan Freh (LSE, Austria)
Report 20: Arno Hollosi and Bernd Martin, egovernment	Stephan Freh (LSE, Austria)
Report 21: Heinz Otter, ehealth	Stephan Freh (LSE, Austria)

Summary of key contributors:

- LSE: James Backhouse, John Baptista, Stephan Freh and Christopher Lovold
- K.U.Leuven R&D: Els Kindt, Michaël Vanfleteren and Xavier Huysmans
- ICPP: Martin Meints and Martin Rost
- TUD: Andreas Westfeld and Sandra Steinbrecher

Table of contents

1 EXECUTIVE SUMMARY

James Backhouse, LSE and Michaël Vanfleteren, K.U.Leuven

This report highlights the spread of opinion amongst a group of European experts in application areas of identity management on the issue of interoperability of such systems. It builds from an earlier report that presented a literature review and an account of research in interoperability. It uses the three-part conceptual framework of technical, formal and informal dimensions through which to frame the questions posed and interpret the answers given. The 23 interviewees from 5 different European countries, while differing in detail, display a remarkable consensus on much of the issues. Application areas from which the experts are drawn cover egovernment, ehealth and ecommerce, and while, given their specific nature, there may be many points on which such areas diverge, the likelihood of interoperability is deemed to turn on a small number of key questions, mostly non-technical. Importance is given to building trust in the citizen and end-user through good communication, usability, compliance with data protection and privacy principles.

While a selection of some 13 full interviews is provided in the Appendix (3 from each partner), Chapters 5, 6 and 7 provide analytical summaries of the responses in the 3 application areas. Readers are directed to review the interviews in the Appendix as they contain interesting and detailed reference to the current state of play in the respective countries and application areas.

2 INTRODUCTION

James Backhouse, LSE

The aim of this deliverable is to investigate the high-level requirements for interoperability of identity management systems and to prepare for a survey on the topic to be undertaken in 2006. This is the second written deliverable in Work Package 4 on interoperability within the FIDIS Network of Excellence. It builds on the conceptual groundwork set out in deliverable 4.1[1] taking the schematic overview of technical, formal and informal elements and using it to review expert opinion in three key areas of development that were declared as the main focus for WorkPackage 4 at the outset – ecommerce, egovernment and ehealth. The experts were selected from 5 countries: Austria, Belgium, Germany, Norway and the United Kingdom and this enabled a reasonable spread of approaches and experiences to the issues under scrutiny.

2.1 This deliverable

The objective of this report is to canvass expert opinion on interoperability using the concepts and findings that emerged from the first deliverable 4.1 of this Work Package and in effect to validate that literature review by sounding out the responses of experts in the field. Given the trajectory of work in this Work Package, with best practice guidelines and a survey planned, it was important to be able to validate the ideas that emerged from the earlier work to see whether they were robust enough to support the later investigations. This deliverable is important because it allows us to develop the requirements for interoperability that will be essential for the proper functioning of so many of the e-systems that are being planned and launched. Without proper regard to interoperability, many administrative and service delivery systems will remain isolated and fragmented, while cross-border systems will remain just a dream.

As befits the FIDIS network of excellence, this deliverable has been realised thanks to a community of researchers working together from different perspectives on common objectives. The value of this deliverable results from the quality of the interviews and analysis, with contribution from 11 different researchers in 4 different institutions. The number of interviews carried out amounted to 23 from 5 countries and the level expertise and domain knowledge of the respondents was clearly high. The interview reports have significant independent value - they have been edited to include context and analysis. The summaries in 3 core chapters are only meant as guidelines and the interviews represent in themselves a valuable testament to the state of informed thinking on this subject currently.

Appropriately this exercise has taught some lessons, or rather reinforced existing ones. Project management remains a very important skill when running collaborative exercises of this kind as is a clear commitment to a sound methodology and good communication. We are indeed very grateful to the respondents featured here for their

[1] http://www.fidis.net/fidis_del.0.html#511

generosity in making time and space for our work to proceed and complete. It was no mean task for 11 researchers in 5 countries to organise interviews and get feedback on the reports during the summer period.

Overall, we can point as key learning from this exercise that requirements contain technical, formal and informal elements. There was considerable agreement that, of this trinity, the most important barrier to interoperability remains the informal and cultural one. Clearly there are specific issues attached to the particular type of system, so that egovernment and ehealth have different features that emerge as key for the experts, but in general there is a considerable degree of uniformity of landscape for all three chosen application areas.

2.2 Structure of this document

In the next chapter (chapter 3), we present the methodology used and the panel of interviews. In chapter 4, we discuss the main themes addressed in the interviews and the process that led to their choice. In the next three chapters, we summarise and analyse all interviews. In chapter 5, we analyse the interview in the ecommerce sector. In chapter 6, we analyse the interviews in egovernment, and in chapter 7 we analyse the interviews in ehealth. Chapter 8 provides a global overview of the interviews in all sectors and proposes a new model of requirements for establishing interoperability. In chapter 9, we conclude the substance of our deliverable. In chapter 12 we include a selection of 13 interviews which we found of key relevance for this deliverable.

3 METHODS AND PANEL OF INTERVIEWS

John Baptista, LSE

In deliverable WP 4.1 we reviewed the literature and projects on the interoperability of Identity Management Systems. We proposed an adapted conceptualisation of this topic and illustrated its applicability using case studies. We also highlighted key issues in the literature which we found to be critical in this area of research. In this deliverable we use the key findings from the review in the first deliverable to canvass 23 experts in 5 countries in Europe on their views of those key topics. The interviews were conducted by 11 interviewers from the 4 core FIDIS institutions that contributed to this deliverable.

3.1 Methodology

Owing to the number of people involved in this process (11 researchers) and the decentralised nature of the project (4 institutions working in 5 different countries) considerable effort was put into maintaining a consistent methodology and project management. Coordination was mostly conducted by email but the editorial team also met face to face during the analysis stage.

In the first stage we analysed D4.1 looking for key themes that, based on the literature review, looked to be critical. We then sent a list of topics to the network of researchers and asked for suggestions, and we assessed the relevance of the three suggested sectors of analysis (ecommerce, egovernment and ehealth). As a result of this interaction we developed a final list of topics that we then converted into questions. In the next stage, we sent the interview questionnaire to all contributors and requested all partners to organise interviews with key experts in identity management in the three sectors. The four participant institutions arranged 23 interviews in 5 European countries.

The interviews took place during the summer months of 2005 in June, July and August (see appendix 1 for the complete schedule). This timing proved to be difficult because most interviewees were on holiday or busy during most parts of this period. Because of the delays in conducting the interviews, this report suffered some delay given its original deadline.

In order to maintain standardisation and consistency and to help during the analysis stage, all participants used the same questionnaire. Some interviews were recorded and where recording was not possible, interview notes were taken. The LSE, as coordinator of this deliverable, wrote the first interview report and circulated among the 11 researchers to be used as a reference for all other interview reports. All reports followed this guideline and a selection of 13 can be consulted in the Annexes of this document.

A small editorial team was then created between the LSE and KUL to analyse all interview reports and write this final deliverable based on the 23 interview reports

received. We first read the interviews and discussed key common themes among the interviews. We then agreed on a structure of themes and analysed the interview using those key themes as guides. We then summarised the findings from the interviews in the three chapters of this document creating three different sections for each of the three sectors of ecommerce, egovernment and ehealth.

We do not include all 23 interviews reports in the annexes of this deliverable document due to space limitations. We selected 13 of the most relevant for inclusion and aimed to include at least three reports from each partner. Out of the 23 reports from all partners we selected 13 with the following distribution among the partners: 3 reports from LSE, 4 reports from KUD, 2 reports from ICPP and 4 from TUD. Each report contains a combination of direct transcriptions of the most relevant quotes from the interviewee and contextual information added after the interview for a better understanding of the issues discussed. This additional effort in providing context to the interviews makes the reports rich and of independent significance, providing a valuable contribution to FIDIS research. Therefore, the analysed summaries of the interviews in the three core chapters of this deliverable are intended as guidelines only and they do not substitute the reading of the rich interview reports included in the annexes.

3.2 Panel of experts

The selection of experts was decentralised and decided by the four institutions separately according to their own contacts in the three sectors. The key requirements for all partners were that the interviewees had to be recognised experts in their field and that they were available and happy for their views to be published in this report. Some respondents requested that certain documentation and parts of the transcripts of the interviews to be kept confidential. However all agreed that we could use their views for the analysis.

As described before, we looked for experts in the three chosen sectors: ecommerce, egovernment and ehealth. Each partner had to identify experts in the three sectors to interview. The following tables show the interviews conducted in the three sectors.

Table 1: Interviews in the **ecommerce** sector

	Country	Interviewer	Interviewee	Profile
1	Belgium	KU Leuven, Els Kindt	Marc Sel	Director Pricewaterhousecoopers, Antwerp, Belgium. Responsibility for projects, including the Belgian Electronic ID card project as well as the Belgian Digital Tachograph Project.
5	Germany	ICPP, Martin Meints	Bernd Burckard	Technical project manager for the PKI-infrastructure of the Federal Land of Hessen. Project manager for the project "HCN 2004", which is one of four elements of the so called "egovernment Masterplan"[2] of the Federal Land of Hessen.

[2] See http://www.hessen-egovernment.de/mm/Masterplan.pdf; current version: 1.3

7	Germany	TUD, Andreas Westfeld and Sandra Steinbrecher	Hannes Federrath	Full professor for management of information security at University Regensburg. His research interests are security and privacy in communication networks, development of systems that provide anonymity and unobservability, location management strategies considering privacy in mobile communication systems, cryptography, steganography and data security. He is the leader of the project AN.ON/JAP, Anonymity Online, which enables users to surf the Internet anonymously and unobservably.
8			Gerhard Weck	Gerhard Weck is a licenced IT Baseline Protection Auditor and Chief IT Security Officer at INFODAS. His working focus is security of operating and information systems and the development of the IT security database at INFODAS. He is IT security lecturer at the Ulm Academy for Data Protection and IT Security (Ulmer Akademie für Datenschutz und IT-Sicherheit, www.udis.de) and spokesman of the DECUS professional group for security (www.decus.de)
11 **12** **13**	Norway	LSE, Christopher Lovold	Virginia T. Ringnes Arild Lund and CasperChristophersen Semming Austin	*Central Bank of Norway* Casper Christophersen is in the payments department, and works with technical issues that are associated with payments that involved the Central Bank. Arild Lund is the head of the financial stability department at the Central Bank of Norway. Virginia Ringnes works as a translator in the communications department. Semming Austin works in the Financial Stability department under Payment Systems. He has recently be instrumental in defining and acquiring a new payments settling system for the Central Bank
14			Erik Lindmo	*DNB NOR bank* Erik Lindmo has a MSc in civil engineering from Stanford, CA, and has been working in the banking sector for 25 years. He is currently the CIO for payment systems in DNB NOR, and has been working on the BankID project for the past year.
15			Nils Inge Brurberg	*Nordea Bank* Nils Inge Brurberg has been involved with the Norwegian BankID project and has been instrumental in formulating business logic, application requirements and implementation. He has also been involved in talks with Nordea (and other banks) in Sweden and Denmark in exploring the possibilities for BankID expansion across borders in Scandinavia.
19	Austria	LSE, Stephan Freh	Herbert Leitold	Mr. Herbert Leitold holds the position of Director Technology at A-SIT, Zentrum für sichere Informationstechnologie – Austria. A-SIT is a

				friendly society and was founded by the Austrian Ministry of Finance, the Austrian National Reserve Bank and the Technical University Graz in 1999. Its mission is to undertake ICT research for the use of egovernment. In recent years A-SIT worked closely with the IKT-Board and the CIO of Office of the Austrian Federal Chancellor. Mr. Leitold is the author of several international recognized studies including topics on eVoting, eID Solutions and electronic signatures. Mr. Leitold is further an advisor to the Austrian government on egovernment projects.
22	UK	LSE, James Backhouse, John Baptista and Chris Lovold	Mark Drew	*British Telecom* Mark Drew is Principal Researcher in the BT Security Research Team (BT Research Labs). He has over 30 years experience in IT security in banking and consultancy sectors.
23			Tom Buschman	*Shell* Tom Bushman is within Shell responsible for the TWIST project (Transaction Workflow Innovation Standards Team). TWIST is a not-for-profit industry group delivering non-proprietary XML standards aimed to enable straight through payments processing between businesses from end to end.

Table 2: interviews in the **egovernment** sector

	Country	Interviewer	Interviewee	Profile
2	Belgium	KU Leuven, Michaël Vanfleteren	Olivier Libon	Project Manager, FedICT Security Architect (FedICT: Federal Public Service on Information and Communication Technology; www.fedict.be). Adviser for the Tractebel Group and the European Commission, he then joined GlobalSign (the European leading certification authority) as Vice President. He joined FedICT (the Belgian ministry of ICT) in 2002 before the launch of the BelPIC project (Belgian electronic Personal Identity Card) as security architect and PKI expert
3			Paul Timmers	Paul Timmers is head of unit for egovernment in the European Commission, Directorate-General Information Society & Media. Previously he was a member of the Cabinet of the European Commissioner for Enterprise and Information Society. Dr. Timmers has also been deputy head of unit for electronic commerce in the European Commission, where he was involved in policy and program development. He has published on a wide range of topics, including a book on electronic commerce strategies and business

				models. A visiting professor and lecturer at various universities and business schools.
6	Germany	ICPP, Martin Meints	Bettina Neke	Ministry of Social Affairs of the Federal Land of Schleswig-Holstein, working for the e-health card project in Schleswig-Holstein. Mrs. Neke works as officer in the Ministry of Social Affairs Schleswig-Holstein. Within the Ministry she is co-ordinating all political activities concerning this project. She has a professional background as lawyer.
16	Norway	LSE, Christopher Lovold	Asbjørn Følstad	Asbjørn Følstad is a research scientist in the ICT division working on interoperability, quality assurance and usability of information systems. Recent work has involved assessing the level that trust plays in system adoption and system use when new technologies are introduced. SINTEF Group is the largest independent research organisation in Scandinavia. Every year, SINTEF supports the development of 2000 or so Norwegian and overseas companies via their research and development activity.
20	Austria	LSE, Stephan Freh	Arno Hollosi and Bernd Martin	Mr. Arno Hollosi (2005) joined the Stabstelle IKT-Strategie des Bundes in 2001 and he was since then been its Technical Director. The Stabstelle IKT-Strategie des Bundes is also called Chief Information Office (CIO) of the Austrian government. Mr. Hollosi is responsible for developing and coordinating the technical aspects of the egovernment projects in Austria.

Table 3: interviews in the **ehealth** sector

	Country	Interviewer	Interviewee	Profile
4	Belgium	KU Leuven, Xavier Huysmans	Frank Robben	Mr. Robben is general manager of the Crossroads Bank for Social Security, an institution he conceived and founded. The Crossroads Bank for Social Security elaborates the E-government strategy within the Belgian social sector and coordinates the implementation of the E-government projects in this sector.
6	Germany	ICPP, Martin Meints	Bettina Neke	Ministry of Social Affairs of the Federal Land of Schleswig-Holstein, responsible for the e-health card project in Schleswig-Holstein. Mrs. Neke works as officer in the Ministry of Social Affairs Schleswig-Holstein. Within the Ministry she is responsible for all political activities concerning this project. She has a professional background as lawyer.
9	Germany	TUD, Andreas Westfeld & Sandra	Bettina Müller	Bettina Müller is specialist in neurology and specialist in psychiatry and psychotherapy. Since

		Steinbrecher		fifteen years she is senior consultant and for more than ten years head of a neurological department. She is an expert in IT security for the medical area of application at the Gesellschaft für Informatik (GI, http://www.gi-ev.de)
10			Rüdiger Dierstein	Mr Dierstein is founder member and honorary member of the Gesellschaft für Datenschutz und Datensicherung (GDD, German Society for Data Protection and Data Security), member and fellow of the Gesellschaft für Informatik (GI, German Society for Informatics), spokesman of the executive board IT security of the GI for several years, and lecturer for IT security at the Technische Universität München since 1972
17	Norway	LSE, Christopher Lovold	Espen Haavardsholm	*Hospital Doctors in Norway* Espen Haavardsholm is currently working as a doctor at Diakonhjemmet Sykehus in Oslo. This hospital also houses a large research centre at which Haavardsholm is currently working on his PHD in Rheumatoid Arthritis.
18			Ingunn Hellebostad Toft	Ingunn Hellebostad Toft reports on her experience working in a hospital in Eid and in the medical centre at Stryn on the West coast of Norway. Her work has given her unique insight into the concerns and differences of how district health services operate as opposed to those that are located in larger urban centres.
21	Austria	LSE, Stephan Freh	Heinz Otter	Director of Chipkarte. Mr. Heinz Otter (2005a) joined the SVA (Sozial Versicherungsanstalt – Social Security Office) as project manager in 1997. Mr. Otter was since then responsible for coordinating the eCard Project and he recently became appointed to Director Strategy at SV-Chipkarten Betriebs- und Errichtungsges.m.b.H.

One key requirement for the interviews was to have expert views on each sector from various countries in Europe so that in the analysis we could compare and contrast the approaches of different countries. We also wanted to involve experts from various backgrounds to cover the legal, technical and social dimensions.

The tables above show the diversity and richness of the contributions for this deliverable. For example, in the ecommerce sector we interviewed a Director of PriceWaterhouseCoopers in Belgium, representatives of three large banks in Scandinavia and the Director of the A-SIT European project. In egovernment we interviewed Austrian and German government officials and the Director of egovernment for the European Commission. In ehealth we interviewed hospital doctors in Scandinavia, ministers for ehealth in Germany and the government manager for ehealth card in Austria.

We believe that the above interviews have provided a solid basis for deriving key requirements for interoperability in Identity Management Systems.

4 MAIN THEMES ADDRESSED IN THE INTERVIEWS

John Baptista, LSE

As described in the methodology section above, the themes for the interviews were in the first instance derived from the previous deliverable, D4.1 "A structured account of interoperability approaches". In that document we reviewed the key literature in this field and the most relevant projects. From the literature review we developed a conceptualisation of interoperability at three levels: technical, formal and informal. We now expand on these three levels and use the experts to gather requirements at the technical, formal and informal levels of interoperability.

We focused our analysis in three sectors: ecommerce, egovernment and ehealth. These sectors were considered critical for identity management by the FIDIS network and agreed by the partners of WP4 as the most relevant for further analysis.

The questionnaire starts with identification of the key identity issues in the expert's field. We query the importance of interoperability in that context. We ask for the interviewee to explain his/her own understanding of the meaning of interoperability. We follow this up with a question about how the experts see an ideal scenario of a full interoperable world. The next questions address directly the requirements for establishing interoperability at the three levels (technical, formal and informal). We ask about the benefits and barriers for the main stakeholders involved (users, government and merchants) and gather expert's opinion on what actions are required from these stakeholders for improved interoperability. Lastly, we ask their views on the role of governments, users and merchants in this process.

There are 9 key themes addressed in the questionnaires. Each key theme was then translated into one or more questions. The following is a list of the themes and questions used during the interviews.

1. Main identity issues
   - What are the main identity management issues in the chosen field of analysis (e-government, e-health, e-commerce)?

2. Importance of interoperability
   - How critical is the issue of interoperability of IMS for this field?

3. Definition and what is enabled
   - How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?

4. Ideal scenario of full interoperability
   - Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?
   - How far are we currently from that scenario?

5. Requirements for users, governments and merchants

- What are the requirements for interoperability for the USERS?
- What are the requirements for interoperability for the GOVERNMENTS?
- What are the requirements for interoperability for the MERCHANTS?

6. Benefits for users, government and merchants
   - What are the benefits of interoperability for each of these stakeholders?

7. Barriers for interoperability
   - What is hindering the establishment of interoperability at the technical, legal and cultural levels?

8. Actions and relative importance at the technical, legal and cultural levels
   - What can be done at the TECHNOLOGICAL level to establish interoperability?
   - What can be done at the LEGAL/POLICY level to establish interoperability?
   - What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?
   - Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

9. Role of government, merchants and users to foster interoperability
   - What should be the role of governments in addressing interoperability of IMS?
   - What should be the role of merchants and industry groups?
   - Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

We now provide a summary and analysis of the interviews in the three sectors of the analysis. The next chapter (chapter 5) is focused on ecommerce. Chapter 6 focuses on egovernment and chapter 7 on ehealth.

5 ECOMMERCE

Michael Vanfleteren, Xavier Huysmans and Els Kindt, KU Leuven

Country	Interviewer	Interviewee
Belgium	KU Leuven, Els Kindt	Marc Sel
Germany	ICPP, Martin Meints	Bernd Burckard:
Germany	TUD, Andreas Westfeld and Sandra Steinbrecher	Prof. Hannes Federrath Dr. Gerhard Weck
Norway	LSE, Christopher Lovold	Virginia T. Ringnes Arild Lund and Casper Christophersen Semming Austin Erik Lindmo Nils Inge Brurberg
Austria	LSE, Stephan Freh	DI Herbert Leitold
UK	LSE, James Backhouse, John Baptista and Chris Lovold	Mark Drew Tom Buschman

5.1 Main identity issues

The experts emphasised that several issues were at stake on identity management.

First of all, as suggested by Mr Sel (Annex, 13.1 Report 1, p 51) for any identity management system (IMS), it is necessary to understand that individuals operate in distinct ‘spaces’ in which they act with different characteristics. In general, four ‘spaces’ can be defined:

- government
- private
- commercial
- PPP (private-public partnerships)

He continues, these ‘spaces’ are in principle separate and do not interact, unless explicitly designed to do so. One of the issues is to understand to what extent individuals, who are assumed to control the identity management application, would desire to act as one and the same interoperable individual across these ‘spaces’. In other words, one of the basic questions is whether individuals require interoperable IMSs?

Interoperability of IMSs could lead to a loss of privacy. Consequently, either the IMSs may be confined to a specific ‘space’ or it will be the individual who will decide in which ‘space’ she/he will act and/or which individual information could be shared across the ‘spaces’.

Secondly, one of the cornerstones of an IMS is an adequate management of the privacy and data protection issues. Interoperability is often seen as opposed to privacy. As an example, it is unlikely that individuals want to give up their privacy which they enjoy in the distinctive ‘spaces’ and which they may enjoy nowadays without interoperable systems. The use of privacy profiles, which are transparent,

understandable and manageable by the end-users could be a tool to offer such privacy. Privacy must be protected. A solution proposed by Mr Sel is the use of privacy profiles. Privacy profiles seem therefore very important for any identity management system.

Moreover, identity management in e-commerce has only a chance to succeed if it is clear from the beginning that the user remains in control of the identity management system. Interoperability of systems as such will not be accepted by the users unless it is, by default, controlled by the user.

Another important issue is on security. Identification must be secure and this security must be guaranteed. For Mr Leitold, it is the art of "egovernment application design" to find a solution with ensures high interoperability when necessary but that at the same time guarantees a highly secure and privacy-rich environment.

Mr Weck pointed out that for him the main issue has to be found in accountability.

5.2 Importance of interoperability

Interoperability is currently seen either as an important issue or as being uncritical.

At national level, interoperability issues have been discussed for a long time. However, interoperability issues at the EU level only became a real point of discussion at late stage. As explained by Leitold, European countries usually develop their national solutions without thinking in European terms first and only at a later stage think about European collaboration.

As already introduced, across the different spaces, there should be no interoperability, or full control of the end user. But within a given 'space' as described above, it is likely that individuals will use and want to use interoperable trusted identity systems. This is also correct for e-commerce as it will lead to additional benefits of the users, such as in efficiency, but also in privacy, if privacy profiles are correctly implemented. Within a given space, interoperability is critical, especially in interconnected transactions.

Example: as consumer, we like convenience when ordering a plane ticket, combined with a rented car and a hotel. So interoperability is good. However, we don't want to be further bothered by cross-selling efforts from the rented car company 3 months later when they learn that we are embarking on another trip.

Weck says that there are only isolated applications at the moment. Consequently the interoperability of IMS is relatively unimportant for ecommerce. However, with the growth and development of applications, IMS might become critical

5.3 Definition and what is enabled

Different definitions are proposed for interoperability in e-commerce.

- Interoperability is the technical connection between systems with the goal to exchange information – on a European level across borders. An interoperable ecommerce eID supported solution is able to work between technologically different systems. Interoperability is a major necessity that ultimately enables identification and authentication of IMS in ecommerce. (Leitold)

- Another definition of interoperability could be that a system can take reliance on the form and contents of another system's judgment or service outcome. Interoperability of IMS should in the first place rely on the ability of the system to identify and authenticate a given individual. This is particularly important in the field of e-commerce, where individuals have to be identified online or in a remote way. This functionality to identify persons, however, should be in a given, well-determined and specific way. This should allow using a trusted identity more than once and in several systems (interoperability). In addition, the IMS system should allow for authorisation(s). This would mean that the system should allow for identity and access management. The design of an authorisation functionality, however, is much more complex, but is a factor which may be an enabler of interoperability. (Sel)

- The function of an interoperable IMS should be to enable the user to apply an identity used in one application also to another application. Such systems have compatible authentication mechanisms that are a prerequisite for interoperability.

5.4 Ideal scenario of full interoperability

The experts described the systems which were in use in their countries. Some experts when discussing an ideal scenario shifted from the ecommerce to the egovernment context. We summarise what they answered regardless:

- Austria (Leitold) says that the concept of the Austrian Citizen Card entirely fulfils the interoperability requirements on a national level. However, on a European level there is still much to do as currently only 2 countries (Italy and Estonia) have solutions interoperable with Austria. Additional countries (i.e. Finland and Belgium) will soon be integrated. The goal should be to have a solution which is fully interoperable with all European national authentication and identification solutions. The EU is still a long way from a European-wide interoperable eID solution. As mentioned earlier, European countries usually develop their national solutions without thinking in European terms first and only at a later stage think about European collaboration. Apart from some EU projects like GUIDE or FIDIS, there is hardly any structured EU-wide discussion about interoperable eID solutions. Relatively early on Austria passed laws such as the Electronic signature or egovernment law which are required for a national eID solution, while some European countries are far behind.

Although Austria passed a law which allows the acceptance of other countries eIDs for egovernment purposes, there is no structured integration process of other countries eID solutions. Integration processes are more or less individual projects and on *ad-hoc* basis.

- Belgium (Sel) There seems to be a difference between developments taking place in the public and those in the private sector. In the public sector, the developments for an

interoperable eID are under way. From September 2004, electronic identity cards (eID) are being distributed to all Belgian citizens living in Belgium. The eID is a plastic card, in the format of a banking card, with an electronic chip. The eID contains personal information printed on the card, including picture, name and written signature. The personal information is also electronically stored on the card, and also includes the digital signature and certificates of the owner of the card. The eID allows the owners/users of the card to consult their own personal information kept in the central personal register[3], but also to contact, exchange or file information with the government.

In the private sector, it seems that private companies have not yet made much progress in the development or use of interoperable identity management tools. Initiatives exist, such as the IBM Tivoli software system[4], but are not yet widespread.

- Other experts presented elements which should be considered as important in order to reach a system which would meet their requirements. For Weck, an interoperable system would be based on certificates. The problem is that what hinders the development of interoperability is incomplete or imprecise existing standards. Mr Lindmo presented a BankID project in Norway, which is a cooperation between the five major financial institutions/banks in Norway to establish a fully interoperable PKI based electronic ID system. He believes it could be the solution for the future.

5.5 Requirements for users, governments and merchants

Different requirements have to be taken into account:

For the users

For the users to accept IMS, it will be important that there is a correct balance between the 'automatic' interoperability of identity and the control that users desire to exercise over the use of their identity. In any case, privacy and anonymity are key factors for the interoperability of IMS for users.

Another aspect is transparency. What is important is that the solution is easy to understand and not too sophisticated technologically because most people, for instance, use their paper-based driving licence for identification purpose and that has been true for more than a generation (Leitold)

In the same vein, for Følstad, the most important and challenging issue with electronic identities is users' understanding. Users are accustomed to physically signing papers, handling ID cards, and being asked for forms of identity in stores or other service outlets. In the electronic environment, users are not always aware of when they are releasing information about themselves, or how much information is being released. As such, there is a tendency to over-release when asked for ID online. It is therefore important to be sure that people know what they are doing when using eIDs.

[3] www.mijndossier.rrn.fgov.be.
[4] See at http://www-306.ibm.com/software/tivoli/

Therefore, when people's entitlement is affected, there can be inappropriate gains and losses in the market that negatively affect trust and participation by users (Sel).

The closely related problem to people's understanding of eIDs is that these need to be easy enough to use. If users are bothered too much with the management or handling of eIDs, they are not going to have any incentive to use them over conventional IDs.

Mr Drew thinks that in addition to the development of potentially massive number of unique IDs, people are going to want to have multiple IDs per person. This has to do with a desire for anonymity, but also to do with the inherent nature of people to act in different capacities throughout their lives. Those who have a job, a private life, and possibly multiple social commitments, are actors in multiple environments, all of which need separate IDs both to protect their privacy, but also to differentiate their level of access to data in different capacities to avoid conflict of interest situations[5].

For the governments

To reach an efficient level of interoperability, the services of the government need to be coordinated efficiently[6]. Coordination seems to be a key element of the development of interoperability for the governments.

As for the users, transparency has also been pointed out by experts as an important element for governments. It is of extreme importance for the success of an interoperable citizen card that the users in the government agencies trust the system, see a clear advantage in it and find the solution as an improvement for doing their daily work. If we want to have a further integration of the EU 25 member eID solutions, it will only be possible if the integration can be achieved by adding additional connectors centrally. If the integration of other eID solution also requires adoption of all the locally installed client solutions, the integration would not be possible because of the high cost and complexity. (Leitold)

One of the additional requirements is that the technical tools and means need to be available in order to realise interoperability.

For the merchants

Several requirements are expected on the merchants' side:

-Merchants require from an IMS system its security and reliability. Some companies may use an internal IMS, which is designed to offer accountability and quality assurance within the company - two essential requirements. The IMS creates mutual trust and quality assurance within the global company. However, although national eID could be used internally, it is probably not going to be used for the whole external system. (Marc Sel)

5 An example of this happening already is people's use of multiple e-mail addresses, or their tendency to establish multiple user accounts at the same online vendors to purchase things in different capacities (such as for personal use vs. business use).

6 In Belgium, the FEDeral organisation for Information and Communication Technologies (FEDICT) was established in order to initiate, elaborate and advise on the e-government projects for the federal services: www.fedict.be

-Companies are usually very much under pressure to be cost-efficient. Therefore, businesses should be able to capitalise where possible on the progress of the government in the establishment of IDMs. Such progress could be, for example, the establishment and the issuance of eID cards. Other (public) institutions could also develop such tokens. Credit cards do not seem to be a valuable alternative for such IMSs. Although the use of a credit card is widespread, one cannot expect or require every individual to hold one

5.6 Benefits for users, government and merchants

Most experts agree on the benefits for each of the stakeholders.

As a general thought, with an interoperable IMS system, reliability and trustworthiness is increased, ecommerce is strengthened and efficiency is improved for the users (citizens), the governments and the merchants.

Moreover, for the user, it brings comfort, makes communication easier via electronic channels and provides better services.

From the government point of view, it indirectly stimulates the economy, provides greater efficiency and should save costs by way of standardisation

Finally, interoperability of IMS not provides more efficiency for the merchants, lowers costs by implementing user requirements for interoperability and it facilitates cross-selling for merchants where in the interest of the customers. Internal IMS systems of merchants and companies are driven by the need for accountability of the individuals working with such global companies.

5.7 Barriers for interoperability

Barriers were analysed at three different levels: Technical – Legal – Cultural

Technological/technical barriers

In some countries, interoperability seems to have been fully achieved (Austria[7] – Leitold). However, at EU level, standards should be defined in order to grant technical interoperability. In the same vein, the expert says that any system which is defined in a way that it does not require any specific hardware is most likely easily interoperable with other national solutions. It can be concluded that the use of specific technology (i.e. smart card, etc.) would hinder interoperability at a technical level.

On the other hand, Marc Sel says that one of the obstacles is the existence of massive installed legacy databases. It will take a long while, probably decades, before they are all replaced by systems which enable interoperable IMSs. Technology will also have to meet the different interests of the parties involved; Users may want restricted interoperability, over which they keep control, while merchants favour more far-

7 The Austrian Citizen Card is an open system and it does not depend on any specific hardware. “It can be concluded that the solution is fully interoperable”. (Leitold).

reaching interoperability, for example, to be able to cross-sell. Moreover, the merchants as a group may not be interested in cooperating with each other, because they also have different interests and may lose competitive advantage if they work with interoperable IMS.

Legal barriers

One problem comes from the fact that some countries come with their own solutions and as it has been noted by Weck, particular countries naturally try to push through their solution, which of course may create problems.

Another obstacle comes from the fact that the legal framework needs to be further adjusted to the use of interoperable and cross-country IMS. The legal gaps need to be identified by the specialists.

As an example, Leitold says that the EU Signature Directive was not sufficient to fulfil Austria's requirements on privacy and data protection. This will most likely also be the case with other EU country's legislative regulations. As a result most EU members will pass additional laws that might hinder interoperability on a legal level.

Cultural barriers:

One of the biggest cultural problems comes from the force of habit. Weck notices that people are used to established structures and are tied to existing infrastructures, so that it makes them reluctant to change. Leitold explains that because of immense differences in the historic backgrounds of countries a European-wide interoperable eID solution will take a while. Austria for example is a country in which only a minor percentage of the population owns an ID card, which makes it difficult to elaborate a full IMS system.

Interoperability of IMS is also often not well understood and therefore, creates doubts and uncertainty in the minds of the users, government and merchants. At the specific side of the users, there is also fear of surveillance, of 'big brother' watching everything they do, and of potential misuse (Sel). Moreover, as a result of the EU Signature directive, an eID solution designed only according to this directive is not workable in practice. For example the EU Signature Directive defines that identification is also sufficient after a specific transaction has been completed. In practice this is not possible as most working processes require an identification and even authentication before a specific working progress can be started. This is only a small example but shows that most EU member states will handle their processes in different ways. These different work practices and many other issues will hinder a European-wide interoperability on a cultural level.

Finally, Weck underlines a lack of knowledge. It is hard to see where interoperability is missing. Moreover, there are targeted attempts to let interoperability fail (hoping for an advantage in competition).

5.8 Actions and relative importance at the technical, legal and cultural levels

Technical:

At the technological level, there is the feeling that the development of common technical standards would help interoperability (Leitold, Weck).

It will be of importance which level of technical detail these standards define. One recommendation should be to define the technical standards at the highest possible level: at the policy level rather than on the IT artefact level.

The standardization is necessary because the current methods for verifying IDs, such as providing a utility bill or a driver's licence are not adequate in today's market to prevent fraud (Drew). The consequence of not having an accurate system (for identity checking and verification) will be that we will get duplicates. This in turn will affect people's entitlement.

Other tools, such as the development of the 'Universal Message Engine' tool will be necessary to make different systems and languages interoperate. It is obviously also important to have user-friendly systems because low trust in new technology often comes from poor usability.

Legal:

The challenge to create an interoperable environment in IMS is huge. For some experts, there is the feeling that there will probably never be a global system. Even a European identity system seems – politically - a rather big challenge.

Recommendations or also regulations to utilise specific standards could be issued to accomplish interoperability, but also funding will support it. Moreover, Mr Sel underlines the fact that interoperability requires open standards. Open standards should be promoted and in some cases be required (see for example, the recent actions of the EU Commission towards Microsoft). Nevertheless, policy decisions need to be taken. Within the EU community, a policy decision as to the use of smart cards as ID carrier and management tool as opposed to checks against centralised databases seems to have been taken. Smart cards are preferred because the user has more control over the use of her/his identity information. This is an important policy decision.

However, Mr. Leitold is not convinced that the EU member states are yet in the position to discuss the legal domain of eID interoperability. For him, the member states have still to engage in a serious discussion on the policy level. This has not yet happened. It is true that there are some research efforts such as GUIDE or FIDIS but there is no broad discussion taking place.

Cultural:

The experts proposed several actions to help interoperability but they do not seem all to take into account the impact of the cultural aspects.

For Mr Sel, it is by showing the cultural benefits of interoperability that interoperability could be improved. The IMS systems could be used to facilitate or promote skills, for example, learning languages. For others, the countries have to decide for themselves whether and what kind of national identity solution they want to implement and at a second stage they can discuss European consequences. Others also think that increased pressure should be put on manufacturers to implement standards precisely. For example, Microsoft frequently implemented standards, but they had a snag, i.e. they had proprietary properties to make the interoperability with competitor's products fail.

Importance of the 3 factors:

Although the experts agree on the main actions to be undertaken at the different levels, their views are not similar when it comes to their rating. It is therefore interesting to list the different approaches.

Mr. Leitold ranks the cultural/institutional factor as the first in terms of importance; he considers the policy aspect as being also very important; legal and technical aspects follow. This order is explained by the fact that eID projects are high profile projects, politically very controversially discussed and extremely costly. Therefore, a country has to create a vision first before it can think about a specific solution.

As national eID solutions often challenge constitutional rights and deal with the very basic rules of democratic society, no decision can be made on EU level in the first place – only in a second step after the member countries made their individual decision.

As an example Mr. Leitold points to the failure of eTEN. eTEN is the European Community Programme designed to help the deployment of telecommunication networks based services with a trans-European dimension (Information Society and Media DG 2005d). The program is split into the following six research areas: egovernment, ehealthcare, eInclusion, eLearning, Services for SMEs (eBusiness), and Trust and Security services components. eTEN focuses heavily on the legislative level as well as on the technical level. However, it hardly addresses issues at the informal level and it is found that eTEN has low relevance to interoperability (Freh 2005). Mr. Leitold confirms that this analysis is correct and he outlines that because of the missing discussion on the policy level eTEN was doomed to fail from the outset.

Mr Sel puts in another perspective. First of all, for him policy decisions need to be taken and the legal framework should allow or facilitate the development of interoperable IMS. The legal and policy factors are therefore to be seen as the basis and the prime factors to deal with. Almost at the same time, technology needs to come up with answers and solutions to problems of operability. If the technology is not there, there is no need to consider the interoperability of IMS issue at the legal or policy level. Finally, institutional and cultural acceptance of the interoperability conclude the development towards interoperable IMSs. We see that Mr Sel puts importance on the fact that technical aspects must be present to allow the development of the others. So does Mr Weck who underlines that technological level is the most important, then the legal/policy level follows and finally the cultural/institutional.

Another element was presented by Mr Lindmo. Mr Lindmo said that the most important thing to understand is not the technical side of the ID market. To fully understand ID markets one must understand the concept of two-sided markets. Lindmo then refers to the importance of considering both aspects to ensure success of electronic IDs as "two-sided markets".

In the ID market, the two sides that need to be considered are:
- those who receive an ID
- those who must trust another's ID

Simply resolving the technical side of interoperability is not enough. Lindmo emphasized that the other aspects mentioned are the more challenging hindrances to successful interoperability.

5.9 Role of government, merchants and users to foster interoperability

Governments:

Obviously, governments have important roles to play, roles which they have not always fulfilled.

Following the experts, the impact of governments' actions regarding interoperability should be assessed by the following criteria:

- Governments have to create a vision on a specific IMS, to state clearly the goals and define the requirements of the solution proposed. eID egovernment applications are usually more complex than commercial eID solutions owing to the greater number of stakeholders involved.
- Governments should further invest in country-wide eID processes, such as for example, the distribution of eID cards. This could be used by industry as a reliable basis for the further development of IMS[8].
- Governments should therefore offer funding and information and should establish pilot projects to spread standards.
- Asbjørn Følstad presented his view by saying that there have been attempts by government organizations to establish ID systems in a top-down manner, but not enough resources have been allocated for any of these to become efficient. As such, most currently active initiatives (in the field of electronic identification) have gone over to a bottom-up approach where industry is leading.

Merchants

As a common perception by the experts, merchants and industry groups should ideally be the enablers of an eID solution, creating the infrastructure and carrying the main brunt of the costs. In return, they should be able to generate revenue by offering

8 An example of the development of an interoperable IMS by the government is the tachograph system, that has been developed on the European level. See Commission Regulation N° 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport, http://www.digitach.be/NL/PDF/1.2.2.CommissieVerordening13602002.pdf (last visited on 11 August 2005)

services in connection with the eID. To put it another way, they have to be the driving force to spread the technology, because they earn the money and will negotiate the investments.

Major players, such as for example companies in banking or consulting, have developed their own internal transnational network systems, including interoperable identity features. Examples are Swift, or PricewaterhouseCoopers. They work with their own standards in proprietary networks. Their interoperable IMS, however, is not used in their external communication networks. Another model is being implemented by TWIST[9] as consortium led by Tom Bushman (interviewee from Shell). TWIST aims to define open standard payment systems which can be freely used by all merchants in the network to for payment transfers. In this system, identity management is one of the key factors and they have joined up with Identrus for this purpose. TWIST is a unique approach in the sense that it is based on open standards and will shake the business model of proprietary networks if it becomes widely adopted.

As described above, industry should be able to rely on the investment and efforts of the governments in IMSs. Where the basic structures for IMSs are developed by governments, merchants could without doubt offer additional value to the IMSs. On the other hand, however, it is also possible that each industry will want to remain in its own 'space'.

Moreover, within the industry sector, Mr Lindmo believes that the easiest method for electronic identity to be disseminated into societies is by the banks. Although there are many industries that could offer e-IDs, none have such an infrastructure of users who regularly connect to their services online as banks. This frequency of use means that users will be used to using the eIDs, will have less problems forgetting passwords, or how to use their accounts, and will be agile enough to take advantage of other services that might be associated with the eID throughout the market, such as online vending, or egovernment. The existing cooperation common to the banking industry, and their position within the financial communities puts them in a unique position to be the provider of these IDs.

Users

Users are the receivers of the developed systems. They don't have an important active role in the development of IMS but they need to understand the value of the systems proposed. For this reason, accurate and reliable information is necessary. In order to favour interoperability, one should also show the benefits to the communities of the users. Without interoperability, too many IMS will exist and will complicate life.

In addition, a common terminology is seen as a requirement in order to explain the issues of interoperability to the users. This terminology should be the same or should be useable in different areas, such as privacy and identity management.

[9] More information on http://www.twiststandards.org/

6 EGOVERNMENT

John Baptista, LSE

The interviews for the egovernment sector were the following:

Country	Interviewer	Interviewee
Belgium	KU Leuven, Michael Vanfleteren	Olivier Libon Paul Timmers
Germany	ICPP, Martin Meints	Bettina Neke
Norway	LSE, Christopher Lovold	Asbjørn Følstad
Austria	LSE, Stephan Freh	DI Arno Hollosi DI Bernd Martin

6.1 Main identity issues

Libon points out that the main identity issues are in establishing collaboration among different government bodies at the political level. He notes that the federal state political system in Belgium, where competencies are distributed between the various authorities, makes it impossible to offer integrated services without collaboration among the different governmental bodies in the country. For him, central administration must act as enabler removing obstacles and creating the correct environment for cooperation.

Timmers, in his position as head of the egovernment unit in the EU, sees the main issue related to changing the culture of public administration towards a more modern system.

Hollosi and Martin are responsible for developing and coordinating the egovernment projects in Austria, headed by the Stastelle IKT-Strategie des Bundes (also called the Chief Information Officer of the Austrian government). One of the most important projects of this unit is the implementation of the Austrian Citizen Card which will become the "Official identity document" used for all electronic administrative procedures. Interoperability is seen as critical in this project and the slogan for the card is "Open interfaces for egovernment". Hollosi and Martin said that the main issues with the interoperability of identity systems to be security, privacy, costs (High costs must be justified with reasonable added value) and the legal framework.

6.2 Importance of interoperability

Libon referred to the critical importance of interoperability in security and exchanging criminal records. Interoperability in criminal records was seen as more important for interoperability of eID systems because he saw less demand for cross-border functionality in ID cards. Libon also points out the importance of establishing common rules about names, categories and understanding of the terms. He sees his

role as head of the Fedict (Belgium's Ministry of ICT) as key to establishing this common syntactic and semantic interoperability.

Timmers sees interoperability in identity systems as the key driver for innovation and progress in Europe. For him identity management and interoperability across member states remains a key driver for innovation and progress in Europe. He positions interoperability as an issue related with eID projects. He has promoted European collaborative research projects in this area because of previously lack of understanding and fragmented approaches.

Both Hollosi and Martin held interoperability to be a critical factor in the success of the new Austrian identity card. Platform independence was considered essential for selecting the technology infrastructure for this project.

6.3 Definition and what is enabled

Libon sees interoperability as a way to exchange information and services between systems and different stakeholders without effort from either side. An interoperability framework is comprised of policies, standards and rules describing the arrangements that organisations agree to "talk" to each other.

Libon sees interoperability at three levels:

- Syntactic: structure of data
- Semantic: common definitions of terms
- Transactional: ability to use systems decentralised

Libon also states that interoperability requires actions at three levels:

- Organisational: defining rules and responsibilities of the various actors involved
- Semantic: creating agreement between various parties on meaning of terms
- Technical: creating standards for presentation, processing and exchange of information

Timmers also refers to three levels: Semantic, organisational and technical. For Holosi and Martin highlighted the importance of semantic interoperability across countries.

6.4 Ideal scenario of full interoperability

For Libon, an ideal system is one that respects privacy and transparency for the user and one that can be used digitally from home. There should be one document comprising driving licences, ID card, passport, etc… renewed every 5 years in their local government agency. He sees the implementation of this system in two phases. The first is one of integration of data and the second of establishing synergy among ministries. For Libon the main challenges are in creating a financial model that makes it financially interesting for all parties to adopt the same systems and in developing common laws and a regulatory framework.

Timmers refers to the existing European projects on egovernment, the sub-group for eEurope Advisory Group and the importance of cross-border use of the identity systems. He sees an ideal system as one that not only makes sense for public administration but also makes sense for the private sector. Timmers stated that the

objective is by 2010 interoperable electronic identification and authentication should be available and used in a number of practical cases of key importance (cross-border electronic procurement, citizen mobility and others). Timmers also refers to the key importance of trust in the egovernment services. Both Hollosi and Martin referred to the Austrian card as a reference model and said that a particularity of this model is the inclusion of the Power of Attorney.

6.5 Requirements for users, governments and merchants

For Libon, the new system should not just map the paper-based system into the digital environment, rather, new processes should be created. The new system should be user-centred rather than government-centred. For him, users require simplification and privacy. They also want faster services, more convenience, fewer contact points and increased transparency and participation on decisions for sharing personal information. Governments are more concerned with data management and the legal environment for data exchanges. Governments require sound governance models for managing information, appropriate information management policies and solid information regulation. Libon also refers to the creation of a government platform to which all ministries could connect and share data. He sees syntax and semantic agreement as the main requirement in developing this platform.

From the government perspective, Timmers highlights the need for establishing a common terminology which he sees as a starting point to tackle the problem. Timmers sees as the key requirement for users to have easy access and transparency of the internal administrative processes. The system should be user-centric and users should not need to replicate data entries: the user should be given the possibility of using the same data across applications. Users also require data protection, privacy, citizen rights and democratic control.

However, for Timmers, the most important aspect is that users should feel that the system works properly and they trust it. He sees trust and acceptance as a vital issue for technology adoption. Creating awareness and communicating to the users is critical.

Hollosi and Martin say that in Austria the new ID card ensures that a person cannot be tracked across various databases, as every sector, or even application, must use a different identifier. This regulation is an important and specific requirement in the Austian egovernment legislation. They also say that users want to be able to use the card at home through their computers. This requires new equipment (card readers). For governments the main requirement is security and communication with the users.

6.6 Benefits for users, government and merchants

Hollosi and Martin maintain that the main benefit for the users is that they can carry out their public administration procedures from their homes over the internet. Another benefit is that this solution is highly secure and may also improve the security of other applications such as ecommerce. Users will also have faster processing of requests and convenience. Merchants gain the same type of benefits as users. The main benefits for the government are speed, efficiency and costs.

6.7 Barriers for interoperability

Libon identifies the main problems at two levels:

- Communication: lack of a culture of exchanging information and talking to each other
- Interpretation: even when different parties "talk" to each other, there are problems of meaning when they don't share the same interpretative frames.

Timmers views the main challenges as establishing interoperability at the organisational and semantic levels. He believes that the technology and legal frameworks are now in place but there are institutional and semantic barriers to overcome. In the current deployment of egovernment services, he sees as problematic the multitude of approaches taken by public administrations at the national, regional and local levels and lack of integration between them.

Timmers underlines the main challenge in establishing interoperability of IMSs in creating user awareness and communicating to the users the benefits and functioning of the new system. Users may not adopt the system because of lack of trust or concerns of data protection or security.

Hollosi and Martin hold that the Austrian's Citizen Card has been designed with the highest emphasis on technical interoperability. At the legal level, the commercial risk still lies with the parties using the ID card. They view cross-border interoperability at the legal level as difficult given the differences in legislation between Austria and other European countries in the area of identity management. At the cultural level, they referred to the fact that citizens wanting to use the card across borders would be too confused with many different legislations and their implications for risk management.

For Følstad, the greatest challenge is in user's adoption of and trust in the system. If users don't have confidence about data protection or functionality, they will not want to use the cards and share information. Usability could also be another major obstacle.

6.8 Actions and relative importance at the technical, legal and cultural levels

At the technical level, Libon stresses that it will be very hard to replace all the existing technology installed base of card readers and other technologies or to enforce common standards. Countries follow different technology solutions and while linking all the different systems is possible, it requires a major effort. Libon also refers to the difficulty in managing constant change in technology and functionality, since the cards should last 5 years. As each new functionality is added to newer cards, older cards become outdated and replacement may be needed. For example security functionality may need to be scaled up or new functions may become available.

Timmers also sees some challenges at the technical level owing to the lack of standards. However, he sees cultural issues to be the most important area. He states that even if we establish a cross-border interoperable system, the existing cultural

practices would probably not conform to the system and could react against it. According to Timmers, cultural practices should be addressed first. He also points to the need for creating a legal framework that enables interoperability and interchange of information. In his interview, he lists a number of areas of research at the social, technological and economic levels (see his response to Q.14 in the annexes). Timmers also provides a list of European research projects on legal barriers to interoperability in eID and egovernment in general (see Qs. 17 and 18)

Hollosi and Martin referred to the latest regulation in Austria, the egovernment Act that came into force on 1st March 2004 and considered the Data Protection Act of 2000. They say that the EU should define a set of terms for all countries to use in relation to ID cards and decide which terms and fields constitute an identity. Hollosi and Martin argue for a press campaign communicating the benefits to the users following the implementation of the cards. Hollosi and Martin provided exact details of technical and legal specification employed in their Austrian ID card scheme (See their interview response to Qs 11 and 12 for more details). At the cultural level, public campaigns are planned. They also said that Austria is trying to set an example of success to other countries and to be considered best practice in eID. They said that all three levels (technical, legal and cultural) are equally important.

Følstad highlighted the importance of user acceptance. The system needs to be easy to use and users have to trust and use it with confidence. He said that the most important and challenging issue was user's understanding because users are accustomed to signing paper and will probably see the new technology in the same way. Also users need to be reassured of data protection, especially because vendors tend to request excessive information from their users. For Følstad the most important success factor is user's trust in the system which is dependent on good communication from the government to the citizens.

6.9 Role of government, merchants and users to foster interoperability

At the legal level, Libon declares that new eID cards and interoperability should respect existing laws and regulatory framework especially on privacy and transparency for the users. Libon sees the most important role to be that of governments in establishing political commitment for harmonisation and interoperability among members states.

Timmers said that the private sector has to date led the progress in interoperability but governments are catching up. Governments are now leading the interoperability agenda, using private partnerships at different levels in different countries. Timmers argues that the partnership between government and private sector is the best reference model.

Hollosi and Martin said that although government is coordinating the implementation of the eID card, they have outsourced the development as much as possible to the private sector. They say that the Government *"came up with the vision but commercial partners brought the card to life"*, even the certification provider is private (no physical card is issued by the government).

7 EHEALTH

John Baptista, LSE

Country	Interviewer	Interviewee
Belgium	KU Leuven, Xavier Huysmans	Frank Robben
Germany	ICPP, Martin Meints	Bettina Neke
Germany	TUD, Andreas Westfeld & Sandra Steinbrecher	Dr. Bettina Müller Rüdiger Dierstein
Norway	LSE, Christopher Lovold	Espen Haavardsholm Ingunn Hellebostad Toft
Austria	LSE, Stephan Freh	DI Heinz Otter

7.1 Main identity issues

Robben heads the egovernment projects in Belgium's social sector. Robben highlighted the importance of identity in the overall context of government's responsibility for social care. He also pointed out that identity management would allow for gains in efficiency and cost reductions given that information on tests and analysis could be reused, for example x-rays (taken several times by different health care units). The role of the GP is also reinforced, given the greater access to information and control over patients. He also highlighted that interoperability is not just about managing identities, but rather it encompasses the understanding of the whole functioning of ehealth so that it reflects the existing different roles and responsibilities in the system. He also stressed the importance of ensuring high standards in the registration and authentication procedures across entities in different countries. He said it was important to guarantee "quality insurance criteria for the registration procedures that are used to determine the identity, relevant characteristics or mandates before linking it to authentication or verification means".

Neke emphasised the importance of reliable information about identities in dealing with patients. She also referred to the communication between GPs, pharmacists and between other care providers. For Müller, the most important issue is data protection, including availability of the service and protection against unauthorised access.

Otter is Director at the Austrian's Social Security Office Austria. This office started the distribution of the eCard to all socially insured Austrian Citizens on 30th May 2005. It is planned to finish the roll-out of the 8 million-plus eCards in December 2005. Otter stated that Austria has a centralised resident register system or "Zentrales Melde Register" (ZMR) where every person born in Austria gets a social security number. This number consists of the birth date plus a 4-digit number. The eCard is distributed to all Austrian citizens, but non-Austrians who have no such number, had to be added to the system. Avoid multiple entries in the database was a key concern. This problem begins with trivialities such as typing people's names correctly: Austria

has a regulation that every citizen can ask to be addressed by his "original" name including characters like ä, ë, í, õ, ü etc.. The new eCard uses a newly developed numbering system – the so called bPK (sector specific personal identifier).

7.2 Importance of interoperability

Robben believes that interoperability is very critical but he sees this to be a greater challenge in ehealth than in other fields because of the need for absolute reliability of identification - wrong information leads to wrong decisions. Neke agreed that interoperability was a major issue in the healthcare industry. Müller thought that in the long term the issue of interoperability of IMS would become critical but that the bar for the identity management systems should not be raised to a level at which any savings effect is lost.

Otter categorised interoperability as of high importance to any ehealth project especially in Europe. The Lisbon convention, Europe 2000, Europe 2005 etc. all define interoperable social security systems coupled with an interoperable identification system as a major goal for the public health care sector.

7.3 Definition and what is enabled

Robben used the same definition as proposed by the EU's ATHENA project "The ability of two or more networks, systems, devices, applications or components to exchange information between them and to use the information so exchanged."[10]

For Neke, interoperability is more a question of technical standards, interfaces and gateways. She says that a central topic is the introduction of a new system for social security numbers in Germany, which have to be unique and valid for the lifetime of a patient. For Müller, an Identity Management System binds an identity in the network to a person and their role; an interoperable IMS also provides a general standard interface.

For Otter, interoperability of IMS figures as the ability to exchange information on identities correctly in a syntactical way by means of technical integration, with the goal of authentication and identification of physical and legal entities across different systems. An interoperable eCard system in the healthcare sector provides the citizen with the option to visit any doctor or hospital.

7.4 Ideal scenario of full interoperability

Robben presents and proposes a conceptual framework for interoperability of IMS (See his response to Q.4 in the annexes). He highlights the need to establish common terminology and define a priori roles and responsibilities of the users in the system. Robben believes that electronic information exchanges should take place on the basis of a functional and technical interoperability framework that evolves continually but

[10] This definition of Interoperability was presented in the white paper of the ATHENA's project (http://www.athena-ip.org)

gradually in accordance with open market standards, independent of the methods of information exchange used.

Robben describes the current identification system using a PID (Patient Identifier) and the government restrictions on its use because it needs to be separated and not linked to other government databases. For Müller the ideal scenario system is where the users have a data device (e. g., Professional Card) which is used to check the role for access regarding data and grant or deny that access to various systems. She says we are still far from this scenario. For Otter, the data model for the eCard assures that people can not be tracked by looking for one unique identifier across all data bases.

Otter foresees a system which grants a correctly insured Austrian citizen medical treatment in all the 25 EU countries by simply using an eCard and the logistical/administrative back office system behind the cards ensuring correct payment exchanges. Otter says that by the end of 2006 in Austria any citizen will be able to authenticate himself with any partner chip card, such as a bank card at the hospital and doctor, with no further paper work needed.

7.5 Requirements for users, governments and merchants

Robben stressed the importance of roles and responsibilities in the system as more important than interoperability per se. For example, in a hospital scenario, there might be people accessing data that are not their own. Mandates are necessary to determine who can act on behalf of another person. It can be a central database of mandates or a set of local databases. He sees the need for the creation of a sub-committee of the Privacy Commission specialised in ehealth and responsible for protecting information. This committee would decide on: what entity is allowed; what access; what personal information; about which patient; in which capacity; and in which situation; during which period of time.

It is important that the system that works with the IMS maps the governance structure of the organisation, so that different users only have access according to their permissions. He stressed the importance of accurately ascertaining the identity of both the patient and health care provider (HCP). Robben said that interoperability should be achieved by finding a balance between efficiency, security and privacy protection. He believes that a combination of independent sectoral committees and a good system of sanctions for instances when rules are infringed should make it possible to obtain the adequate level of security and privacy protection.

Neke proposes the following requirements for users (in this context are understood as patients and care providers):

- operational speed of the solutions,
- low cost,
- reliability and
- integration into established operational procedures
- patient has more control over the data

Neke says that merchants (pharmacists and health care industry in general) would prefer a non-proprietary system that is not monopolised by one vendor. Müller says

that users want uniformity (just one card), confidentiality and legal assurances. For governments, she says that compliance with existing laws is critical and compliance with what users have authorised in terms of data usage.

Otter says that users need to have trust in the system and to be educated on how to use the new system. He also believed that the system would only be socially interoperable if it is granted to specific groups, such as the elderly and the disabled. He also says that users need to be given or to buy a card reader to be able to communicate with government agencies from their home computers.

7.6 Benefits for users, government and merchants

According to Robben, the new system improves efficiency for all parties. Neke says that interoperability brings additional optimisation of communication and documentation management. Users gain from the introduction of emergency data, immunisation data and medication data, reduction of dangerous double examinations and better structure of therapies. Pharmacists can improve service through more information being available through the health cards.

For Müller, users benefit because it becomes easier for patients when they see the doctor: they don't have to pick up x-rays and lab results everywhere, and pharmacy is only one mouse click away. For governments, it saves time as medical staff is less troubled with time-consuming administration tasks and reduces risk of misuse.

Otter stated that one benefit for the citizens was that they could use the services for which an electronic signature is required. These signatures are fully supported in Austria and will be widely supported on a European level. Secondly, the citizens are not required to take a health insurance voucher with them when visiting the doctor or hospital. In general, the work and communication processes between practitioners, insurance companies and government agencies will be less paper-based, faster, probably simpler, and as a result cheaper and more accurate.

7.7 Barriers for interoperability

Trust in the system is the most important aspect for Robben. He stresses that *"this system will not work without the trust of the general public"*. Robben says that the best way to get trust in the system is to have it managed by the people concerned - representatives of the health care sector, patients-sickness funds. If they trust the system, it will be used. The best way to convince medical doctors and patients to use the system is to involve them in it. Robben believes that the establishment of interoperability is very difficult without the creation of a unique identification number for all services. Robben also highlighted the problem of dealing with so many national languages in Europe.

Neke emphasised the embedded power of industry monopolies and the economic model behind the health card system, and the standards and interoperability framework. Müller refers to the lack of technical infrastructure and economic incentives for implementing interoperability. She also argues that the new system

reduces face-to-face contact between stakeholders in the process, owing to a more digitalised environment.

For Otter, the lack of technical standards in regards to the translation process of national citizen register among 25 EU member states is hindering interoperability. Another barrier and often overlooked issue in regards to European wide ehealth solutions, is the fact that each country has a different understanding of how to treat certain illnesses, what kind of medication to give the patient, what types of illnesses to regard as serious or minor, etc. However for Otter, privacy is the biggest challenge to the creation of a pan-European ehealth solution. Another barrier from the user perspective is users' trust in the system; citizens might not trust the newly-developed IMS and therefore might reject the system.

7.8 Actions and relative importance at the technical, legal and cultural levels

At the technical level Robben mentions a number of existing standards that could be used for the interconnection of networks (TCP/IP, etc), information exchange (XML, UML, PDF…) and security (SSL, X509). Therefore he thinks that the technical dimension is not too complex. He proposes the following five principles for interoperability:

- Information modelling: mapping information use and its key stakeholders
- Single collection and re-use of information: information should only be collected once and by certified bodies in the government
- Information management: active management of useful information
- Electronic information exchange: maximise re-use and synergies between functions that require data from the users
- Protection of information: users should be assured of data protection through good internal practices.

Neke says that from a technical perspective standards and open platforms can be implemented. She points out that these initiatives require political support. Müller says that a legal framework/general conditions for the definition of clear technical standards should be created, responsibilities assigned, and independent, certified trust centres should be fostered.

For Robben, the most important dimension is the cultural and institutional. Neke also views politics, society and institutions as the priority. For Müller, the most important is the legal/policy dimension, followed by technology and then cultural/institutional which will develop on its own.

Otter stated that the privacy issue was a major point of discussion while conceptualising the eCard. The Austrian parliament had to introduce two new laws in order to create the necessary legal basis for the eCard concept. The new laws were designed according to the Austrian egovernment Strategy

According to Otter, every doctor and hospital in Austria will be equipped with a "Medical Practice Unit" (MPU). In a first phase, over 12,000 of these readers will be installed. The MPU consists of software client and a card reader. At the technical

level, Otter suggests the development of further standards, more specifically to agree on clear "exchange tables" of the EU's national citizens registers.

Otter believes that the cultural/institutional level is the hardest to achieve and the technological most likely to be the easiest one. Awareness is critical and he demonstrated and compared the eCard project to the introduction of ATM machines. Only 3-4 years after the first installation of an ATM, the concept of getting money by using a bankcard and a PIN was explained in Austrian school books and thought about in primary schools. This kind of public relations is of extreme importance in rendering a sophisticated and completely new system widely accepted among the public

7.9 Role of government, merchants and users to foster interoperability

Robben highlighted the importance of integrating the ehealth plans with the global egovernment objectives. Creating public awareness is one of the main roles of governments. He underlined the problems of leaving the development to the private sector and said that the system is in the public interest and should not be driven for profit maximization.

Neke defines the role of the governments as moderators in the process of developing interoperable systems. For Müller governments should stop the proprietary developments of health insurance, associations, and industries and create and enforce standards. She also says that it is the role of the users to be aware of how they may prevent too much personal data being given to governments and insurances.

Mr. Otter recommends awareness and education programs on how to use the eCard especially for fringe groups. Overall it is important to build confidence in the system. Specifically in regards to the eCard, one of the most powerful stakeholders was the Austrian Medical Association. Without their support any development of a new system would be useless. They feared that the eCard would give the Social Security Offices access to the doctors' surgeries. The project management should be separated from any political position as politicians tend to interfere with the working progress. The IKT-Board[11] has experts from all significant stakeholders; it is politically independent but at the same time enjoys the political and financial commitment of the government.

[11] The IKT Board (Information and Communications Technology Board). See interview report: Arno Hollosi, Technical Director Stabstelle IKT-Strategie des Bundes.

8 TOWARDS A SET OF REQUIREMENTS

Some important themes were highlighted in the summary of interviews:

1. Despite the obvious importance of other elements to the information society, in terms of interoperability, this exercise has shown that the **social, institutional and political dimensions are seen as the most important** by all experts as opposed to the technical and the legal. Only one expert saw the technical to be more relevant. In particular, semantic issues of meaning and interpretation, and syntactic issues of format and rule in interoperability were seen as the most critical.

2. Apart from the development issues, the question of whether such systems will be used and adopted seems for most experts to be a critical issue of trust. In this regard, the **ability to communicate to the citizens and user**s in general about how the system works and its benefits is vital.

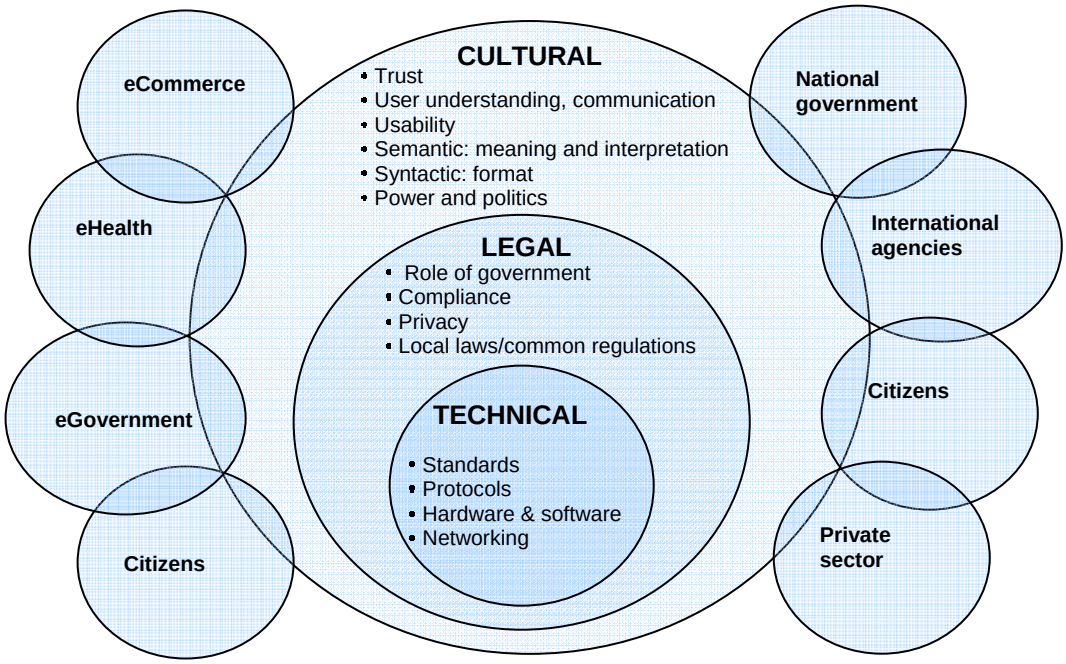
3. **Privacy** of personal information and **compliance with data protection** legislation figures unsurprisingly as one of the main requirements for an interoperable system. There can be no interoperable systems that ignore the issue of protection of personal information. European regulation requires all the European states have legislation on this and it is a matter of how differing approaches may be reconciled.

4. Of all the actors involved in interoperability, government were considered to play the key role in establishing interoperability technology standards and laws. The private sector was seen as key partners for the implementation. **Government should create right environment** for fostering the interests of the private sector.

5. In line with most systems development issues, **usability was seen as a vital factor**. If the end-user is able to cope with the interface to the system there is a better chance of the interoperable system being accepted and trusted. Systems may be rejected merely on the grounds of poor usability.

6. **Opinion amongst the experts diverged as to the importance of technology**. Some said that all necessary standards are now available, others said standards have yet to be developed and implemented. Clearly more investigation on this issue will be required of our later work on interoperability.

The following diagram illustrates the main themes derived from the analysis of the interviews:



9 CONCLUSION

James Backhouse, LSE

To the lay person, the issue of interoperability of identity management systems, indeed of most information systems, would likely be expressed in terms of finding the appropriate technical standards to deal with issue of technical platform, operating system, database standards and formats, communication protocols and the like. Having resolved these issues, one might well feel that the problem is mostly resolved. What emerges from these interviews is another picture. The experts rarely stress the key role of the technology in achieving interoperability and instead seem to take the technical questions as mostly resolved, or resolvable. What remains a barrier for the experts interviewed in this exercise is the problem of dealing with the issues of the social, the political, the cultural and the semantic nature.

At a trivial level, sharing a common set of concepts that refer to common ways of dealing with identification and authentication, with security and with privacy would seem to be a sine qua non. At the level of adoption of the systems, given that they are inherently interoperable, issues of trust, of usability, of confidence lurk beneath the surface. Governments are seen as the main protagonists in this scenario and can use their central positions to alter perceptions and beliefs about such systems in egovernment, ehealth and ecommerce. It would seem impossible for the private sector on its own to be able to render systems interoperable at these non-technical levels.

Also emerging is a picture of different degrees of progress being made in different countries. The Austrian example in ehealth is inspiring, in that many necessary pre-requisites for interoperability seem to be built into their pioneering systems, although it will require more than mere capability to turn potentiality into reality.

This deliverable has served an important purpose of confirming the intellectual basis on which we sought to develop the study into interoperability, proving that a simple yet coherent conceptual framework as found in the technical, formal and informal deconstruction, could support quite penetrating analysis and yet remain comprehensible to the less experienced in the identity field. Furthermore the results of our interviews lay a firm basis for our upcoming deliverables: the larger survey and the best practice guidelines. Both these form part of the second workplan for FIDIS Work Package 4 on Interoperability of Identity and Identity Management Systems.

10 REFERENCES

Many cited references are included in the main text or in footnotes. Due to the predominant empirical nature of this deliverable most references shown bellow refer to sources given by the interviewees. We were not able to check all references provided here but we decided to list them exactly as they were given to us in the interviews.

Benjamin Franklin, letter to David Hartley, Dec. 4, 1789

Freh, S. (2005) Analysis of Global Eid Projects with Focus on Interoperability by Using the Tfi Model.

Frank Reiländer, Gerhard Weck: Datenschutzaudit nach IT-Grundschutz – Konvergenz zweier Welten. Datenschutz und Datensicherheit 27 (2003)http://www.infodas.de/download/DuD_11-2003.pdf

Friedrich von Schiller in the “Words of Faith”

Gesellschaft für Datenschutz und Datensicherung e.V., http://www.gdd.de

Gesellschaft für Informatik e. V., http://www.gi-ev.de/english

Günter Müller, Kai Rannenberg (eds.) Multilateral Security in Communications, Addison-Wesley, München, Reading, Massachusetts, 1999

Hayat, A., H. Leitold, C. Rechberger and T. Rössler (2004) "Survey on EU's Electronic-Id Solutions" *10.08.2004* Vienna.

Hollosi, A. (2005) *Requirements for Interoperability in Ims at the Example of Austria's Bürgerkarte* 30.06.2005. (Personal communication).

Hollosi, A. and G. Karlinger (2005) *Die Österreichische Bürgerkarte: Einführung* A-Sit Last accessed: 10.07.2005 Last updated: Address:

ICA 35th Conference Report (2001) in *ICA 35th CONFERENCE* Berlin.

Information Society and Media DG (2005d). "What Is Eten?" http://europa.eu.int/information_society/activities/eten/index_en.htm Accessed On 20.03.05

Marie von Ebner-Eschenbach, Aphorism

Martin, B. (2004) in *egovernment Workshop*Vienna.

Martin, B. (2005) in *FIDIS workshop 3.5* IKT-Stabstelle, Frankfurt.

Otter, H. (2005b) in *Managing Identity* German Embassy Info Center.

Personen am Lehrstuhl Management der Informationssicherheit, 2005, http://www-sec.uni-regensburg.de/federrath/

Posch, R. and M. Holzbach (2005) A-SIT Secure Information Technology Center.

Project AN.ON/JAP, Anonymity Online, 2005, http://www.anon-online.de/

Rundfunk und Telekom Regulierungs-GmbH (2005) *Electronic Signature: Legal Information* Rundfunk und Telekom Regulierungs-GmbH Last accessed: 10.07.2005 Last updated: Address: http://www.signatur.rtr.at/en/legal/index.html.

ICA 35th Conference Report (2001) in *ICA 35th CONFERENCE* Berlin.

Otter, H. (2005a) *Requirements for Interoperability in Ims at the Example of Austria's Ecard* 30.06.2005. (Personal communication).

Otter, H. (2005b) in *Managing Identity* German Embassy Info Center.

11 ACRONYMS AND GLOSSARY

IMS	Identity Management Systems
ATHENA	Advanced Technologies for interoperability of Heterogeneous Enterprise Networks and their Applications - is an Integrated Project sponsored by the European Commission http://www.athena-ip.org/
eID	Electronic identity tokens
eCard	Electronic identity card
MPU	Medical Practice Unit
WP	Workpackage (a working group of FIDIS focused on a specific topic)
IKT	Also known as the Austrian's Chief Information Office
ATM	Cash dispensers machines
HCP	Health Care Provider
PID	Patient Identifier
ZMR	Zentrales Melde Register is a type of central citizen registry
GP	General practitioner medical doctor

12 APPENDIX A

Owing to space limitations, we have only annexed a limited number of interview reports (13 out of a total of 23 reports), others are available for consultation on request. We selected to annex those which we used more in the writing of this report.

Belgium (Michael Vanfleteren, Els Kindt and Xavier Huysmans)

#	Field	Interviewee	Date of interview	Annex
1	ecommerce	Marc Sel: Director Pricewaterhousecoopers, Antwerp, Belgium. Responsibility for projects, including the eID project of the government in South Africa'.	29 June	Annexed: Report 1
2	egovernment	Olivier Libon: Project Manager, FedICT Security Architect (FedICT: Federal Public Service on Information and Communication Technology; www.fedict.be)	27 June	Annexed: Report 2
3		Paul Timmers (e-govt unit, EU Commission)	27 June	Annexed: Report 3
4	ehealth	Frank Robben: General Manager of the Crossroads Bank for Social Security. More information about him at http://www.law.kuleuven.ac.be/icri/frobben/	6 July	Annexed: Report 4

Germany (ICPP, Martin Meints)

#	Field	Interviewee	Date of interview	Status
5	ecommerce	Bernd Burckard: Technical project manager for the PKI-infrstructure of the Federal Land of Hessen	18 Aug	Annexed: Report 5
6	egovernment ehealth	Bettina Neke: Ministry of Social Affairs of the Federal Land of Schleswig-Holstein, political co-ordination for the e-health card project in Schleswig-Holstein	22 Aug	Annexed: Report 6

Germany (TUD, Andreas Westfeld & Sandra Steinbrecher)

#	Field	Interviewee	Date of interview	Status
7	ecommerce	Prof. Hannes Federrath	5.7.05	Annexed:Report 7
8		Dr. Gerhard Weck	6.7.05	Annexed:Report 8
	egovernment			
9	ehealth	Dr. Bettina Müller	2.8.05	Annexed:Report 9
10		Rüdiger Dierstein	10.8.05	Annexed:Report10

Norway (LSE, Christopher Lovold)

#	Field	Interviewee	Date of interview	Status
11	ecommerce	Central Bank of Norway ▪ Virginia T. Ringnes	01/08/05	Not annexed

12		▪ Arild Lund and Casper Christophersen	01/08/05	Not annexed
13		▪ Semming Austin	11/08/05	Not annexed
		DnB Nor		
14		▪ Erik Lindmo	04/08/05	Not annexed
		Nordea Bank		
15		▪ Nils Inge Brurberg	07/08/05	Not annexed
	egovernment	Sintef (largest research centre in Norway)		
16		▪ Asbjørn Følstad	29/07/05	Not annexed
	ehealth	Hospital MDs in Norway		
17		▪ Espen Haavardsholm	12/07/05	Not annexed
18		▪ Ingunn Hellebostad Toft	10/07/05	Not annexed

Austria (LSE, Stephan Freh)

#	Field	Interviewee	Date of interview	Status
19	ecommerce	DI Herbert Leitold (Director at A-SIT)	13.07.05	Annexed:Report 19
20	egovernment	DI Arno Hollosi and DI Bernd Martin (Austrian Government Managers)	30.06.05	Annexed:Report 20
21	ehealth	DI Heinz Otter (Director of Chipkarte)	30.06.05	Annexed:Report 21

UK (LSE, James Backhouse, John Baptista and Chris Lovold)

#	Field	Interviewee	Date of interview	Status
22	ecommerce	British Telecom (UK)		
		▪ Mark Drew	18/07/05	Not annexed
		Shell, London (UK)		
23		▪ Tom Buschman	15/07/05	Not annexed

12.1 Report 1: Marc Sel, Belgium, ecommerce

D4.2: Requirements for interoperability in IMS

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer: Els Kindt
Interdisciplinary Centre for Law and Information Technology, KU.Leuven, Belgium
Tel.: +32165421, Email: els.kindt@law.kuleuven.be
Interviewee: **Marc Sel, Director**
PricewaterhouseCoopers,
Generaal Lemanstraat 67
B-2018 Antwerpen, Belgium
Web: http://www.PwC.be
Tel.: +3232593410, Fax: +3232593396, Email: marc.sel@pwc.be
Location: Antwerp, Belgium
Date: 29.06.2005

Background Information:

Marc Sel joined PricewaterhouseCoopers in 1989 as a management consultant. Over the years, he specialised in information security. He performed security consulting and review assignments worldwide. His clients include financial services corporations, providers of telecom services, pharmaceutical companies, utilities and the public sector. He has been involved in the Belgian Electronic ID card project, as well as the Belgian Digital Tachograph project. He is currently based in Antwerp, as Director in the Performance Improvement / Information Technology Management department of PwC Belgium.

Questions:

13 What are the main identity management issues in e-commerce?

Trust and span of control by the user

Identity management in e-commerce has only a chance to succeed if it is clear from the beginning that the user remains in control of the identity management system. Interoperability of systems as such will not be accepted by the users unless it is within the span of control of and is controlled by the user as default.

These defaults should in addition be 'prudent'. It means that the defaults should favour the protection of the common interest and the protection of the less knowledgeable members of the society.

Common interests to protect include:

The e-commerce infrastructure and applications (internet, mobile networks, interconnections etc) may be hampered according to various scenarios, e.g. through impersonation of one or multiple genuine users, and misuse of their authorizations. There may be direct and consequential damage going well beyond the single impersonated genuine user. Such common interest can include the reputation and trust of a product or service, or a government

agency; If trust is lost e.g. in electronic ID cards, this can have devastating effects on public service processes, and consequently on the benefits they bring onto their society.

Furthermore, once damage would be done and detected, there will be a burden on people "make it right again", sorting out responsibilities, re-allocations etc. Damage may be done by one malicious individual, but the rectification may require the coordinated efforts of many members of society.

Taking into account the 'digital divide', it is clear that we will probably have to protect three groups in particular:

- Youngsters (e.g. in the age bracket between 7 and 12 years) – they may have access to computer infrastructure with internet connectivity, and cannot be considered as mature enough to understand all potential traps;
- People that for one reason or another, are not familiar with and do not favor the use of IT solutions but are forced to use them for a particular purpose – they can be sufficiently mature but may lack practical knowledge and skills to circumvent undesirable situations;
- Elderly people – because they may take longer to adapt to new ways of working.

Need to understand the 'spaces' in which individuals operate

For any identity management system (IMS), it is required that one understands that individuals operate in distinct 'spaces' in which they act with different characteristics. For example, one individual acts in an environment in which she/he is employed or is a professional, conducts a private life with family members, purchases products or services of third parties as a consumer, and acts in relation with the local and federal government. In general, four 'spaces' can be defined : government /private/commercial/ PPP (private-public partnerships). A good example of the PPP space is demonstrated by the Estonian approach of their electronic identity card roll-out. It remained the government's responsibility to maintain the national identity database, but they made use of the banking sectors distribution network to correlate the identity of the requestor and the person that finally picked up the card. Also, the card serves two purposes, as identity document and as bank card.

These 'spaces' are in principle separated and do not interact, unless explicitly designed as in the case of e.g. an approach as with the Estonian identity card.

One of the issues is to understand to what extent individuals, who are assumed to control the identity management application, would desire to act as one and the same interoperable individual across these 'spaces'. In other words, one of the basic questions is whether individuals require interoperable IMSs ? Interoperability of IMSs could lead to a loss of privacy. Therefore, IMSs may well be confined to a specific 'space'. Alternatively, it will be the individual who will decide in which 'space' she/he will act and/or which individual information could be shared across the 'spaces'.

Moreover, in each of these spaces, the individual may have specific requirements as to an identity management system.

Once this issue is solved, the requirements of the businesses and of the governments will further design the IMSs.

Use of privacy profiles

One of the cornerstones of an IMS is an adequate management of the privacy issues. As stated above, it is unlikely that individuals want to give up their privacy which they enjoy in the distinctive 'spaces' and which they may enjoy nowadays without interoperable systems.

The use of privacy profiles, which are transparent, understandable and manageable by the end – users could be a tool to offer such privacy. The profiles should range from full anonymity to no anonymity, depending upon the use thereof. Profiles should also enable systems to use attributes instead of identity information. Privacy profiles seem therefore indispensable for any identity management system.

The use of a GUID has advantages and disadvantages. With the current state-of-technology, PwC uses a Lotus Notes GUID internally to let every individual comply with some international (mainly US) regulations on independence. When I work on local client files, I use my national UID. When I file my independence statement, I use my GUID. The advantage of this split (having both a UID and a GUID) is that authorizations can be managed independently, and that compromises are not automatically transferring into the other sphere. On the other hand, we have to manage two different id-strings and two different passwords. The current (combined UID/GUID) approach works very well. The GUID is now gradually being used to provide access to global knowledge etc. As it is separate from really 'local' work, I like this approach. It ties in with the concept of 'different spaces'.

Geographical reach of identity management issues

In the design phase of any identity management system, one should also consider what geographical reach one intends to span with such system. Does the system need to cover worldwide applications or only European ones ? Any identity management system will depend on underlying systems and applications, but also upon distinct views of governments and countries.

How critical is the issue of interoperability of IMS for this field?

Across the different spaces, there should be no interoperability, or under full control of the end user. Within a given 'space' as described above, it is likely that individuals will use and want to use interoperable trusted identity systems (again). This is also correct for e-commerce as it will lead to additional benefits of the users, such as efficiency, but also privacy, if privacy profiles are correctly implemented. Hence, within a give space, the interoperability is critical. It is however critical within the realm of a set of connected transactions. Once the 'chain of events' breaks, I am more interested in safeguarding my privacy on the longer term.

I look at it this way: as consumer, I like convenience when I order a plane ticket, combined with a rented car and a hotel. So interoperability is good. However, I don't want to be further bothered by cross-selling efforts from the rented car company 3 months later when they learn I go on a new trip.

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?

A definition of interoperability could be : that a system can take reliance on the form and contents of another system's judgement or service outcome.

Interoperability of IMS should in the first place rely on the ability of the system to identify and authenticate a given individual. This is particularly important in the field of e-commerce, where individuals have to be identified online or in a remote way. This functionality to identify persons, however, should be in a given, well-determined and specific way. This should allow using a trusted identity more than once and in several systems (interoperability).

In addition, the IMS system should allow for authorisation(s). This would mean that the system should allow for identity ànd access management. The design of an authorisation functionality, however, is much more complex, but a factor which may be an enabler of interoperability.

With regard to legal persons, interoperability does not seem too complicated. A legal person does not live a life on his own, it is through the natural persons that the legal person acts. So what we need is a kind of registry that from time A to time B, person x could bind legal person Z. I don't see how you want to give e.g. tokens or smart cards to legal persons – seems a lot easier just to keep records of the relationship legal-natural.

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

Belgian eID project

Since September 2004, electronic identity cards (eID) are being distributed to all Belgian citizens living in Belgium. The eID is a plastic card, in the format of a banking card, with an electronic chip. The eID contains personal information printed on the card, including picture, name and written signature. The personal information is also electronically stored on the card, and also includes the digital signature and certificates of the owner of the card.

The eID allows the owners/users of the card to consult their own personal information kept in the central personal register[12], but also to contact, exchange or file information with the government.

Next steps in Belgium

The Belgian government is preparing for the interoperability of the electronic identity of individuals (eID).

The next step is to use the eID database of the government in other area's, such as in the health care sector. For these purposes, the system would not only identify and authenticate individuals, but also authorise individuals to have access to certain applications in the e-health environment, for a given period, e.g., 24 hours.

The technical developments are ongoing. They include the use of a new language, such as the use of the 'security assertion mark-up language' (SAML), in order to enable the system to authenticate and to authorise given individuals.

[12] www.mijndossier.rrn.fgov.be.

How far are we currently from that scenario?

Public sector

In the public sector, the developments for an interoperable eID are under way, as described above (see section 4.2).

FEDICT's (see also below, section 7) FSB or the Federal Services Bus is a software model to let various government agencies share/exchange information. It should facilitate information use and reuse, for example, in the context of joint electronic procurement capabilities for the government.

Private sector

In the private sector, it seems that private companies have not yet made much progress in the development or use of interoperable identity management tools. Initiatives exist, such as the IBM Tivoli software system[13], but are not yet widespread.

Large banks in Belgium have tried to set up IMSs, but without much success. One of the reasons is that these large companies rely on systems which were designed and encoded decades ago. Nevertheless, these systems are still operated nowadays and remain crucial to their activities. These 'legacy systems' cannot be easily replaced by other systems just to enable interoperability of IMS. The application of new IMS tools to these systems' is therefore far from easy. Rewriting or replacing these systems for the use of IMS is presently, apparently, not yet an option.

What are the requirements for interoperability for the USERS?

For the users to accept IMS, it will be important, as described above, that there is a correct balance between the 'automatic' interoperability of identity and the control that users desire to exercise over the use of their identity (see above section 1.1 and 1.2).

In addition, privacy and anonymity are key factors for the interoperability of IMS for users (see above section 1.3).

What are the requirements for interoperability for the GOVERNMENTS ?

First of all, the services of the government need to be coordinated in an efficient way. In Belgium, the FEDeral organisation for Information and Communication Technologies (FEDICT) was established in order to initiate, elaborate and advise on the e-government projects for the federal services[14]. The mission of FEDICT is to advise and assist the federal governmental services in an efficient use of the internet and new communication technologies for its internal and external tasks. The agency has also a coordinating role between the governmental services.

One of the additional requirements is that the technical tools and means need to be available in order to realize interoperability. An example hereof, on European level, is the digital tachograph system (see below, section 15). Another example, on the national level, is the development of the Universal Messaging Engine (UME) by FEDICT of the Belgian government. The purpose of this engine is the interoperability between the systems and applications of the government on one hand and the web browsers of the end-users on the other hand. UME is based on user management for government officials. It should enable

[13] See at http://www-306.ibm.com/software/tivoli/
[14] See www.fedict.be

that the information contained in the distinct systems and applications of governmental services can be consulted, exchanged and used. Today, it enables, for example, that several types of certificates (e.g., the certificate of the registration of a company, the certificate of payment of the social security taxes, …), can be exchanged between the governmental services.

A third example is the development of the 'Enterprise Application Integration' (EAI) of the public e-procurement applications of the governmental services in Belgium. This development shall enable the interoperability of the (legacy) information systems in the procurement process of the government.

It is not required nor recommended that government should rely or depend upon GUIDs developed by businesses, for example, the credit card industry. Credit cards become in some countries increasingly important as GUID, but such development is not free from risks. The delivery of public services or the right to enjoy government benefits should be kept separate from having a credit card. Some parts of the population may never quality for a credit card, or may never be interested to apply.

What are the requirements for interoperability for the MERCHANTS?

Security and reliability

Merchants require that an IMS system is secure and reliable.

Internally, companies may use their own IMS that they have developed. Such IMS does not necessarily have to function outside the company. The internal IMS is designed to offer accountability and quality assurance within the company, two essential requirements.

PricewaterhouseCoopers, for example, has several IMSs, such as for the internal access to its national and worldwide networks, but also for the access to its worldwide document database and file and client management. The IMSs for the document database and the file and client management are designed on a national level with an own public key infrastructure (using global PKI-based Lotus Notes). The IMSs rely for that purpose on the identity as certified by the national authorities, e.g., an official national identity card. Each national IMS allows interoperability of identity management for this and other global in-house processes. The functionalities of the IMSs include not only identification and authentication, but also internal authorization. The IMS authorizes certain persons to work for a particular client, and will exclude others. The IMS shall create mutual trust and quality assurance within the global company. The IMSs are, for example, also linked with other systems which enable internal quality review processes, such as, e.g., the 'Global Portfolio System'. This system keeps track of potential conflicts of interests of the auditors based on stock purchased.

The internal IMSs of PricewaterhouseCoopers, however, are not necessarily fit for external use, e.g., in e-commerce. One of the reasons is that the internal IMSs are designed on a national level and make use of the tools/tokens available on that scene.

PricewaterhouseCoopers Belgium, e.g., could use in the future the eID that is distributed to its citizens in Belgium, for its internal IMS. The Belgian eID, however, is not likely to be use in an external worldwide IMS system. An external worldwide IMS could make use of the distinct national eID system, but one national eID system is probably not going to be used for the whole external system.

Tokens developed by the government

Companies are most of the time very much under pressure to be cost efficient. Therefore, the businesses should be able to capitalise on progress of the government in the establishment of IDMs where possible. Such progress could be, for example, the establishment and the issuance of eId cards. Microsoft, for example, has already shown interest in tokens developed by the Belgian government, in particular the Belgian eID.

Other (public) institutions could also develop such tokens. Credit cards do not seem to be a valuable alternative for such IMSs. Although the use of a credit card is wide spread, one cannot expect or require that every individual has such card.

This does not exclude the possibility of public-private partnerships where needed. An example, as already mentioned above, is the distribution of the eID card in Estonia. In Estonia, the PKI infrastructure is operated by the public authorities but the eId cards are distributed by the private sector (bank sector).

Tokens which are not developed by public authorities, may only offer some technical guarantee that an individual has been registered, without warranties about the registration procedure or the authenticity of the claimed identity (for example, the Passport identification tool of Microsoft). Retailers will probably be hesitant to rely on such tokens developed by private parties for these reasons.

What are the benefits of interoperability for each of these stakeholders?

An interoperable IMS system shall improve the efficiency for the users (citizens), the government and the merchants and companies.

Interoperability of IMS systems also means for merchants that they might be able to cross-sell their products and services to customers.

Internal IMS systems of merchants and companies, as described above (see section 8.1), are basically driven by the need for accountability of the individuals working with such global companies.

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

Technical

One of the obstacles for the interoperability of systems and IMS in particular is the existence of massive installed legacy databases. It will take a while (probably decades) before they all are replaced by systems which enable interoperable IMSs.

Another factor is the different interests of the parties involved. Users may want a restricted interoperability, over which they keep control, while merchants favour a more far reaching interoperability, for example, to be able to cross-sell.

In addition, the merchants as a group may not be interested to cooperate with each other, because they also have different interests and may loose their competitive advantage, if any, if they work with interoperable IMS.

Legal

The legal framework needs to be further adjusted to the use of interoperable and cross-country IMS. The legal gaps need to be identified by the specialists.

Cultural

Interoperability of IMS is also often not well understood and therefore, creates doubts and uncertainty in the minds of the users, government and merchants.

At the side of the users, there is also fear of 'big brother' watching upon everything they do. And there is potential misuse (for example, the reasons why the Netherlands decided to distribute their population register after World War 2 (to avoid potential misuse as done by the Nazi's).

What can be done at the TECHNOLOGICAL level to establish interoperability?

As explained above, different tools, such as the development of the 'Universal Message Engine' tool will be necessary to make different systems and languages interoperate.

In addition, such tools are necessary, as the legacy systems are abundantly present.

What can be done at the LEGAL/POLICY level to establish interoperability?

Interoperability requires open standards. Open standards should be promoted and in some cases be required (see for example, the recent actions of the EU Commission towards Microsoft).

The challenge to create an interoperable environment in IMS is huge. There will probably never be a global system. Even a European identity system seems – politically - a rather big challenge.

Nevertheless, policy decisions need to be taken. Within the EU community, a policy decision as to the use of smart cards as ID carrier and management tool as opposed to checks against centralised databases seems to be taken. Smart cards are preferred because the user has more control over the use of her/his identity information. This is an important policy decision.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

One factor to improve interoperability could be to show the cultural benefits of interoperability.

IMS systems could be used to facilitate or promote skills, for example, learning languages.

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

First of all, policy decisions need to be taken, and the legal framework should allow or facilitate the development of interoperable IMS. The legal and policy factors are therefore to be seen as the basis and the prime factors to deal with. Almost at the same time, technology needs to come up with answers and solutions to problems of operability. If the technology is not there, there is no need to consider the interoperability of IMS issue at the legal or policy level.

Finally, institutional and cultural acceptance of the interoperability shall conclude the development towards interoperable IMSs.

What should be the role of governments in addressing interoperability of IMS?

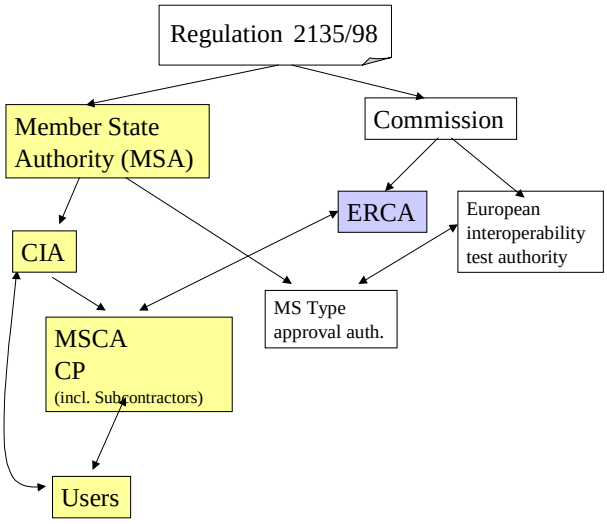
The governments have an important role. As already pointed out above, governments should further invest in the country wide eid processes, such as, for example, the distribution of the

eID cards. This could be used by the industry as a reliable basis for the further development of IMS.

An example of the development of an interoperable IMS by the government is the tachograph system, that has been developed on the European level[15]. The tachograph regulations provide for the obligation for vehicles to install recording equipment which processes data relating to the driver activities. The tachograph cards allow for the identification by the recording equipment of the identity (or identity groups) of the cardholder and allow for data transfer and storage. The tachograph cards are smart cards. A tachograph card may be a driver card, a control card, a workshop card or company card, hereby enabling the actors in the system to have access to the recording equipment and the recorded data. For the functioning of the system, it is essential to be sure that the information is coming from a party whose identity can be verified. For this reason, use is made of digital signatures that allow the recipients of data to prove the integrity and authenticity of the data

The tachograph system is to be implemented by the Member States. In Belgium, the tachograph system is in effect since August 5, 2005. The digital tachograph system is one of the first successfully applied European root public key infrastructures. A European private key is used to certify member states' public keys. The member states' private key is used to certify public keys used with authorized tachograph equipment, such as the tachograph cards and the vehicle units. The European Root Certification Authority (ERCA) which is operating under the authority and responsibility of the European Commission has responsibility for the management of the European key pair. The Member State Authorities certify public keys and manage the certificate policy.

An illustration of the tachograph system organisation is shown in the figure below[16]:

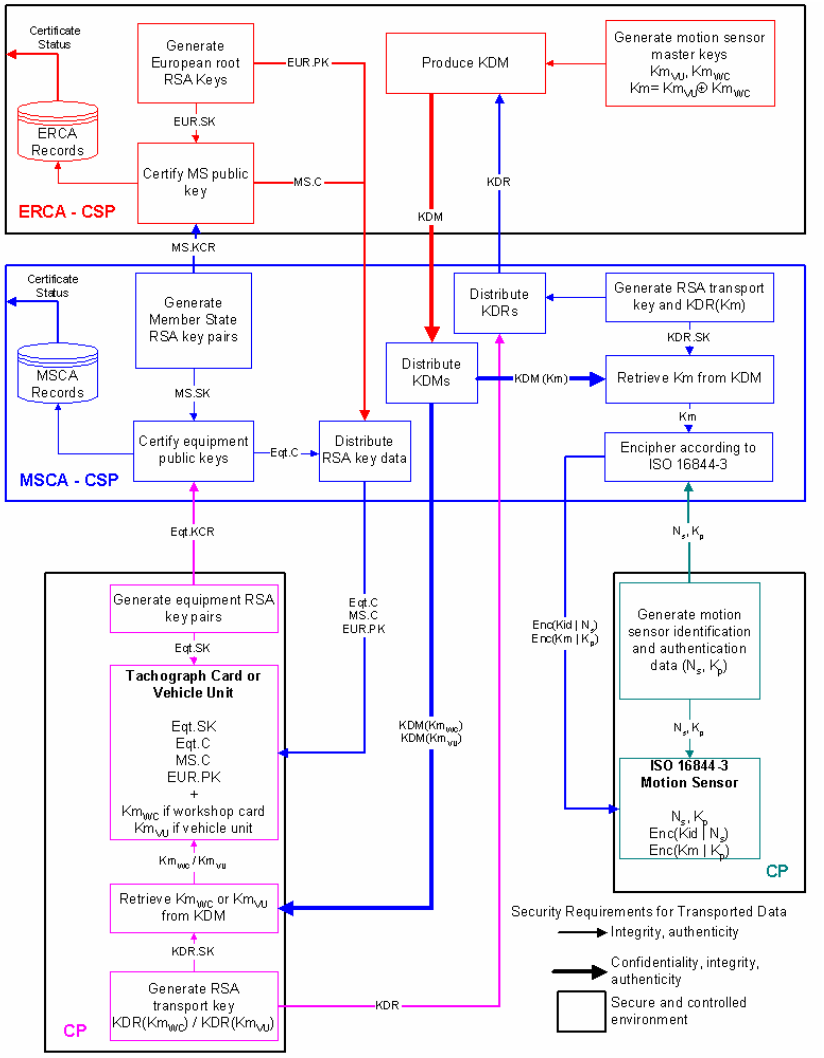


15 See Commission Regulation N° 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport, http://www.digitach.be/NL/PDF/1.2.2.CommissieVerordening13602002.pdf (last visited on 11 August 2005).

16 As shown in the Belgian Member State Certification Authority policy for the tachograph system, p. 9 (see http://www.digitach.be/images/Belgian%20SA%20Policy%20v%201%2013versiononline.doc (last visited August 11, 2005).

The vehicle units and the tachograph cards use the public-key cryptographic system to provide for (1) authenticity of transmissions between vehicle units and cards, (2) transport of session keys between vehicle units and tachograph cards, (3) digital signature of data downloaded from vehicle units or tachograph cards to external media and (4) the mutual recognition between the workshop card, vehicle unit and motion sensor. The system also uses a symmetric cryptographic system for data integrity and confidentiality purposes.

An overview of the tachograph system keys, certificates and equipment is shown below[17] :



A database is available for the member states certification authorities as to who are the card holders and which cards are operated. The databases are accessible via a network, Tachonet. More information about Tachonet can be found in the Appendix.

[17] Id, p. 12

The tachograph system could probably be used by the industry for new applications, such as route planning, fleetmangagement, etc. However, it is clear that other interests are at stake, and that interoperability for these new applications and purposes should not be automatic.

One challenge which remains for the governments is to indicate who will be the data owner. This data owner will determine the conditions under which the identity information could be exchanged.

What should be the role of merchants and industry groups?

Major players, such as for example companies in banking or consulting, have developed their own internal transnational network systems, including interoperable identity features. Examples are Swift, or PricewaterhouseCoopers. They work with own standards in proprietary networks. Their interoperable IMS, however, is not used in their external communication networks.

As described before, the industry should be able to rely on the investments and efforts of the governments in IMSs. In case the basic structures for IMSs are developed by the governments, merchants could without doubt offer additional value to the IMSs. On the other hand, however, it is also possible that each industry will want to remain in its own 'space'.

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

In order to favour interoperability, one should also show the benefits to the communities of the users/consumers/citizens. Without interoperability at all, too many IMS will exist and complicate life.

In addition, a common terminology is required in order to explain the issues of interoperability to the users/consumers/citizens. This terminology should be the same or should be useable in different areas, such as privacy and identity management.

Appendix : Tachonet

TACHONET is a telematic network in operation across the EU. It acts as a central hub for the exchange of information between the national administrations responsible for issuing tachographs (in-vehicle recording equipment) to enforce rest periods and monitor the driving times of professional drivers.

In order to contribute to the successful implementation of new road regulations, a new electronic device called the digital tachograph is used in conjunction with smart cards. Tachographs are recording instruments that measure speed, miles travelled and the number and duration of stops.

TACHONET minimizes duplication of work across the Member States and maximizes efficient tracking of drivers.

Objectives

TACHONET was created with two key objectives :

- To ensure fair competition between drivers, hauliers and other modes of transport; and
- To enhance road safety by avoiding driver fatigue and controlling compliance with the legislation on speed limits.

How does it work?

TACHONET is based on a system of message-exchanges between the EU Member States. The new system comprises a smart card and an electronic on-board tachograph. The digital tachograph guarantees better compliance with rules on driving times, rest periods and road safety and puts an end to the most common abuses of the present mechanical system (accident risk data demonstrates that after an 11-hour work span the risk of being involved in an accident doubles).

To take a concrete scenario: John is a long-distance lorry driver based in the UK. He regularly drives from Newcastle to Lyon in France. Although he is aware of the dangers of driving when fatigued, he decides to make an application for a tachograph and smart card both in the UK and in France. In this way, he hopes to bypass the system and not be caught driving for too long periods without a rest.

- Member States are responsible for issuing the smart cards on time and in a reliable and secure manner. Therefore, when John goes to register in either France or the UK, the Administrator will automatically enter the request details into the card issuing software application developed by the UK/France.
- The local software application will in turn 'notify' the central TACHONET application which acts as a 'hub and spoke' for sending requests and receiving responses from other Member States.
- When the central TACHONET application receives a request from a the local software application in the UK/ France it will validate it, store it and return an acknowledgment of receipt to the original administrator dealing with John's request.
- It is also able to broadcast the request to all Member States, receive responses and provide a consolidated response to the original requester. The TACHONET system ensures that these transactions take place efficiently and securely. It is at this point that John's attempt to misuse the system will be detected. He cannot make more than one application within the EU.
- The Administrator will not only refuse his application, but will also follow proceeds against him for attempt to defraud the system. However, if John has only made one application, then he will be cleared to receive his card and tachograph.

Achievements

- The feasibility study has been successfully completed and both the functional and non-functional requirements of the initiative have been identified. These include:
  - The ability to automatically transmit alert messages
  - The ability to allow the authorities in the Member States to track the status of a card in case it is lost or stolen - 24 hours a day, 7 days a week.
- Furthermore, it was determined that the system structure should pose no restrictions on its users; it should have the capacity to support other types of message structures (for example, for the development of a driving licence network) and each Member State should be able to organise its data with no constraints on operating systems or technology used.
- In October 2002 a complementary study, entitled Planning and Design Phase, was launched.

Who benefits?

Citizens: By enforcing road safety regulations and ensuring fair competition, TACHONET will make roads safer for professional drivers and the general public alike.

Public Administrations: All EU Governments dealing with transport and road safety will benefit from the harmonized exchange of information on Smart Cards, resulting in more rapid and efficient communication.

12.2 Report 2: Oliver Libon, Belgium, egovernment

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer: Michaël Vanfleteren
Interdisciplinary Centre for Law and Information Technology (www.icri.be), Katholieke Universiteit Leuven, Belgium
Tel.: +321625256, Email: michael.vanfleteren@law.kuleuven.be
Interviewee: **Olivier Libon, Security Expert**
Fedict (Federal Information & Communication Technologies),
1/3, rue Marie-Thérèse
1000 Brussels, Belgium
Web: www.fedict.be
Tél: +32 2 212 96 55, Fax: +32 2 212 96 99,
Email : Olivier.Libon@fedict.be
Location: Brussels, Belgium
Date: 28.06.2005

Background Information:

Civil Engineer in Computer Sciences graduated from University of Louvain-La-Neuve, Mr Libon is specialized in ICT security. Successively adviser for the Tractebel Group and the European Commission, he then joined GlobalSign (the European leading certification authority) as Vice President. He joined FedICT (the Belgian ministry of ICT) in 2002 before the launch of the BelPIC project (Belgian electronic Personal Identity Card) as security architect and PKI expert.

Questions:
What are the main identity management issues in e-government?

Belgium is a federal State. Competences are distributed between the various authorities. Consequently, it is impossible to offer services integrated without collaboration among the different entities of the country

E-government is a manner basically new, integrated and continuous to provide services by using in a maximum way the possibilities of new communication and information technologies.
On the one hand, administration must act as "allowing" (enabler). That means that it must remove the obstacles (legal and administrative) and must create the conditions necessary to the realization of the company of information. The administration must create a context and a climate in which the various actors can benefit the maximum of the chances that the company of information offers to them. Moreover, the administration must fill itself a function of example by the way in which it uses the

ICT and of which it interacts with its customers. Indeed, the administration is itself the one of most important suppliers of services based on information
The cooperation agreement (pdf) concluded in March 2001 by the federal administration with the unit from the Areas and the Communities, in which was formally expressed the wish to also collaborate with the provinces and the communes, is thus an essential base. The cooperation agreement provides in particular that the various authorities begin to offer electronic services in a way coordinated and integrated while respecting specific competences of each one. The citizens and companies will be able, for the use of public services, to use the same infrastructure (terminal, basic software...) with the same keys of single identification and the same electronic signature

How critical is the issue of interoperability of IMS for this field?

The question of interoperability among governments has important impact for instance on rules on the exchange of information for criminal records. However, it has less impact when it concerns interoperability of e-ID among governments because there is not so much done at the moment. The question of interoperability for the e-ID exists for instance when it concerns how it is accepted in third country but it is very limited. There are few programmes which are launched and few things have started (for instance a small project with France, and also some possibilities with Germany).
The interesting thing in Belgium is that there is an obligation to deliver an ID card to all the persons on the territory, and being in the centre of Europe, this include

In Belgium, there is an obligation to provide an ID to all the persons on the territory. The international function of Brussels makes it more difficult than in other parts of the world. It covers Belgian people, civil servants of the European institutions, those from the NATO (American military) and people working for international companies as well as the European banking network swift and Fedict personally delivers an ID to these people. The result is that the system receives data coming from all the directions.

The other point is to know how far will the ID card be used outside the country (apart from the visual functions of the card) can not really be answered today. The situation is that there is no need for other countries to provide card reader for instance as they did not implement an e-ID themselves.

And as this situation is evolving, we are then exposed to interoperability for instance for what concerns the names' rules and characters to be respected. This represents a case for interoperability for the creation of common rules on names, signs. In this, Fedict plays the role of stimulating thoughts on the topic.

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?

It is the common understanding of all what is syntaxic (data structured in a way that we can translate them in a comprehensive way), semantic (content/definition should not be identical but it should be possible to translate them from one sector or environment to another) and transactional (it is the capacity to make modifications directly into a system which is not the one the administration normally regulates).

Interoperability allows the exchange of data and services between systems which are different. In a wider sense, interoperability relates to the exchange of information between administrations or between one administration, a citizen or a company, without requiring any effort from their side.

Three aspects of interoperability are important:

- Organisational interoperability, which defines the actors and their responsibilities with respect to its implementation in supplying protocol models regarding the access to the interoperable information, in establishing the integrity and confidentiality policy of this information and in proposing the necessary mechanisms for its localisation and diffusion. It then allows the collaboration between the different services of an administration, which differ from others in their internal organisation and the structure of their operations.

- The semantic interoperability, which consists of giving a « sense » (a semantic) to the exchanged information and to insure that this sense is distributed in all the systems between which exchanges must be put in place.

- The technical interoperability, which tries to resolve the technical problems produced by the inherent complexity coming from the networking of informatics systems and the services that it creates, in describing the standards applied to the presentation, processing, exchange, security and transfer of information

In conclusion, an interoperability framework is a whole of policies, standards and rules, describing the arrangements that organization (i.e. administrations) agree upon to talk to each other. An interoperability framework is then, by essence, a dynamic document that evolves with the needs of the administrations and end-users, et which adapts itself to the technological changes and the emerging of new standards.

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

An ideal system would allow citizens to manage most of the interactions from their home. The transparency aspect is also an important point which should be reached. From a government point of view, an ideal solution could be twofold:

1. It would be to see citizens going to their town hall every 5 years to receive their new ID cards, the thing is that cities deliver different kinds of documents, which are quite similar in respect of the information (driving licence, ID card, passport, …)
2. Transparency: to create a society/company in Belgium, there are different steps necessary regarding validity of registration and it necessitates different contacts with the administration. You must be register, you must check with Vat services, financial services, but from the point of view of the user, it is only and registration…to open a company. The idea is to centralize/integrate this information in only one service which would also be developed more in

the perspective of the user. It is true during the creation of the company but also during the life of the society.

This is a first phase.

A second one would be to say that administration already have all this data in their services. (for instance if you want to work for the government, you must be ok for what concerns your social taxes…this information is already in the hands of the ministries, now they already check on-line)
Other example is the online tax declaration where 80% of the people have a normal declaration and administrations already have the information…The information already exists.

How far are we currently from that scenario?

The solution for obtaining a more adequate solution would be to have 2 phases:

* On a first one, there is a need of integration. It should only be necessary to provide one document and only one time. There is no need like now to send several copies of the same document.

* In a second phase, the question to analyse is that most of the time, ministries already have the data that they need or can receive it from other departments. There is then no need for the people to declare all, there is only need of a good synergy among ministers in their organizational structures.
The problem of synergy has become the "raison d'être" of the creation in Belgium of 4 horizontal ministers. Fedict, Budget, P&O (Human Ressources) and the chancellery of the prime minister.
The role of Fedict within this system is that even though it can't impose anything (for instance it does not have regulatory powers) it has a role of stimulation and creation of synergy in finding cases where the idea of working together allows finding more interesting solutions for the ministries themselves.

3 views on the development of synergy:

- the need of financial interest to create a framework of interoperability and of synergy: A good example is the network within the federal government and all ministries regarding phones, internet connections, etc…. By the synergy, the aim is not to spend less, because ministries have their budget, the aim is to have a better service with the same amount of money.
- a second level is that, there is not only a need to have a financial interest from the ministries, but to be useful, there is also a need to invest within the system so that it could lead to an harmonized solution. This is also linked to the idea of reforming the administrations and is a very sensitive topic for them. As a collateral effect, there is also the security aspects: The Fedman network interconnects all the federal institutions via the EU Commission network to the other networks of the other countries. There is then a need of harmonization of all the security policy among governments and this is managed in Belgium by Fedict and if ministries want to participate, they must follow what is being developed and agreed by Fedict.

- a last element relates to the adaptation of the legislation and new regulation put in place forcing the administrations to respect them. Data protection legislation is an example of it (see question 12).

What are the requirements for interoperability for the USERS?

Administrative simplification goes together with the simplification of the administration in a broad sense for citizens and not only in his relation with the government. The project is not to make a mapping of the paper situation to the electronic one. The idea is still to make something original, which will take into consideration the expectancies of the citizens all along their lifes. In a functional way, information must not be presented from the administration point of view but from the end-user point of view

The egovernment will modify the provision of services of the administration to the customers on 4 levels:

- Faster: because the user should not move any more for any provision of services, it is not any more question of displacement, of administrative formality and latency making double employment; the feedback could be given in real time.
- More convivial: because the citizens and the companies will have access 24 hours - 7 days a week to the administration, where they are. One will be able to always call upon the information easiest to find and the rendered service will be more personalized.
- Fewer contacts: since the data of the citizens and the companies will have to be collected only once, that data will be exchanged in a maximum way between the administrations and that information will be managed in a pro-active way.
- More transparent: the citizens and the companies will have greater participation in the decisions, will be able to communicate directly with qualified public services and will have access to the personal data of which the administration lays out in their connection

In trying to find the needs and interests of citizens towards those solutions, there are disparities, for instance between the regions of the country (between the North and the South) and also discrepancies depending on the age's scales (young people are reached more easily than older people).

What are the requirements for interoperability for the GOVERNMENTS ?

The notion of authentic sources.

To take care that the data already available in an administration are not requested every time, the principle of the "authentic sources" was introduced. This principle means that the administration which, functionally speaking, treats more one set of data, is designated as the only person in charge for the request and the update of the data.
Other administrations which need these data must consequently be able to use them. (for instance, the ministry of finance can not ask anymore the address of any citizen, it

must ask it to the ministry of interior, where it is stored in the database of citizens). It is done by using other bases like keys of single identification and Universal Messaging Engine. To protect to the maximum the private life, this data exchange must be always founded on a legal basis and in accordance with the principles of finality and proportionality. A sub-commission of the Commission on the protection of the private life controls the whole process.

There was also the necessity of a platform to interconnect all the ministries together. The platform is a unique single contact point through which any ministry can come and connect itself to it using a common syntax and semantic and where it can exchange information with other ministries. If this process has been easily done for the syntax point of view, it was however less clear for the semantic. For instance, there were some notions that were not interpreted in the same way by the different ministries, which of course, could have created problems. Some work has been done on a common terminology.

The problem arising with this system is to be seen at the technical level because if access is granted at one of the entry point, then there is a security risk which is created.

What are the requirements for interoperability for the MERCHANTS?
What are the benefits of interoperability for each of these stakeholders?
What is hindering the establishment of interoperability at the technical, legal and cultural levels?

One of the problems relating to the end-users is connected to a general problem of communication of relevant and efficient information to them. For some respects, there is a feeling of bad communication to the citizens. And this starts already when communicating the correct information to the administrations and among the administrations themselves, so that they can also take benefit from previous experiences.

Another problem may come from a difference of interpretation of terms among governments. There is a need of common terminology to avoid this kind of problems. The solution could come from the legal side through legislative initiatives. However, it was not certain that this kind of regulation be necessary

What can be done at the TECHNOLOGICAL level to establish interoperability?

The e-ID should be usable for different services (in comparison with a bank card which is used for specific purposes)
The e-ID must follow a distributed model. The problem in an open world is that when problems appear, people must know to whom they have to address them.

The e-ID in Belgium, when delivered has no more links with the provider of the card. This is a different situation from for instance, a bank card in Belgium. Any time a card from a bank is used in a cash machine, the information is passed to the bank itself. On the contrary, with the e-ID, there are no more links with the provider (Fedict) unless you are using one of their services (for an online tax declaration, the

data will go to the government, and especially to the ministry of finance, but at the same time, the ministry of interior is not aware of this)
This means that it is a completely **distributed** model.
What happens when there are problems…defect of card, people go back to government/cities
When the problem is related to the applicative use of the card, the problem will have to be solved by the provider of the service.
There is an intermediary layer element in the card that makes the translation between the card and the software application like a browser internet or an internet e-mail like outlook. For the rest, it is the provider of application who has to deliver help for the use of the system.

Another problem which also exists relates to the evolution of the card
A card has life duration of 5-10 years but the format of cards is changed more or less every 6 months, which means than during those 5-10 years, there can have 10 to 20 different formats of card to manage.

The changes occur for different reasons:

- Security reasons: cryptographic key, etc
- New functions: new things added, integrated to them
- Modifications to existing functions, which is the more problematic change: the card responds differently. If there is a change regarding the format on how the data are structured in the card that will lead to a difference in format of data between a person having received a card in 2004 or 2006.

The difficulty is to explain to the one who will use it. It is why the software part is important in the card. It is in this part that can be included software to recognise the different formats of cards (and this makes the card reacting in the same way even though it has been differently developed)

Problem is those who do not want to use the card itself with the software part provided and want to use their ones. There is then a necessity to conclude a contract with them and let them know well in advance (~6months) that a change in the card will occur so that they can work on their versions. The actors needing this are: Banks (readers where application software is in the reader (terminal of payment)), actors in the security social sector.
Agreements on this are developed sector by sector.

All what is explained above means that we can't really, at the moment, talk about interoperability. For this, we should need other cards. There are some similar situations in other countries (for instance in Sweden or Finland but for the latter, the process is currently purely voluntarily (60.000 volunteers only)).
Weather

What can be done at the LEGAL/POLICY level to establish interoperability?

There is an important respect of the legislative framework, especially for what concerns the data protection aspects, which were not fully taken into consideration at the early stage of the development of the e-ID. However, in a certain sense, this strict legislation is a barrier, in the sense that it makes the integration of the administrative simplification more difficult. As an example, the legislation around the use of a

unique ID Number coming from the national registry of citizens has an impact. The respect of this legislation can also send a clear signal to companies in the sector in order to make them compliant with the legislation.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

What should be the role of governments in addressing interoperability of IMS?

Regarding interoperability among member states, during a long time, there has been a lack of coordination. At several moments, there have been talks about the interoperability of the notion of electronic identity at the European level which have not been really successful so far. There are problems of harmonization due to a lack of strong political commitment.

What should be the role of merchants and industry groups?

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

12.3 Report 3: Paul Timmers, Belgium, egovernment

D4.2: Requirements for interoperability in IMS

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer: Michaël Vanfleteren
Interdisciplinary Centre for Law and Information Technology (www.icri.be), Katholieke Universiteit Leuven, Belgium
Tel.: +321625256, Email: michael.vanfleteren@law.kuleuven.be
Interviewee: **Paul Timmers, Head of Unit for egovernment**, **Directorate-General for Information Society and Media, European Commission**
Web: http://europa.eu.int/egovernment_research
Tél: +32-2-2990245, fax +32-2-296 4114
Email: paul.timmers@cec.eu.int
Location: Brussels, Belgium
Date: 01.09.2005

Background Information:

Paul Timmers is head of unit for egovernment in the European Commission, Directorate-General Information Society & Media. Previously he was a member of the Cabinet of the European Commissioner for Enterprise and Information Society, Erkki Liikanen, responsible for the information society (eEurope) and telecoms policy portfolio. Dr. Timmers has also been deputy head of unit for electronic commerce in the European Commission, where he was involved in policy and program development. He has also held management positions in product marketing and software development in a large IT company and has co-founded a software start-up. He has published on a wide range of topics, including a book on electronic commerce strategies and business models. A visiting professor and lecturer at various universities and business schools, Dr. Timmers holds a Ph.D. in theoretical physics from the University of Nijmegen in the Netherlands and an M.B.A. from Warwick Business School in the United Kingdom.

What are the main identity management issues in e-governement?

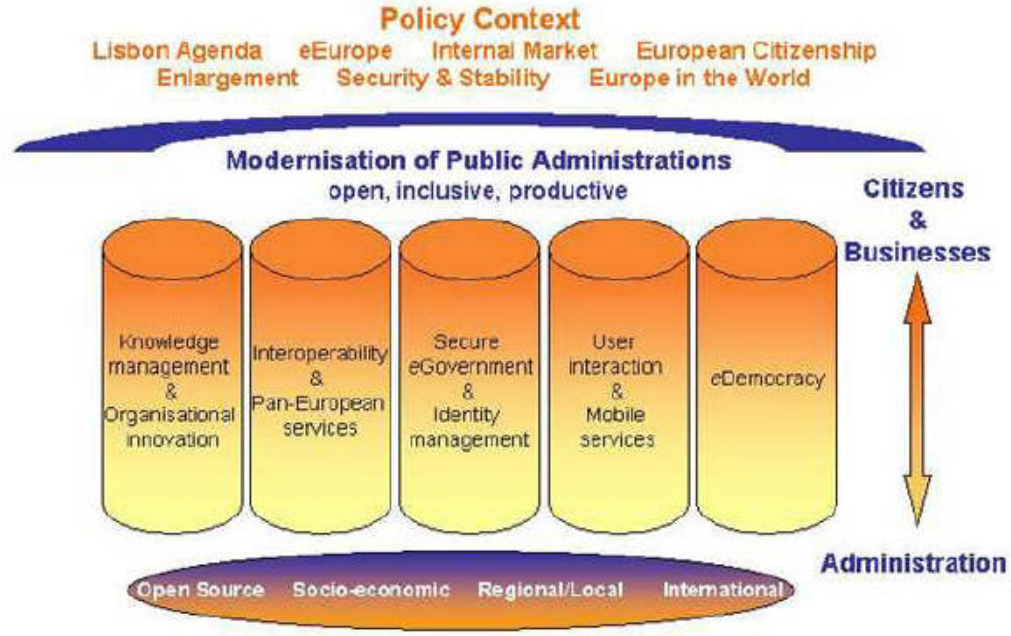
The EU is pursuing the policy development for electronic identification and authentication for government services as well as research & development[18] into such services solutions (for instance in electronic ID systems that can be used in public services, cross-borders). Basing that work and research in the policy government on the actual practices (i.e. the good practices) that are happening and in place right now for which there is a separate scheme to collect such good practices to support them and to promote them. Among those promoted through an award scheme or through a good practice framework

[18] RTD on interoperability applied to eGovernment plays a central role to move away from eGovernment islands towards Networked Governments which will enable the virtual integration of the different layers of public administrations (local, regional, national, EU and worldwide) as well as citizens, business and civil society. See also: http://europa.eu.int/information_society/activities/egovernment_research/focus/interoperability/index_en.htm

Three groups of issues for egovernment beyond 2005 have been detected[19]:

- The first set of issues is about the challenge to move from today's state of play of bringing services online towards more profound modernisation of public administrations with the help of ICT, organisational change, and improvement of human resources in public administrations, in order to deliver sustainable benefits.
- The second set of issues addresses the challenge to achieve innovation in government services and governance in order for public administrations to realise their full potential as key contributors to economic and social development and to meet future demands. Governance meaning the rules, processes and behaviour that affect the way public administrations function. One could also say: the organisation and culture of public administration.
- The third perspective focuses on contributing to European egovernment objectives: the emergence of pan-European egovernment solutions, contributing to a European public asset of egovernment building blocks, implementing European policies, and increased cooperation at European level in order to better address eGovernemnt at all levels.

The three sets of issues follow from taking three different analytic perspectives on eGovernemnt of the future. They are partially overlapping. This is to be expected. For example, consistently pursuing modernisation is likely to lead ultimately to innovation. Both modernisation and innovation can be looked at from a European perspective. And there will be some common issues such as interoperability or identification/authentication. Addressing them can help to make progress in modernisation, open the way for further innovation, and contribute to realising European-level objectives.



[19] See also the Working Paper on eGovernment Beyond 2005 – An overview of policy issues.

How critical is the issue of interoperability of IMS for egovernment?

- Any comment on joint actions on interoperability relate back to the sphere of e-ID. It is in a much longer process which started in 2003. There was an egovernment communication that signalled that there was **fragmentation**. He did not propose solution but underlined the need of work on that area. Nowadays, research and development projects (ex: EU project Modinis) are working on but the solution will not only come from this. There is work, which needs to happen in **investigating** the situations. In another view and complementary to the R&D projects, there are also debates among the policy makers themselves (see below on the policy subgroup), putting the elements in place and complementary to that, there has also been the set up of a group practice framework in order to make sure that there is visibility of solutions. The different e-ID solutions are integrated in this group practice framework and on its promotion.

- Therefore in 2003, there was the signalling of the issue and some of the components were already in place. But from 2003 till 2004, the other components have been put in place. In that respect, things are now moving forward. Policy makers are likely to define an objective (see below on the outcome coming from the next ministerial meeting in November) and whether they can agree upon and get something like a roadmap that moves towards an objective in the 2010 timeframe. But many of these components are now in place. Some are still missing, not so much of the technical, neither from the legal issues because there is also work happening on the legal issues as well as work happening on semantic and organisational interoperability and technical interoperability.
- Although the components are getting into place, the question of what are the main barriers is difficult to answer because it is a combination of elements and maybe over time, other priorities will be emerging. Today people are signalling that there are issues around, for example common terminology, which seems to be a starting point to tackle the problem, hopefully that is away soon, problems around mutual recognition, the way e-ID are handed out (registration procedure) but in 2008 timeframe, we might talk about the acceptance of a legal intervention if needed at all. It is then difficult to say what is more important because it could take a too narrow and too short time perspective. We can't have a definite view on current issues; we must have at least a 5 years long term perspective.

egovernment has been developed so far in a very fragmented manner. egovernment services have been deployed by a multitude of public administrations at the national, regional and local level. Those services are islands of automation which cannot work together.

This fragmentation may severely handicap the wide take-up and widest possible impact of egovernment unless joining-up administrations and inter-linking online services is made possible through the interoperability *egovernment* services. This should be approached in a stepwise manner by addressing the most compelling problems where economic and societal impact could be achieved.

This is among others the case of egovernment services having a Pan-European dimension. Services involving the participation of administrations from different Member States is one of the domains in which interoperability is required.

egovernment users should be able to access any possible service online in a transparent manner regardless of the administration(s) actually providing the service or whether the services of several Administrations need to be combined.

egovernment interoperability is the enabler which will make the above possible. This involves research work to ensure the interoperability of diverse back-offices of different administrations, dynamically build and follow the workflow of those services, discovering and using services using semantics and supporting civil servants with knowledge management techniques

How would you define interoperability of IMS? What is an interoperable IMS in terms of the egovernment? What would interoperability enable?

This definition has already been broken down into several types of interoperability in all the little components that there are in IMS: the semantic, the organisational and the technical interoperability. It is made of a combination of things. There is not one single solution for defining it. There are different kinds of issues behind the interoperability with solutions which can be close to the user with high technical specifications to solutions which are not necessarily visible to the end-user but which dealt purely between the administrations.

If we take any simple application on online eGovernement service attached to e-ID, we would deal, for instance, from the user side, the technological side and within the member states. Then, if it is multiplied by x numbers fields of research, we will see the complexity of it. That is where there has to be understanding on what mechanism people would have, what is being done for that particular application on e-ID. For instance, could this be applied to 5 other member states? How much changes those member states would need to make in terms of their own technology, legacy system and also organisational side. Those are issues that don't turn out very often in the current discussions.

To take another example, for instance the work on mobility and registration, where we can have the option that the actual identification is just happening purely locally, where nothing happens from the user perspective but there is an inter-administration interoperability where users have to go to a website of the other country where they use their national identification token and it is possible that there could already have an interoperability at the technical level, which is very close to the user, which the user see with their ID token and their authentication means which correspond to what is expected from the other side.
There are different kinds of solutions for application services that can be implemented and that shifts the interoperability from perhaps very close to the user (very kind of physical and technical interoperability) to something that might be not visible from the

end-user but maybe dealt with purely between the administrations and that has also a lot to do with technical interoperability and also with the semantic interoperability

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

For Electronic Identification and authentication at the policy side, the EU is working closely together with the Member States, in the so-called subgroup of the eEurope Advisory Group of leaders of national egovernment initiatives ('the egovernment subgroup'). It brings together the people who are leading the national egovernment initiatives.
At the European level of interoperability on egovernment, there are discussions on what are the next steps to go from a situation where there are many e-ID solutions emerging, not at the European level, but at national level, within the public sector and of course also looking at the situation that a lot is emerging in the private sector. The issue it to know how do we go from that situation to something where you can use e-ID crossborders for public services in a way that also makes sense for the private sector.

How far are we currently from that scenario?

The EU is going towards an objective that should be reached in 2010
That is at the policy side timing: there will be a Ministerial egovernment Conference held on 24th & 25th November in Manchester, UK. It is the most important event in 2005 featuring achievements and Best Practices and analyzing the future of egovernment in Europe. It will bring together ministers and politicians responsible for egovernment in Europe together with CEOs, managers and practitioners from industry and public administrations. There, a ministerial declaration on what the Members States want to achieve on electronic identification for public services is expected.
The Commission will release an action plan for e-government in April 2006 and following that, there will be further work on executing and following a roadmap till 2010.
Within that, all kind of components will contribute within a framework:

- there is work on legal uncertainties, on the technical nature of achieving a system, an approach which allows for federation and multiple levels of e-identification and authentication, that allows also for the choice and the option to put it into one solution (combined with biometric passport, or to put in a variety of solutions, for example for mobile phones, or different levels of e-ID and strength to authentication)
- There is also need of work on common terminology, test-beds, user impact assessment, work on promotion and user involvement.

In a policy perspective, the process can be described as follows: it is the research of what is desirable, what is the objective that should be achieved, through the situation we are standing today, and then do a gap analysis and also what could be a Roadmap to move to that objective: 2010.

The objective is that, by 2010, interoperable electronic identification and authentification should be available and used in a number of practical cases of key importance: Electronic procurement cross border, citizen mobility, application crossborders, etc

To summarize what wants to be seen from the EU, it is that the egovernment services are wider in a secure manner and that is the way it is believed the e-ID can help. that is the positive aspect it has to come through.

The **trust** of egovernment dealing, services is something which people should feel. If it comes from the e-government, this is something they can trust and it is secure and once they have confidence in it, they get the services faster without worrying. All those aspects are linked to the original e-ID.

What are the requirements for interoperability for the USERS?

Many activities are happening on interoperability (projects, etc…), but they are not only necessarily dealing with electronic identity itself, but are analysed in a wider sense.
There is a need to look at what interoperability means from a user point of view. The questions raised touch upon into which application the user enters certain data and which applications he accesses information and he may to provide something. When a user provides data entry for one case, he should be given the possibility to use the same data across the bunch, irrespective of the system he uses, the applications he uses. How he is not being asked to duplicate his data and is neither being forced to buying other systems simply because something which is sent to him is not accessible to him for whatever limitation.

Some recommendations have been proposed by the eEurope Advisory Group (cobra recommendations[20]), which form the basis for the much more concrete work that happens today. These recommendations lead now to the development of roadmaps.

An important guiding principle is to reduce the administrative burden for citizens and companies. Cooperation is needed to exchange approaches to information management policies, data provision, protection, sharing and re-use. A possible way to achieve user-oriented service delivery and optimal re-use of information is once-only data provision (meaning that the citizens and companies do not have to give twice the same information to the administration), also across border, while ensuring that data protection, privacy, citizen rights and democratic control are respected. These ties back to the approach of an e-ID perspective.

The perception is that the technical solutions exist and can be used to achieve what is necessary. Number of things need to happen almost in parallel. Of course, the interoperability is one of the key aspects.
The people have to feel that it is working:

- Via mutual recognition
- To get acceptance of this by the people. At the early stages of e-ID, there were number of trials, people are learning from their experience, mistakes will be made and it will take some time. Necessity of good mechanism to try to explore at a

[20] See "Cobra Recommendations" to the eEurope Advisory Group, eGovernment Beyond 2005, Modern and Innovative Public Administrations in the 2010 horizon, 25th October 2004

more higher level to build awareness (to feel comfortable with and get used to). Are there still fears..etc Unless you get to this level of acceptance, chance of practicability are higher. It is not looked enough by research activities. One part of acceptance.

What are the requirements for interoperability for the GOVERNMENTS ?

From a Government point of view, it is a similar situation. The question is to know if they want to put in systems for every single application, irrespective of the technology basis or the application, the use of base. They need to find some mechanisms, some ways which are going to work. An information provider has to find usable solutions. It can seem simpler but from a technological and organisational point of view, it is rather complicated. And it has to be looked at not only from a necessarily electronic identity point of view, but it is much a wider problem, but it can be narrowed down in analysing only the electronic identity and then maybe find a solution at the interoperability issue

Stakeholders' involvement is important. The R&D projects involve those who build the system, basically the public administrations themselves and they test the system with users, so that it is visible to see what works and what does not work, to open the debate and see the fears and allows going one step further, because it is then based on practical examples.

Approach chosen = keeping the various elements of advanced development in real practices from stakeholders AND the approach is to do from the services (executing a scheme like the one developed (see page) what was be selected as examples when it will be tested.
What are the keys that have more sense (electronic cross borders applications services)
For instance, when electronic identification is more necessary for enterprises than for citizens.

What are the requirements for interoperability for the MERCHANTS?

What are the benefits of interoperability for each of these stakeholders?

There are important points which are currently being studied and evaluated:

- User awareness and acceptance
- Validation & relevant key application (otherwise, we would only be talking at a theorical level). The focal point is from the perspective of the needs of the public administration. It is not at all the e-ID systems but more about the services that have to work, in an efficient and user-friendly way. To be precise, it is not coming from specific pre-conceived perceptions of what an e-id should be, but more what should be the delivered benefits.
- Technical and functional interoperability at European level, based on national e-ID systems which have to be in place (but are not at the moment)
- e-ID & authentication management at national level

- Legal certainty, because it is not necessarily sure that we are talking about legal barriers and it is precisely where studies are going on (ex project Modinis).
- The issue about common terminology/principles, common registration principles for obtaining an e-ID. The commonality has to be "perhaps" formalised in mutual recognition. It is a completely open question at the moment, as there are questions whether there is a need of legal intervention from the Commission side. The Commission needs to see evidence before intervening.

Components of intervention of the policy framework: The Commission contributes at the European level in different ways through studies, R&D, test-beds consolidating specifications and if needed, make legislative proposals

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

What is missing in the current discussion on interoperability in egovernment is more the debate around user awareness and user acceptance that is an important issue which may come back through the backdoor if this debate gets connected closely to, for instance, biometric passports because in the other dimensions of security, this debate comes into it.

What can be done at the TECHNOLOGICAL level to establish interoperability?

For what concerns a precise solution at the technical side: at this moment, experiments leave the question open.
- It is also possible that today's technology does not allow for the most elegant solution.
Another solution at the technical side could be to link a French ID to a Finnish system could be the creation of entry points to the other system (=using your identification number to a different system where your data would be translated into the other system and this becomes of course an inter-administration problem to supply the function). Several problems could then arise (multiplication of systems, etc..) but a lot of things are coming to place: is it manageable, efficient, desirable, sustainable.

What can be done at the LEGAL/POLICY level to establish interoperability?

Legal issues may be addressed (recognition of electronic documents, recognition on registration procedure) making sure that the implementation of the electronic signatures correctly fits with it.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

Cultural/institutional factors can come up more strongly, once we go into the specific application area, they may be very strong: ex: it is not taken for granted that electronic procurement if you can do it cross-border, is also really accepted cross-border. There are cultural practices behind it. If we talk about citizen mobility applications, there may be work regarding semantic, organizational and technological interoperability but also the way people are executing these services and expectations they have around them can be quite different and within sectors and community, this may come up again. But it is difficult to say which one will be the case. Another point is that even if a system is technologically usable, it could not have the acceptance. Administrations do not want something that does not work automatically.

The place of the services directive (e-ID has to enter and play a major role in it) has also a lot to do with cultural expectations.

Finally, the issue on electronic certification can also play a role.

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

Today, the priority is to get an agreement on where do we want to move in policy terms. And immediately after that, which is almost in the same timeframe, there is the question of what is user acceptance and usability, working on the solutions that are already there (ex: technology already there). It is not perfect but it gives a feedback on what is the real experience. And then it can break down into individuals at lower level issues than technological may have to be solved (delegation, roles,…)

Electronic Identity Management for *egovernment* requires a combination of technological, social, economical and application-oriented research, which includes:

- Security and privacy of the identity data;
- Public trust and acceptability;
- Technological, organisational and linguistic interoperability;
- Study into coherent approach for identity at EU level;
- Identity Management ontologies and their categorisation;
- Smart card technologies for identification and authentication;
- Priority applications of electronic identity and authentication for *e*Goverment;
- Standardisation issues and their solutions;
- Legal aspects for a coherent approach at EU level;
- Cross border identification;
- Biometrics for electronic identification;
- Differentiation of identification and authentication;
- Case studies and large scale pilot demonstrations;
- Potentials for mis-use of electronic identity and ways of preventing them

What should be the role of governments in addressing interoperability of IMS?

- The private sector has had the lead so far. The governments, over the past 2 years, have become much more active on this and in some countries, they have

taken the leading role with the private sector either following the lead of the governments, or in some countries, the governments have said they would use the solutions coming from the private sectors (for instance in Finland). At this stage, there is no doubt that there should have a partnership where the emphasis is somewhere different depending on the country.

- Regarding the role of governments to get involved in the leading role, given the fragmentation of solutions, there were hopes that government would intervene in the market. This has been achieved mainly through p**artnership** and increasing role by governments. However, governments are not going on their own. There are variety of initiatives (in Italy, it is the government which is issuing the card). At this level of partnership, the private sector is then more like the technology provider but not necessary acting as the service provider (for integration, testing, etc…).

What should be the role of merchants and industry groups?

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

There are different projects of regulation at the moment

- cross-border payments in public procurement within the internal market. And a related action plan to electronic public procurement (investigating the barriers existing in practices) executed… this is implemented differently from one member states to another, apart from the **technical** barriers where solutions can be found

- There is also a study on the **legal** barriers cross-borders (Modinis) based on the practices which are emerging.

- There is also a separate study about **legal** barriers in eGovernement in general
3 years projects

- within this project, there is study for its approach and its domain what are legal and cultural barriers that are bound in the integrated solutions proposed…
- some work done on article which focus on practical cases where test bad can be run such as social security for workers mobility
- this is finally accompanied by institutional and other kinds of barriers which are appearing when executing large scheme test.

Any other comments?

FP6 projects related to Identity Management in egovernment

- Emayor: www.emayor.org
- Guide: http://www.guide-project.org
Guide will conduct research and technological development with the aim of creating an architecture for *secure and interoperable e-government electronic identity* services and transactions for Europe. By establishing an open identity management architecture for egovernment solutions,

Guide will enable governments to offer higher quality services to businesses and citizens reducing administrative costs whilst fighting the negative consequences of identity theft. Guide will address issues relating to the dramatic improvement in the efficiency of inter-administration communication to harness the full potential that pan-European process integration brings.

- Hops: http://www.bcn.es/hops/

- Modinis:
Under the auspices of the eEurope 2004 MODINIS programme, the European Commission initiated five studies in December 2004 to illuminate key aspects of the egovernment agenda by:

- **Assessing the** financing, benefits and **economics** of egovernment
- **Identifying** the remaining **legal** regulatory and organisational **barriers**
- **Advancing identity management** within the EU
- Intensifying the **exchange** of information on practical egovernment **interoperability experiences**
- Making available services to reinforce the **exchange of good practice** in egovernment

They will use a variety of methods over the next three years, including studies, surveys, workshops, expert groups, reports, websites and symposiums to deliver their objectives.

12.4 Report 4: Frank Robben, Belgium, ehealth

D4.2: Requirements for interoperability in IMS

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer: Xavier Huysmans
ICRI, Katholieke Universiteit Leuven
Tel.: +32-16-325177, Email: xavier.huysmans@law.kuleuven.be
Interviewee: **Frank Robben, Crossroads Bank for Social Security**, Sint-Pietersteenweg 375, 1040 Brussel, Web: http://www.ksz.fgov.be
Tel.: +32-2-7418402, Fax: +32-2-7418300, Email: frank.robben@ksz.fgov.be
Location: Leuven, Belgium
Date: 07.07.2005

Background Information:

Mr. Robben is general manager of the Crossroads Bank for Social Security, an institution he conceived and founded. The Crossroads Bank for Social Security elaborates the E-government strategy within the Belgian social sector and coordinates the implementation of the E-government projects in this sector[21].

In October 2002, the Belgian social sector case was mentioned as best practice in the web-based survey on electronic public services ordered by the European Commission. During the second Conference on egovernment in Como in July 2003, the global eService project of the Belgian social sector was nominated in the category

[21] In the Belgian social sector, a major business process re-engineering and computerization was carried out during the past twenty years by about 2,000 Belgian actors. Their close collaboration led to the implementation of a network for electronic information exchange which includes public and private institutions from different levels (national, regional and local). An integrated electronic work flow has consequently been developed between companies and social security institutions. A social security portal is available containing integrated services (information and transactions) (see www.socialsecurity.be). The portal is intended for citizens, companies and social workers. The actual eServices in the Belgian social sector demonstrate the results of a strategic information management plan based upon common basic principles and the use of common tools for data sharing and exchange.

Further reading on the reform process in the Belgian social sector: F. Robben, "eServices in the Belgian social sector: a successful combination of business process re-engineering and computerization", published on his website http://www.law.kuleuven.ac.be/icri/frobben/publication%20list.htm. It describes the basic principles applied to rationalize information management in the Belgian social sector (and the Belgian public sector in general), the results obtained in the social sector, a number of critical factors for a successful development of eGovernment and a number of specific risks that need to be managed.

'European, Central and Local Government eCo-operation and Public eServices' as one of five 'best practices', selected from some 500 projects.

In December 2004, the Crossroads Bank for Social Security received the Belgian egovernment Champion Award for the quality of its results, both in back office integration and improvement of front office service delivery. At the same time, the Belgian social security institutions received a Belgian egovernment Award for an improved service delivery to the companies.
Mr. Robben is also strategic advisor at FEDICT, the Belgian Federal Public Service for Information and Communication Technology. In that function, he developed the concept of the electronic identity card[22] and the company register, and he worked out the general information security and privacy protection policy of the Belgian federal government.

He is a member of the Belgian Privacy Commission[23], the Belgian Commission about telematics standards in the health sector, the steering committee of the Belgian federal public service for administrative simplification and the Dutch Commission about reduction of the administrative burden for citizens.

The interview:

Mr. Robben is undoubtedly a key expert of both egovernment and ehealth field of analyses. We decided to interview him about the most specific and less documented one, namely ehealth.

Mr. Robben's views on egovernment and his approach of the Belgian Federal government are well documented. In annex, you'll find the slides Mr. Robben has presented on 4 May 2005 about identity management in e-government, in the framework of the FP6 project Modinis, and the article Mr. Robben has written together with Mr. Deprest (CEO of Fedict) about the e-government approach of the Belgian federal administration. Both the article and the slides can be found on Mr. Robben's personal website http://www.law.kuleuven.ac.be/icri/frobben.

Questions:

What are the main identity management issues in the chosen field of analysis (ehealth)?

Health care objectives

Mr. Robben stressed that ehealth is a way to implement (general) health care objectives. The most important (current) health care objectives are:

1) *To acquire a high standard of health care provision for patients*

[22] More info: http://eid.belgium.be/en/navigation/12000/index.html.
[23] http://www.privacy.fgov.be.

There are many good reasons why it is necessary for health care providers to be able to access data that are already available from other health care providers. One of them is to make the system financially acceptable.

An example of x-ray photographs can be mentioned. These are often taken more than once. The concept therapeutic freedom is surely important, but it should not lead to unnecessary things being done.

In the end, an ideal system is one that is not obligatory (as then it might not be accepted by the health care providers), but one that is based on best practices.

2) *To build a cost-effective system. One of the building blocks of such a system would be the reuse of data that are already available*

3) *To reinforce the role of the general practitioner (GP)*

The role of the GP has to be reinforced. This can be done by stimulating patients to go to a GP, before going to a specialist, e.g. by charging them more for their visit, if they go directly to a specialist.

Application to ehealth

The abovementioned objectives can be better achieved by using ehealth.

Interoperability in the field of ehealth is mainly about exchanging data among health care practitioners. Mr. Robben emphasized that identity management is not only about managing the identity.

Roles, mandates and functions are also relevant. He referred to the previously mentioned presentation he delivered within the Modinis project framework on 4 May 2005 on the topic "Identity Management in egovernment", in which he explained the importance of these concepts.

For the sake of clarity, we include 3 chapters of Mr. Robben's presentation in the report[24]:

*"**Objectives to be achieved**:*

- *To be able to electronically*
  - *identify all relevant entities (physical persons, companies, applications, machines, …)*
  - *know the relevant characteristics of the entities*
  - *know that an entity has been mandated by another entity to perform a legal action*
  - *know the authorizations of the entities*
- *in a sufficiently certain and secure way*
- *in as much relations as possible (C2C, C2B, C2G, B2B, B2G, …)*
- *using open interoperability standards"*

International context: some issues

[24] Besides the quoted chapters, the presentation also contains a proposed conceptual framework and the choices made in Belgium (see annex I.).

- *determination of the means by which an entity can be identified within each country and across countries*
- ***the way identity management and characteristics management are well separated in order to guarantee the multifunctional use of identity authentication means***
- ***the quality insurance criteria for the registration procedures that are used to determine the identity, relevant characteristics or mandates before linking it to authentication or verification means***
- *the quality insurance criteria for authentication and verification means and their use*
- *an organizational, functional and technical interoperability framework to exchange identity, characteristics, mandate and authentication data based on open standards*
- ***the necessary legal framework for identity, characteristics and mandate management, with a good balance between trust enhancing measures and measures guaranteeing a free market.***

International context: proposed method

- *to work out a common conceptual framework, a common vision and common basic principles*
- *to translate these principles in common, measurable objectives*
- *to ask every state to develop an action plan to achieve these objectives*
- *to elaborate an architecture and guidebooks to implement the principles*
- *to create a forum for the exchange of best practices."* (bold format added)

How critical is the issue of interoperability of IMS for this field?

Mr. Robben believes that it is very critical. The main issue in ehealth is of course the health of persons. Wrong information leads to wrong decisions, which is very dangerous especially in this field.

Mr. Robben admitted that ehealth could theoretically exist without interoperability, but it would have to be local, with the consequence that a person would always have to go to the same hospital. Good health care cannot be organized without IMS. This is clearly a sector where specialists need to work together.

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?

We submitted Mr. Robben the definition on interoperability used in the ATHENA project (*"The ability of two or more networks, systems, devices, applications or components to exchange information between them and to use the information so exchanged."*[25]).

[25] This definition of Interoperability was presented in the white paper of the ATHENA's project (http://www.athena-ip.org)

Mr. Robben expressed his approval of this definition, with the reservation that definitions should not hinder practical application, and thus it could possibly be amended to be consistent with the practical requirements.

He emphasized the need for a common conceptual framework, but stressed that the concepts of identity, roles, and mandates are much more important than the concept of interoperability.

Hereafter follows Mr. Robben's proposed conceptual framework, as presented in the above mentioned Modinis' presentation:

*"**Conceptual Framework***

- *entity: someone or something that has to be identified (e.g. a physical person, a company, a computer application, …)*
- *attribute: a piece of information about an entity*
- ***identity**: a number or a set of attributes of an entity that allows to know precisely who or what the entity is; an entity has only one identity, but this identity can be determined by several numbers or sets of attributes*
- *characteristic: an attribute of an entity, other than an attribute determining its identity, such as a capacity, a function, a professional qualification, ...; an entity can have several characteristics"*
- ***mandate**: a right granted by an identified entity to another identified entity to perform well-defined legal actions in her name and for her account*
- *registration: the process of determining the identity, a characteristic or a mandate of an entity with sufficient certainty, before putting at the disposal means by which the identity can be authenticated, or the characteristic or the mandate can be verified*
- *authentication of the identity: the process of checking whether the identity that an entity pretends to have, corresponds to the real identity; authentication of the identity can be done based on the verification of knowledge (e.g. a password), of possession (e.g. an electronic card), of biometrical characteristics or on a combination of those*
- *verification of a characteristic or a mandate: the process of checking whether a characteristic or a mandate that an entity pretends to have, corresponds to a real characteristic or mandate of that entity; the verification of a characteristic or a mandate can be done by the same kind of means as those used for the authentication of the identity, or, after the authentication of the identity, by consulting a database that contains information about characteristics of mandates related to identified entities*
- *authorization: a permission to an entity to perform a defined action or to use a defined service*
- *authorization group: a group of authorizations*
- ***role**: a group of authorizations or authorization groups related to a specific service*
- *role based access: a method of assigning authorizations to entities by means of authorization groups and roles, in order to simplify the management of authorizations and their assignment to entities."* (bold format added)

He noted that interoperability stems not only from technical standards and organizational components, but also from legal measures (which can be hard law, soft law, and auto regulation).

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

Background information

For a better understanding of Mr. Robben's answers, it is good to first go over his views on interoperability in egovernment in general.

Mr. Robben believes that electronic information exchanges should take place on the basis of a functional and technical interoperability framework that evolves continually but gradually in accordance with open market standards, and that is independent of the methods of information exchange used.

Hereafter follows Mr. Robben's and Mr. Deprest's description of the elements of such a framework[26].

"[a.] ***Technical standards***

Many international bodies and organisations elaborate permanently changing open ICT standards. Government bodies responsible for the co-ordination of E-government initiatives can benefit by using these standards as a basis for developing an interoperability framework. Such frameworks have been developed for instance under the United Kingdom Govtalk initiative and the New Zealand E-government programme.

Typically, these frameworks set standards on

- *interconnection: networks (TCP/IP), mail (SMTP), directory services (LDAP), data transfer (HTTP and FTP), …*
- *information exchange: structured data and open text (HTML and XML-schemes), locked text (PDF), data modelling (UML), data transformation (XSL), web services (SOAP, UDDI), service repositories (WSDL), …*
- *security: transport security (SSL), secure mail (S/MIME), digital certificates (X509), …*

[b.] ***Agreements***

Apart from technical interoperability based upon these standards, there is however a great need for agreement on how to ensure functional interoperability and how to ensure that investment made by parties won't become worthless each time standards change.

Topics to be treated within such agreements are:

- *standardized encoding (e.g. return codes, …);*
- *standardized use of objects and attributes;*
- *standardized layout of message headers, independently of the information exchange format (EDI, XML, …) or the type of information exchange (on line, batch, …);*

[26] The extract originates from the above mentioned publication with Mr. Deprest (pp. 20-23, see annex II).

- *version management;*
- *backwards compatibility;*
- *SLAs on availability and service performance;*
- *access authorization management;*
- *anonymization rules;*
- *the availability of acceptance and production environments;*
- *priority management.*

[c.] ***Single identification keys***

The exchanging of information could be greatly simplified and the accuracy of information exchange could be better safeguarded through the use of common identification keys within all (governmental) information systems. Of course, the presence of such keys makes it easier to interlink data.

That's why [Mr. Robben and Mr. Deprest] *propose subordinating the interconnection of information to a previous authorization made by an independent committee. But when information exchange is allowed through such an authorization, it should take place in a way that best guarantees the accuracy of the information exchanged.*

Each entity (e.g. a person, a company, a plot of land, …) that might be the subject of information management or exchange should have an identification key, with which the entity is identified within all (governmental) information systems. These identification keys should be

- *single: this means each entity has only one identification key, and that the same identification key is not assigned to several different entities;*
- *exhaustive: this means every entity to be identified has an identification key;*
- *stable over time: this means the identification key doesn't contain variable characteristics of the identified entity, doesn't contain references to the identification key or characteristics of any other entities, and doesn't change when a feature of the entity being identified changes.*

From an international perspective, either a country prefix can be added to the national identification keys, or conversion tables can be managed between national identification keys of different countries. […]

In Belgium, each private individual has a single identification number, allocated either by the National Register for private individuals registered in a Belgian population or aliens register, or by the Crossroads Bank for Social Security in the case of private individuals who have a file at a Belgian social security office or public service, but who are not or no longer registered in a Belgian population or aliens register. […]

Since 1 January 2003 the companies and their plants have received a single identification number, allocated by the Crossroads Bank for Enterprises. For those firms that already had a VAT number before 1 January 2003, the company number is the VAT number. […]

[d.] ***A shared, publicly accessible information model***

[The] *information has to be modeled* [see below, chapter d.1] *and to be collected* [see below, chapter *d.2*], *managed* [see below, chapter d.3] *and exchanged in accordance with the* [information] *model* [see below, chapter d.4].

The model typically contains standard elements, with well-defined characteristics, and the relations between those elements.

The model should be electronically and publicly accessible by a multiple-criteria search environment, with facilities to consult the model by element, scheme, version, ….

The model should be the outcome of a participatory process between all parties dealing with the modelled information. Workflow should be available to validate standard elements and their characteristics.

To comply with current standards, the model should be object-oriented, i.e. permitting inheritance within a multilingual environment.

A very important aspect is version management within the model, allowing transparent and easy access to changes between versions. Elements with their characteristics should be defined only once within the model

with a facility to view that definition in different formats." (bold format and text between brackets ("[…]") added)

Mr. Robben believes that in an e-government context, government bodies should deal with information as a strategic resource for all government activities. This implies effective and efficient treatment of information in compliance with basic data protection regulations.

He distinguishes the following principles that should be complied with (5 topics)[27]:

"[d.1]. *Information modelling*

Information should be modelled through government levels and government bodies in such a way that the model reflects the real world as closely as possible. This means the definition of items of information, their attributes and interrelations is based on an abstraction from reality and not on legal concepts. In so doing, changes to the information model are avoided due to changing legal environments.

[27] Extract from Robben, F., "eServices in the Belgian social sector: a successful combination of business process re-engineering and computerization", downloadable from Mr. Robben's website.

The information model should take into account as far as possible the likely uses to which information will be put. This requires a sufficient insight into the working of various government bodies, which can be ensured by creating a modelling committee that will agree on the information model and its subsequent changes.

Special attention should be paid to the time aspect during the information modeling process. The information may relate to a situation at a specific moment (for example the residence on 1 January of a given year) or to a situation during a period (for example the salary relating to a certain working period). It is important to have consistency in the basic temporal units with which information is used for various purposes.

The real world changes continuously, and not all uses of information are foreseeable. Thus, it should be possible to extend or adapt the information model flexibly when the real world, or uses made of the information, change. A good way to implement these information modelling principles is to use objectoriented information modelling techniques and modelling languages such as Unified Modelling Language (UML).

[d.2.] ***Single collection and re-use of information***

Information should only be collected by government bodies for well-defined purposes and in a way that is proportional to those purposes. All information should be collected only once, as close to the authentic source as possible. Multiple government bodies should not be collecting the same information repeatedly from citizens or companies. Nor should they collect information from a source other than the one at which information was first created.

For instance, an employer doesn't have to determine whether an accident which occurred at the workplace can be legally qualified as an industrial accident, but an industrial accident insurer must do so. Hence, this question must be addressed, not to the employer, but to the insurer.

Information should be collected using a channel chosen by the supplier of that information, but preferably electronically, using standard basic services (single signon,
receipt upon arrival of a file, notification for each message, and so forth).

Information should be collected in accordance with the information model and on the basis of uniform administrative instructions throughout all government bodies.

Ideally, the supplier of the information should have a facility to check the quality of information before passing it to a government body. This implies the public availability of governmental software to check the quality of information.

Once arrived at government, the information collected should be validated only once, following an established task sharing system, by the most suitably qualified government body or by the government body that has the greatest interest in its correct validation.

Only after this validation process, can information be shared and re-used by authorized users. Otherwise, errors will be distributed among government bodies. Moreover, suppliers of information risk being contacted by different government bodies to rectify the same incorrect information.

[d.3.] *Information management*

Information in all its forms (for example spoken, printed, electronic, or image) should be managed efficiently throughout its life cycle.

Functional task sharing should be established, indicating which body stores which information in an authentic way, manages that information and makes it available to authorized users. In this way, an authentic source for every piece of information is set within the government as a whole.

Information should be stored in accordance with the information model and it should be possible to compile information flexibly in accordance with ever changing legal concepts.
Every government body has to report suspected information inaccuracies to the body that has been designated to validate that information.

Every body that has to validate information in accordance with the agreed task sharing system, has to examine any reported suspected inaccuracies, to correct them where necessary and to report the correct information to every government body known to have an interest.

Information should be retained and managed only while there exists a business need, a
legislative or policy requirement, or - preferably in an anonymized or encoded format - when it has historic or archive importance.

[d.4.] *Electronic information exchange*

Once collected and validated, information should be stored, managed and exchanged electronically to avoid transcribing and re-entering it manually. Electronic information exchange can be initiated by the body that holds information, a body requiring information or a service integrator. Electronic information exchanges should take place on the basis of a functional and technical interoperability framework that evolves continually but gradually in accordance with open market standards, and that is independent of the methods of information exchange used.

Available information should be used for the automatic granting of benefits, for prefilling
when collecting information and for information delivery to those concerned.

[d.5.] *Protection of information*

Security, integrity and confidentiality of government information should be safeguarded through an integrated set of structural, organizational, technical,

physical, staff screening and other security measures in accordance with agreed policies. Personal information should be used only for purposes that are compatible with the purposes for collecting the information. Personal information should only be accessible to authorized bodies and users in accordance with business needs, legislative or policy requirements.

The authorization to access personal information should be granted by an independent committee designated by Parliament, after having checked whether access conditions are met. Access authorizations should be published.

Each electronic exchange of personal information should be preventively checked for compliance with current access authorizations by an independent service integrator.

Each electronic exchange of personal information should be logged, to ensure the subsequent traceability of any abuse.

Each time information is used to take a decision, the information used should be notified to the person concerned together with the decision made. Each person should have the right to access and correct personal data held about him/herself." (bold format and text between brackets ("[…]") added)

The interview: application to ehealth

Mr. Robben did not mention all the aspects of the above described system during the interview; he concentrated on those parts which are to be adapted for ehealth. The other parts are *mutatis mutandis* applicable to ehealth.

It should also be noted that the described interoperability system, is part of a much broader approach of e-Government (see annex II), which contains several other aspects, such as:

- an integrated information security policy;
- a co-operation agreement between government levels;
- a customer-oriented re-engineering of service delivery processes of government bodies and value chain management;
- the legal embedding of the principles regarding strategic use of information an adapted ICT regulation;
- sufficiently consistent concept definitions;
- adequate ICT law;
- adequate measures to prevent a digital divide; etc.

a. Single identification keys

When exchanging information about patients in a ehealth context, it is extremely important to ascertain the identity of the patient. Both the identity of the health care provider (HCP) and of the patient are equally important.

1. Patient identity

Currently, two ways how to make sure that data are being exchanged on the right patient are being discussed. Both of them are based on identification numbers (organizing data by any other means than a number is not really feasible):

The *first scenario* is to identify a patient throughout the whole health care system with one unique PID (patient identifier) and to use this PID for every information exchange. It should be a number which is not connected to the patient's national number, i.e. without contextual data in it (e.g. date of birth, gender).

The Belgian Privacy Commission has confirmed that the use of such a unique patient ID number which is derived in an irreversible way from the SSID number (Social Security Identification Number)[28] (e.g. through hashing), is acceptable, if the use of this number is strictly limited to the health care sector.

Thus, one can be sure that when one has to identify the patient throughout several systems, one will always have the same result.

When processing health information for specific purposes, does not require identification of the patient, one could make use of derived identifiers. These numbers are derived from the PID and are specific for each purpose.

Consequently, as another contextual identifier would be used for each different purpose, interconnections of information between those purposes would not be possible, and no cross-purpose information could then be connected to a specific patient.

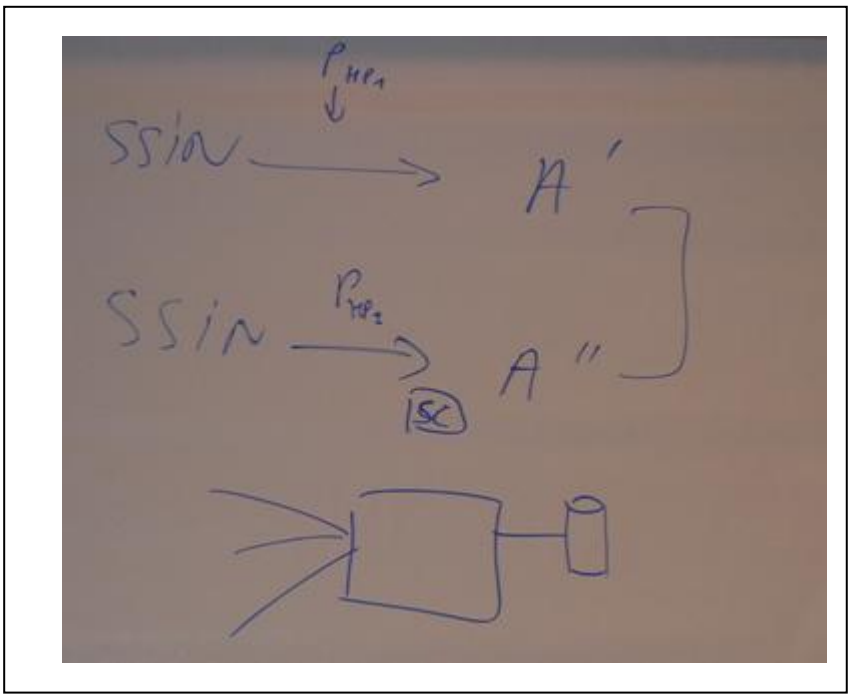
This scenario is based on organization and rules; if there are clear rules with a high level of sanctions, it should be working properly.

The *second scenario* is to use a local PID. This number will be used in a system where the PID is local to each health care provider. In practice, the SSID number of a patient and a parameter that is specific to each health care provider will be used. This parameter could, for instance, be the HCP's own social security number. This does not cause real privacy issues, as the processed sensible medical data do not concern him. Both numbers will be combined, resulting in a local PID.

The local PIDs are different among different health care practitioners. An external body, a kind of a Crossroads Bank for the Health Sector, will be necessary to identify patients between different health care providers by providing the conversion of several local PIDs.

[28] Ths number uniquely identifies each private individual in the social security. If these persons are registered in the Belgian population or aliens register, the number coincides with the National Registry number. If not, a *single identification number is allocated by the Crossroads Bank for Social Security (see also above, chapter [c]*.

Mr. Robben draws a diagram, see hereunder – the PID is A' and A" in the diagram:



An analogy can be drawn with egovernment, where there are also two schools. One of them, represented by Dr. Reinhard Posh, describes a similar system under the notion of "contextual identity"[29].

Mr. Robben noted that while this system provides the best protection against interconnection of databases, it will probably not be easily implemented at the moment as it is too complex. He stressed that it would probably take time to implement it in Belgium.

In summary, interoperability should be achieved by finding a balance between efficiency and security and privacy protection. Mr. Robben believes that a combination of independent *sectoral committees*[30] and a good system of sanctions for instances when rules are not executed correctly should make it possible to obtain the adequate level of security and privacy protection.

2. Health care provider's (HCP) identity

The necessary elements on this level are: the identification of the HCP, mandates and the relation between the patient and the HCP.

Firstly, the identification of the HCP (whether he has a "full capacity" (in Dutch: *hoedanigheid*) or not) will be done by a normal social security number; authentication on the level of a HCP can be done by means of an identification/authentication certificate on an eID card.

If the HCP does not want to use an eID card for this purpose, e.g., if he wants to stress that he acts as a professional rather than a Belgian citizen, he could get another authentication means.

[29] Kim Cameron's Identity Weblog on this topic: http://www.identityblog.com/2005/02/06.html.
[30] See above, section 4.1, d.5.

To prove that he is a health care provider, this information does not need to be reflected in a certificate: a database at the Ministry of Public Health (in Dutch: *Volksgezondheid*) with the relevant information is sufficient.

This database already exists and states who is a doctor, who is a pharmacist, and so on and since it is an electronic database it can also be electronically accessible.

Secondly, in a hospital scenario, there might be people accessing data that are not their own. Mandates are necessary to determine who can act on account of another person. It can be a central database of mandates or a set of local databases.

3. International aspects

Mr. Robben stated that international interoperability is not so difficult from a technical point of view, as there are common standards already. In countries where a unique national ID number already exists for administrative purposes, the patient number will be derived from it and the whole process will be easier. A conversion will of course be necessary.

However, there will never be an integrated high standard service delivery without the existence of a unique identification number. He remarked that even the British Queen has admitted this in her recent speech about the identity cards for UK citizens.[31]

A system of exchanging information is impossible without unique identification numbers. Those countries that do not accept the consequences of this will be suboptimal in their service delivery. However, they should not impose constraints arising from their choice on countries, where the choice has already been made to organize the social system.

b. A shared, publicly accessible information model

1. Information management

There are two kinds of relations between patients and HCPs, namely "stable relations" and "volatile (one-time) relations".

On the one hand, stable relations are for instance relations between patients and their regular general practitioner, who has access to their official electronic medical file.

Here, the patient should not have to authenticate himself every time to allow the access to his data. The fact that a doctor is a patient's GP will be managed through a (centralized?) reference directory.

When this doctor asks for the information from another HCP, he should be able to access the data. The type of relationship determines which kind of data he can access (e.g. an ophthalmologist does not need to know about the stomach problems of the patient).

On the other hand, volatile relationships are relations where a patient has a problem which he does not want to discuss with his GP (e.g. typical "male problems" could be

[31] See http://news.bbc.co.uk/1/hi/uk_politics/4034699.stm.

difficult to discuss with a female GP) or he wants to get a second opinion without compromising the trust relationship he has with his GP.

Mr. Robben stressed that this should be made possible without the patient's regular GP having to be informed. In practice the patient who has a volatile relationship with a doctor, would authenticate himself as a patient towards this doctor with his eID.

2. Protection of information

The authorization to access personal information should be granted by a sectoral committee, composed in majority by medical practitioners, not by lawyers. The role of the sectoral committee is to apply mainly the principle of proportionality. Therefore, specialists with the knowledge of the actual "state of the art" will be necessary. Mr. Robben specified that he sees this committee as a new subcommittee of the Privacy Commission.

This sectoral committee should a.o. grant access authorizations to entities (e.g. a HCP's or health care institutions), by pointing out

- which entity is allowed
- which access to
- which personal information
- about which patient,
- in which capacity
- and in which situation
- during which period of time.

These authorizations will not be delivered on a case-by-case basis. On the contrary, they will be in general terms for each type of exchanges. Consequently, there will also be a need for an external body that checks whether the actual data exchange conforms to the authorized rules.

The external body will identify patients between different health care providers should be a kind of a Crossroads Bank for Health Care, distinct from the Crossroads Bank for Social Security.

This body should not necessarily be a state institution. For instance, it could be a non-profit association that would have to:

- work out a network in which all the HCPs are interconnected;
- work out business processes among these institutions;
- implement the business processes by electronic services and messages;
- produce a database containing stable relationships and indicating when there is a relationship between the patient and the HCP, where and which kind of data are available;
- give access to the authentic sources of capacities and mandates (databases outside of this system – thus: no central storage of personal health information);
- cooperate with a sectoral committee that will implement authorizations for data access within the system and check whether the actual data exchange conform to the rules.

In the described system, where the described guarantees are available, the sanctions may also be very high (e.g. three months service suspension and then loss of license for institutions perpetrating the rules). Thus, the risk of abuse will be diminished.

It is based on the principle of four or six eyes (it is not possible that one person does something without being controlled by another one) – there should always be an external trusted third party with a real overseeing power.

How far are we currently from that scenario?

Mr. Robben believes that the described proposal is continuously gaining support; there is already a first proposal of a law that describes components of such a system (*n.b. Mr. Robben refers to scenario 1*).

However, he underlines that this system will not work without the trust of the general public. Trust is gained by having the system managed by the people concerned, for instance in the management board of such an institution: health care providers, hospitals, medical doctors, sickness funds as representatives of patients etc.

The described system is 60-70% based on the social security sector, where it took 3-4 years to put into practice. At that moment, however, there was neither such a system nor the technical standards existing. Today, the existence of internet and a lot of standards in the field of identity management might enable a quicker implementation.

Again, the best way to get the trust in the system is to have it managed by the people concerned (representatives of the health care sector, patients-sickness funds). If they trust the system, it will be used. The best way to convince medical doctors and patients to use the system is to involve them in it.

What are the requirements for interoperability for the USERS / GOVERNMENTS / MERCHANTS?

(Mr. Robben believes that distinguishing among the three is not necessary at this point.)

In the area of interoperability, it is necessary to elaborate several levels of interoperability.

Conceptual interoperability

As far as conceptual interoperability is concerned, Mr. Robben pointed out the following issues: what is identity, what are capacities (sometimes integrated under identity), mandates, relationships, and what the interrelation of all these concepts is.

He noted that clarifying these issues is essential, because "if you don't speak the same language, you will not be able to implement an interoperable system".

Mr. Robben mentioned that he himself is active several different environments that work around ehealth, namely the Commission on Telematic Standards in Healthcare, which aims to create concrete algorithms to make the above-described system possible (*Mr. Robben refers to the above mentioned, more complex second scenario)*, the B-Health-platform (a number of people developing together a common platform that

can be used to exchange data), several informal groups (one of them works on the way a patient identification number will be derived from) and the Privacy Commission, where he had a first discussion about the described proposal.

He confirmed that all these environments agree on around 90% of the proposal. Thus, since they have the same kind of thoughts, it is only necessary to find common concepts and to reach an agreement.

In the attempt to gain trust, one should take the time factor into account. It is advisable to proceed gradually (e.g. start with data exchange on not so sensitive data) to gain trust.

Mr. Robben identified several priorities in clarifying the conceptual confusion that exists today:

First, identity or identities. He noted that Microsoft has developed a concept of redirection of identities. However, in theory, it is only possible to have a single identity (not multiple identities), while identifiers to identify a person in certain circumstances may be different. The authorization to get identifiers of a person is not only a decision of the citizen (such a system would not work).

Second, identities and roles. A single entity, e. g. a person, has different roles. There can be several identifiers for each of the roles, but for data exchange, a system with either a unique identifier or a system with conversion between multiple identifiers will be necessary.

Knowledge of the identity itself is only rarely sufficient – the context is almost always necessary. Decision to provide a citizen with an identity should not be up to him only.

Third, identity management. Mr. Robben prefers the term *"user and access management"* to identity management. To achieve interoperability, one needs to know who the users are and what they are entitled to do (capacities, mandates, roles, etc.).

Technical interoperability

Technical interoperability is not as complex as conceptual interoperability. There already exist several standards today.

International aspects

Of course, agreements on patient identification numbers will have to be made on the international level. Every country will in the long run have the same problems.

Advantages of interoperability on the international level, are on the one hand that when accessing data via this system becomes general practice (and not accessing it leads to liability of the HCP), this will lead to a better quality of health care and on the other hand the reuse of the data of the other HCPs will lead to financial savings.

What are the benefits of interoperability for each of these stakeholders?

Merchants

Mr. Robben pointed out that although officially, the analyzed sector is not commercial, the situation with hospitals is well-known.

He stated that the employers should not be able to access the sensitive medical data, but it is the sectoral committee that decides what is acceptable and what is not. For example, every medium and big employer has a contracted practitioner for work-related medical problems who will of course need access to some information.

Users

The benefits are clear for the patients. As far as the HCPs are concerned, the main benefit they will gain is the ability to deliver the best service.

Governments

The fact that data will become interchangeable should normally diminish their costs.

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

Technical and legal levels

Mr. Robben referred to his previous answers.

Cultural level

Mr. Robben pointed out that the underlying problem is that health care is not a positive science. Nobody will question whether high quality standards of health care service delivery should be strived for, or whether the patients should be treated well, etc.

However, there is a fear on the side of the HCPs, especially of liability issues. There is also a possibility of discrimination (if the data can be accessed by private companies, they could discriminate job applicants based on their medical record). Thus, in this area, it is also necessary to prevent interoperability in certain aspects.

What can be done at the TECHNOLOGICAL level to establish interoperability?

Mr. Robben referred to the current abundance of technical standards.

What can be done at the LEGAL/POLICY level to establish interoperability?

The role of the law is to provide the sanctions when the system is not working properly.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

The best system is based on a good organization, i.e. how it is put in place on an organizational level (elements described above, including sectoral committee, crossroads bank, etc.).

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

Mr. Robben stated that if he had to choose one of the factors as the most important one, it would certainly be the institutional level.

What should be the role of governments in addressing interoperability of IMS?

The main role of the governments should be to strive to implement the described model. Mr. Robben noted that as it is unlikely that the solution would come from the sector itself, it is up to the government to take the initiative to put together the actors, work out the general framework and to convince everyone of its merits.

In Belgium, the ideal scenario would incorporate a cooperation of the federal level and communities.

As far as the role of the Crossroads Bank for Social Security and FEDICT is concerned, Mr. Robben mentioned that some technological components that were developed at these institutions would be reused to help the system start up. However, neither of them should in his opinion cover contextual and content solutions in several sectors.

He suggested that the initiative could possibly come from the B-Health platform where the collaboration of the minister of social affairs with representatives of several communities and sickness funds is currently going on.

What should be the role of merchants and industry groups?

Mr. Robben admitted that these actors can help to work out solutions, but stressed his belief that for issues such as ehealth and egovernment, the system should not be drawn by people whose main goal is to generate profit. The system should be based on open standards and open specifications. He added that the industry should not be working out the concept, as it follows a private interest, but the system is in general public interest.

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

Mr. Robben highlighted the importance of public awareness (e.g. a patient should not be kept away from the information about his medical state, which allows him to get a second opinion from another doctor, etc).

Annexes:

I. F. ROBBEN, Modinis' presentation on the topic *"Identity Management in egovernment"*.

II. F. ROBBEN and J. DEPREST, *"E-government: the approach of the Belgian federal administration"*.

12.5 Report 5: Bernd Burkert, Germany ecommerce

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer: Dr. Martin Meints
Independent Centre for Privacy Privacy Protection (ICPP)
Tel.: +49 431 988-1226, Email: LD102@datenschutzzentrum.de
Interviewee: **Bernd Burkert, Project Manager Hessen Corporate Network 2004 (HCN 2004)**
Hessische Zentrale für Datenverarbeitung, Mainzer Str. 29, 65185 Wiesbaden, Germany, Web: http://www.hzd.de
Location: Wiesbaden, Germany
Date: 18th of August 2005

Background Information:

Mr. Burkert joined the "Hessische Zentrale für Datenverarbeitung" in 2003. He was since then project manager for the project "HCN 2004". Mr. Burkert has a strong technical background as project manager for ICT projects as well in the private as in the public sector.

The project "HCN 2004" is one of four elements of the so called "egovernment Masterplan"[32] of the Federal Land of Hessen. Target of this "Masterplan" is the implementation of all necessary instruments for successful e-government for the 90,000 users within the public administration in Hessen by the end of 2008. This project includes the implementation of central directory services, central e-mail services and PKI (public key infrastructure) for the public administration. Currently it is strictly focused on the central needs of the public authorities in Hessen. Interoperability of directory services and PKI are currently no central issue of the project. Nevertheless interoperability in a later phase of the project will gain increasing importance.

First step of the project "HCN 2004" is the integration of the various existing active directory implementations and the implementation of a so called meta-directory. Basing on this structure the e-mail service currently is available for 10,000 users[33]. In a further step each user will get the necessary equipment (signature card, type III card reader, software) and qualification to use an advanced electronic signature according to the German Signature Act (Signaturgesetz). The implementation of a qualified electronic signature is planned in a later project phase after 2008. The technical systems and the corresponding infrastructure is planned to be according to the standards concerning PKI established and checked by the German Federal Office for

[32] See http://www.hessen-egovernment.de/mm/Masterplan.pdf; current version: 1.3
[33] Burkert, B., Einsele, J., *HCN 2004: Neue E-Mail Technik im Detail*, Inform (2) 2005, pp. 14-16. Download available via http://www.hzd.de/internethzd/broker?uMen=a30509a9-004a-aafc-76d9-4549a562af49

Information Security (BSI). This ensures the integration in the public and commercial PKI in Germany in a later project phase.

The project currently is partially in an advanced conception phase and partially in the implementation phase. The basic concepts for the directory services are finished, implementation has been started. For PKI the basic concept is finished; currently various APIs (application programming interfaces) towards additional applications are being tested; pilot implementations for more than 100 users are available.

Questions:

What are the main identity management issues in the chosen field of analysis e-government?

Mr. Burkert explained that account management (type 1 identity management) basing on directory services (in this case active directory and DirX by Siemens as meta-directory) for the employees of the Federal Land of Hessen is the central identity management platform within the project "HCN 2004". These directory services are the platform for the internal PKI implementation as well. Compared to today's situation further integration of areas of application and the improvement of the security are targets of this project. This includes

- Improvement of security for the use of account management in general, e.g. login at local computers
- Integration of access control for rooms and buildings with special requirements concerning security
- Electronic payment at least for the employees within the public sector
- Electronic signatures

How critical is the issue of interoperability of IMS for this field?

Concerning interoperability the project is focused on

- Interoperability within the public sector of the Federal Land of Hessen
- Interoperability between the different administrative procedures and the participants which have to take part in those procedures.

This creates the need of interoperability to the public PKI implementations in Germany, which causes quite high technical requirements if qualified signatures are planned to be used.

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?

From the perspective of Mr. Burkert as a technical expert a main focus of interoperability is technical compatibility to external signature procedures, technical components such as card readers and card types and applications used there. Concerning directory services, X.500-based interfaces and certificates basing on X.509v3 are important solutions. Concerning the integration of PKI into applications

the first draft of the SigBüAPI[34] is of high relevance for the project "HCN 2004". This API currently has a national (German) focus.
Further development of national and international standards and technical solutions using them could improve compatibility (and thus interoperability) in the area of directory services and connected additional services such as PKI a lot.

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

From the perspective of this project a worldwide compatible directory service and many connectable applications and services are a far reaching future vision.

How far are we currently from that scenario?

In the area of directory services LDAP is an important standards which is a good platform for interoperability on the level of directory services. But concerning the connectivity of PKI with directory services and the integration of PKI into other application main standards are missing.

What are the requirements for interoperability for the USERS?

From the perspective of the user (in this context employees of the Federal Land of Hessen) convenience is a central issue. The user wants to use only one chip card and only one PIN for as many authentication procedures and applications as possible. Technical problems and the requirements of (multilateral) IT security or data protection are not a central issue of the users. This is a result of the pilot project in Hessen and matches with the results of other pilot projects in Germany.

What are the requirements for interoperability for the GOVERNMENTS?

A central requirement from the perspective of public authorities is the (mainly organisational) standardisation of administrative procedures to make them interoperable. A main motivation to do that is the reduction of administrative costs.

What are the requirements for interoperability for the MERCHANTS?

In this context merchants are understood as the private sector in general. For the private sector connectivity to the administrative procedures of the Federal Land of Hessen are central issue of interest. A basic requirement for that is the interoperability of the existing PKI implementations at least in Germany. An example for a cross-

[34] Application programming interface issued by the German Signature-Alliance (Signaturbündnis); see http://www.signaturbuendnis.de/; currently no public information on the specifications of this API seems to be available.

sector application using different PKI implementations is an internet platform for electronic procurement.

What are the benefits of interoperability for each of these stakeholders?

In the concept for the current phase of the project the convenience aspect for the user is a major topic – this matches well with their expressed interests.
For the public administration improvement of IT security and standardisation of central administrative procedures are a main benefit. The reduction of costs is expected in a later phase of the project.
Benefit for the citizen and private sector is no central topic of the current project phase, so no benefit can be expected soon.

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

Technical

A lack of national and international standards especially for the integration of PKI and directory services and the integration of PKI and various applications is hindering the establishment of interoperability.

Legal

From the legal perspective the technical implementation of requirements stated in law are still a matter of debate. In this project it is still open if a specific technical implementation is sufficient for the requirements for an advanced electronic signature or not.

Cultural

From the perspective of the users the fear to be logged and tracked in their every day's work is a major aspect. According to existing data protection legislation in Germany this clearly would be illegal.
In addition usability of user interfaces is very important to reach interoperability on the cultural level.

What can be done at the TECHNOLOGICAL level to establish interoperability?

Standardisation in the described areas will improve interoperability on the technological level.

What can be done at the LEGAL/POLICY level to establish interoperability?

In this area further technical comments on the current legislation on electronic signatures could improve the situation.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

To overcome the fear to be logged and tracked, transparency of logging-procedures and independent checks carried out e.g. by the data protection commissioners can improve the situation.
Concerning the user interfaces development, practical testing with pilot users and good user documentation could be used to improve interoperability

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

Mr. Burkert made the ranking as follows:

1. Legal/political
2. Technological
3. Cultural/institutional

From his (technical and project-related) perspective the legal and political requirements and targets are essential for the implementation of identity management systems including aspects of interoperability. Technical standards are the next step; they establish the platform for the technical development of applications. Optimisation and social/cultural integration of these applications is the final step.

What should be the role of governments in addressing interoperability of IMS?

The role of the government is to create the necessary legal and to promote the technological platforms (such as standards). Another aspect is transparency of the resulting technical implementation of the administrative procedures and independent checks concerning IT-security and data protection.

What should be the role of merchants and industry groups?

The private sector can essentially promote technological platforms and good technological implementations. Transparency and independent checks are important in this sector as well.

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

Important factors for the success of interoperable systems are informed users taking an active role in the development and implementation of the technical solutions. Thus active information and stimulation of active participation are important actions.

Any other comments?

None.

12.6 Report 6: Bettina Neke, Germany, ehealth and egovernment

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer:	Dr. Martin Meints Independent Centre for Privacy Privacy Protection (ICPP) Tel.: +49 431 988-1226, Email: LD102@datenschutzzentrum.de
Interviewee:	**Bettina Neke, political co-ordination within the project "Gesundheitskarte Schleswig-Holstein"** **Ministry of Social Affairs Schleswig-Holstein**, Kiel, Germany, Web: http://www.schleswig-holstein.de/[35]
Location:	Kiel, Germany
Date:	23rd of August 2005

Background Information:

Coordinated by the Federal Ministry of Social Affairs and Health the introduction of an e-health card[36] in Germany is planned for 2006. In eight so called "Modellregionen"[37] pilot implementations and prototypes of the e-health card are being tested. The project of the "Modellregion" in the Federal Land of Schleswig-Holstein is called "Gesundheitskarte Schleswig-Holstein"[38]. This project is supported by the Ministry of Social Affairs Schleswig-Holstein.

Mrs. Neke works as officer in the Ministry of Social Affairs Schleswig-Holstein. Within the Ministry she is co-ordinating all political activities concerning this project.[39] She has a professional background as lawyer.

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

- Identification of a patient as insurant of the public health system at the office of a medical doctor or in hospital (today already supported by a chipcard)

[35] Complete Link: http://landesregierung.schleswig-holstein.de/coremedia/generator/Kategorien/Ministerien/MSGF/Aktuelles/Aktuelles__Treffer.html?NavSit=Soziales,%20Gesundheit,%20Familie,%20Jugend%20und%20Senioren
[36] See http://www.staat-modern.de/Buerokratieabbau/Projekte-im-Ueberblick-,11922.553645/Elektronische-Gesundheitskarte.htm?global.back=/Buerokratieabbau/-%2c11922%2c3/Projekte-im-Ueberblick.htm%3flink%3dsmo_liste%26link.orderby%3ddatum%26link.orderdir%3ddesc
[37] See http://www.telematik-modellregionen.de/content/index_ger.html
[38] See http://www.gesundheitskarte-sh.de/
[39] Changes in the structure of the project that took place in November 2005 are not taken into account.

- Transfer of information which is stored on paper today such as allergy data, permanent medications, blood type and immunisation certificates if needed by the medical doctor
- Referral to other medical doctors
- Prescriptions and purchase of medicine at a pharmacy

Access to emergency data currently is not possible even in cases when they are needed by a medical professional. The introduction of emergency data on the e-health card is a functional enhancement compared to the situation in Germany today.

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

An abstracted view on the data stored on the e-health card is shown in Figure 1. In addition to the storage on the card in some cases the data are stored in a post box on a central server. This post box essentially is a transfer directory from which the data can be received and processed by the corresponding recipients (e.g. medical doctors or pharmacists). The concept to store information concerning organ donation and maternity for a longer period is not finally decided yet.

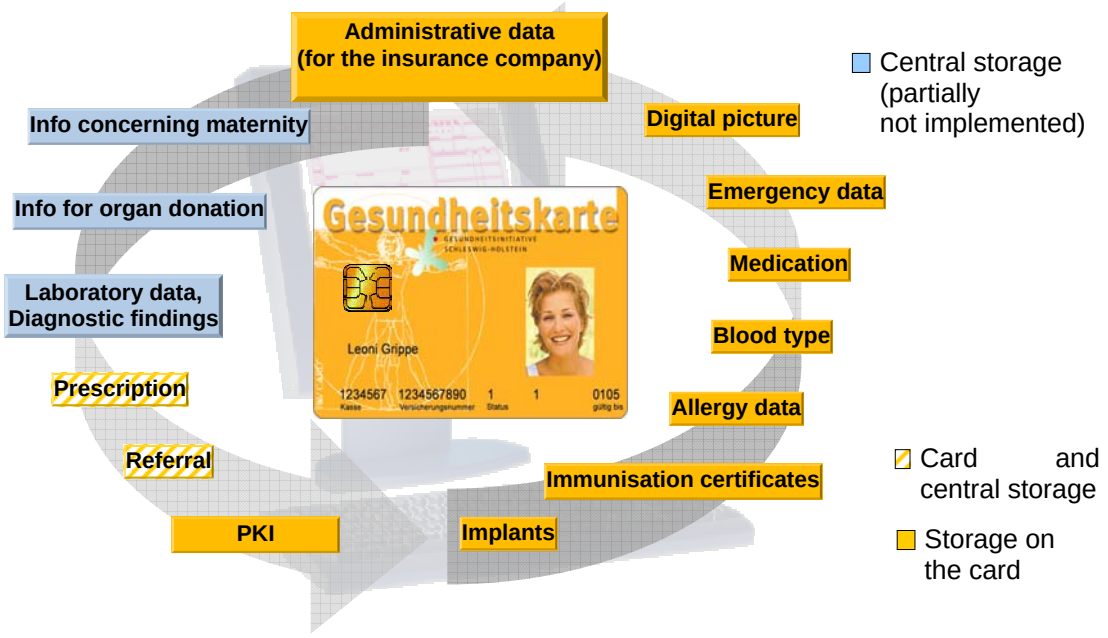


Figure 1: Concept of the storage of data in the German e-health card

Currently more than 1,000 e-health cards are issued within the pilot project. Numerous medical doctors organised in the "Gesundheitsnetzwerk Flensburg", numerous pharmacies, two hospitals in Flensburg and a number of partners from

industry are integrated into this project. The server structure and a secured network for data transfer purposes is available, together with PKI infrastructure and interfaces for a number of software systems used by medical doctors, pharmacies, and hospitals. In addition the pilot phase is observed by the privacy commissioner of the Federal Land of Schleswig-Holstein.

Questions:

What are the main identity management issues in the chosen field of analysis e-government?

Mrs. Neke did not observe the use of the term "identity management" or "identity management system" in the area of e-health due to her non-technical perspective. Establishing telematics in the area of health is a long term strategy in which the "Gesundheitskarte" is one element only.
An important aspect of identity management within telematics is the reliable identification of a patient as an insurant within the public health insurance system in Germany. Other important aspects of identity management are secured and reliable communication among care providers such as medical doctors, pharmacists etc. and between care providers and patients.

How critical is the issue of interoperability of IMS for this field?

According to Mrs. Neke highly critical – reliable identification is a major issue within this project for communicational and economic security. The (proven) identity of care providers together with their liability (e.g. for diagnosis, prescriptions etc.) are important as well..

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?

Compatibility of software used by medical doctors, in pharmacies and in hospitals is an important issue towards interoperability. Main tasks were in the past and will be in future common interfaces, gateways, and standardisation. In contrast to the situation concerning technical solution operational procedures in the public health system in Germany are standardised in general. The development of new procedures is not a topic within this project.
Central topic is identification in among the systems of care providers as described above. An additional important aspect is the introduction of a new system for social security numbers in Germany, which have to unique and valid for the lifetime of a patient.
Interoperability can mainly be enabled by technical measures such as the described development of standards, interfaces, and gateways.

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

In addition to the described care providers additional academic and non-academic care providers such as psychologists, physiotherapists and speech therapists should be integrated into electronic support of the operational procedures.

How far are we currently from that scenario?

The standardisation for additional electronic cards for the described care providers currently is running, the development of interfaces for the corresponding software systems used by those care providers will be the next step. For medical doctors, pharmacists and hospitals the cards are standardised and only a few minor technical problems concerning the implementation of interfaces are left.

What are the requirements for interoperability for the USERS?

Users in this context are understood as patients and care providers. General requirement are
(1) operative speed of the solutions,
(2) low costs,
(3) reliability and
(4) integration into established operational procedures.

What are the requirements for interoperability for the GOVERNMENTS?

In addition to the requirements listed in answer 6 the support of the knowledge and the sovereignty for patients is a requirement for interoperability. Consequently the technical solution of the e-health cards gives control about patient data to the patient himself/herself and makes him/her able to access medical information concerning his/her health.

What are the requirements for interoperability for the MERCHANTS?

In this context especially pharmacists and the health care industry are concerned. Main requirement from their point of view is the introduction of open standards to counter monopolistic structures of single players or industries in the health market. Within this project this is supported by the government as well to avoid a situation where monopolists are in a position to hinder general modernisations within the health sector.

What are the benefits of interoperability for each of these stakeholders?

Medical Doctors

Especially optimisation of communication and documentation within patient records are a major benefit.

Patients

For patients the introduction especially of emergency data, immunisation data and medications is improved functionality compared to today's procedures. And additional aspects are the avoidance of annoying or even dangerous double examinations and better structured therapies.

Pharmacists

Pharmacists can do better consulting concerning medication that does not need any prescription using emergency and medication data on the e-health card.

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

Technical

See answer 3, first section.

Legal

In this area necessary requirements are met in general.

Cultural

In the economic sector proprietary solutions with the target to establish a monopoly and the interests of special groups in the sector of health are hindering factors. A factor discussed especially in politics is the negative vision of the "glass patient", with personal and sensitive data being transparent e.g. for employers.

What can be done at the TECHNOLOGICAL level to establish interoperability?

The development of standards and open platforms can be done.

What can be done at the LEGAL/POLICY level to establish interoperability?

Politics can provide support for technologic standardisation.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

In this area open communication can improve the situation. To integrate a patient hot-line and interviews are part of the project. In this project central information including technological details is public[38].

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

Politics, society and institutions (understood in this case as organisations within the health sector) are important in the same way and at first place in the ranking. The reasons are the many interactions and interdependencies among them to get consensus on the requirements for the project in general. Technology comes next, mainly with implementation tasks.

What should be the role of governments in addressing interoperability of IMS?

The main role of the government is moderation of processes within the project and promotion of consensus among the actors.

What should be the role of merchants and industry groups?

A major role is open communication and co-operation together with the elaboration of standards.

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

An important role is the informed testing and use of the e-health card and user feed-back.
Care providers bring in their competencies towards processes and IT systems and give feed-back especially in working groups and sub-projects.

Any other comments?

None.

12.7 Report 7: Hannes Federrath, Germany, ecommerce

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer: Andreas Westfeld
Technische Universität Dresden
Tel. +49/351/463-37918, E-mail westfeld@inf.tu-dresden.de
Interviewee: **Prof. Dr. Hannes Federrath,**
Lehrstuhl Management der Informationssicherheit, Universität Regensburg, Universitätsstraße 31, D-93053 Regensburg
Tel. +49/941/943-2870, Fax +49/941/943-2888,
E-mail hannes.federrath@wiwi.uni-regensburg.de
Location: Regensburg, Germany
Date: 05.07.2005

Background Information:
Prof. Hannes Federrath is a full professor for management of information security at University Regensburg. His research interests are security and privacy in communication networks, development of systems that provide anonymity and unobservability, location management strategies considering privacy in mobile communication systems, cryptography, steganography and data security [1]. He is the leader of the project AN.ON/JAP, Anonymity Online, which enables users to surf the Internet anonymously and unobservably [2].

Questions:

What are the main identity management issues in the chosen field of analysis ecommerce?
Prof. Federrath has two views on identity management. On the one hand there are the familiar systems like Liberty Alliance (www.projectliberty.org) and Microsoft .net Passport (www.passport.net), login string and passwords, and Single-Sign-On. On the other hand there is identity management in the face of particular business partners as utilisation of pseudonyms according to the own privacy requirements.
There are two main issues in the field of ecommerce:
- The identification has to be secure (where it is necessary) and
- privacy has to be protected (where it is possible).

How critical is the issue of interoperability of IMS for this field?
The issue of interoperability of IMS is as critical as the interoperability of the underlying services.

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?
An interoperable IMS is at least so broadly usable as the service for which it is needed.

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

There are still no interoperable IMS, if so then only in isolated applications. Otherwise it should fulfil the already mentioned conditions to be at least as broadly usable as the service for which the IMS is needed.

How far are we currently from that scenario?

Very far. (see Question 4)

What are the requirements for interoperability for the USERS?

For the users, an IMS should be easy to use and free of charge. IMS should guarantee privacy (no passing on of personal data etc.).

What are the requirements for interoperability for the GOVERNMENTS?

To prevent lawsuites it is most necessary to have secure identification and a clear balance of power between all parties (in the sense of multilateral security [3]).

What are the requirements for interoperability for the MERCHANTS?

In addition to the requirements of the government (see Question 7), the merchants need financial security, i. e. the creditworthiness of the customers has to be ensured.

What are the benefits of interoperability for each of these stakeholders?

Citizens

Their privacy protection becomes easier.

Governments and Merchants

More evaluated, standardised secure clearing and settlement.

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

(see Questions 11–13)

What can be done at the TECHNOLOGICAL level to establish interoperability?

The most important goal should be to establish standards. The industry's displeasure to establish standards is one of the main obstacles for interoperability. We should try to overcome this displeasure.

What can be done at the LEGAL/POLICY level to establish interoperability?

At this level, incentives to establish standards should be created.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

Nothing.

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

The technological factor is most deciding.

What should be the role of governments in addressing interoperability of IMS?

The governments should offer funding for such projects to foster them as an alternative to the credit card number. And they should give the citizens information about IMS, the advantages against previous systems and the value of privacy.

What should be the role of merchants and industry groups?

They should support as many systems as possible. There will be probably several different IMS at the same time, also in future. It is the same as with credit cards at the moment: merchants support Mastercard, Visa, Amex etc. at the same time and there is no trend that this diversity will disappear.

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

No.

Any other comments?

Prof. Federrath stated that these questions are a bit unspecific and that perhaps the questions should be splitted in questions where on the one hand current applications are considered and on the other hand applications that scientists can imagine or invent.

References

[1] Personen am Lehrstuhl Management der Informationssicherheit, 2005, http://www-sec.uni-regensburg.de/federrath/
[2] Project AN.ON/JAP, Anonymity Online, 2005, http://www.anon-online.de/
[3] Günter Müller, Kai Rannenberg (eds.) Multilateral Security in Communications, Addison-Wesley, München, Reading, Massachusetts, 1999

12.8 Report 8: Gerhard Weck, Germany, ecommerce

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer: Andreas Westfeld
Technische Universität Dresden
Tel. +49/351/463-37918, E-mail westfeld@inf.tu-dresden.de
Interviewee: **Dr. Gerhard Weck, Leiter IT-Sicherheit der INFODAS Gesellschaft für Systementwicklung und Informationsverarbeitung mbH,**
Rhonestraße 2, D-50765 Köln, Germany, Web: http://www.infodas.de,
Tel. +49/221/709120, E-mail g.weck@infodas.de
Location: Cologne, Germany
Date: 06.07.2005

Background Information:

Dr. Gerhard Weck is a licenced IT Baseline Protection Auditor and Chief IT Security Officer at INFODAS. His working focus is security of operating and information systems and the development of the IT security database at INFODAS. He is IT security lecturer at the Ulm Academy for Data Protection and IT Security (Ulmer Akademie für Datenschutz und IT-Sicherheit, www.udis.de) and spokesman of the DECUS professional group for security (www.decus.de). [1]

Questions:

What are the main identity management issues in the chosen field of analysis ecommerce?

In this field, Identity Management Systems (IMS) bind a network specific identity to my person. The validity of this binding is or can be restricted to single applications. Usually, an IMS offers a string of one's choice and a password. The main issue is accountability.

How critical is the issue of interoperability of IMS for this field?

There are only isolated applications at the moment. Consequently the interoperability of IMS is relatively uncritical for ecommerce. The more these isolated applications grow together, the more critical the issue of interoperability will be.

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?

An interoperable IMS enables the user to apply an identity used with one application also to another application. Such systems have compatible authentications mechanisms, that are a prerequisite for interoperability.

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

An interoperable system would be based on certificates. The user has a carrier (e. g., a chipcard medium) on which the certificate is stored according to specific standards.

How far are we currently from that scenario?

Existing standards are incomplete or imprecise. For instance, X.509 describes the structure of certificates. However, the specification of attributes is not sufficiently detailed. So it is possible, that these attributes cannot be recalled because the freedom let by the standard was interpreted in a different way.

What are the requirements for interoperability for the USERS?

Users have the same requirements for interoperability as the merchants (cf. question 8). In addition, it should be possible to construct identities as pseudonyms. The identity of the merchant should be backed (possibly the merchant acts also anonymously).

What are the requirements for interoperability for the GOVERNMENTS?

Governments act possibly as trusted third party which results in certain requirements.

What are the requirements for interoperability for the MERCHANTS?

IMS have to guarantee accountability. It has to be ensured that it is a real identity and no fake. Another requirement is secured communication so that for instance the State cannot eavesdrop on it.

What are the benefits of interoperability for each of these stakeholders?

For all stakeholders, the reliability and trustworthiness is increased and ecommerce is strengthened.

Citizens

It is comfortable, the user does not have to move himself or herself to “go” shopping.

Governments

(Indirectly:) It stimulates the economy.

Merchants

It decreases costs.

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

Technical

The lack of knowledge – one is unable to recognise where interoperability is missing. On the other hand there are targeted attempts to let interoperability fail (hoping for an advantage in competition).

Legal

Particular countries try to push through their solution.

Cultural

People are used to established structures and are tied to existing infrastructures.

What can be done at the TECHNOLOGICAL level to establish interoperability?

Standardisation has to be expedited.

What can be done at the LEGAL/POLICY level to establish interoperability?

Recommendations or also regulations to utilise specific standards could be issued to accomplish interoperability, but also funding will support it.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

Put increased pressure on manufacturers to implement standards precisely. (For example, Microsoft frequently implemented standards, but then they had a snag to it, i. e. they had proprietary properties to make the interoperability with competitor's products fail.)

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

Dr. Weck believes that the technological level is the most important, then the legal/policy level follows and finally the cultural/institutional.

What should be the role of governments in addressing interoperability of IMS?

The governments should offer funding, information, and should establish pilot projects to spread standards.

What should be the role of merchants and industry groups?

They have to be the driving force to spread the technology, because they earn the money and will negotiate the investments.

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

At this level, better information is necessary. Consumers should be more self-confident in postulating interoperability.

Any other comments?

n/a

References

[1] Frank Reiländer, Gerhard Weck: Datenschutzaudit nach IT-Grundschutz – Konvergenz zweier Welten. Datenschutz und Datensicherheit 27 (2003)http://www.infodas.de/download/DuD_11-2003.pdf

12.9 Report 9: Bettina Müller, Germany, ehealth

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer: Andreas Westfeld
Technische Universität Dresden
Tel. +49/351/463-37918, E-mail westfeld@inf.tu-dresden.de
Interviewee: **Dr. Bettina Müller, Senior Consultant**

Location: Germany
Date: 02.08.2005

Background Information:
Dr. Bettina Müller is specialist in neurology and specialist in psychiatry and psychotherapy. Since fifteen years she is senior consultant and for more than ten years head of a neurological department. She is an expert in IT security for the medical area of application at the Gesellschaft für Informatik (GI, http://www.gi-ev.de).

Questions:

What are the main identity management issues in the chosen field of analysis ehealth?
Most important is the data protection, including availability of the service and protection against unauthorised access. In particular, a role-based access control should be used. If physicians have a "Professional Card" as an occupational pass in the future, then it has to be distinguished whether they heal a patient and need access to his or her data for this reason, or they are working for an insurance, that could use the anamnesis to discriminate its clientèle.

How critical is the issue of interoperability of IMS for this field?
There is still no interoperable "Professional Card." Maybe large hospitals have an internal system (e. g., SAP). In the long term the issue of interoperability of IMS will become critical. The bar for the IMS should not be raised to a level at which its saving effect falls flat.

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?
An IMS binds an identity in the network to a person and its role and offers pseudonymous access if applicable. An interoperable IMS provides a general standard interface, which has to be usable. Furthermore, particular service providers can define their specific roles and dependent subtasks. (For instance, only a head of department may use, create and sign specific data.)

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

The users had a data medium (e. g., Professional Card) which is used to check the role regarding data and grant or deny access. In case the cards are also valid outside the own house, an import function for roles and a house internal trust center is needed.

How far are we currently from that scenario?

Very far. In doubt, third-party (proprietor, liveware) can see all data without informing the data owner.

What are the requirements for interoperability for the USERS?

There should be a *uniform* medium (e. g., Professional Card). Its architecture should guarantee confidentiality and also legal certainty by an evidential certified signature option.

What are the requirements for interoperability for the GOVERNMENTS?

The system has to ensure the compliance of the necessary authorisations (keep charlatans away). It has to implement the requirements of the data protection act: Who is allowed to ascertain health data and which details? (When should be anonymised, when cumulative data is sufficient?) Cancer registries still contain identities, although this is needed only for infectious diseases. Also cases of borreliosis (Lyme disease) are still ascertained by name for epidemiological purposes. The attending physician *has to* provide this data by law (Sächsiches Infektionsschutzgesetz [Saxon Infectious Diseases Protection Act], but also federal law, Sächsisches Krebsregistergesetz [Saxon Cancer Registration Act] – doctor-patient confidentiality conflicting with official requirements).
The privatisation of social security systems calls for a better protection of patient data. Today, life insurances already ascertain “voluntary” information about health. There are copyright objections, since physicians are the originators of this data. The data may not be used without their consent.

What are the requirements for interoperability for the SUPPLIERS?

The IMS has to guarantee accountability and privacy, e. g. to what extent data in the case history may be used. Further requirements result from split payment. For instance, peripheral hospitals could outsource their radiological diagnostics, make external radiographs and assess them together with external experts without their physical presence.

What are the benefits of interoperability for each of these stakeholders?

Citizens

It saves errands. It becomes easier for patients to see the doctor (they don’t have to pick up pictures and lab results everywhere [and pharmacy is only one mouse click away – AWe]).

Governments

It saves time in the first place; medical personnel are disburdened from time-consuming administration tasks. The risk of misuse decreases.

Suppliers

Interoperable IMS decrease the complexity of the processes or electronic means guide through complex structures. The services of the supplier become more easily reachable. The suppliers can protect their clientèle, if the clients get faster the necessary information from their services.

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

Technical

There is a lack of infrastructure at the technical level (e. g., trust centers).

Legal

At the economic level, the fear of simplified change of the supplier and increased turnover (fluctuation) of customers hinder the establishment of interoperable solutions. This can easily lead to a monopoly of large suppliers.

Cultural

From the cultural point of view the therapeutic relation is lost. There is a tendency to reduce it to an electronic relation to an anonymous swarm of physicians, therapists, etc.

What can be done at the TECHNOLOGICAL level to establish interoperability?

Standards and uniform interfaces should be defined at the technological level.

What can be done at the LEGAL/POLICY level to establish interoperability?

A legal framework/general conditions for the definition of clear technical standards should be created, responsibilities assigned, and independent, certified trust centers should be fostered.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

Not much, it will shape up well. Perhaps we should have a dialogue between the different systems of data protection about terms like *informational self-determination*. There are differences between the Anglo-American and the German system. There is a rather restrictive passing on of data in Germany, and not all data that stimulate the economy may be ascertained. For instance, it is compliant to the data protection act in England, to randomise data (i. e., to take a random sample for further processing – AWe) and ask for consent for the randomised data only (ask only the people contained in the random sample – AWe).
(Reference: Declaration of Helsinki [http://www.wma.net/e/policy/pdf/17c.pdf]:
20. The subjects must be volunteers and informed participants in the research project.)

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

Most important is the legal/policy factor before the technological. It is technically feasible for a long time, what is needed here. Money has to be invested now, so that

the technology does not lie dormant. I attach the least value to the cultural/institutional factor; it will develop itself.

What should be the role of governments in addressing interoperability of IMS?

They should charge their sub-organisations with the definition of standards and, above all, ensure that companies that implement these standards do not back the wrong horse (protection of investment). They have to stop the proprietary developments of health insurances, associations, and industries.

What should be the role of merchants and industry groups?

They should state what they offer. For instance: We can do a benchmark (an official comparison of quality), without revealing patient data; patients can determine the rate of complications and see, who made the most surgeries, who makes it safe.

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

The users should be sensitised how to handle their data in a way that governments/insurances don't get their hands on it unnecessarily; users should be sensitised to be aware of their responsibility as authors and originators of the data (physicians, therapists etc.) resp. to exercise their *right to authorise every single access to their data*[40] (patients).

Any other comments?

Please do not directly reference Dr. Müller's employer.

[40] in German: Datenhoheit

12.10 Report 10: Rüdiger Dierstein, Germany, ehealth

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer: Andreas Westfeld
Technische Universität Dresden
Tel. +49/351/463-37918, E-mail westfeld@inf.tu-dresden.de
Interviewee: Rüdiger Dierstein, S. M., Weichselbaum 13, D-82234 Weßling, Germany, Tel. +49/8153/952363, E-mail r.dierstein@in.tum.de
Location: Dresden, Germany
Date: 10.08.2005

Background Information:

Rüdiger Dierstein studied mathematics and physics at the University Stuttgart and space technology at the MIT in Cambridge MA, USA. He is founder member and honorary member of the Gesellschaft für Datenschutz und Datensicherung (GDD, German Society for Data Protection and Data Security) [1], member and fellow of the of the Gesellschaft für Informatik (GI, German Society for Informatics) [2], spokesman of the executive board IT security of the GI for several years, and lecturer for IT security at the Technische Universität München since 1972.

Questions:

What are the main identity management issues in the chosen field of analysis ehealth?

- A user (e. g., the doctor in attendence in Germany) should understand the characters (data) that are accessible to him in the same way the producer (e. g., a specialist in Spain) has meant them. It is important that the representation of information at the producer side is not only correct, but will also be correctly interpreted (geographically independent etc.) or at least can be correctly interpreted.
- As far as possible, the identity has to be reconstructible independently of the environment and perception. The Munich cabaret artist and comedian Karl Valentin hits the point with his character "bookbinder Wanninger." Wanninger is more and more desparately trying to leave his message regarding finished books at the building firm Meissner. He is passed on from contact to contact; in almost Kafkaesque manner he never reaches the responsible person and has to repeat his introduction (= statement and claim of his identity) with increasing disintegration of speech over and over again: "Ich habs jetzt dene andern alle schon *so oft* gesagt. Ich bin der Buchbinder Wanninger, …" (I already said it to all the other people so many times. I'm the bookbinder Wanninger …).
- It has to record the essential, crucial attributes of the identity for a given environment and context. In Germany a code for diseases was proposed, where the disease is represented by a numeric code. However, there was no field for important background information like "acute," "cured," and "suspected." In case of emergency, a different doctor has to assume the worst case and cannot prescribe a helping medicine because of possible contraindication.

How critical is the issue of interoperability of IMS for this field?

Very critical, if hospital A wants to (or is supposed to) misinterpret documents from hospital B …
The issue of interoperability of IMS is critical, where doctors interact. Only for the family doctor, who is a general practitioner and does everything by himself and knows the patient since he or she was born, this issue could be uncritical.

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?

IMS determine whether two entities (objects or subjects) are still the same. IMS contain a mapping function that indicates, whether an entity is still authentic, i. e. unchanged and not manipulated, or whether the mapping between an object and its producer is still valid.
One has to distinguish structural authenticity (Is the structure of the object still what it is supposed to be?) and functional authenticity (Is the object still doing, what it is expected to do according to the requirements?).
Example 1: A signed program contains an error. A third party repairs it and modifies the program text (its structure). This destroys the signature, but establishes the required (expected) functionality. Which version is authentic?
Example 2: Is an executive still identical before and after his holidays, if
(a) he returns with full beard and bald-headed, or
(b) he was reversed by the adversarial intelligence service (or competitor)?

An IMS is interoperable if different specialists (medical instances) can use all possible means independent of location and time. Geographic independence would enable interoparability.

The doctor has to be able to interpret the data "correctly." His role assumes education, qualifying him to do so. It is difficult to establish a border between interoperable IMS for ehealth and interoperable health services. As soon as we depart from the pure structural concept of integrity, it gets nebulous.

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

See Question 3.

How far are we currently from that scenario?

We just tread this new path to interoperability. How far we are from interoperability depends on how demanding we set ourselves the target and on our concept of integrity.

What are the requirements for interoperability for the USERS?

The IMS should work geographically and application independent.

What are the requirements for interoperability for the GOVERNMENTS?

- It has to comply with the relevant standards.
- It has to guarantee the freedom of the users. "Man is created free, and is free, even though born in chains." (Der Mensch ist frei geschaffen, ist frei, und würd' er in Ketten geboren. [3]) "Contended slaves are the most acrimonious antagonists of

> freedom." (Glückliche Sklaven sind die erbittertsten Feinde der Freiheit. [4]) "God grant that not only the love of liberty but a thorough knowledge of the rights of man may pervade all the nations of the earth, so that a philosopher may set his foot anywhere on its surface and say: 'This is my country.' " [5]

What are the requirements for interoperability for the SUPPLIERS?

It has to be affordable, i. e., to sell well.

What are the benefits of interoperability for each of these stakeholders?

Citizens

Better service is offered to the users. Diagnoses are connected with less ways (and costs).

Governments

The state has financial problems with the health-care system and hopes for discharge [crediting?] and enhanced influence by standardisation.

Suppliers

They can earn money if they implement the user requirements for interoperability.

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

Technical

On the technical level, ambiguities in the semantic field is hindering the establishment of interoperability. Which search term should be used, e. g., if we look up a medicine: "ciclo*" or "Zyklo*" etc.? The understanding of people in natural language is based on non-syntactic, non-formal definitions.

Legal

Cultural differences are hindering the establishment of laws.

Cultural

There are different conceptions about what should be accomplished by an identity management system. The English don't have identity cards, and it is also difficult to enforce this legally.

What can be done at the TECHNOLOGICAL level to establish interoperability?

It should be researched in the semantic area, in computer sciences, in social sciences etc.

What can be done at the LEGAL/POLICY level to establish interoperability?

Laws may be enacted but much research in the psychological area is necessary and influence has to be exerted on the society.
Research groups should be set up for international discussion to deal with social and cultural differences.

Example: After World War II, the administration of the French zone of occupation in Germany tried to introduce identity cards with fingerprints (as common in France). However, this led to opposition in the populace: "Aha, we all are treated as criminals now." The introduction of these identity cards was waived.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

See Question 12.

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

All three factors are similarly significant. Especially the legal/policy and cultural/institutional factors are tightly coupled.

What should be the role of governments in addressing interoperability of IMS?

The governments should back and foster the points in 11 to 13. They should also support (here not differently than in general) research and the communication between the respective groups.

What should be the role of merchants and industry groups?

They should implement IMS as demanded by the governments and as required by the users.

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

Users should demand that identity management systems are implemented according to their requirements. The dependency of the patients on such a system should not be underestimated. Should governments minimise this dependency?

Any other comments?

n/a

References

[1] Gesellschaft für Datenschutz und Datensicherung e.V., http://www.gdd.de
[2] Gesellschaft für Informatik e. V., http://www.gi-ev.de/english
[3] Friedrich von Schiller in the "Words of Faith"
[4] Marie von Ebner-Eschenbach, Aphorism
[5] Benjamin Franklin, letter to David Hartley, Dec. 4, 1789

12.11 Report 19: Herbert Leitold, Austria, ecommerce

D4.2: Requirements for interoperability in IMS

*Semi-structured interviews with experts in IMS and Interoperability. This interview is analysing the Austrian Citizen Card and answers IMS interoperability questions in relation on **ecommerce**.*

Interviewer: Stephan Freh
London School of Economics
Tel.: +447906344477, Email: freh@gmx.at
Interviewee: **Dipl.-Ing. Herbert Leitold, Director Technology**
A-SIT, Zentrum für sichere Informationstechnologie - Austria
Inffeldgasse 16a, A-8010 Graz, Austria
Tel. +433168735521, Fax. +433168735598, Email: Herbert.Leitold@a-sit.at
Location: Vienna, Austria
Date: 13.07.2005

Background Information:
Mr. Herbert Leitold holds the position of Director Technology at A-SIT, Zentrum für sichere Informationstechnologie – Austria. A-SIT is a friendly society and it was founded by the Austrian Ministry of Finance, the Austrian National Reserve Bank and the Technical University Graz in 1999. Its mission is to undertake ICT research for the use of egovernment. In resent years A-SIT worked closely with the IKT-Board and the CIO of Office of the Austrian Federal Chancellor. Mr. Leitold is the author of several international recognized studies including topics on eVoting, eID Solutions and electronic signatures. Mr. Leitold is further an advisor to the Austrian Government on egovernment projects.

The probably most relevant paper for the FIDIS project Mr. Leitold co-authored is a survey on "EU's Electronic-ID Solutions" (Hayat *et al.* 2004). The survey's abstract: "Administrative processes in the public and the private sector are increasingly carried out electronically. For both e-Government and e-Commerce identification and authentication of the parties involved is needed. Several states have launched or are in the process of defining electronic identity (e-ID) solutions, such as citizen card projects. This document surveys e-ID projects of EU member states and gives an overview of pilot projects and standardization efforts."

Questions:

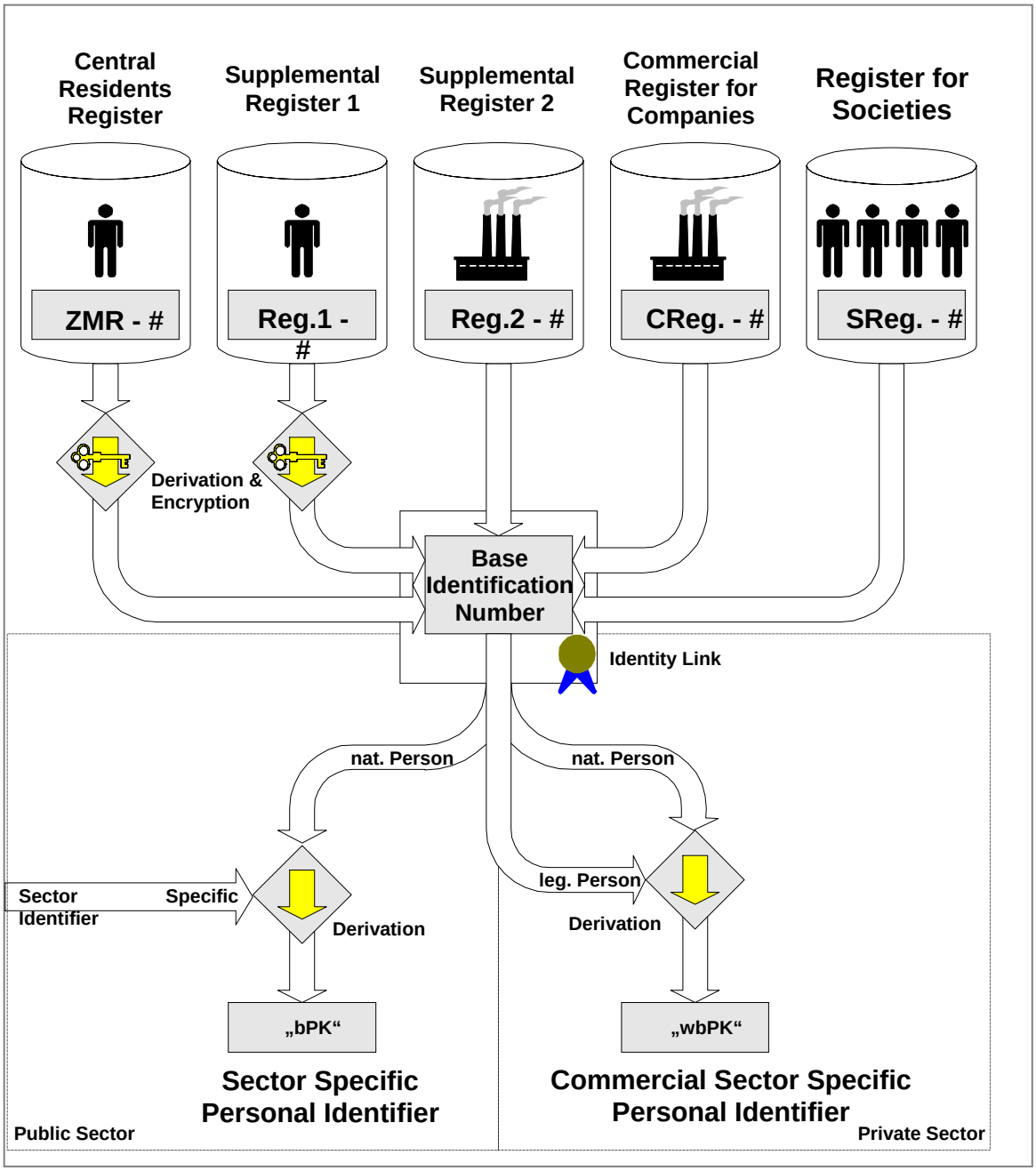
What are the main identity management issues in ecommerce?

Privacy and data protection Issues

Mr. Leitold explains that interoperability is a major issue in regards to IMS. Interoperability is often seen as a kind of counter player to privacy. However, it is the art of "egovernment application design" to find a solution with ensures high interoperability when necessary but at the same time guarantees a highly secured and privacy rich environment. Austria solved this challenge with the so called "Sector Specific Personal Identifier". This concept is defined in the Austrian egovernment Strategy. The Austrian egovernment Strategy defines how to use privacy enhanced data modelling solution, consisting of (Otter 2005b):

- ZMR: Citizen's Identification Number (supplied by „Residents Register")
- SZ: Base Identification Number (derived by strong encryption of ZMR, identifies each person registered in Austria uniquely)
- BKZ: Sector Specific Identifier (identifies different Applications of E-Government)
- bPK: Sector Specific Personal Identifier (cryptographic derivation out of „SZ & BKZ")

This data model assures that people can not be tracked by looking for one unique identifier in all data bases. It shall be noted that the Austrian eID solution called "Bürgerkarte" works with the same principle and the signatures of these two systems are fully interoperable.



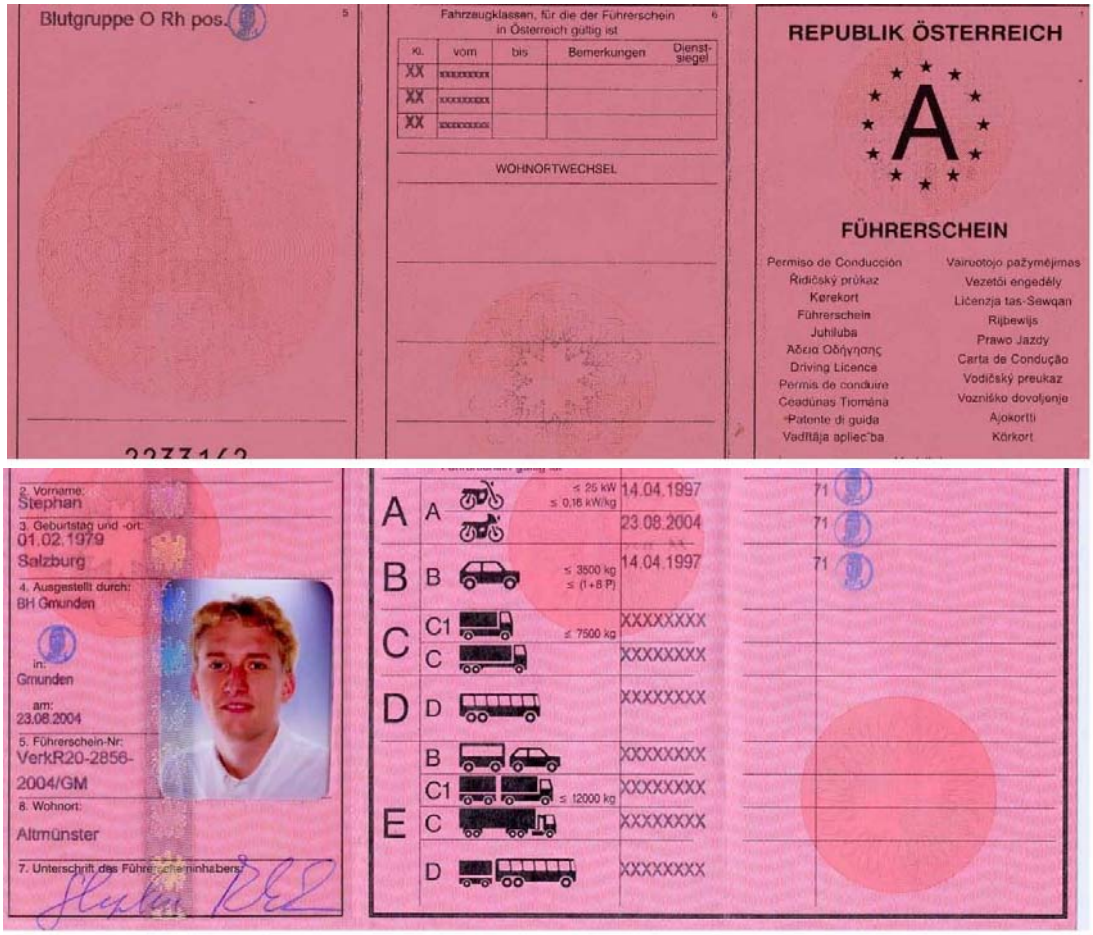
IMS in ecommerce versus egovernment

Mr. Leitold points out that egovernment IMS interoperability is usually a greater challenge then ecommerce IMS interoperability. This is mainly the case as egovernment applications involve more stakeholders and usually include more complicated work processes.

The Austrian Citizen Card was the first major electronic signature project in Austria. Before that several companies developed plans to offer electronic signatures put these plans became never realised.

Austrian law in relation to identification

Austrian law requires every citizen older than 14 years to carry a form of identification with him/her. However, this law is usually not enforced and most Austrians do only carry bank cards or driving licences with them for indemnification purpose. It shall be noted that the Austrian driving licence is still a paper document as seen below.



Austria also has a National ID Card (shown below) but this card is mandatory, costs 55 Euros and only a small proportion of Austria's population owns such a card.

Mr. Leitold describes that because of these legal and practical conditions the Austrian government wanted to have a solution with uses modern technologies can be used for egovernment as well as ecommerce and is highly interoperable. In addition to that the concept of the Austrian Citizen Card was designed as an open and technology independent solution.

How critical is the issue of interoperability of IMS for this field?

National versus EU-wide interoperability

Mr. Leitold described that national interoperability issues were discussed from the very beginning of the Austrian Citizen Card project. However, interoperability issues on the EU level became rather late a real point of discussion. Mr. Leitold adds that this is most likely the same in other countries, which of course is an obstacle when it comes to European interoperability issues.

Example: Austrian eID interoperable with Italian eID

Mr. Leitold explained that the Austrian Identity Card is fully interoperable with the Italian and Estonian eID. In order an Italian eID holder can use all eID supported egovernment services in Austria he/she would needs to register his/her Italian eID once at an Austrian authority. Austria then enters him in the ZMR for foreign people. From that moment on he/she can use his Italian eID.

Mr. Leithold remarks that at the moment there are no quality standards defined in Austria, which would state which national eID comply with Austria's quality standards and which one do not. Currently it is handled according to the motto "If the Italian eID is good (secure, etc.) enough for Italy it is also good enough for Austria."

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?

Interoperability is the technical connection between systems with the goal to exchange information – on a European level across borders. An interoperable ecommerce eID supported solution is able to work between technologically different systems. Interoperability is a major necessity that ultimately enables identification and authentication of IMS in ecommerce.

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

National level

Mr. Leitold tells that the concept of the Austrian Citizen Card entirely fulfils the interoperability requirements on a national level.

European level

However, on a European level there is still much to do as currently only Italy and Estonia have interoperable solutions with Austria. Finland and Belgium will soon be integrated. The goal should be to have a solution which is fully interoperable with all European national authentication and identification solutions.

He adds that it would be extremely important that all member countries pursue a national eID solution which is technologically independent and has an open hardware concept. For example countries should not define that their solution has to be based on a smart card or requiring specific technical installations at companies in order to use the concept. He further adds that over 90% of the European adults have a mobile phone. Therefore this is the most widely used technology and smart card chips in mobile phones could easily be used for authentication and identification applications (the Austrian Citizen Card uses mobile phone chips already).

How far are we currently from that scenario?

Mr. Leitold very clearly answers that the EU is still extremely far away from a European wide interoperable eID solution. European countries usually develop their national solutions

without thinking in European terms first and only at a later stage think about European collaboration. – This was the same in Austria.

Apart from some EU projects like GUIDE or FIDIS there is hardly any structured EU-wide discussion about interoperable eID solutions. Austria has relatively early passed laws like the Electronic signature or egovernment law which are required for a national eID solution but some European countries are far behind.

Although Austria passed a law which allows the acceptance of other countries eIDs for egovernment purpose, there is no structured integration process of other countries eID solutions. Integration processes are more or less individual projects and on ad-hoc basis.

What are the requirements for interoperability for the USERS?

Mr. Leitold answers "transparency". Most important is that the solution is easy to understand and not technologically too sophisticated. Remember, at the moment most Austrians use their paper based driving licence for identification purpose and that has been the case for more than one generation.

Recent analysis shows that about 70% of the Austrians who have electronic signatures use that technology while filing their tax statements. However, it should be noted that mostly only so called early adopters are using the concept of the Austrian Citizen Card.

What are the requirements for interoperability for the GOVERNMENTS?

Mr. Leitold again answers this question with "transparency". It is of extreme importance for the success of the Citizen Card that the users in the government agencies trust the system, see a clear advantage in it and find an the solution being an improvement for doing their daily work.

Future integration of other EU 25 member eID solutions will only be possible if the integration can be done by adding additional connectors centrally. If the integration of other eID solution would also require an adoption of all the locally installed client solutions the integration would be not possible due to high costs and complexity. In other words if i.e. the French system can be made interoperable by adding some plug-ins on the central repository than that is no problem, should it require additional work processes on client side (government agency user) Austria would most likely not offer an integration to the French system.

What are the requirements for interoperability for the MERCHANTS?

Mr. Leitold describes that the requirements for interoperability in relation to the Austrian Citizen Card for governments and merchants are the same.

What are the benefits of interoperability for each of these stakeholders?

Users:	comfort, easier communication via electronic channels
Government:	costs saving, higher efficiency
Merchants:	costs saving, higher efficiency

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

Technical level

From the current point of view ISM interoperability on a national level in Austria has been fully achieved. The Austrian Citizen Card is an open system and it does not depend on any specific hardware. It can be concluded that the solution is fully interoperable.

On EU level, standards should be defined in order to grant technical interoperability. Mr. Leitold adds, any system which is defined in a way that it does not require any specific hardware is most likely easily interoperable with other national solutions. It can be concluded that the use of specific technology (i.e. smart card, etc.) would hinder interoperability on a technical level.

Legal level

The EU Signature Directive was not sufficient to fulfil Austria's requirements on privacy and data protection. This will be most likely also the case with other EU country's legislative regulations. As a result most EU members will pass additional laws and this additional law might hinder interoperability on a legal level.

Cultural level

Due to immense differences in the historic backgrounds of countries a European wide interoperable eID solution will take a while. Austria for example is a country in which only a minor percentage of the population owns an ID card.

As a result of the too soft EU Signature directive an eID solution designed only according to this directive is not workable in praxis. For example the EU Signature Directive defibes that identification is also sufficient after a specific transaction has been completed. In practise this is not possible as most working processes require an identification and even authentication before a specific working progress can be started. This is only a small example but already shows that most EU member states will handle their processes entire different. These different work practises and many other facts will hinder a European wide interoperability on a cultural level.

What can be done at the TECHNOLOGICAL level to establish interoperability?

Mr. Leitold recommends defining technical standards. He adds that it will be of importance which level of technical detail these standards define. He recommends defining the technical standards at the highest possible level- at the policy level rather than on the IT artefact level.

What can be done at the LEGAL/POLICY level to establish interoperability?

Mr. Leitold is not convinced if the EU member states are already in the position to discuss the legal domain of the eID interoperability. First, the member states have to engage a serious discussion on the policy level. This has not yet happened. It is true that there are some research efforts like GUIDE or FIDIS but there is no broad discussion taking place.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

First the countries have to decide for themselves if and what kind of national identity solution they want to implement. In a second step they then can discuss European consequences.

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

Mr. Leitold ranks it:
1. cultural/institutional
2. policy
3. legal
4. technical

eID projects are high profile projects, political very controversially discussed and extremely costly. Therefore, a country has to create a vision first before it can think about a specific solution.

As national eID solutions often challenge constitutional rights and deal with the very basic rules of democratic society, no decision can be made on EU level in the first place – only in a second step after the member countries made their individual decision.

As an example Mr. Leitold points to the failure of eTEN. eTEN is the European Community Programme designed to help the deployment of telecommunication networks based services with a trans-European dimension (Information Society and Media DG 2005d). The program is split up in the following six research areas: egovernment, ehealthcare, eInclusion, eLearning, Services for SMEs (eBusiness), and Trust and Security services components. eTEN focuses heavily on the legislative level as well as on the technical level. However, it hardly addresses issues at the informal level and it is found that eTEN has low relevance to interoperability (Freh 2005). Mr. Leitold confirms that this analysis is correct and he outlines that because of the missing discussion on the policy level eTEN was doomed to fail from the very beginning.

What should be the role of governments in addressing interoperability of IMS?

Governments have to form a vision on a specific IMS, clearly state the goals and define the requirements of the solution proposed. eID egovernment applications are usually more complex than commercial eID solutions due to the greater number of involved stakeholder.

What should be the role of merchants and industry groups?

The merchants and industry groups should ideally be the enabler of an eID solution, create the infrastructure and carry the main junk of the costs. In return, they should be able to generate revenue by offering services in connection with the eID. As example Mr. Leitold names certificate authorise, telecommunication providers, etc.

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

No.

Any other comments?

No.

References

Freh, S. (2005) Analysis of Global Eid Projects with Focus on Interoperability by Using the Tfi Model.

Hayat, A., H. Leitold, C. Rechberger and T. Rössler (2004) "Survey on Eu's Electronic-Id Solutions" *10.08.2004* Vienna.

Information Society and Media DG (2005d). "What Is Eten?" http://europa.eu.int/information_society/activities/eten/index_en.htm Accessed On 20.03.05

Otter, H. (2005b) in *Managing Identity* German Embassy Info Center.

12.12 Report 20: Arno Hollosi and Bernd Martin, Austria, egovernment

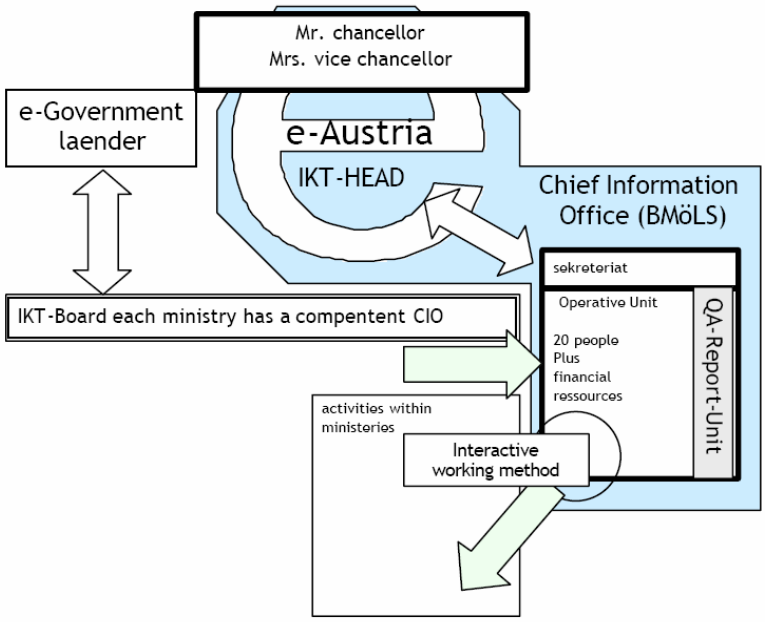
D4.2: Requirements for interoperability in IMS

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer: Stephan Freh
London School of Economics
Tel.: +447906344477, Email: freh@gmx.at
Interviewee 1: **Dipl.-Ing. Arno Hollosi, Technical Director**
Stabstelle IKT-Strategie des Bundes, Ballhausplatz 2, 1014 Wien, Austria, Web: http://www.cio.gv.at
Tel.: +43-1-53115/6141, Email: arno.hollosi@cio.gv.at
Interviewee 2: **Dipl.-Ing. Bernd Martin, Technical and Standards Manager**
Stabstelle IKT-Strategie des Bundes, Wagramer Straße 4, 1220 Wien, Austria, Web: http://www.cio.gv.at
Tel.: +43-1-53115/6166, Email: bernd.martin@cio.gv.at
Location: Vienna, Austria
Date: 30.06.2005

Background Information:

Mr. Arno Hollosi (2005) joined the Stabstelle IKT-Strategie des Bundes in 2001 and he was since than Technical Director of it. Mr. Hollosi is responsible for developing and coordinating the technical aspects of the egovernment projects in Austria, which are headed by the Stabstelle IKT-Strategie des Bundes.



The Stabstelle IKT-Strategie des Bundes is also called Chief Information Office (CIO) of the Austrian government. On the basis of agreement of the ministers on June

6th 2001 Austria has established a strategic office for the co-ordination of information and communication technologies. This office within the Ministry for Public Services and Sports reports directly to the Federal Chancellor and the Vice Chancellor. The IKT Board (Information and Communications Technology Board) incorporates a competent representative of each ministry so that it can build strategies and make decisions that are relevant for the entities of the federal government (ICA 35th Conference Report 2001).

The activities of the board focus on matters that concern more than a single ministry or have strategic relevance. The slim organisation allows for efficient operation. The board and the operative unit have been in operation since August 2001.

Currently the Stabstelle IKT-Strategie des Bundes oversees and coordinates more than 160 egovernment projects. One of the most important ones is the Austrian Bürgerkarte or Austrian Citizen Card.

The Austrian Citizen Cards shall become the “official identity documents” in the electronic administrative procedures, such as filing applications via the Internet. From a technical perspective, chipcards are nowadays a suitable tool to fulfil needed security requirements. The concept is, however, not restricted to chipcards. It is conceivable that commodity devices such as mobile phones, PCs or laptop attachments such as USB tokens follow the Citizen Card concept and thus turn into a “Citizen Card”.

The slogan of the Austrian Citizen Card project is “Open interfaces for egovernment” (Hollosi and Karlinger 2005).

The notion “Austrian Citizen Card” does not stand for a specific card that is the same for each citizen, such as, e.g., a passport. The Austrian Citizen Card is rather a concept that allows designing secure electronic public administration services and thus enables carrying out administrative procedures electronically. Meanwhile several Citizen Cards are available, such as ATM bank-cards, mobile phone signatures, or the so-called “OCG card” (membership card of the Austrian Computer Society). Others will follow, such as the Austrian health insurance eCard.

The Citizen Card concept defines the requirements that are necessary to carry out electronic administrative procedures securely. Based on this rather general approach the citizens are able to choose which Citizen Card(s) implementation they wish to use. Using the above analogue of a passport, the Citizen Card can be compared with an “electronic identification document”: “Identity document” represents a concept that can have different implementations, such as passports, driving licenses, student identity cards, or membership cards. However, official proceedings usually lay down certain security requirements that are fulfilled by “official identity documents” such as passports, identity cards, or driving licenses (Posch and Holzbach 2005).

Questions:

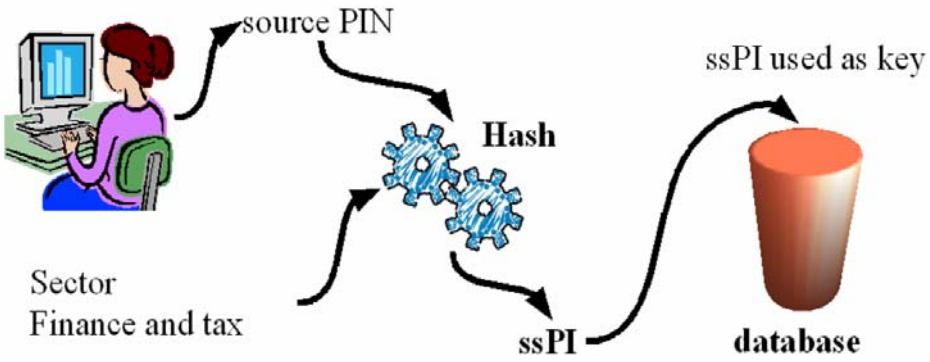
What are the main identity management issues in the chosen field of analysis ecommerce, egovernment and ehealth?

This interview is analysing the Austrian Citizen Card and answers question in relation on egovernment.

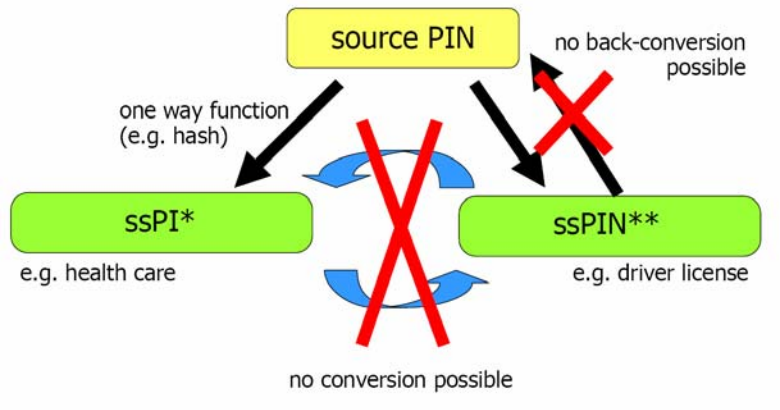
Secure authentication / Privacy Issues

Mr. Hollosi sketches as opening example the well known picture of a dog sitting in front of the computer and surfing the web. Mr. Hollosi adds every one in the egovernment sector knows this metaphor - Austria made its first step towards making this image Austrian history. In other words the fundamental issue for starting the Austrian Citizen Card project was to equip the public with a secure, easy to use and open (!) concept to allow them identifying over electronic channels.

From the beginning, it was rather clear that the Austrian Citizen Card should not use a new "database" but at the same time could not entirely rely on the existing central citizen register (ZMR). As a result the technical concept consisting of a Sector Specific Personal Identifier (ssPI), source PIN and identity link was developed.



This solution ensures that a person can not be tracked in various databases as every sector or even application works with a different identifier. This regulation is an important requirement which had to be fulfil and is specified in the so called "egovernment law".



High costs must justify added value

Probably one of the most discussed topics in the Austrian media in recent years was how much an Austrian Citizen Card would cost and what the benefits would be. Soon it has been clear that Austria would not launch a mandatory eID solution as 70% of the potential owner of such a card have less than two communication contacts which public authorities a year in which they could use such a new eID solution. The concept was established that the Austrian Citizen Card should be a concept rather than a physical token which could be easily transferred to other domains and would not need a specific technical solution to work with. It was the goal to develop a system which is as open as possible and platform independent.

Legal framework

As in any other democratic society, government agencies can only act in accordance to the law. The Austria parliament passed the legal framework which would allow services as the Austrian Citizen Card. The latest regulation – the egovernment Act entered into force on 1st March 2004 and considers the Data Protection Act 2000. These two laws more or less define the terms and rules such as:

- identity and authenticity
- citizen card function (incl. identity link)
- source PIN register (PIN = personal identification number)
- sector-specific personal identifiers
- official signatures
- use of citizen card functions in the private sector
- electronic delivery (service)
- documentation register

Important parts out of the egovernment Act are:

- Citizen Card
  „the logical unit, independent of whether implemented on different technical components or not, combining an electronic signature with an identity link and the associated security data and functions plus any existing data on representation." [§2]
- Citizen Card Function
  „… serves to validate the unique identity of a person making a submission and of the authenticity of a submission made electronically…" [§4(1)]
  „…unique identification of a natural person … by way of an identity link" [§4(2)]
  „the authenticity of a submission made … shall be validated by the electronic signature contained in the citizen card." [§4(4)]

An English version of the Austrian E-Government Act can be found under http://www.ris.bka.gv.at/erv/erv_2004_1_10.pdf.

How critical is the issue of interoperability of IMS for this field?

Interoperability on domestic level

Mr. Hollosi and Mr. Martin both stressed several times the importance of interoperability. Interoperability is very closely linked with high quality of the system, privacy, data protection, cross applications and cross border communication.

Therefore interoperability is a central parameter of all discussions in relation to IMS and enjoys high priority.

On a technical level this means that server based and client based applications have to be technically fully platform independent. In other words even if the server is working with operating system A, standard B, hardware technology C the client has to be able to use operating system X, standard Y, hardware technology Z.

Interoperability on EU level

Austria adopted the EU Directive on electronic signatures. This directive is basis for the Austrian signature law. Mr. Hollosi pointed out that the Austrian signature law has higher requirements on electronic signatures than the EU directive but at the same time it is believed to grant a full interoperability to neighbouring countries of Austria.

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?

Interoperability is the successful communication among several different systems with the intention to exchange information. On the international level semantic correct ID exchange should be possible. Therefore the terminology ID has to be defined and the exact dataset described an ID has to classified.

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

Current Solutuion of the Austrian Citizen Card

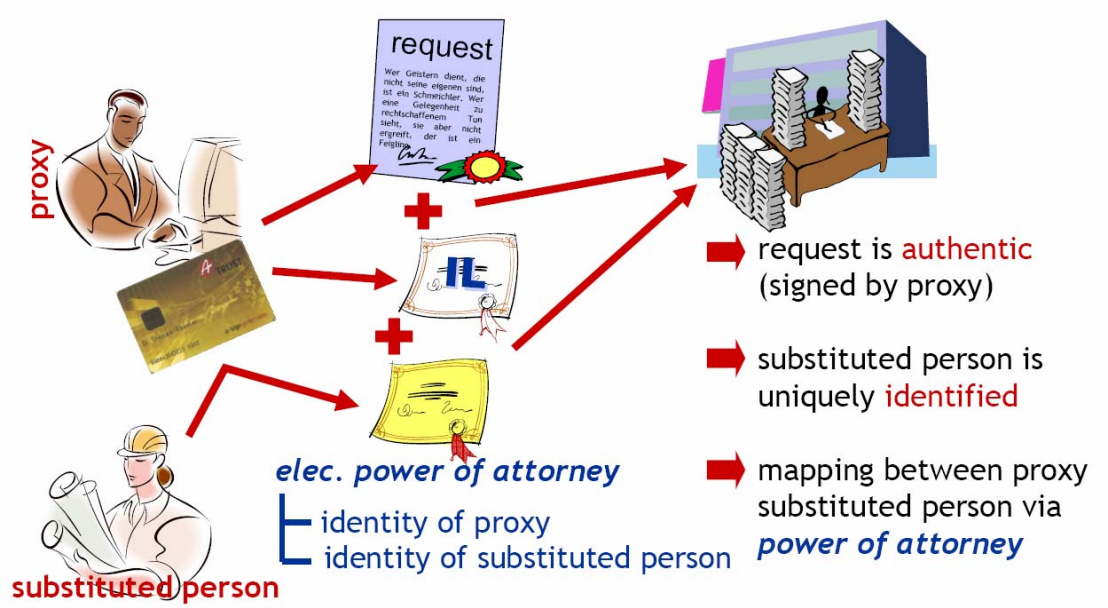
The Austrian Citizen Card is more or less completed and the roll out has started. At the moment Staff Department for ICT pushes other government agencies to offer more services which are relying on the Austrian Citizen Card. Some of the currently available services are:

- Identification
  - Finanz-Online (https://finanzonline.bmf.gv.at)
  - Service of Official Documents (https://www.zustellung.gv.at)
  - services of social insurance institutions, ELAK (electronic file system), portals, etc.
  - Several Austrian high street banks offer to log on using the Austrian Citizen Card. However they do not yet support actively the distribution of the Austrian Citizen Card.
- Authenticity
  - request of the current criminal record (https://labs.cio.gv.at/egov-wip/polizei/strafregister)
  - registration notification (https://meldung.cio.gv.at/egovMB)
  - Service of Official Documents (https://www.zustellung.gv.at)
  - auftrag.at, registration of a business, etc.

Near future of the Austrian Citizen Card

Mr. Martin described that the Stabstelle IKT-Strategie des Bundes plans only one additional functionality which is also significant in relation to national interoperability – the power of attorney. This particular functionality will only be offered in Austria at the current knowledge and is a significant step. In the past preventatives of citizen

often acted in a grey zone and on good will basis, as government agencies often granted services (i.e. a mother calls a local government agency and informs it that her sun will pick up a certain document – all he shows the agent is a hand written document apparently form his mother for authentication purpose) which they should not have granted, taking the law very strict.



In a way this can be described as interpersonal interoperability of power of attorney. It is expected that this functionality will be largely used between trusted partners (i.e. husband - wife) and within families (i.e. mother – sun)

International level (hypothetical)

Mr. Hollosi argues that the EU should clearly define the semantic terms of an EU wide accepted eID. The EU has to reach an agreement on the terminology ID. Further the EU has to define the value of sub terms like name, national identifier, etc. In other words the EU has to reach agreement what specific set of terms make an identity.

How far are we currently from that scenario?

Mr. Hollosi describes that the Austrian Citizen Card is largely interoperable with eID solutions from Finland, Italy, Belgium, etc. The electronic signatures of these systems are 100% interoperable from a technical point of view. However, in terms of authentication no fully interoperable is given.

For example: The Italian eID is technically interoperable however the Italian card holder has to register himself at an Austrian registration service authority in order to use all services. Once he/she did so, sector specific identifier will be generated in the Austrian system and from that moment onwards he/she is able to fully use his/her Italian eID.

What are the requirements for interoperability for the USERS?

Signature card

Signature card is the first prerequisite for using the Citizen Card. A signature card may, for example, look like a bank service card. The card is an integrated circuit card

and has a microprocessor chip and a small memory area, so it can also be seen as a "small computer". The cryptographic keys are stored and the electronic signature is computed on the signature card. Furthermore, the signature card can be used to store some data that is frequently needed by the public administration services and that in this way may become available to each computing environment (e.g., a PC) in which the signature card is used. Signature cards are a common way to implement signature creation devices. Other technologies (mobile phone, PDA, USB-Token, …) may serve the purpose as well.

Certificates and identity link

An electronic signature is computed on the signature card by applying a cryptographic key. In order to inseparably bind an electronic signature with a citizen's identity, the citizen needs an electronic analogue to an official identity document. From a technical point of view, the electronic identity document contains two components, that is, the certificate and the identity link. A prerequisite for issuing these components is that the citizen goes in person to the registration office of a certification service provider (CSP). During the registration procedure, the registration officer will verify the citizen's identity based on an official identity document. The certificate will then be issued by the CSP, and the identity link will be issued by the sourcePIN Register Authority (the Data Protection Commission). Both components (i.e., the certificate and the identity link) will usually be stored on the signature card during the registration procedure at the CSP's registration office. As an advantage versus conventional procedures, personal contact is necessary only once.

Chipcard reader and software

To use a signature card with a PC (e.g., at home), a chipcard reader connected to the PC is needed. When the signature card is inserted into the card reader, the PC can communicate with the card. For secure electronic signatures, the certification service provider (CSP) is supposed to recommend the suitable card readers.

Furthermore, some special purpose software that supports communication with the signature card should be installed on the PC. In this way the PC can communicate with the signature card via the card reader and initiate computation of electronic signatures on the card.

The following companies currently offer such a software, also known as Citizen Card Environment (CCE):

- "trustDesk basic" from IT Solution
  The Federal Republic of Austria has purchased a general license for this product. Therefore you can download this CCE free of charge from the website of the Federal Staff Office for IT Strategies (http://www.cio.gv.at/identity/bku)."
- "HotSign" from BDC:
  You can obtain this product directly, please contact the manufacturer.

What does it cost?

At the beginning a signature card and a card reader are needed. In many cases a citizen does not need to pay for the signature card because it can be provided for free as part of a specific service (e.g., e-card, bank service card or student identity card). A

citizen is, however, free to purchase a signature card on her own at a suitable certification service provider (CSP) (see, for example, the Web page of a.trust[41] that is currently the only commercial CSP issuing qualified certificates in Austria).

A card reader can be purchased for about 20 EUR. Apart from those initial costs, there are annual costs for the certificate related CSP services. All in all, the citizens should perceive the Citizen Card as beneficial rather than costly. It is a challenge for the public administration to achieve a high usage of e-government services by as many citizens as possible.

What are the requirements for interoperability for the GOVERNMENTS?

As described before the Citizen Card is a concept rather than a physical card. In case a government agency wants to offer a service using the citizen card the method is rather simple. The government agency needs to certify themselves, download drivers and application and integrate it in their web portal. Mr. Hollosi explained that from a technical perspective the entire process is very easy and can be completed in a couple of hours.

The government agency has to implement the so called *Security Layer*. This *Security Layer* interface defines the interaction between the application and the Citizen Card Environment. The detailed protocol that can be used via this interface is specified in Security Layer application interface. The possible bindings between this protocol and transport layers such as HTTP or TCP are defined in Security Layer transport protocols.

However, Mr. Hollosi stressed that the government agencies have to fulfil another very important role. They have to communicate the concept to the citizens and they have to win their trust. Via public relation campaigns the government agencies have to educate the citizens what advantages and added value the Citizen Card gives them. Only the emphasis of a well organised and ongoing communication process ensures trust and usage of the Citizen Card in the long run.

Mr. Martin adds that the government slogan for the Citizen Card is “Define functionality rather than form.” and interoperability goals are:

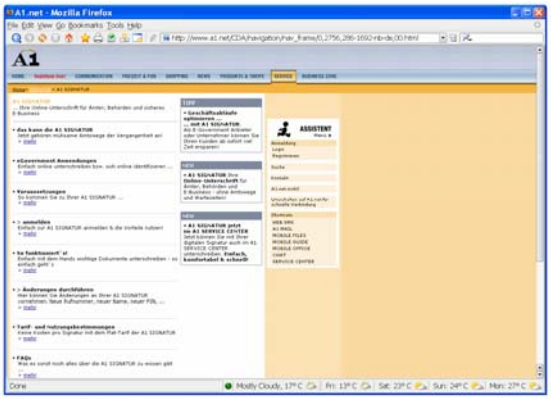
- identification, authentication, confidentiality
- extendibility and modularity a must
- technology independence a must (separate key players - public sector, certification authorities, developers, users account for different technologies
- open market ideology

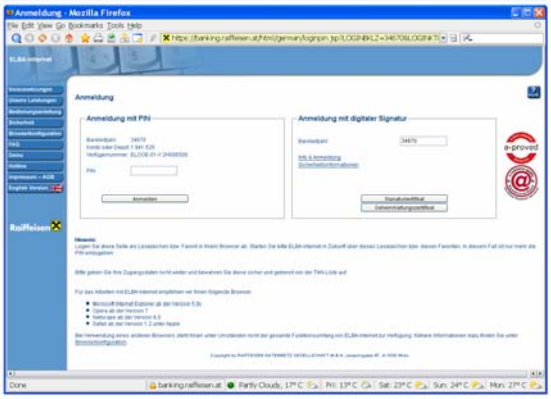
What are the requirements for interoperability for the MERCHANTS?

The requirements for interoperability for merchants are similar to those for

[41] a.trust (founded in February 17, 2000) is an accredited TrustCenter in Austria issuing smartcard based qualified certificates for Austrian citizen used in eGovernment, etc. On March 11, 2002 a.trust has been accredited according to § 17 of the Austrian Signature Law by Telekom-Control-Kommission, the Austrian supervisory body. a.trust's product range comprises user certificates, developer certificates and corporate certificates as well as consultation services and support with the development of e-commerce and signature applications in accordance with the Directive 1999/93/EC.

government agencies. Meanwhile several key commercial players have adopted the Austrian Citizen Card concept. The market leader in mobile communication - A1 offers a certification via mobile phones and its internet portal. Therefore, A1 acts as certification provider. Once citizen have acquired this certification they can use other commercial applications like to logon to their online bank accounts. Raiffeisen Bank, the third biggest high street bank in Austria already offers its customers to logon using the Citizen Card environment. A screen shot of the A1 portal and the Raiffeisen Bank logon page can be seen below.



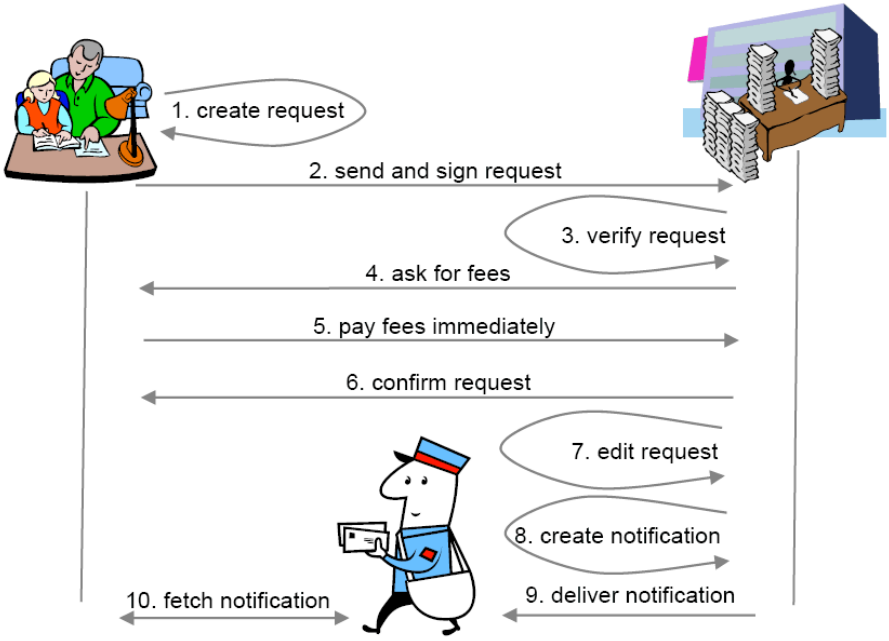


Mr. Hollosi once more addd that the Citizen Card is easily to implement and it is anticipated that all major commercial players, who offer a web-portal solution holding sensitive information (bank accounts, insurance policies, mobile phone bills, etc.) will offer their customers the possibility to logon via their Citizen card.

What are the benefits of interoperability for each of these stakeholders?

Citizens

The citizens can carry out their public administration procedures from their homes, e.g., over the Internet. In their official matters the citizens will enjoy the same convenience they are already used to when shopping in the Internet or when accessing their bank account online, i.e., round the clock and 7 days a week.



Thereby the Citizen Card provides the security level that the citizens may expect: Certainty of the law is provided by secure electronic signatures, which are legally equal to personal signatures, and by high-quality identification procedures. Solely the citizen herself can file applications or examine her records. In addition, the Citizen Card provides services, such as private communication, together with electronic signature, may also enhance security of other applications, such as, for example, Internet shopping.

Finally, the citizens may expect a faster processing of their affairs. The necessary data is already available in the electronical format and no longer needs to be transferred into paper forms. Manual checks are no longer needed, such as identification based on identity documents. Wherever possible, the completion of procedures will occur immediately.

In average the Austrian internet user has 15 user/password combinations. The Citizen Card provides the great advantage to use just one secure identification method. In comparisons to other EU countries the Austrian online shopper are very reluctant to use bank and credit card information over the net and less than 20 % of the population does actually has a credit card. With the Citizen Card, people can sign online orders and the commercial partner can be ensured about the validly of the contract.

Governments

From the public administration's point of view, the introduction of general electronic transactions results in more efficient processing. The public administration services becomes faster, cheaper and of a higher quality. The purpose of the Citizen Card in this scenario is to support secure identification on the one hand, and electronic signatures on the other. Secure identification can thus be implemented securely and efficiently even for a large number of users, and electronic signatures serve as an equivalent to personal signatures. Electronic filing of applications and electronic

delivery complement the Citizen Card and are a prerequisite for an integrated electronic administration without media transitions.

Commerce and Industry

The benefits for the private sector are similar to those for the citizens. Electronic public administration procedures can be carried out with lower costs. The completion occurs more efficiently and faster.

In addition, the Citizen Card establishes a security infrastructure that will be available to all citizens, including the potential commercial customers. Companies can develop secure online services for their customers by building upon the infrastructure provided by the "Citizen Card". The Citizen Card helps eliminate one of the major obstacles for e-commerce, namely the customers' lack of trust in the security of electronic transactions.

Commerce and industry is also a "key account" of the public administration and does not have to spend considerable resources for the public administration procedures. These costs can be reduced as soon as the efficient e-government services and Citizen Cards have been put into action.

The Citzen Card reduces the risk of fraudulent online orders significantly. The "Pizza Example" might sound oversimplified – someone with a pre-paid phone orders a pizza to a non-existing address – but many companies have significant delivery failure rates as they cant authenticate their online customers.

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

Technical level

Mr. Hollosi explains that the Citizen Card was designed with a maximum emphasis on technical interoperability. If the Citizen Card require specific hard- and software interoperability (especially in the commercial sector) would most likely be much smaller.

Future eID solution will most likely involve biometric features. There any eID solution currently designed should offer the possibility to add such features at a later point in time, otherwise the system might soon be outdated and not interoperable. Austria's Citizen Card fulfils this requirement.

Legal level

a.trust (Austria's certification authority) can only be held accountable for a failure according to Austria's signature law. However, this law only foresees compensation for damages accrued during the registration process (i.e. costs to get a new signature, etc.). The commercial risk lies with the parties using the Citizen Card. As the legislation in other European countries differs from the one in Austria interoperability issues especially in cases of cross border communication occur and it can be anticipated that legal issues will be a major problem of electronic signatures in the near future.

Cultural level

From a citizens point of view the fact that different countries have a different legislation and therefore the consequences using the Citizen Card outside the home countries might differ significantly to the one at home puts a great risk on the user. Even an expert in European law would most likely not be sure to what extend he/she might be liable for using his/her electronic signature in all the EU 25 member countries. This will most likely scare people off using their electronic signatures in cross border communication.

What can be done at the TECHNOLOGICAL level to establish interoperability?

Mr. Hollosi gave a clear answer to that question. Most important is that all EU 25 design their solution based on the EU-Sig-RL 1999/93/EG regulation.

- Signatory must be natural person (signature creation data and the corresponding signature verification data are allocated)
- based on qualified certificate
- secure electronic signatures
- electronic signature of public authority

The "technical heart" of Austria's Citizen Card is the so called "Security Layer" and its key characteristics are

- commands in XML-syntax
- simple request-response schema
- high level of abstraction
- independent of underlying technology
- simple binding to a web browser (HTTP-binding)

granting the following functions

- signing and verifying signed documents
- storing/retrieving data
- encryption and decryption of documents
- utility functions
- available for free

Mr. Hollosi describes that a country which designs their eID solution in such a way will have minimal interoperability issues with the Austrian Citizen Card.

What can be done at the LEGAL/POLICY level to establish interoperability?

The basis for acknowledging electronic signatures under Austrian law was created by the Federal Electronic Signature Act (Signature Act, or SigG), BGBl I 1999/190. Austria is therefore the first country to have fulfilled the implementation requirements set forth under Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures. The Signature Act is explained in more detail by the Signature Ordinance. With the Ordinance BGBl II 2002/117 the European minimum criteria for notifying confirmation bodies were published in the Austrian official journal. The A-SIT Ordinance (BGBl II 2000/31) recognized the Secure Information Technology Center – Austria (A-SIT) as a confirmation body (Rundfunk und Telekom Regulierungs-GmbH 2005).

Mr. Hollosi emphasis that it is of great importance due to privacy and security issues that an eID solution and other country's national citizen registers are NOT based on one single number! Further the main identifier should not be included in the electronic certificate – Austria's privacy laws would than forbid collaboration with such a system.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

Mr. Hollosi, Mr. Otter and Mr. Martin all mentioned that Austria adopted the strategy to promote their eCard and Citizen Card heavily among the EU 25 not as it hopes to sell the concept but as Austria hopes by showing a working concept other countries will develop their systems in such a way that maximum interoperability is achieved. If that strategy works Austria will face minimal needs to adapt its solution in order grant full interoperability. In other words by being an early beard and open communicator (marketing jargon) Austria hopes to set trends, positively influence other countries and secure their own interoperability future.

As mentioned before Mr. Hollosi described one of the most important points in relation to inoperability is that the EU agrees on a specific "set of identity features". The Austrian Citizen Card uses the following set:

- National Insurance Number
- Name
- Nationality
- Gender
- Birth date
- Birth place

Although these six components seem to be rather simple, semantic interoperability issues involving the national insurance number, name and nationality can occur and clear regulation is needed in order to avoid multiple identities and grant a technical sound solution.

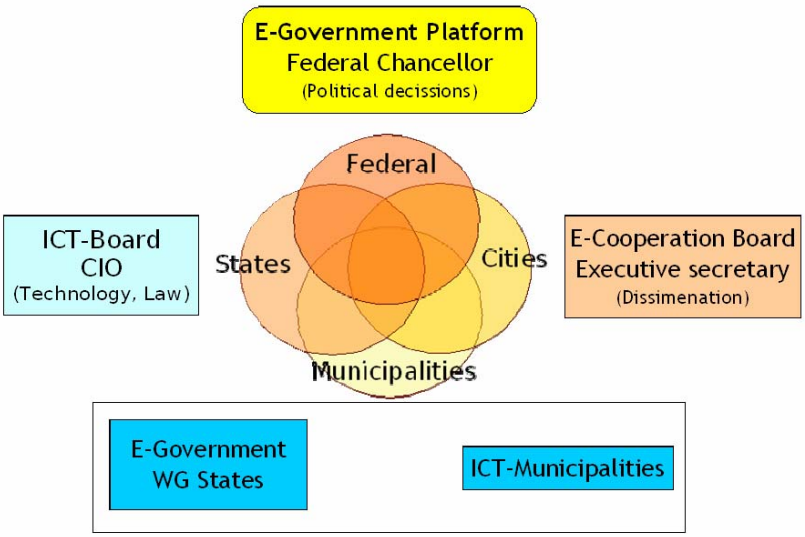
Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

Mr. Hollosi answered that to him this question does not make any scene as without fulfilling one of these three levels no working and long lasting eID solution could be achieved. Therefore all three levels are of significant importance. A prioritising is not recommendable as an eID project should be managed in a holistic approach rather than a silo thinking.

What should be the role of governments in addressing interoperability of IMS?

The Austrian Citizen Card Project was seriously started in 1999/2000 after several smaller and rather uncoordinated initiatives from individual politicians and representatives of the industry had failed. In the beginning the biggest challenges faced was the missing political agreement over how a possible solution should look like among key stakeholders. There was also no "arena" in which different believes and ideas could have been discussed.

Mr. Hollosi and Mr. Martin both underlined the importance that national eID projects are coordinated by the government due to the high costs, the needed political commitment, potential commercial risk, needed legal environments and to grant an international interoperability. However, Austria tried to outsource as much as possible to commercial partners. The IKT board came up with a vision but the commercial partners bring the Citizen Card to life. **Note: Even the certification provider is a privately held company. No physical card is issued by the government.**



The strategy of the Austrian Citizen Card was largely developed by the IKT Board and the federal staff unit for ICT-Strategy. Specifically the federal staff unit for ICT-Strategy is characterized as (Martin 2004):

- experts from all federal ministries
- own budget (mainly for projects)
- not part of a ministry (obligated only to the Chancellor and the Vice Chancellor)
- duties
    - creating technical specifications
    - evaluation of standards
    - preparation of recommendations to the ICT Board

What should be the role of merchants and industry groups?

Mr. Martin described that the merchants and industry groups carry out the concept, their representatives were part of the IKT board from the very beginning but they do not have any strategic roll.

However, Austria opened the project to the commercial world and it wants commercial companies to offer the entire technical and functional infrastructure of the Citizen Card. The service offer in relation to the eCard and Citizen Card is designed to be a revenue stream for commercial providers even though there is a regulatory emphasis that the costs for citizens are as low as possible.

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

The usability as well as the availability of services for the Austrian Citizen Card has to be improved. In addition to that the information distributed to citizens and SMEs

have to be boosted. Fringe social groups have to be especially addressed. On that level there is a big gap at the moment - especially in relation with the eCard.

The goal is to have issued by

2005	8 million eCards
	100,000 Citizen Cards
2008	8 million eCards
	200,000 student cards (specific form of the Citizen Card)
	1,000,000 Citizen Cards

To address the issues described above are critical in order to meet the ambitious targets of the Citizen Card.

Note: At the moment Austria does not have any representative studies if citizens have trust in either the eCard or the Citizen Card. However, Austria has several trial villages for testing egovernment projects. These villages tested the Citizen Card and the feedback on acceptance and usability was positive.

Any other comments?

Mr. Martin (2005) underlined the flowing as critical lessons learnt over the last couple of years:

- cooperative effort necessary
  - federal, state, and local
  - develop once, deploy often (e.g. open source)
  - cooperation on national and international level
- interoperability (identity management)
- recognition of documents
  - involve experts from areas of data protection and law early on
  - rethink of processes
  - rethink financing of projects
  - monitor developments
  - private public partnerships

References

Hollosi, A. (2005) *Requirements for Interoperability in Ims at the Example of Austria's Bürgerkarte* 30.06.2005. (Personal communication).

Hollosi, A. and G. Karlinger (2005) *Die Österreichische Bürgerkarte: Einführung* A-Sit Last accessed: 10.07.2005 Last updated: Address:

ICA 35th Conference Report (2001) in *ICA 35th CONFERENCE* Berlin.

Martin, B. (2004) in *egovernment Workshop*Vienna.

Martin, B. (2005) in *FIDIS workshop 3.5* IKT-Stabstelle, Frankfurt.

Posch, R. and M. Holzbach (2005) A-SIT Secure Information Technology Center.

Rundfunk und Telekom Regulierungs-GmbH (2005) *Electronic Signature: Legal Information* Rundfunk und Telekom Regulierungs-GmbH Last accessed: 10.07.2005 Last updated: Address: http://www.signatur.rtr.at/en/legal/index.html.

12.13 Report 21: Heinz Otter, Austria, ehealth

D4.2: Requirements for interoperability in IMS

Semi-structured interviews with experts in IMS and Interoperability.

Interviewer: Stephan Freh
London School of Economics
Tel.: +447906344477, Email: freh@gmx.at
Interviewee: **Dipl.-Ing. Heinz Otter, Leiter Bereich Strategische Projekte SV-Chipkarten Betriebs- und Errichtungs GmbH.**, Schiffamtsgasse 15, 1020 Wien, Austria, Web: http://www.chipkarte.at
Tel.: +4371436754122, Fax: +4371436753776, Email: heinz.otter@chipkarte.at
Location: Vienna, Austria
Date: 30.06.2005

Background Information:

Mr. Heinz Otter (2005a) joined the SVA (Sozial Versicherungsanstalt – Social Security Office) as project manager in 1997. Mr. Otter was since then responsible for coordinating the eCard Project and he recently became appointed to Director Strategy at SV-Chipkarten Betriebs- und Errichtungsges.m.b.H.

Austria started on 30th May 2005 the distribution of the eCard to all socially ensured Austrian Citizens as well as to theirs dependents. It is planned to finish the roll out of the over 8 million eCards in December 2005. The eCard holder presents his card at each visit of a doctor or hospital. eCard readers and software applications will be installed at more than 12,000 contractual partners (doctors, dentists, etc.). The eCard will replace the over 42 million paper version of the so called "Krankenschein" (health insurance vouchers) used every year. The smart card based eCard holds an electronic signature and the Austrian eID solution "Bürgerkarte" (signatures) can be "saved" on the eCard.

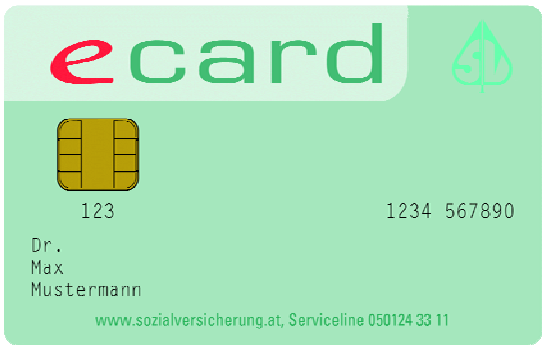
Key government requirements of the eCard are:

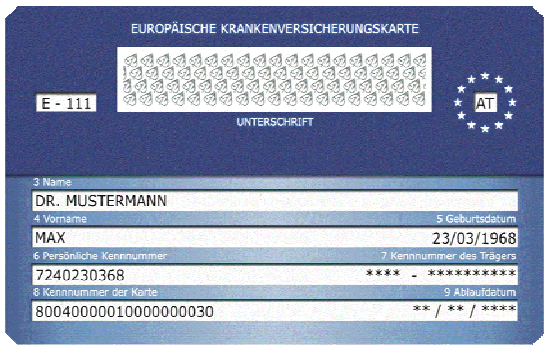
- Design of the eCard as a „Keycard"
- Access to personal data after approval of the cardholder (§31a (2) ASVG)
- Reloadability of health data on the smart card
- The e-card system shall support the transparency of medical services and costs
- Acceptance of other cards with „Citizen Card Functionality" (i.e. prepared for egovernment).

Physically the e-card corresponds to an intelligent token which represents the access key to system-based services and data. The eCard is principally not a carrier of application software functions. The eCard contains identification data which are required for access authorization to applications.

The eCard is like a credit card without a logo. The card holder is equipped with a PIN. By using this PIN the card holder can give access medical staff to certain or all his/her

medical information saved on a central server. Physicians in return know by reading out information saved and protected by the eCard if and to which condition the patient is ensured.





The eCard is interoperable with the EU NETC@RDS project. The NETC@RDS project aims to improve the access of mobile European citizens to the national health care systems using advanced smart card technology. It also aims to implement and evaluate technical solutions for the European Health Insurance Card electronification and for improving additional services such as the inter-European health costs clearing/billing processing.

Questions:

What are the main identity management issues in the chosen field of analysis ehealth?

Data Technical / Unique Identifier Issues

Austria has a centralised residents register system or "Zentrales Melde Register" (ZMR). Every person born in Austria gets a so called social security number or "Sozialversicherungsnummer". This number consists of the birth date plus a 4-digit number. All these numbers are saved in the ZMR. However, as the eCard is distributed to all Austrian citizens people like foreigners, who have no such number, had to be added to the system. It was given a great emphasis to avoid multiple entries in the database. This starts with trivial problems like the correct writing of people's names. (i.e. Austria has a regulation that every citizen can ask to be addressed by his "original" name including characters like ä, ë, í, õ, ü etc.). As far as known today, this goal has been achieved.

Mr. Otter indicated that the Austrian authorities decided not to use the ZIN[42] numbering systems. Instead a „Sector Specific Personal Identifier" consisting out of several registers was developed. Mr. Otter described that the logistical challenge is an often underestimated and extremely significant issue in relation to eID projects of that size. The eCard uses a newly developed numbering system – the so called bPK (sector specific personal identifier).

Stakeholder Issues

The first project of the eCard was unsuccessfully and was ended after 2 years.Some of the main problems were that the stakeholders of the eCard could not reach an

[42] ZIN is European wide known numbering systems similar to national social security numbers.

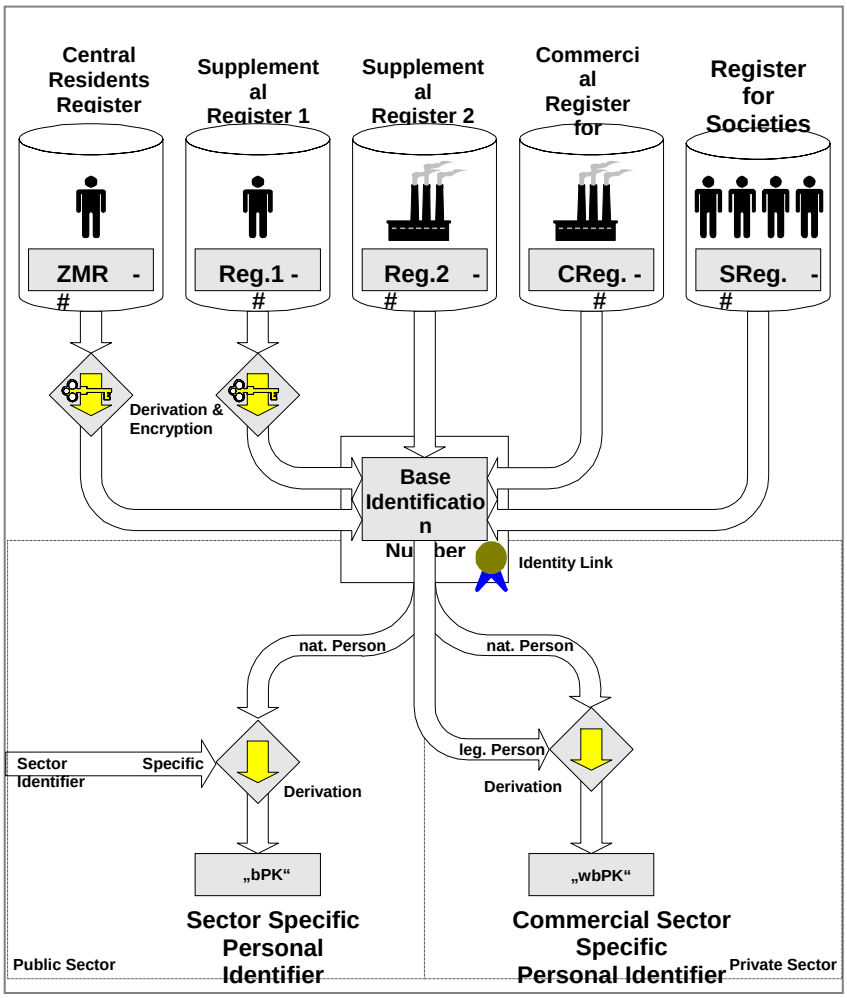
agreement how the system should work, what the goals should be and which services should be realised. However these problems are not IMS specific.

Privacy Issues

Mr. Otter stated that the privacy issue was a major point of discussion while conceptualising the eCard. The Austrian parliament had to introduce two new laws in order to create the legally needed ground for the eCard concept. The new laws were designed accordingly to the Austrian egovernment Strategy. The Austrian egovernment Strategy defines how to use privacy enhanced data modelling solution, consisting of (Otter 2005b):

- ZMR: Citizen‘s Identification Number (supplied by „Residents Register“)
- SZ: Base Identification Number (derived by strong encryption of ZMR, identifies each person registered in Austria uniquely)
- BKZ: Sector Specific Identifier (identifies different Applications of E-Government)
- bPK: Sector Specific Personal Identifier (cryptographic derivation out of „SZ & BKZ“)

This data model assures that people can not be tracked by looking for one unique identifier in all data bases. It shall be noted that the Austrian eID solution called “Bürgerkarte” works with the same principle and the signatures of these two systems are fully interoperable.



How critical is the issue of interoperability of IMS for this field?

Mr. Otter categorised interoperability as of high importance to any ehealth project especially in Europe. The Lisbon convent, Europe 2000, Europe 2005 etc. all define interoperable social security systems coupled with an interoperable identification system as a major goal in the public health care sector.

The eCard is fully interoperable with E111 and the NETC@RD Project. However, Mr. Otter stated that this would only be the minimum case of achieved interoperability.

For the Olympic games in Athens several countries (Austria was one of it) equipped its athletes with electronic cards which held biometric information such as blood group on it and which would also inform the doctor or the hospital if and to what extend the patient would be insured.

As mentioned before the eCard is fully interoperable with the Austrian "Bürgerkarte".

How would you define interoperability of IMS? What is an interoperable IMS in terms of the chosen field? What would interoperability enable?

Interoperability of IMS is the ability to exchange information on identities correctly in a syntactical way by means of technical integration with the goal of authentication and identification of physical and legal entities across different systems.

An interoperable eCard system in the healthcare sector provides the citizen with a solution to visit any doctor or hospital of choice. The citizen is able to prove easily by using his/her card his/her identity and insurance status. The doctor or hospital than holds an electronic identity information of the patient and they can communicate electronically with over 23 different social security offices claiming payment for treating the patient. The patient can grant the medical staff access to certain parts of his/her medical history and other further information saved in a central database.

Interoperability is enabled by a technical solution, requires certain laws to be lawful and probably most important needs the acceptance of the user to work with the system accordingly.

Can you describe in more detail a system (even if hypothetical) that meets your interoperability requirements?

European Level

The next step is to have an interoperable eCard (ehealth) system on a European level. The NETC@RD Project is a first step into that direction in the first phase is planned to be working by 2008. Mr. Otter would regard a system which grants a correctly insured Austrian citizen medical treatment in all EU25 states by simply providing his/her eCard and the logistical/administrative back office system behind the cards is ensuring correct payment as a great achievement of an interoperable European ehealth system.

Next steps in Austria

In Austria a future interoperable scenario would be that any citizen will authenticate themself with any partner chip card such as a bank card at the hospital and doctor and no further paper work is needed. This should be possible by the end of 2006.

Emergency Information

An ever intense discussion and still far from solving is the question whether so called emergency data should be easily access able on eCard solutions or not. Standards for reading this emergency data on national as well as the European level would be needed. What is emergency data? If an insured person is found the question remains - is the eCard in his/her wallet the correct card? Which further tests have to be made due to legal requirements (i.e. in Austria a blood type test has always to be undertaken before giving the patient blood transfers).

Mr. Otter added that in his point of view emergency data is information which prevents emergencies in the first place. He recommends that information on allergies, current medication, etc. should be saved on the eCard so imitate treatment would be less risky and the information would still not be very critical in terms of privacy issues.

How far are we currently from that scenario?

Although the NETC@RD project schedules a first working solution by 2008 many things have still to be done. Europe still needs to agree on clear “exchange tables” of its national citizens registers. A standard for these “exchange tables” still has to be developed.

In the domain of electronic signature many countries still struggle. I.e. Germany still does not have a Bridge CA yet.

What are the requirements for interoperability for the USERS?

In Austria the eCard holder needs the physical token (eCrad) and a PIN. Further the user needs to have trust in the system and has to be educated how to use the new system. This is especially important with citizens which according to the digital device theory are not familiar with any of these new card systems. Only, if it is granted that groups like elderly, handicapped people, etc. have full access to the new system the solution is socially interoperable. In addition the citizen needs to see a clear added value of the new system otherwise he/she might reject using it.

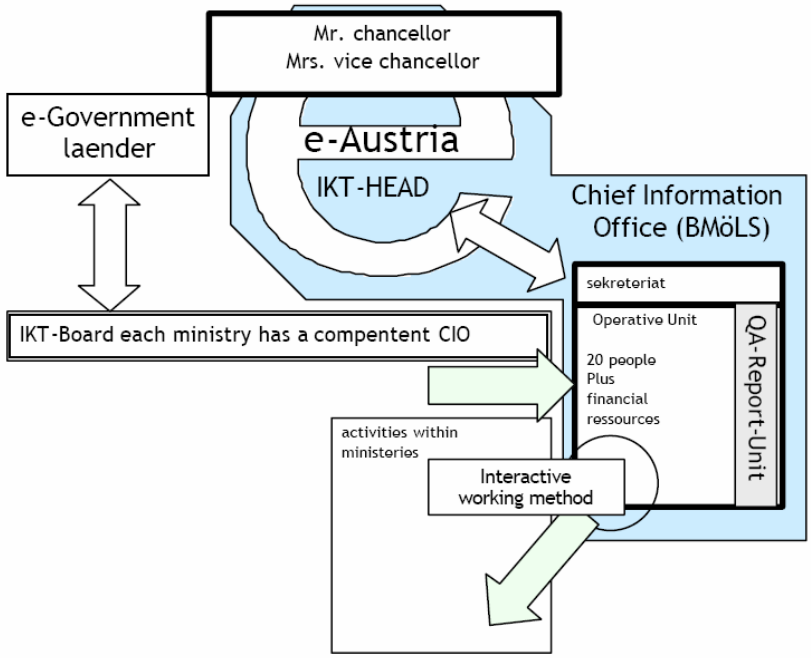
In a second phase the user might need a card reader and home PC equipment in order to communicate with government agencies. Austria’s egovernment Strategy foresees one point user contact strategy. The user than leaves his/her request at this point and the request is correctly distributed to the right government agency.

What are the requirements for interoperability for the GOVERNMENTS?

Mr. Otter is convinced that the government sector is usually the most difficult terrain in terms of achieving interoperability. Any egovernment concept has multiple stakeholders, a great number of regulations and usually a strong resistance against change. egovernment projects require by definition new working processes – electronic ones. Most likely these new processes have a heavy impact on the

"government users". While ISM project managers try to communicate openly to the end-user, ISM project managers often neglect the users inside the government agencies.

Austria formed a small but well equipped task force of experts, who are responsible for coordinating high stake egovernment projects. – The IKT Board – A strategy for egovernment and Information Technology. On the basis of agreement of the ministers on June 6th 2001 Austria has established a strategic office for the co-ordination of information and communication technologies. This office within the Ministry for Public Services and Sports reports directly to the Federal Chancellor and the Vice Chancellor. The IKT Board (Information and Communications Technology Board) incorporates a competent representative of each ministry so that it can build strategies and make decisions that are relevant for the entities of the federal government (ICA 35th Conference Report 2001).



The activities of the board focus on matters that concern more than a single ministry or have strategic relevance. The slim organisation allows for efficient operation. The board and the operative unit have been in operation since August 2001.

What are the requirements for interoperability for the MERCHANTS?

Every doctor and hospital in Austria will be equipped with a so called "Medical Practice Unit" (MPU). In a first phase over 12,000 of these readers will be installed. The MPU consists of software client and a card reader. One of the benefits of the new solution is the ability of electronic accounting of physicians which has been settled by law since January 1st 2003. Physicians need to gain expertise how to use the new solution and medical staff in general has to be training in using the new system accordingly.

In general it shall be noted that users (citizens) will use IMS 2-3 times a year. Merchants and government users will work on a daily basis and they are therefore

key- or so called heavy-user which require special attention. Mr. Otter pointed out that the city of Bremen in Germany is regarded as a best practise example in terms of egovernment projects and its communication strategies towards its stakeholders.

What are the benefits of interoperability for each of these stakeholders?

Citizens

Firstly, the citizens can use the services for which an electronic signature is required. These signatures are fully supported in Austria and will be widely supported on a European level. Secondly, the citizens do not require taking a health insurance voucher with them when visiting the doctor or hospital.

Social Security Offices

The 22 Austrian social security offices will receive payment requests for treating their member patients electronically. The physicians gain the ability doing the accounting fully electronically.

In general the work and communication process between practitioners, insurance companies and government agencies will be less paper based, faster, most likely simpler and as a result cheaper and more accurate.

What is hindering the establishment of interoperability at the technical, legal and cultural levels?

Technical

The lack of technical standards in regards to the translation process of national citizen register among EU 25 member states as well as a missing EU Root CA hinders an advanced level of Pan European interoperability.

An other often overlooked issue in regards to European wide ehealth solutions is the fact that each country has a different understanding how to treat certain illnesses, what kind of medication to give the patient, what types of illnesses to regard as serious or minor, etc. In other words the medical technical level and even basic understandings are fundamentally different and often this is strongly interlinked to cultural backgrounds. The medical profession has grown over hundred of years and to achieve overall agreement on a medical-technical-cultural level will be most likely impossible.

Legal

Most of the current regulations and laws in Austria are written and thought through from a paper based working process. Over the years the stakeholders developed working processes which solve the goal but might not always be 100 percent lawful. These working processes are often more advanced and more efficient. However, if you design the electronic processes of systems such as the eCard the developers have to act accordingly to the law and as a result the “newly” designed system might use “old” and inefficient working processes. As a result the new electronic working processes might be a step backwards.

Mr. Otter explained that one of the hottest topics discussed in the media and the political arena was the level of information which would be access able using the

eCard and PIN. These privacy issues increase if you think of a European wide IMS solution. Privacy issues are most likely one of the biggest challenge creating a pan European ehealth solution.

Cultural

These above issues often have social implications such as that the physicians find the new working processes more complicated than the old ones and sometimes the new system is indeed less simple and efficient than the old one.

Mr. Otter described the instance where the Austrian Medical Association vetoed the eCard solution until the board of the 22 social security offices agreed on not to insist that the patient has to use the eCard every time he/she sees a doctor. Now the patient only has to put his/her eCard into the card reader once a quarter although the patient has to show his/her eCard at each visit. It is believed that the doctors were too afraid that the social security offices would know exactly how often the patient visited the doctor and that might lead to financial losses for doctors.

On the user level trust is a big issue. Citizens might not trust the newly developed IMS and therefore reject to cooperate or boycott the system.

What can be done at the TECHNOLOGICAL level to establish interoperability?

Mr. Otter suggests the development of further standards. Specifically to agree on a clear "exchange tables" of the EU's national citizens registers.

What can be done at the LEGAL/POLICY level to establish interoperability?

The NETC@RD Project is a first step towards a European wide interoperable ehealth solution. However, further similar projects are needed. At the moment the EU health care division is a sub division of the Social Security Department. Mr. Otter suggested organising it the other way around. The current situation put too much weight and emphasis on getting a harmonised European wide pension system rather than an enhanced health care system.

What can be done at the CULTURAL/INSTITUTIONAL level to establish interoperability?

Sometimes politician and companies who have successfully developed an ehealth solution in one country dream of "selling" their solution to other countries. This will never work successfully. It is possible to learn from mistakes others did but Mr. Otter is convinced that it is not possible to transfer systems. I.e. Germany has over 320 social security offices, Austria 22, in the Spanish health care systems doctors are employed by the government in most other EU countries doctors are entrepreneurs.

A too high European interoperability might limit and even hinder the development of national ehealth solutions. Therefore it is of extreme importance to find the right balance of interoperability, added value and unnecessary burdens which might result in an even greater complexity of solution, high costs and less efficiency.

Interoperability should also be viewed with different lenses in regards to the domain of law, processes, logistic and payment.

Can you rate in terms of importance the three factors: technological, legal/policy and cultural/institutional? Discuss their prioritisation.

Mr. Otter believes that the cultural/institutional level is the hardest to achieve and the technological most likely the easiest one. He compared the eCard project with the introduction of ATM machines (Mr. Otter was project leader of the launch in Austria). Only 3-4 years after the first installation of an ATM, the concept of getting money by using a bankcard and a PIN was explained in Austrian school books and thought in primary schools. This kind of PR is of extreme importance to make a sophisticated and completely new system widely accepted among the public.

What should be the role of governments in addressing interoperability of IMS?

The first eCard project (1997-1999) became abandoned mainly due to disagreement among the stakeholders and the inability working together. The whole process was restarted after a basic agreement among the key stakeholders was achieved on clear goals of the eCard. After having the IKT-Board in place the communication and getting things done among the stakeholders become much easier and more efficient.

The government plays a central role in a project such as the eCard. On organisation like the IKT-Board is responsible for a clear and precise project management. A political "order" is needed, needed laws have to be passed and all stakeholders should be represented. However, the project management should be separated from any political position as politicians tend to interfere the working progress which is often counter productive.

The IKT-Board has experts from all significant stakeholders. It is political independent but at the same time enjoys the political and financial commitment of the government. In regards to the eCard the experts of the IKT-Board meet every 14 days and coordinate further development among the stakeholders.

What should be the role of merchants and industry groups?

As described before Mr. Otter believes interoperability on the medical level is far less developed than interoperability of social security office networks. Primarily the industry groups like Medical Association and insurance companies are able to develop the medical level further.

Specifically in regards to the eCard one of the most powerful stakeholders was the Austrian Medical Association. Without their support any development of a new system would be useless. They feared that the eCard would give the Social Security Offices access the doctors' surgeries.

Mr. Otter described that one of the biggest challenge from the point of view of the Austrian Medical Association was to achieve interoperability on the medical level. Even though Austria is a rather small country, different groups (old fashioned doctors, newly oriented doctors, lawyers etc.) had often an extreme divergent view on how the relationship between doctors, patient and insurance companies should look like. Subsequently these different believes had great impacts on the interoperability issues of the eCard.

In order to give an answer to the question it should be said that the industry groups like the Austrian Medical Association are the main stakeholder in developing a vision how a eCard system should look like in order to grant the best doctor-patient relationship possible. This discussion naturally involves a heavy dialogue on privacy issues and interoperability.

One other aspect is the discussion around the emergency information saved on ehealth solutions. This discussion should be addressed primarily from a medical/privacy perspective rather than from a political one and therefore it should be discussed by non-government stakeholders.

Can anything be done at the level of users/consumers/citizens to foster interoperability of such systems?

Mr. Otter recommends awareness and education program how to use the eCard especially for fringe groups. Overall it is important to build confidence in the system. If the Austrian and similar European ehealth projects work successfully other European countries will follow and might join projects like NETC@RD which foster interoperability. It is better to work in an environment of consumer demand rather than pushing a new system into place.

Any other comments?

Mr. Otter stressed that high interoperability might also restrict the national service offering possibilities of European countries as "the least common denominator" might not allow sophisticated national developments due to primarily legal and technical restriction.

References

ICA 35th Conference Report (2001) in *ICA 35th CONFERENCE* Berlin.
Otter, H. (2005a) *Requirements for Interoperability in Ims at the Example of Austria's Ecard* 30.06.2005. (Personal communication).
Otter, H. (2005b) in *Managing Identity*German Embassy Info Center.