FIDIS

Future of Identity in the Information Society

Title:	"D4.1: Structured account of approaches on interoperability"
Author:	WP4
Editors:	James Backhouse (LSE)
Reviewers:	Mireille Hildebrandt (VUB) Ioannis Maghiros, JRC
Identifier:	D4.1
Type:	[Deliverable]
Version:	1.0
Date:	Tuesday, 12 July 2005
Status:	[Final]
Class:	[Public]
File:	fidis-wp4-del4.1.account interoperability.doc

Summary

The question of interoperability in respect of identity and identity management systems is one of growing concern. On the one hand there are many situations where being able to cross-match identity information about citizens and consumers would be of enormous benefit to them. On the other hand, without the appropriate control in the hands of the data subjects, interoperability could be another weapon in the hands of the surveillance society, unwelcome in a world where privacy is still valued. This report prepares the ground for a continuing study into interoperability in this area. It proposes a three-level framework for assessment and study bringing together perspectives as diverse as technical, legal and socio-cultural. A review of current and recent projects and literature on the topic is presented, with ratings for papers for their concerns in respect of the three different perspectives. The work has produced a bibliographic database of the most relevant literature available on the FIDIS web site. There follows a number of case-study type contributions on different applications of identity management systems including credentials systems, driving licences, European passports and government to consumer applications. A review of the interoperability issues in identity management in Ambient Intelligence contexts concludes that this matter will be an important one for determining how this technology will be shaped in the information society that is emerging.

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	25.03.05	• Initial release based on discussion at the March Workshop (John Baptista)
0.2	12.04.05	• Integration contributions from Andrew Wallwork (Ch 4), Stephan Freh and Paolo Spagnoletti (Ch 10)
0.3	22.04.05	• Integration contributions from Martin Meints and Martin Rost (Ch 6), Sandra Steinbrecher (Ch 7) Sabine Delaitre and Ioannis Maghiros (Ch 8) Michaël Vanfleteren and Els Kindt (Ch 9) Mark Gasson, Wim Schreurs (Ch 11)
0.4	16.05.05	• Revision of structure, flow and consistency (James Backhouse). Request for feedback to all partners
0.5	07.06.05	• Integration of final comments from all partners
0.6	14.06.05	• Final revisions and editing (James Backhouse). Draft sent to reviewers
0.7	22.06.05	• Integration of reviewers comments: Mireille Hildebrandt (VUB)
0.8	24.06.05	• Incorporated partners feedback to reviewers comments (John Baptista) • Final editorial revisions (Paolo Spagnoletti)
0.9	30.06.05	• Final version (James Backhouse)
1.0	01.07.05	• Post editing

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
Chapter 4 Database of papers and projects	John Baptista, Paolo Spagnoletti, Andrew Wallwork, Stephan Freh, LSE
Chapter 5 Understanding interoperability	Andrew Wallwork and John Baptista, LSE
Chapter 6 Social aspects of interoperability in identity management	Martin Meints and Martin Rost, ICPP
Chapter 7 Identity and the inherent problem of interoperability	Sandra Steinbrecher, TUD
Chapter 8 Identification and authentication in C2G digital interactions	Sabine Delaitre and Ioannis Maghiros, JRC
Chapter 9 Use of credentials systems in e-commerce	Michaël Vanfleteren and Els Kindt, K.U.Leuven R&D
Chapter 10 Case study: eID projects review, from capability to use	Paolo Spagnoletti and Stephan Freh, LSE
Chapter 11 Case study: the interoperable future of AmI Environments	Mark Gasson, Reading; Wim Schreurs, VUB; Sabine Delaitre, IPTS

Summary of Contributors:

- LSE: James Backhouse, John Baptista, Andrew Walwork and Stephan Freh
- LUISS/LSE: Paolo Spagnoletti
- K.U.Leuven R&D: Michaël Vanfleteren and Els Kindt
- ICPP: Martin Meints and Martin Rost
- Reading: Mark Gasson
- TUD: Sandra Steinbrecher
- JRC: Sabine Delaitre and Ioannis Maghiros
- VUB: Wim Schreurs

Table of contents

1 Executive Summary

James Backhouse, LSE

Interoperability is a term that only recently crept into our consciousness and as yet finds few entries in dictionaries and books of reference. However the advance of the information society has forced citizens, businesses, governments and consumers all to come to grips with this neologism. Information systems began as stand-alone systems, but with networking and improving telecommunications they rapidly encountered the need to link with other systems, such as databases, security systems, and archives. Hence the current drive to achieve the benefits of interoperability. Linking up with other repositories greatly adds to the value of the information already held. This report marks the first output from the FIDIS Network of Excellence on this important topic.

This report presents the three layer framework for analysing information systems that contains technical, formal and informal elements and argues for its use in this first FIDIS examination of interoperability issues. This threefold perspective is referred to constantly throughout the remainder of the document and functions as a strong logical thread conferring both coherence and integrity to the variety of contributions that follow.

The contributions that comprise the report can be divided into those on the one hand that search for concepts and formative notions for interoperability - reviewing the pre-existing and ongoing work in interoperability of identity and identity management systems (IMS) - or reflecting on social aspects of interoperation, and those on the other hand that examine current examples of such systems in a variety of administrative contexts, including e-commerce and e-government, as well as the more futuristic context of Ambient Intelligence (AmI).

Overall, the aim of this report is to set out the stall for the activity of Workpackage 4, testing the ground that will be covered in terms of the practical applications, such as credentials systems and e-commerce, as well as the intellectual terrain that will be worked over from the different disciplinary perspectives. The contributions derive from work in social science, privacy protection, computer science, law and law enforcement, public administration, to name just some, and this report acts as an early marker showing how such disparateness may nevertheless be a source of strength and rendered coherent through the development of a common framework and integrative themes.

A key element in this deliverable is the construction of the bibliographic database including the most relevant 100 papers on the topics of “interoperability” and “identity” that were found. These papers are rated for their relevance in regards of their technical, legal and formal or social and cultural perspective. They form a vital resource for all the FIDIS researchers who are studying IMS from different disciplinary outlooks, all of which have a critical bearing on the possibilities for interoperation. This common resource should aid FIDIS efforts in preparing the ground for the benefits of interoperability while ensuring that privacy protection rests in the hands of every citizen.

2 Introduction

James Backhouse, LSE

Workpackage 4 is the part of the FIDIS Network of Excellence that deals with issues of interoperability of identities and IMS. When using identities as a means of controlling access to ever-larger online and public information systems, especially e-government and e-business systems, the issue of interoperability is a crucial one. In the context of the aims of the European Union and the desire to align and integrate the systems of electronic public administration and health, to support the mobility of European citizens and their equal treatment no matter which country they may migrate to for work or for pleasure, the goal of interoperability presents an exciting and vital challenge.

This Workpackage has the goal of studying the factors that can aid the interoperation of identity systems and has close links with other Workpackages. Think for example of law enforcement agencies throughout Europe that may be tackling crime and terrorism, or public health bodies that, in some emergency, need to access vital medical data on their respective subjects who are temporarily resident in other European countries, or, again, public administrations that need to coordinate the payment of pensions that derive from different periods of employment in various European countries, to be paid in yet another country. To even reach first base on interoperation, there needs to be some basic agreement about underlying terminology regarding identity management and hence Workpackage 2 is one that has close connections with this one, and our researchers have contributed to it. Workpackage 3 on Hi-Tech IDs with its focus on PKI and biometrics also raises interoperability issues. Especially relevant is the need for IMS to be able to authenticate using identity information already verified in third party systems, such as already happens with paper-based passport systems. WP5 with its interest in identity theft and privacy, also has reflections for interoperability. One aspect of interoperability is the perception by the agents operating the systems that the same guarantees and protection of personal information prevails in the other systems with which co-working is being proposed. By contrast, there may be issues of deliberately wishing to deny interoperability in order to protect identities from theft. Profiling (Workpackage 7) will require IMS to be interoperable where the data being mined is drawn from many different systems, as might happen in law enforcement or electronic medicine.

This deliverable 4.1 is intended as the starting point for the study of interoperability and reviews work being undertaken in research and implementation projects in the area, both in Europe and beyond, where issues of identity management and interoperation are critical. Further, it integrates work from FIDIS contributors in different aspects of this same agenda and highlights the many-sided nature of the issue. An overarching framework spanning technical, formal and informal meta-concepts is introduced and adopted as a perspective through which the many aspects of interoperability may be examined in a coherent fashion. It is hoped that the framework acts as a unifying mechanism across the disciplines.

This deliverable contains, *inter alia*, a literature review of papers deemed to fall within the subject and a review of ongoing projects, especially EU-funded ones, that

do likewise. It has produced a database of key papers on interoperability, rating each one for relevance in terms of the underlying meta-concepts of technical, formal and informal focus. Further, the deliverable presents work from FIDIS partners on a variety of systems that all touch on aspects of interoperability, including G2C interactions - , drivers' licenses, passports, the introduction of e-IDs across Europe, Ambient technology and its link with identity systems and its requirement for interoperability.

In the next section (Chapter 3), we present the result of our literature review in the form of the database of papers and projects which is now available to all FIDIS members in the internal website[1]. This research tool has helped in the writing of this document. We also present a review of key EU interoperability projects and review two databases of EU funded projects: CORDIS and eTEN (more information in next chapter).

In Section 4, we discuss the concept of interoperability, aiming to develop a common understanding of this topic. We analyse interoperability in three levels: technical, formal and informal. We then apply this conceptualisation in analysing key eID projects in Europe.

Section 5 discusses in detail the social dimension of interoperability in IMS. Section 6 analyses how the issue of interoperability is inherent to IMS and unfolds the complexity in this domain. In the next chapter Section 7, we analyse the complexity of identity management in Government-to-Citizen relationships. We then in Section 8 discuss interoperability in the context of the use of credentials in e-commerce. Sections 9 and 10 present two case studies. The first looks at electronic ID systems and the second at AmI environments and a future scenario of total interoperability. The last chapter (chapter 11) presents the overall conclusions to this deliverable.

[1] Available in the internal FIDIS website in the FileManager option within WP4 area. See http://internal.fidis.net/143.0.html?&mountpoint=12

3 Database of papers and projects

John Baptista, Paolo Spagnoletti, Andrew Wallwork, Stephan Freh, LSE

A major component of this deliverable is the development of a database of papers and projects which support the writing of this deliverable. We started by collecting up to date literature on the topics of "interoperability" and "identity". We have selected the key 100 papers for these topics and have created a tool to help the FIDIS community in accessing important papers in this field.

In the first stage we selected keywords that we considered relevant. The following key terms were used "Interoperability", "interoperable/operate", "e-Government", "e-governance", "Identity", "Identity Management Systems" and "Semantics". We also used combinations of key words: e.g. "Interoperability" and "eGovernment". We then employed words with more broad scope combined with those above, including: "culture", "social", "society", "formal", "informal", "community", "collaboration", "cooperation", "compatibility", "legal", "framework" and "trust".

We used the main academic search engines such as SwetsWise, EBSCO, ingenta, IEEE, Synergy, SpringerLink, GoogleScholar, ScienceDirect, Emerald, ACM digital library.

We collected over 200 articles addressing issues of interoperability and identity. We then built an Excel database with all articles including authors, date, journal and abstract. In order to find the most relevant papers for the review of current literature we ranked each paper according to its relevance for "interoperability" and "identity".

Because there were three researchers involved in the ranking, each with different approaches, criteria for standardising the allocation of rates had to be developed. The researchers met in the first instance to mark papers and cross-check their choices. They then marked groups of papers and exchanged results for fine-tuning the standardisation process. In the last stage, all papers were double-marked to improve overall coherence of classifications.

Each paper was rated according to the following criteria:

- Relevance for interoperability: the degree to which the paper discusses the topic of interoperability regardless of the application domain;
- Relevance for identity: the degree to which the paper addresses important issues of IMS;
- The extent to which the paper focuses on each of the following dimensions of interoperability:
    - Technical: relates to the ability to interchange data, protocols, technical standardisation
    - Formal: relates to agreement at the policy level, existence of common rules and regulation
    - Informal: relates to socio-cultural understanding, ability to exchange meaning between domains

We then decided to focus on the most relevant 100 papers, discarding those which ranked lower on our scales. The final database includes the most relevant 100 papers on the topics of "interoperability" and "identity" that we found. Figure 1 presents a snapshot of this database.

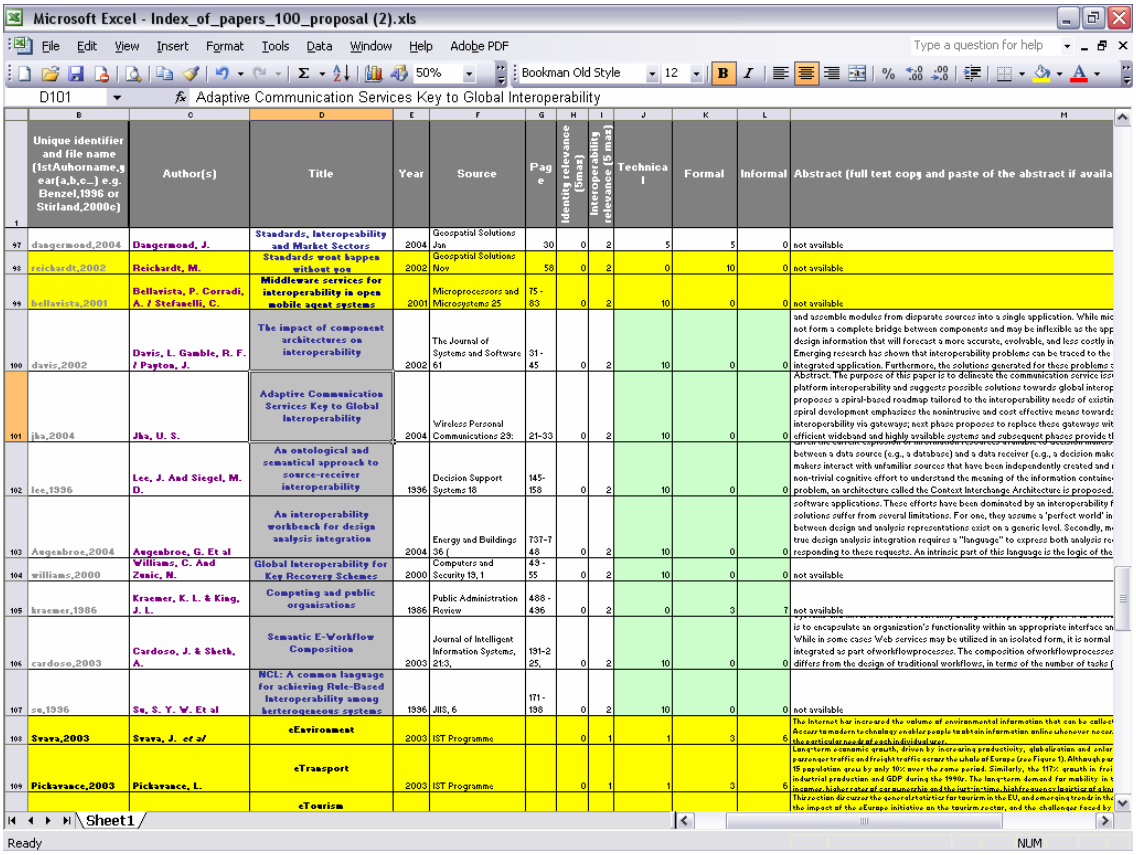

Figure 1: Database of papers and projects

We used this database as a basis for writing this document and as a starting point for WP4. We believe that this will offer a solid base to build up, over time, our work on this Workpackage. This database is in constant development and we encourage contributions. Please send any comments or articles to be included to james.backhouse@lse.ac.uk

In the next section, we present a brief summary of the papers we found most relevant according to the criteria described above.

3.1 Review of papers

We now present the top 10 papers scoring high on relevance in identity and interoperability, giving a brief summary of each.

	Identity	Interoperability	Technical	Formal	Informal
Kinder 2003	5	5	3	4	3
Ouksel,1999	0	5	4	4	2

Lee,1996	0	5	10	0	0
Chen,2003	0	5	4	4	2
Landsbergen,2001	1	5	1	3	6
Klischewski,2003	0	5	2	6	2
Hayat, 2004	5	3	4	4	2
eAuthentication,2004	4	4	3	3	4
Ringwald,2003	5	4	3	6	1
IDABC 2005	1	5	3	4	3

Table 1: Top 10 papers in the database

Kinder 2003 [42]
"Mrs Miller Moves House: the interoperability of Local Public Services in Europe"
Journal of European and Social Policy 13:2

In this article, Tony Kinder analyses the various dimensions of interoperability in public services in local administration. He uses a normal everyday life event as an example to discuss the various levels of interoperability. He presents the case of when Mrs Miller moved house and how seven local councils dealt with this situation. He concludes that the technical dimension of interoperability is only one dimension of the interoperability phenomenon and that other dimensions should be considered.

Ouksel,1999 [60]
Semantic Interoperability in Global Information Systems
SIGMOD Record: 28:1

Aris Ouksel and Amit Sheth present a framework for analysing interoperability which looks at the various dimensions of this phenomenon: Semantic, Structural, Syntactic and Systems Interoperability. They discuss the need for interoperability in the light of increased complexity and need to interlink systems.

Lee,1996 [48]
"An ontological and semantical approach to source-receiver Interoperability"
Decision Support Systems 18 145-158

Jacob Lee Michael D. Siegel present a strongly technical solution for interoperability, based on semantics and ontology approaches.

Chen,2003 [15]
"European initiatives to develop interoperability of enterprise applications—basic concepts, framework and roadmap"
Annual Reviews in Control 27

David Chen and Guy Doumeingts discuss FP6 EU projects on interoperability, such as IDEAS, INTEROP and ATHENA. They discuss interoperability at three levels: Business, Knowledge and ICT Systems. State-of-the-art and user requirements are presented.

Landsbergen,2001 [47]
"Realising the promise: Government Information Systems and the fourth generation of Information Technology"
Public Administration Review 61, 2 page 206 - 220

David Landsbergen and George Wolken argue that "Interoperability is more than digital plumbing". They argue that interoperability is about people talking and sharing information. They discuss the political, organisational and economical dimensions of interoperability. They discuss the willingness to share information and the need to establish proper dialogue prior to engaging in data interchange.

Klischewski,2003 [44]
"Top Down or Bottom Up? How to establish a common ground for semantic interoperability within e-government communities"
Working paper, Copenhagen Business School, Informatics Department

Ralph Klischewski thoroughly discusses the relationship between ontology and interoperability. Are semantic agreement and common worldviews required for the establishment of interoperability? He uses semantic web research on e-government research to discuss semantic interoperability.

Hayat, 2004 [27]
A-SIT 2004: Survey on EU's Electronic – ID Solutions

This document presents a survey on e-ID projects in EU countries. The authors discuss the need for identity systems in e-government and e-commerce.

eAuthentication, 2004 [13]
Towards an electronic ID for the European Citizen, a strategic vision

This is an EU document reporting the views from the participants of the Workshop on eAuthentication. It presents the state-of-the-art on electronic ID in Europe.

Ringwald,2003 [64]
Electronic Identity White Paper "eEurope smart cards / Trailblazer 1 'Public Identity'"
Information Society IST, European Community

This is an EU document discussing the interoperability of electronic IDs in Europe, providing a good review of smart cards and other technological advancements in electronic ID.

IDABC 2005 [30]
European Interoperability Framework

The IDABC is a key source of information on interoperability in Europe. The authors have developed the European Interoperability Framework which has the following mission statement: "The European Interoperability Framework defines a set of recommendations and guidelines for eGovernment services so that public administrations, enterprises and citizens can interact across borders, in a pan-European context."

3.2 Review of projects

Paolo Spagnoletti LSE

We have also researched projects that focus on interoperability. To date, we have focused on the European context only, but we plan to extend this research to other countries.

Several research projects on interoperability and identity have been financed through the EU's 5th and 6th Framework Programme in the context of Information Society Technologies (IST) actions. IST is a single, integrated research programme building on the convergence of information processing, communications and media technologies. IST has an approximate budget of 3.6 billion euro and is managed by the Information Society DG of the European Commission. IST Project Fact Sheets are stored in the RTD Projects database of CORDIS (http://www.cordis.lu/ist/projects/projects.htm) and projects can be browsed or searched using various criteria.

eTEN is another EU programme designed to help the deployment of telecommunication network-based services (e-services) with a trans-European dimension. This programme aims to accelerate the take-up of services in order to sustain the European social model of an inclusive, cohesive society. Its objectives lie at the very heart of the eEurope mission of "an information society for all". It promotes public interest services that give every citizen, enterprise and administration full opportunity to gain from the e-Society. The eTEN projects can be found in the eTEN database (http://europa.eu.int/information_society/activities/eten/cf/project/index.cfm).

3.2.1 Database overview

We now present some results obtained performing queries on the Cordis and the eTen databases using keywords related to interoperability and identity concepts. Figure 2 shows the number of projects for both topics in these databases:

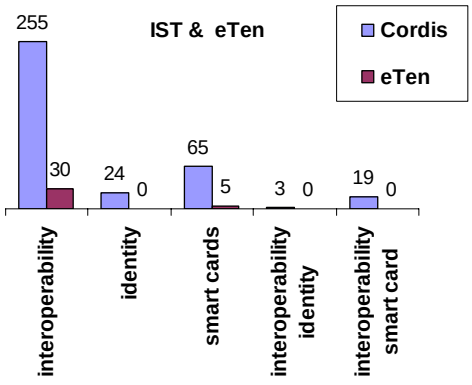

Figure 2: distribution of projects (1st March 2005)

As a first result, we can see that the number of projects related to "interoperability" is 285 from a total of 2915 projects in both databases. Therefore 10% of the overall number of projects in both databases is related to interoperability matters.

Second, grouping the Cordis database projects around the different strategic objectives in FP5 and FP6, we observe a shift in the area that includes the majority of interoperability-related projects. In FP5, more than 50% (75 projects from a total of 147) of financed projects are classified in the area of "Essential technologies and infrastructure", while in FP6 interoperability-related projects are less concentrated on a single strategic objective and 23% of the projects (9 out of 40) are in the "Networked businesses and governments" area.

This shift can be related to a change in the definition of the term "interoperability" as evidenced in the literature. During the life of FP5, the term interoperability was used to indicate the ability of systems to exchange data and the perspectives were more focused on technology and infrastructures, whereas in FP6 the holistic view of interoperability makes this concept horizontal and the focus is more on services than infrastructures.

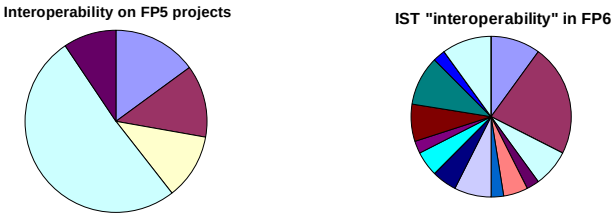

Figure 3: Data chart of interoperability projects for strategic objectives

3.2.2 Key EU interoperability projects

To complete this overview of the state of the art in EU research projects on the interoperability of identity, we briefly describe some of the projects that we chose from the Cordis and the eTen database. To find the latest information, we suggest that readers refer to the web pages of each project in the specific area. In this section, we present some of the projects, giving a brief introduction and then reporting the Fact Sheets information available on the database.

Issues relating to the interoperability of identity arise when the interoperability of technological systems, systems, processes and people have been addressed. Therefore we start this section by introducing two of the main EU projects related to interoperability: the ATHENA Integrated Project and the INTEROP NoE.

The ATHENA project aims to remove the barriers to interoperability between "networked organizations" and to transfer and apply research results in industrial sectors using a holistic perspective and a multi-disciplinary approach to address interoperability in respect of all layers of an enterprise (including ICT Systems, Knowledge, Business and Semantics). ATHENA will be a source of technical

inventions for interoperability and will also lead to prototypes, technical specifications, guidelines and best practices.

Another important EU project addressing interoperability is INTEROP NoE. This project aims to develop industrially significant new knowledge in order to interlink systems (information, production, decision support) of European Enterprises, including SMEs. It also aims to have strong interaction with Integrated Projects, such as ATHENA, in the same domain of interest.

When interoperability of services is achieved, new issues on identity management will need to be addressed. The PRIME Integrated Project aims to research, develop and evaluate solutions for privacy-enhancing identity management that focus on end-users, in order to reduce the risks to citizens' privacy in critical domains, such as mobility, health care and the exercise of democracy. Furthermore, the GUIDE Integrated Project is focused on creating a European conceptual framework for electronic identity management for eGovernment. Here the issue is to examine the growth of identity theft and the related massive security and economic consequences. GUIDE has a long-term vision to make Europe the global leader of eGovernment services by creating an open architecture for eGovernment authentication.

Two small projects are also mentioned in this section, the PISA FP5 project and the eTEN RISER project. The former is examining privacy-enhancing technologies that remove all unnecessary linkages to users' personally identifying information. Such agent-based technology can enable users, as consumers or citizens in e-commerce and e-government transactions and communications, to protect themselves against loss of information privacy. The latter is an example of a service that will improve the interoperability of secure cross-border exchange of sensitive personal data within Europe, offering the verification of address information as a seamless eGovernment service.

We now present a brief synopsis of the most relevant EU projects on interoperability:

ATHENA (Integrated Project IST FP6)
Advanced Technologies for interoperability of Heterogeneous Enterprise Networks and their Applications
http://www.athena-ip.org/
26.51 million euro

INTEROP (NoE IST FP6)
Interoperability Research for Networked Enterprises Applications and Software
http://interop-noe.org/INTEROP/presentation
18.19 million euro

PRIME (Integrated Project IST FP6)
Privacy and *Identity* Management for Europe
http://www.prime-project.eu.org/
13.14 million euro

GUIDE (Integrated Project IST FP6)
Creating a European Identity Management Architecture for eGovernment

http://istrg.som.surrey.ac.uk/projects/guide/
Project Cost: 12.47 million euro

PISA (IST FP5, completed)
Privacy Incorporated Software Agent: Building a privacy guardian for the electronic age.
http://pet-pisa.openspace.nl/pisa_org/pisa/index.html
3.26 million euro

RISER (eTen 2003)
Registry Information Service on European Residents
http://www.tssg.org/public/archives/RISERAbstract_english.pdf
1.8 million euro

In the next section we discuss the concept of interoperability by reviewing the existing literature. We also present a framework to support the analysis of projects and the development of requirements for achieving interoperability.

4 Understanding interoperability

Andrew Wallwork and John Baptista, LSE

"The shift from the total integrated approach to interoperability development is not only a technical change, but reflects organisational, economical and social trends/requirements of the society. To successfully tackle this very complex and highly detailed endeavour, it is necessary to develop research involving knowledge and competencies of all domains concerned."
Chen 2003 [15]

Establishing interoperable systems is a complex operation and goes far beyond the technical interconnectedness of databases and systems. Interoperability emerges from the need to communicate data across different domains for a specific purpose. Transferring the data may represent a technical challenge because of different protocols, standards, and so forth. However, the key challenge is with the purpose, use and changes consequent on transferring that data. Changes in data ownership and custodianship have an effect on power structures, roles and responsibilities and on risk. These issues go well beyond the technical dimension into the formal and social spheres. We discuss these different dimensions in this section. We will also strive to develop a holistic conceptual understanding of this phenomenon which can support the work of the FIDIS consortium.

4.1 Interoperability – to define, or not to define?

According to Harvey *et al* (1999) [28], it is broadly accepted that 'interoperability' has emerged as a new paradigm, which facilitates a more efficient use of information resources through the linkage of heterogeneous ICTs into synergistic units (1999: 213). Indeed, as far back as 1994, in Moen's research, interoperability and data sharing were considered to have evolved into critical features necessary to achieve standardisation given the development of international *"electronic networks [and] the electronic delivery of government information and services"* (Moen 1994: 368 [56]).

However, interoperability still lacks a dictionary definition. A thorough examination of relevant literature reveals a notable absence of a common definition for the term. Many (Lee & Siegel, 1996 [48]; Harvey *et al*, 1999 [28]; Ouksel & Sheth, 1999 [60]; Choi & Whinston, 2000 [16]; Brodeur *et al*, 2003 [9]; and Kinder, 2003 [42]) simply avoid offering a definition at all, and among the papers that do attempt to give a meaning, there is a surprisingly varied selection to choose from. In this chapter, we aim to develop a common understanding of this term in order to develop solid conceptual ground from which to build future work within FIDIS.

For Miller *et al* (2001)[54], (information) interoperability is, *"the ability of processes and systems to effectively exchange and use information services"* (2001: 259), although their study seeks to address the shortcomings of this definition. Moen (2000) [57] provides a similar but richer definition seeing it as *"the ability of different types of computers, networks, operating systems, and applications, to exchange*

information in a useful and meaningful manner" (2000: 129). These two offerings reflect perhaps a relatively technical perspective. This is understandable considering the historical context in which, ever since computerised networks began to support and interrelate more than one single unit of independent function, interoperability has been an important concern for systems development (Klischewski, 2003: 18) [44].

Woodall declares a technical level definition of interoperability as

> *"The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users"* (Woodall 2000: 310 [80]).

Woodall is motivated by the undeniable, exponential increase in system complexities and components, and their related coding and data processing requirements (Ibid). Thus, he puts interoperability into a technical context, which can be approached and hopefully resolved through technical and technological means.

In stark contrast, Landsbergen & Wolken (2001) [47] argue that interoperability is *"more than getting bits and bytes to flow properly"* (2001: 206). In their view, within an ICT environment, the fundamental goal of interoperability is to overcome the challenge of assimilating people and organisations and to encourage the sharing of information – it is *"people talking and sharing information"* (Ibid). Here we are presented with a much broader, holistic view of interoperation. Technology is certainly an essential element, but we can also start to envisage a sense of social interoperability.

In fact Miller *et al* [54] admit that interoperability can fail even if the associated processes are properly exchanging logical units of data. Could there even be confusion between compatibility and interoperability? To ensure against an overzealous technical bias, one approach might be to distinguish between the proper *exchange* (compatibility) of a service and the ability to *use* (interoperability) the service – *"compatibility is a requirement for interoperability but not a sufficiency"* (2001: 267). As will be illustrated later, meaning and semantics are decisive elements to help reconcile the interoperability challenge, and to further exemplify Miller's axiomic distinction, Mulley & Nelson (1999) [59] highlight *interconnectivity* as a term related to interoperability, yet similarly guard against complete assimilation, proposing that *"achieving interconnectivity is a necessary preliminary step towards interoperability"* (1999: 94) but it cannot complete the 'big picture'.

So, to define or not to define? Certainly, the over-concentration of technical bias in the literature suggests a reframing of the definition of interoperability. Perhaps the answer to the question is neither, and instead, a holistic *notion* of interoperability can serve as an umbrella, beneath which can exist many disparate but complementary definitions, according to perspective or layer of abstraction.

This section has tried to address the problem of first coming to a simple definition, or at least of negotiating one that is mutually acceptable. It points to semantic discordances and difficulties, that can be linked to a body of work concentrating on

semantic interoperability - a concept to which we will be return later. The next section will continue this line of thinking to illustrate that a purely technical lens limits the dynamics of the interoperability paradigm and it will be argued that government agency information policy makers *"must make this conceptual leap before any real progress in improving interoperability can take place"* (Landsbergen & Wolken, 2001: 212; *emphasis added [47]*).

4.2 Technical to Social and back again

> *"Technological systems are socially produced. Social production is culturally informed" (Castells, 2001: 36 [13]).*

Technology alone may appear *compatible*, and standards and policy may *enable* interoperability, yet there is some dynamic missing in this 'bigger picture' – people. Landsbergen & Wolken (2001) [47] hint at social interoperability in their definition and research, and requested additional *"support mechanisms to understand the range of economic, political, technical and organisational issues involved with information sharing"* (2001: 213).

Historically, we can find these elements in advice offered by Kraemer & King (1986) [46], relating to fundamental, innate problems of IT management within the environment of public administration. Crucially, we need to consider these elements in context and in *practice*:

> *"Computing fits within existing organisational life and exerts subtle influences. This does not mean, however, that computing is an activity that is easily managed. The challenge for public administration…is to focus on the actual experiences of computing technology as guides for how best to channel its use"* (Kraemer and King, 1986: 494 [46]).

Choi & Whinston (2000) [16] are supportive of this 'bigger picture' in their research, firstly by stressing, "Technological standards at the infrastructure level are relatively easier to reach than those at the applications and business process levels" (2000: 38). Of course, they do not suggest technical-formal elements are trivial or easy; they are merely easier than those at the applications and business process levels. Moreover, they continue describing culture and practical differences as contributing to some of the many pitfalls to establishing standards in the application layer and ultimately to ensuring interoperability (2000: 40).

The failure of interoperability projects has not been confined to the technical realm, but to political – informal – friction among public agencies (Ibid). Undeniably, as Homburg & Bekkers [29] note, "e-Government initiatives can be characterised as political" (2002: 8).

In the following section, we propose a framework comprising Technical, Formal (policy and standards), and Informal (TFI) notions to engender a holistic

understanding of interoperability[2] functions and as a useful tool for analysing EU interoperability projects, providing a direction for future research and practice.

4.3 Using the TFI model to understand interoperability

The following framework will help to fulfil the interrelationship between abstracted layers of interoperability leading ultimately to conclude that *technical requires formal and formal requires informal*[3]. Stamper *et al*[4] *[69]*, succinctly illustrate this interrelation of abstracted layers explaining that,

> "*Informal* norms are fundamental, because *formal* norms can only operate by virtue of the informal norms needed to interpret them, while technical norms can play no role…unless embedded within a system of formal norm." (2000: 19).

Metaphorically, this can be viewed as a 'Russian doll' effect, where the *informal* is the outer shell containing the *formal*, which in turn contains the *technical*. Inside out, the technical cannot be removed from the toy without consideration for (unwrapping) the outer layers:

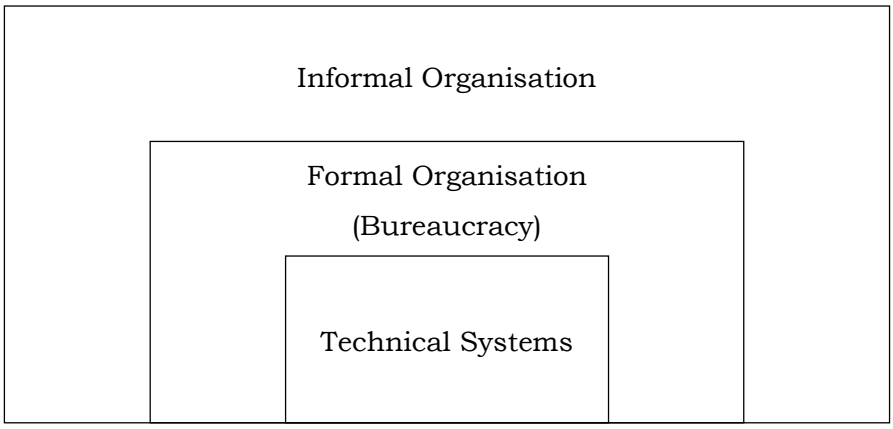

Figure 4: The embedding of computer systems in the formal and informal organisation (Stamper et al, 2000:19)

Relating abstracted norms to the dynamics of interoperability assumes the capacity to infer an affiliation between the two. The line of thought supporting this deduction is as follows: if "norms and signs are inseparable" and interoperability is "people talking and sharing information" (Stamper *et al*, 2000: 22), then signs – i.e. semiotics, "the study of signs, signals and symbols, *esp.* in language and communication" (Chambers Dictionary, 1999) – provides the link in the chain connecting norms and interoperability.

[2] The TFI Framework refers to continuing (2005) research conducted within the Information Systems Department of the London School of Economics. The framework draws from other research, including Stamper (2000).

[3] Thank you to one of the reviewers who pointed out that the relation between the three levels is not unilinear nor unidirectional. For example, law demonstrates that it is possible to create and implement formal rules that do not relate to informal rules, depending on prosecuting transgressions.

[4] This supportive evidence assumes the capacity to relate deductively their research on signs and social norms within an organisation to a holistic notion of interoperability (which is inescapably social).

Much interoperability literature explores 'semantic interoperability', whereby semantics is defined as "the area of linguistics dealing with symbols (*comput*) – (loosely) differences in, and shades of, meaning *esp.* of words" (Chambers Dictionary, 1999). Hence semantics can refer simply to computer linguistics, or to linguistics of words that make up standards and policy, or could even *infer* an approach to treat "meaning as a relationship between signs and human behaviour" (Stamper *et al*, 2000: 23).

Chen & Doumeingts (2003) [15] postulate that semantics runs through all layers of an organisation, and so, the adapted Figure 5 below suggests that a similarity exists between the three 'layers of interoperability' and the TFI framework. Chen & Doumeingts' model incorporates semantics across the three layers in a similar way to the TFI. Additionally, the three building blocks on the left might be seen to reflect the abstracted domains of the TFI, as suggested in italic brackets.

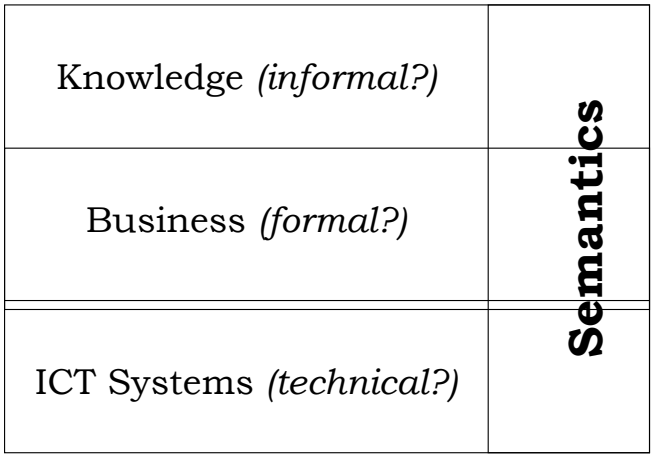

Figure 5: Adapted framework showing 'interoperability on all layers of and enterprise' (Chen & Doumeingts 2003:154)

Consistent with general interoperability research discussed above, much of the literature on semantic interoperability focuses on the technical domain (Harvey *et al*, 1999: 228 [28]). One such protagonist - Sheth (1996) [71] - approached semantic differences with an engineering orientation, working on the concept of semantic proximity, demanding *"declarative language to articulate definitions of objects, and very strong ontological definitions"* (Ibid). Yet by 1997, working with Oeksel, an approach is taken to support a more general notion of semantics transpired, which relates the *"content and representation of information resources to entities and concepts in the real world"* (Beech 1997 [7]; Meersman 1997 [54]; Sheth 1997 [72]). That is, *"the limited forms of operational and axiomatic semantics of a particular representational or language framework are not sufficient"* (Ibid).

For Bunge (1974), semantics is "concerned not only with linguistic items, but also, and primarily, with the constructs such items stand for and their eventual relation to the real world" (*in* Lee & Siegel, 1996: 151 [48]). Accordingly, this gives credence to the proposition of a TFI framework *incorporating* the addition of cross-sectional semantics (see Figure 6). Thus, uniting the findings from Stamper *et al* (2000) [69]

and Chen & Doumeingts (2003) [15] with current research at the London School of Economics conducted using a TFI model applied to interoperability, a potentially useful 'tool for thinking' materializes, see Figure 6 bellow:

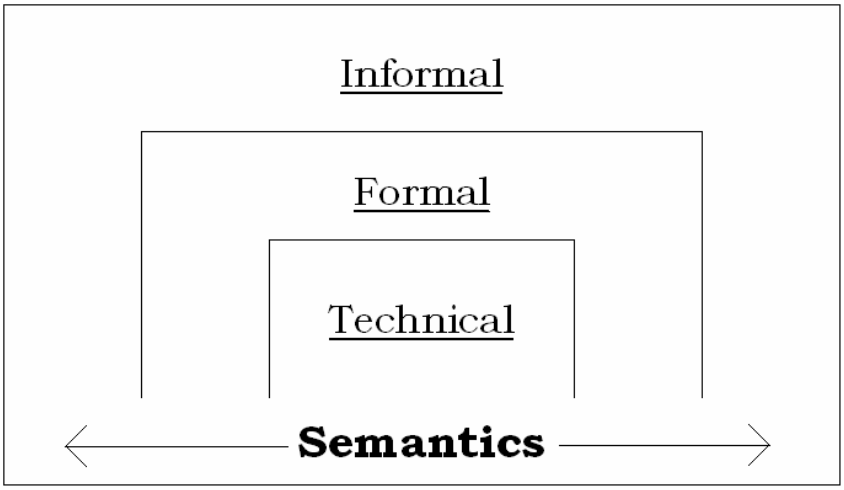

Figure 6: Adapted TFI framework to include the dynamics of semantics

Metaphorically, this diagram can offer further value to incorporate the potential for 'seepage' between the different domains of the TFI. This embodies the impossibility of navigating differences in meaning to ensure absolute conformity, if this is possible, between disparate and dispersed social groups. A complex interoperability project may resemble more of melting pot than an assemblage of distinguishable layers of abstracted meaning. Furthermore, individuals construct different parameters according to their internal biases, norms and assumptions, and continually translate and interpret associated meanings – solidifying the argument for the presence of semantics at each level of the TFI.

Evidently, the scope of the interoperability literature is vast, with its range of contrasting theories, frameworks and conceptualisations. In the next section, we present a framework debate based on the dichotomous approaches of 'bottom up' or 'top down' interoperability.

4.4 'Bottom-Up' versus 'Top-Down' in interoperability development

A *'Top-down'* approach argues that at the peak of a hierarchy, a powerful administrative body "prescribes the interoperability methods and resources to be applied by all actors on lower levels" (Klischewski, 2003: 22 [44]). In contrast, a *'Bottom-Up'* approach suggests that at the base of the hierarchy, administrative bodies propose and "share interoperability methods and resources from their point of view; centralised prescription is only accepted where there is consensus on all lower levels" (Ibid).

There is no agreement on how interoperability should emerge. Stamper *et al* hint at the failure of a top-down approach, pointing out that often "*technical experts are called in to interpret [the] formal layer with extra expense and a fair chance of*

misinterpretation" (2000: 19), i.e. the Russian doll effect; '*technical requires formal, formal requires informal'*. Experience confirms

> "that standardisation and the adoption of standards are very difficult processes, even…where the subject matter [appears] clear-cut and of limited complexity…Social issues make things complicated" (Klischewski, 2003: 23).

In which case does Kinder's (2003) [42] proposal convey more verisimilitude?

> "Big system, top-down approaches to interoperability are much more likely to fail than planned incremental bottom-up change" (2003: 154).

Especially in relation to web technology, most standardisation efforts assume an open process. This enables community members to contribute their specifications and requirements, within the network, to an accepted interoperability solution. For example, "local administrations publish their service interface using bilateral or mutual service to reconcile the technical, syntactic and semantic differences as much as possible" (Klischewski, 2003: 23). In essence, this represents a 'bottom-up' approach to interoperability (Ibid).

However, despite being useful conceptualisations encouraging two very opposing perspectives on interoperability, when taken alone, neither methodology can succeed, particularly when considering the e-Government community of Europe. For sure, 'top-down' is a useful conception, as we must have some sort of foundation (Stamper *et* al, 2000: 20), but often top-down standardisation efforts have been "countered by mistrust and ignorance from the local level" (Klischewski, 2003: 23), whereas "grass-root [bottom-up] initiatives mostly failed to reach the impact they had hoped for" (Ibid). Consequently, to accomplish interoperability Klischewski proposes to combine,

> "the more technical 'top down' approach to ensure that agents of other system components make sense of the resources encountered, as well as the social network orientated 'bottom up' approach to ensure that semantics processed in the systems effectively relate to the world view of the local actors in charge" (Klischewski, 2003: 24).

From this last quote from Klischewski (2003), one can begin to see overlapping and quite striking similarities between the TFI model and Semantics. Technical, Social (informal) and Semantics are all incorporated and - despite lacking a direct reference - the 'Formal'[5] element of the TFI is necessarily implied in the framework's consideration for standards and standardisation.

[5] For clarification, the formal level is here represented as law with embodied authority over behaviour.

4.5 Cases of Interoperability in identity systems in Europe

Threlfall (2003) [75] describes[6] how "the transferability of state pension rights was enlarged…in 1998 and became 'portable' through freedom of cross-border payments" (2003: 130). Interestingly, until the 1992 Treaty on European Union, free-moving pensioners were not at liberty to burden their host country's health system. However, such restrictive health entitlements made the "maintenance of such compartmentalised health-care non-viable" (ibid) if not impossible in critical cases. By 1997, all community free movers were granted medical benefits, thus "freedom of choice of residence for pensioners has therefore been widely enhanced, subject to the constraints of an individual's means" (ibid). This brief case is unavoidably associated with the messy, convoluted matter of interoperability *and* identity - and is moreover devoid of any reference to technical concerns. Hence, the e-Pensions domain will face political, organisational and social challenges, *as well as* having to build the foundations of an interconnected, interoperable *technical* platform. Not only does this support Klischewski's (2003) [44] consideration for simultaneous middle-up-down considerations, but also the case appears amenable to interpretation using the TFI framework.

A similar discussion by Threlfall (2003) [75] within the health care domain offers supplementary evidence to consider interoperability in Europe also as an Identity issue, as well as one which incorporates the abstraction of interoperability across the full spectrum of the TFI framework. The European Commission aims at improving the EU's healthcare system without direct interference in each country's delivery of health services (2003: 130-131). Nonetheless, in 1998,

> "Twin phenomena of 'patient mobility' (Wavell, 1998 [77]) and a 'Europe of Patients' (European Commission, 1999 [25]) had been created *de jure*, so that from the point of view of the patient's healthcare, they were living in the EU as in one country" (Ibid).

Again, for the domain of e-Health, we are confronted with a plethora of interrelated technical, formal and informal elements. For example, an European Health Card will replace form E111 by 2005, entailing much work on technical interoperability and the creation and revision of formal standards. Lastly, to exemplify an informal (behavioural) concern, "implications [may ensue] arising from patients circumventing waiting lists by going to another member state" (Ibid). e-Health also relates to identity, requiring consideration of all levels of the TFI to enhance likelihood of success.

Overcoming purely technical hurdles will do little to reassure communities of the merits of a potential information system, which may threaten privacy, trust and undermine cultural beliefs, i.e. a feeling of "*but that's not the way we do it round here*". For Wimmer (2002) [79], identity considerations are crucial because "citizens feel vulnerable when using e-Government systems…they want to have security solutions, which provide subjective trust" (2002: 1). Here, the issue of privacy

[6] The work by Threlfall is adapted out of Council Directive 98/49/EC, OJ L 209 25.07.1998: 0046-0049.

surfaces, as identity data exchange is a very sensitive subject (Homburg & Bekkers, 2002: 4-8 [29]). Further, privacy concerns become politically charged *in practice* as information exchange and standardisation across boundaries may "reflect, legitimate and re-produce the discourses of powerful groups, validate their ways of steering and thinking, and give tangible force for their influence on organizational life" (Bellamy, 1998 [4]).

The two examples of pensions and health have brought further evidence to suggest interoperability goes well beyond the technical, and that within the EU, identity is a term that also needs to be given value and meaning. The following section presents an overview and summary of the current EU interoperability context, discussing the challenges and proposing directions for future research and practice.

4.6 The Great Interoperability Challenge – A Discussion

The eEurope Action Plan 2005 called on the European Commission "to issue an agreed interoperability framework to support the delivery of pan-European eGovernment services to citizens and enterprises" (IDABC, 2005 [30]). More than just e-Pensions and e-Health, this plan of action encompasses an abundance of services including harmonising tax, social security systems, educational systems, jurisdiction for divorce and family law, driving risks and benefit and welfare regimes across Europe – all of which currently remain in their infancy (Kinder, 2003 [42]; Threlfall, 2003 [75]). In addition, the establishment of a common Visa Information System is slowly becoming reality, although "there is currently no interoperability between existing national visa systems in Europe or the possibility to check reliably whether an applicant for a visa has applied under another identity" (BTT, 2003: 1 [10]). Nevertheless, this too is a highly charged, emotive interoperability of identity project – a branch located on the biometric technology tree.

Many authors (Moen, 1994 [56]; Prokopiadou, 2000 [62]; Homburg & Bekkers, 2002 [29]) view the complexities in developing an integrated social dimension for e-Government applications (*in practice)* as the broadest, most difficult challenge. Owing to the multilevel, hierarchical nature of local, national and international public administrations, government procedures for production and dissemination of information are considered overcomplicated, rigid, fragmented and dispersed (Moen, 1994; Prokopiadou, 2000; Homburg & Bekkers, 2002; Virginadis [76]). Szulanski calls this 'internal stickiness': a resistance by local Public administrations to adopt new ideas from outside. (Szulanski, 1996 *in* Kinder, 2003: 143 [42]). In addition, Choi & Whinston [16] warn that the time needed to reach consensus among Public Administrations may prove too lengthy to support rapidly changing technologies and practices. (2000: 40)

Within the broad complexities of public authorities lie three concepts: technical challenges relating to data homogeneity and system interoperability for proper and efficient metadata exchange (Prokopiadou, 2004: 189 [62]); formal concerns lying within the policy realm of the creation, communication and diffusion of commonly accepted standards (Moen, 1994: 358 [56]); and informal elements encircling these two with politics, culture and behaviour (Choi & Whinston, 2000: 41 [16]). Isolated successful interoperability within each of the three domains is not a guarantee for

complete interoperability. For example, referring back to e-Health and privacy, beyond infrastructure, systems and standards for practice, a genuine feeling of trust and control is required by *citizens* before a government can overcome the social, political, cultural and legal barriers to interoperability. (Homburg & Bekkers, 2002 [29]; Landsbergen, 2001 [47])

Challenges to interoperability have been identified from an analysis of the holistic notion of interoperability and identity, using the TFI model. Further, semantics are integral to every level of abstraction and to the individual and contextual characteristics of citizens and communities, whether relating to the creation and exchange of metadata and communication protocols, establishing common agreed standards and policy between different national, legal and language borders; or relating to the flexible and dynamic meanings of interoperability and identity – and the associated understandings of their technical and formal structures.

4.7 Holistic understanding of interoperability

> *"Within informal cultures, openness and trust are necessary to assimilate cross-boundary norms to guarantee adequate communication and control"* (Stamper et al, 2000: 22, emphasis added [69]).

Only through sound understanding of interoperability as a holistic notion applying at varying levels of abstraction, can we hope to achieve a seamless transition to successful interoperability in practice. As a forewarning, Mulley et al (1999) [59] construct a prophetic but disturbing conundrum,

> *"Enhanced interoperability… may be a catalyst for closer links between nation states, integrating and consolidating the EU and achieving a more equitable distribution of wealth. This may be broadly consistent with the aims of EU regional policies. Alternatively, greater interoperability… may be a centralising force which concentrates wealth and leads to greater inequality; in opposition to the aims of regional policy."* (1999: 97)

Hopefully, steps being made towards multidisciplinary interoperability research will help avoid the problems outlined by Mulley *et al* and instead lead to a substantial reorganisation of the research activities and cooperation in Europe (Chen & Doumeingts, 2003:162 [15]).

Ultimately however, Kinder (2003) [42], offers the following comment,

> *"the usefulness to users of interoperable public service systems increases in proportion to the extent to which users cannot detect where one organisation's system begins and another ends"* (2003: 156).

Thus, the litmus test for successful pan-European interoperability endeavours rests in addressing all levels technical, formal and social in a seamless and integrated manner.

In the next section we focus on the social/informal dimension of interoperability in IMS.

5 Social aspects of interoperability in identity management

Dr. Martin Meints and Martin Rost, ICPP

The target of this chapter is to investigate from a social perspective how interoperability in various communicational contexts is supported by different types of IMS. For this approach we take a look at formalised and interactional types of communication which are provided by social systems. As a result we get an understanding in which communicational context interoperability is supported and by whom and where we can observe obstacles towards or special aspects within interoperability.

This chapter uses

- Social systems as they are described in D5.2 and D2.3
- The model of authentication / authorisation in social systems as described in D5.2
- The three defined types of IMS as described in D3.1 (chapter 3)

To enhance understanding and readability of this section, the mentioned terms and models are summarised.

5.1 Authentication and authorisation in social systems

From a sociological point of view, the specific identity as "person" [49] is a construction through a specific situation which is mainly formed by a specific social system. Sociologists model at least three types of social systems [50]:

- Interactional systems (forms of community in which participants are not subject to documented rules, but nevertheless schemes apply; examples are neighbourhood, friendship, spontaneous encounters) [40],
- Organisational systems (characteristics are membership and effective production of decisions; examples are public bodies, institutes and companies)[51],[3],
- Functional systems (economy, law, politics and science as "self-conducted" communication systems).

Functional systems are characterised by communication that has specialised functionality. Organisations have to be connectable to all four functional systems, but normally have a main emphasis on one of them:

- Economics: payment / non-payment; programme: price; generic person: e.g. "client" and "employee"
- Law: legal / non-legal; programme: laws; generic person: e.g. "citizen"
- Politics: power / non-power; programme: political programmes; generic person: e.g. "responsible citizen" in the meaning of the French term „citoyen"
- Science: true / false; programme: theories and methods; generic person: e.g. "the human being"

For some authors [41] religion (immanence / transcendence; programme: religious program; generic person: "priest", "member of the community") is discussed among other issues as a further functional system.

Sociologists understand social systems as a pool of schemes, events and communicational components which are used by persons. The thinking of persons taking part in communication is focused by the components mentioned within the appropriate social system. The different types of social systems operate using different addressing modes to link these communicational components.

The social subsystems reproduce particular patterns of communication that have particular social functions (e.g. the above-mentioned generic persons also correspond to typical roles within these systems). These functions, in turn, generate pointed sense horizons for organisations, which create particular sets of expectations (role conformity as "client", "citizen", "responsible citizen", "human being") for the persons acting in them.

When communication in social systems starts, the participants run through a procedure of authentication and authorisation, albeit informally at times. We therefore understand interoperability between the participants of the communication as an essential requirement especially in this start-up phase of communication. Authentication / authorisation have three dimensions:

- The social dimension (concerning social systems and roles taken therein)
- The personal dimension (concerning personal identity)
- The technical dimension (concerning technical support for authentication / authorisation).

The procedure of authentication / authorisation runs through up to four steps:

1. Authentication - determination of the social systems and functional system
2. Authentication - role taking / role making[7]
3. Authentication - personal identification / verification
4. Authorisation - determination of the rights a participant is granted respective to the requirements he has to meet

5.2 Types of IMS

Taking a look at the market for existing IMS of prototypes, concepts and IM-related tools, we determine several approaches towards IMS which differ for example in:

- Procedure of management (by whom? which operations on data possible?)
- Type of managed data (person or organisation controlled data? comprehensive profiles or selection of roles or partial identities? anonymity or identifiability?)

With respect to these properties, we observe three main types of IMS explained and further investigated in Deliverable 3.1:

[7] Role making is the active interpretation and creative shaping (forming) of a role. See e.g. http://www.sowi.uni-mannheim.de/lssoz3/lehre/LehreWS04/G1/G1_WS04_VL11.pdf

1. Type 1: IMS for account management,
   implementing authentication, authorisation, and accounting[8],
2. Type 2: IMS for profiling of user data by an organisation,
   e.g. logging or data warehouse tools which support personal profiling e.g., personalised services, or group profiling such as the analysis of customer behaviour[9],
3. Type 3: IMS for user-controlled context-dependent role and pseudonym management

5.3 Interoperability of IMSs with respect to social systems

Depending on the type, IMS act as a bridge function for the managed identities from the point of view of the organisation itself (type 1 IMS) and the roles (e.g. "member", "client") taken by persons (type 3 IMS) in various social systems. Some of the generic roles within social systems will be discussed in their interoperability aspects in detail. In this context we do not further examine the personal dimension of authentication / authorisation in the context of interoperability. The reason is that the personal dimension depends on the communication content and related security needs, especially of organisations and thus cannot be generally defined.

One example might be a customer of a shop (social system: organisational system; functional system: economics) purchasing something. In the case he pays with cash, no personal authentication is required; he stays anonymous throughout the communication and the subsequent transaction. In the case he uses a credit card, he is additionally identified (and authenticated) personally.

Organisational systems:

Role as "member": Members get access to information that is highly important for internal decisions and thus can be more or less confidential (e.g. protected by law: politics and law; trade secret: economy; internal rules: religion); organisation-specific, globally not usable authentication systems for higher security requirements can be used (e.g. using special, not common tokens, ID cards, biometrics etc.).

It could be argued that interoperability (social and technical) with other organisations or clients is often not a main emphasis nor especially desired. The bridge function of IMS cannot easily be performed even if it is needed e.g. in a network of trusted organisations.

As a result we see much expenditure on creating special solutions of type 1 IMS[10] to resolve those problems. In addition, the development and maintenance of personal trust among key members of the participating organisations, the social network within

[8] http://infosecuritymag.techtarget.com/2002/apr/cover_casestudy.shtml, http://www.oracle.com/technology/products/id_mgmt/index.html http://www3.ca.com/Solutions/ProductFamily.asp?ID=4839

[9] http://www.lumeria.com/what.shtml http://www.epic.ca/TechnologyDay/October05_2004/MoreInformation/Presentations/RandallBartsch%20-%20Identity%20Mgmt.pdf

[10] E.g. federated identity management systems, see D3.1

the cooperation, is a key factor for success for the whole network.[11] Commercial needs and the possibility of considerable financial investment create the potential to overcome the social and technical hindrances of interoperability.

This does not apply to scientific functional systems as far as the results of the research are consolidated and published in the case that commercial use (e.g. through patents, licenses etc.) is not planned. In this case, open scientific discourse is a standardised method for generating and exchanging knowledge. If commercial use is planned, these systems clearly belong to the category of commercial systems and experience the same hindrances in interoperability.

Role as "client": To reach as many potential clients as possible, organisations need universal addressing and authentication systems. As a result we often see socially accepted, simple and generic authentications using three or four observable steps. Authentication is often simply role-based (e.g. the customer entering the store is not personally authenticated as long as he pays cash). If personal authentication is necessary, commonly available IDs are used, such as a credit card number, an assigned or chosen username / password, an identity card, or a PIN.

Interoperability (social and technical) therefore is a main emphasis for organisations with respect to their clients. The bridge function of IMS can easily be performed.

Resulting from the social acceptance and easy, universal use of the authentication systems in combination with strong authorisation, we often observe vulnerability in respect of identity fraud[12]. In turn, the introduction of new, commonly used and secure IDs, such as biometrics in passports, or using PKI, is not an easy task. Over and above the investment in infrastructure, the acceptance and trust of the user is always a major task within the enrolment process[13].

Type 1 IMS and many tools and systems of type 3 are available. The lack of central organising forces for the development of type 3 IMS from the perspective of many clients from various organisations leads to numerous insular technical solutions[14]. They are mainly caused by the lack of technical standards (e.g. for the integration of PGP in various mailers).

Interoperability (social and technical) between one or more clients and various organisations is hindered by the lack of central organisation and financing.

Interactional systems:

In view of the informal and oral way of communication, authentication of participants is not typically supported technically; authentication with respect to certain expectations within a relation between two persons such as friends is done visually and over a longer period of time in which informal communication takes place.

[11] See http://www.tzw.biz/www/home/article.php?p_id=476
[12] See D5.2
[13] This aspect is further developed within D3.2
[14] See D3.1

When digital media are used, we observe organisational shares in informal communication such as written communication, technical supported login to access the internet and so on. Following the traditional understanding of interactional systems, identity management mainly is directed to this organisational aspect of informal communication, such as address (role: citizen), telephone number (role: client of a telecommunication provider), e-mail address (role: client of an ISP). But in these cases the informal content of the communication when using a chat room, blog or avatar is not connected to the formal, organisational exchanges (such as the login to access the internet). One reason for this is that there is no direct link between the login procedures to use the internet and authentication/authorisation procedures within interactional digital communication platforms. What remains as a core difference to the traditional understanding of interactional systems springing from the technical communication platforms, are written communication and the absence of physical presence. In this context a new description of the borderline between interactional and organisational systems might be necessary.

Operators of technical systems acting as platform for informal communication have the same need for simple and universal addressing and authentication as organisations have towards their clients. The technologies used to authenticate are in many cases very similar and thus directed towards compatibility (the technical part of interoperability) between operator and client. These platforms delegate especially the making of roles (e.g. “the evil” in an avatar), while organisations typically “make” (create, form, shape) roles themselves (e.g. the customer or supplier formed by an enterprise) together with new designed or adapted behavioural schemes. Apart from general guidelines such as insults being forbidden, interactional platforms do no provide the well defined behavioural schemes that are typically found in organisational systems. Instead the social dimension of authentication and thus the interoperability takes place among the users of such a platform. The technical parts of the interoperability, the compatibility, is needed between the operator of the platform and the clients (users), while the social part of interoperability takes mainly place among the users themselves.

In this context we can see a clear dichotomy in interoperability in the two types of systems. For example, the formal roles of the organisational type presume informal rules of the interactional type. In the next section we discuss the impact on privacy of interoperable IMSs.

6 Protecting identities and inherent interoperability problems

Sandra Steinbrecher, TUD

In this section we deal with the problem that any definition of identity and identity attributes and their management or administration by organizational measures alludes to the topic of protecting a person's privacy. This inherent problem raises the question of interoperability of identity and identification concepts because interoperable concepts often need more personal data than stand-alone concepts would need.

From the perspective of technical data protection identity is any subset of attributes which uniquely characterizes a specific individual within any set of individuals. So there is no such thing as 'the identity', but rather several of them. Further, each identity of a person comprises many partial identities of which each one represents the person in a specific context or role as shown in the example of Figure 7.

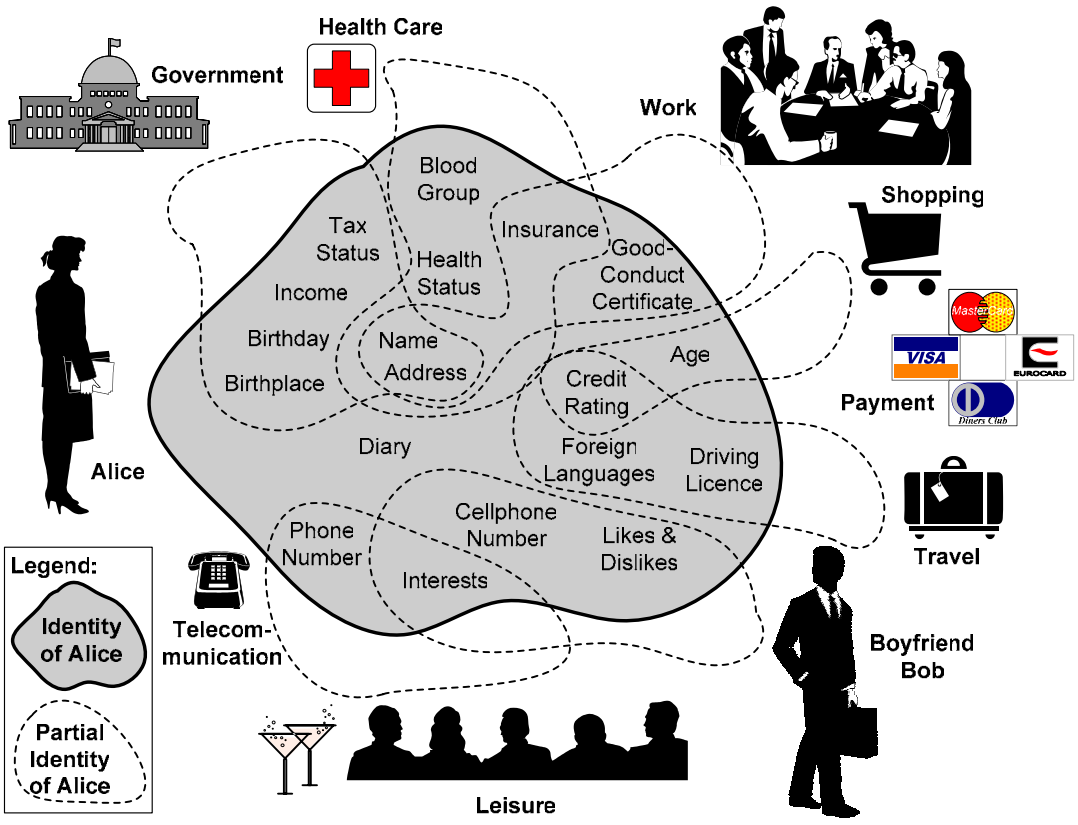

Figure 7: Example of partial identities

Digital identity denotes attribution of properties to a person, which are immediately operationally accessible by technical means."[PfKo_04]. This means a digital partial identity within a given system consists of a set of attributes maintained within the system.

[PfKo_04] Köhntopp Marit and Pfitzmann Andreas (2004); "Anonymity, unobservability, and pseudonymity - a proposal for terminology". Draft v0.20., September 2004, available from http://dud.inf.tu-dresden.de/Literatur_V1.shtml (v0.5 and all succeeding versions).

Identification systems try to identify such digital partial identities in order to grant them certain rights, especially access to certain technical services or systems. If a person claims to have a specific digital partial identity, some of their attributes have to be verified by the identification system. As we have seen in other FIDIS deliverables, the attributes usable for identification systems can be classified into the following identification attributes:

1. something the person possesses (e.g., smart card),
2. something the person is (biometry) or
3. something the person knows (e.g., password).

Identity management means managing the various digital partial identities that

- a user has,
- is assigned by others,
- can create himself or herself.

There are various views as to what identity management means in detail and how it can be technically realised. A more detailed classification of existing digital IMS is made in FIDIS Work Package 3.[15]

Identity management needs multidisciplinary interoperability with reliable identification systems. Using the TFI model, a user has to have an informal notion as who and how he wants to interact with under given circumstances, choose formally the corresponding partial identity and use its technical representation within an identity management system in order to grant him rights. Technical education systems (potentially integrated into IMS) can help the user in the informal process of taking a partial identity and lead him to the point of formally choosing it by demonstrating him several alternatives for partial identities and showing him the potential consequences of using him.

Interoperable identification and IMS have to take into account that, because of the first and the last identification attributes' transferability, they are not able to guarantee the correct identification of a specific person's partial identity. If only these transferable identification attributes are used, an identity management system allows one person to manage another's partial identities if the other person transferred the corresponding identification attributes to her. Only the second identification attribute type makes it possible to identify a partial identity of a specific person but it may reveal a larger subset of a person's digital identity, because these identification attributes typically lie at the intersection of different partial identities (see Figure 7). If the same attribute is used as identification attribute not only for one partial identity, but for several, such as the e-Government partial identity (including in Figure 7, tax status, income, birthday, birthplace, name, address) and the travel partial identity (included in Figure 7, driving licence, credit rating, foreign languages) and the attribute is unambiguous for all users in both databases, an straightforward

[15] Matthias Bauer, Martin Meints (ed.): Structured Overview on Prototypes and Concepts of Identity Management Systems; FIDIS Del. 3.1; available from http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.pdf

comparison of the two databases leads to larger partial identity that becomes known to the providers of these databases. Note this may not only happen for biometric attributes but also for other identification attributes, yet can easily be prevented by an appropriate system design, although it becomes more difficult for the second type of identification attributes.

Privacy-enhancing identity management is driven by the right of informational self-determination and tries to enable users to enforce this right in the digital world. It gives them the power to create and handle digital partial identities corresponding to their informal notion in the TFI model and according to the privacy interests they have. This means that they should, for example, be able to determine how linkable to each other their partial identities might become for interactors and possible attackers. Privacy-enhancing IMS need interoperability with identification systems on all network layers in the sense that they use just the attributes needed and known for a certain partial identity, but no more, implementing thereby the least-privilege-principle: collecting only as much data as is needed for identification and use. This has the disadvantage that the usability might decrease if users have to identify themselves explicitly under a certain partial identity whenever they want to change their partial identity. If a user has identified himself under a large set of attributes assorted to him (e.g., the ones assorted to the e-Government and travel partial identities in figure 7) to one application (e.g., in this case an e-Government application) he would not need to identify himself against another application (e.g. in this case a travel agency) if the two applications collaborate regarding identification (Single Sign-On applications).

A privacy-enhancing identity management system consists of elements from both partners in any communication, and typically the user-server scenario is considered on a technical level. The identity management tool on the user side controls a person's communication to the outside world. For identification, the identification attributes necessary to identify a respective partial identity with a communication partner are transferred. An identification system verifies this partial identity for a communication partner with the help of part of the identity and identification system. The architecture of privacy-enhancing IMS is shown in Figure 8.

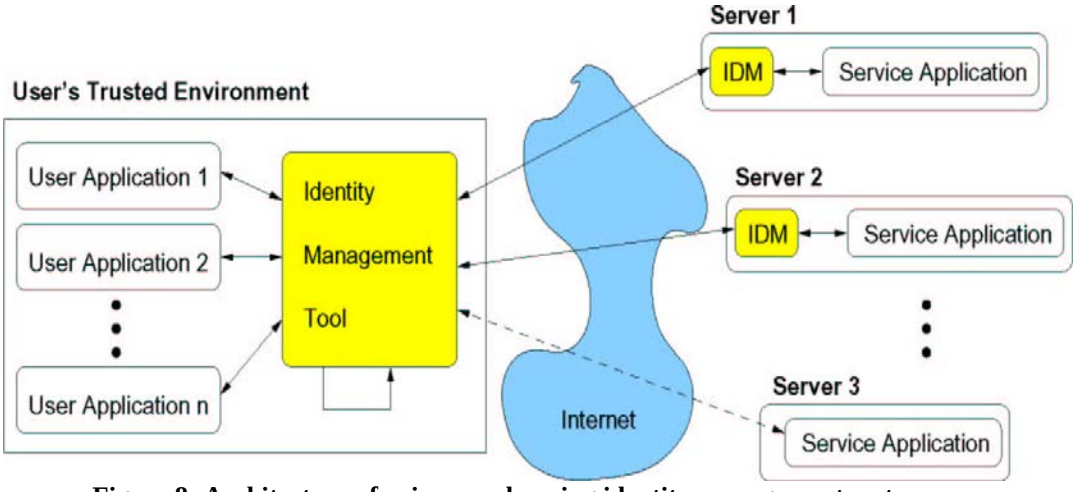

Figure 8: Architecture of privacy-enhancing identity management system

Interoperability of identity and IMS helps users to identify themselves for several applications with only one Single Sign-On. Typically in current applications this is done on the server side which federates an identified partial identity to other servers where the respective partial identity wants to be identified. This leads to a reduction in the number of digital partial identities and a concomitant increase in the single partial identities.

A Single Sign-On in the user's trusted environment is possible. In a database on the user side a variety of identification attributes associated with digital partial identities can be stored. While a user identifies herself against her trusted user device with an identification attribute representing a large digital partial identity, the database transfers to other servers only the minimum identification attributes of the partial identity needed in the context of this server.

In the case of the first and last identification attributes, interoperability between appropriate systems can be designed very easily, but whenever attributes are requested to identify a user, the different servers can collaborate and identify a larger partial identity of the respective person than the one every server could using only the information it has stored. Here interoperability becomes a threat to privacy.

But transferring identification attributes to other persons means giving these other persons access to all the attributes of this partial identity within a technical system, and hopefully many service applications will be satisfied with transferable identification attributes - given all the difficulties biometrics currently still faces.

This section summarised the issues arising in the technical and formal approach on interoperable identity and IMS. We also addressed the informal level dealing with the self-determination people have to interact with others or systems or allowing these systems to use personal data in an interoperable way with other systems. As outlined, this is not only a question of technical interoperability between systems or concepts but also of the formal notion of identity and partial identity that is or will become established in different application areas. Both a top-down and a bottom-up-approach (regarding the TFI model) alone, seem unsatisfactory therefore we argue that privacy-enhancing technologies need to be approached from both bottom and top in order to reach a consensus.

7 Identification and authentication in G2C digital interactions

Sabine Delaitre and Ioannis Maghiros, JRC

This section first introduces the European context of the identification and authentication of Citizen to Government (C2G) in digital interactions. The reverse digital interaction, G2C, or government to citizen, is then defined along with the related processes of identification and authentication. In addition, we will examine interoperability. In order to illustrate the G2C interaction, two case studies and the related interoperability issues are presented: the European passport and the driving license.

7.1 Introduction

Modernisation will enable the inter-linking of systems, information and ways of working, within or between administrations, nationally or across Europe, or with the private sector. Therefore, an agreement on common standards and specifications is essential to support life-event and information sharing eGovernment services, as well as R&D into interoperability for networked organisations that in future will deliver new and innovative public services (see Figure 9 below). The policy context encompasses privacy, secure services and access to services related to the availability of services. More precisely, the policy context for the present topic is under the terms of the Lisbon Agenda (for the driving license for instance), eEurope 2005 and Pan-European for interoperability. The challenge of eGovernment is to ensure trust and security and this requires special attention to the use of identity in identification and authentication processes.

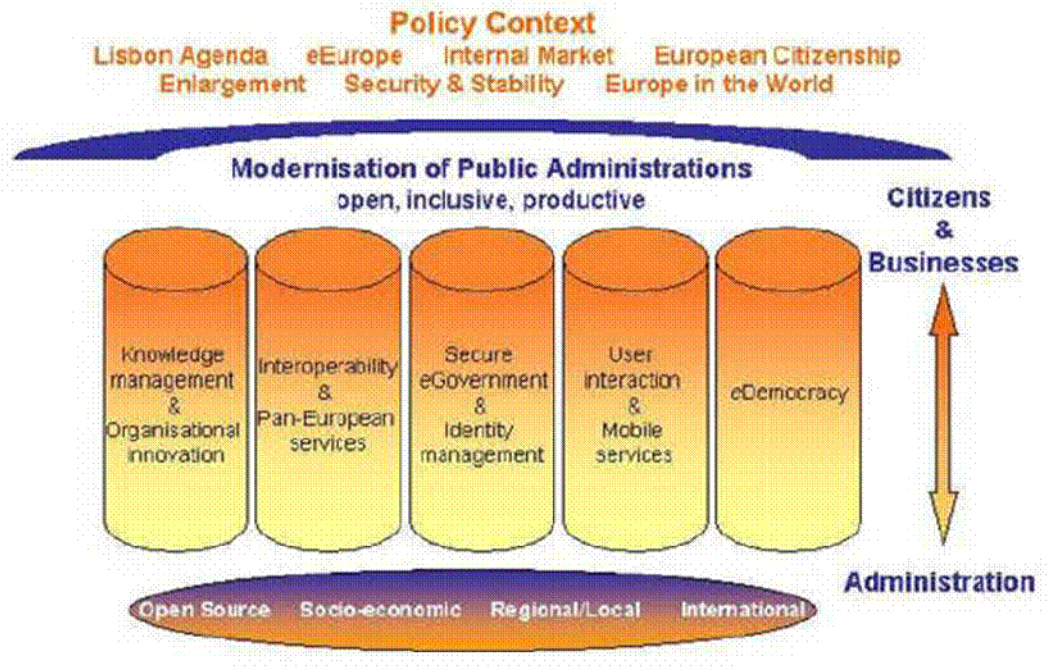

Figure 9: European framework of eGovernment

In general, three categories of interactions characterise eGovernment:

- G2C, government to citizen
- G2B, government to business and
- G2G, government to government

7.2 Digital interaction G2C

This section focuses on G2C interactions. The following figure (see Figure 10) describes this type of interaction and shows who is the citizen for the government and who is the government for the citizen.

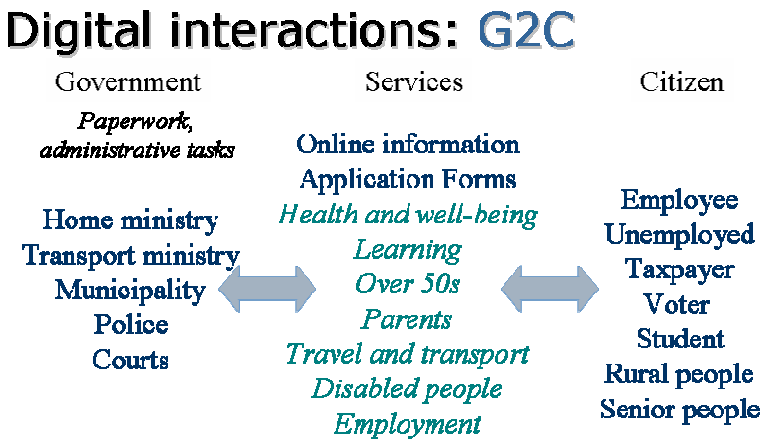

Figure 10: G2C interactions in eGovernment

For the citizen, government is composed of various ministries, offices and institutes, and for the government, the citizen is an employee, a taxpayer, a voter. To achieve interaction between both sides, several types of services are placed by government at the disposal of citizens. With a view to the good management of these services, security and trust are two key pillars. Hence the need arises to identify and authenticate the citizen, and to facilitate internal communication within government. Therefore, interoperability and identity play a vital role.

7.3 Chain of trust: identity and interoperability

Firstly, interoperability is essential for digital interaction in eGovernment in order to facilitate internal communication and to ensure security. Several characteristics of interoperability come into the picture. Vertically, interoperability is required within the same sector, while horizontally interoperability is needed across both public and private sectors and the scope of interoperability has to be regional, national, and even European. The framework of the interoperability is composed of three dimensions: social and political (informal), formal and technical. The social and political

(informal) dimension encompasses a top-down vision (from national to local, e.g. UK and France), the bottom-up vision (from local to national, e.g. Germany) and the mixed vision (e.g. in Austria). It also includes being able to identify the actors and organisational processes involved in the delivery of a specific e-government service and achieve agreement among these on how to structure their interactions, such as defining the integration of services according to the life or business situation of users. At the informal level it relates to ensuring that the meaning of the information exchanged is not lost in the process - that it is contained and understood by the involved people, applications, and institutions. The formal dimension relates to contracts and policies. The technical dimension refers to merging IT systems and software, defining and using open interfaces, standards and protocols, covering technical issues stemming from linking up computer systems, including open interfaces, middleware, accessibility and security services.

Secondly, identity is a vital concept for digital interaction. Indeed, identity and online interaction directly involve the enactment of the identification and authentication processes for ensuring trust and security. The identity requirements are related to:

- security of the collection, transmission and storage of information in secure databases and servers,
- privacy concerning the information exchanged and shared
- robustness and availability of services and transactions made online
- legislative and regulatory framework, including electronic documents, digital signature and records management.

Identification is a process (1:N) for recognising the user - who is the user? - whereas authentication is a process (1:1) for confirming a user's identity. In the latter case, different information can be used such as a password or PIN, i.e. "what the user knows", a smart card or a driving licence, i.e. "what the user has", or biometrics data, fingerprint or voice, i.e. "what the user is or does". Both processes require two steps, registration and enrolment (see Figure 11).

The registration step is the process by which a citizen (C) obtains a user ID to access online services.

The enrolment step is the process by which a user provides government (G) information, e.g. user ID and personal data, in order to obtain a credential, such as a PIN, for subsequent authentication. Enrolment is completed when the user returns to the site in order to activate the PIN.

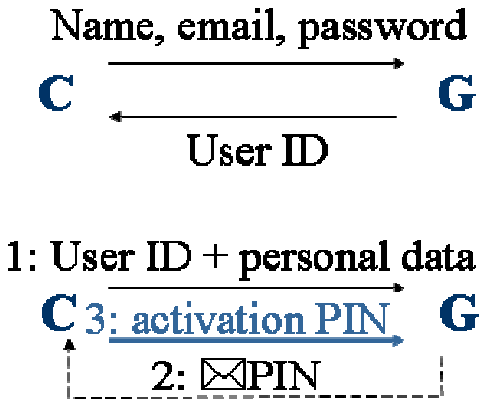

Figure 11: graphical view of registration and enrolment processes

These different processes demonstrate the need for a chain of trust at different levels for the identity.

7.4 Use of PKI

In most European countries there are continuing e-government initiatives which are considering PKI for access and digital signatures. These initiatives are pursuing the following benefits:

- Time savings for information processing inside the government bodies and reduced response time for citizens,
- Cost savings as a consequence of decreased transaction time and cost, increased accuracy and productivity, reduced paper-based maintenance and operating costs, better and more trusted ways of allowing users to pay for services provided,
- Enhanced service to inside users, to public and other entities,
- Improved quality and integrity of data, compared with paper-based systems.

Although the implementation of PKI systems for digital signatures, e-ID, or e-Government services is only in the initial stages, it has already come up against the following barriers:

- Complexity and initial investment required to set up infrastructure,
- Lack of consumer initiatives (e-applications, convenience) vs. costs (card reader, software),
- Lack of standards, in particular for the interoperability of certificates and signed envelopes, the cross-checking of certificates issued by a third party Certification Authority (CA), the usage of certificates by applications, the certificate handling by directories, and time stamping. In the absence of standards, some countries in the process of implementing PKI for digital signatures, have developed their own specifications which may lead to interoperability problems in the future,
- The legal and procedural regulation aspects of building mutual trustworthiness recognition across CAs and across countries and related jurisdiction, that is, mutual recognition of policies, contractual agreements and legal frameworks (on digital signatures and contractual liabilities),
- Difficulties in building technical interoperability across different CAs in particular, at application level, in the use of cryptographic techniques, attribute certificates, smart card technologies and registration schemes.

National, European and global working groups are actively debating these issues, developing potential interoperability models (e.g., Cross-certification, Bridge CA, Certificate Trust List, etc.) and carrying out pilots to achieve both technical and legal interoperability (e.g., ICE-TEL and PKI challenge projects, PKI interoperability Testbed, etc.).

7.5 Case studies

This section deals with two case studies: European passport and driving licence. In both cases the main objective is to ensure security, safety and freedom of movement. Because these identity documents may be equipped with microchips, digital interactions are possible.

7.5.1 European passport

The policy framework for European passport[16] encompasses several ISO standards and a European directive. The solution will be fully conformant to relevant standards, such as ISO 7816-15 for the identification cards, part 15: cryptographic information application, ISO 14443 concerning contactless chips, ISO WG3 for security techniques, and will collaborate with Schengen Information System and ICAO (International Civil Aviation Organization) specifications. The directive 95/46/ECon data protection is applicable as it concernes the processing of personal data, including biometric data.

From a technical point of view, the European passport is a smart card addressing security needs, including two biometric data for verifying the authenticity of the document as well as the identity of the holder. This approach aims to render the passport more secure by a legally binding instrument on minimum standards for harmonised security features, and at the same time, to establish a reliable link between the genuine holder and the document by introducing biometric identifiers. The smart card would be contactless and would have the capacity to store digital signatures, ensuring authenticity and integrity of data, together with the capacity to store encrypted data. The two biometric identifiers are the digital photographs of face and fingerprint (not the template). As to the second biometric identifier, it is left to the discretion fo the Member States whether they store the fingerprints on the storage medium and/or in a national database.

Resolution 6 (Porvoo group[17]) supports the provision for interoperability aspects to be included in international standards in the smartcard, certification infrastructure, and biometric domains. ICAO recommends a 32K chip as a minimum standard. However, as it may be necessary to store a facial image and fingerprint images, a 64K chip would be more appropriate, especially if Member States wish to add some alphanumeric data. In order to ensure interoperability, the quality standards for the digital photograph set out by ICAO should be respected.

7.5.2 Driving licence

The policy framework for the driving license encompasses the Lisbon agenda and several European directives. The directive 91/439/EEC is the reference text and mainly describes the categories of driving license, of vehicles, the conditions for the issue of a driving license, the minimum ages for the various categories, the driving tests and the minimum standards of physical and mental fitness. The directive 96/47/EEC concerns the plastic card model and the directive 2003/59/EC deals with the professional drivers.

The driving license is a plastic card aimed at giving high protection against fraud, and in the case of microchips, the stored data would be the information printed on the card. No subsequent usage is foreseen. But a need for harmonization remains as to the validity periods and the periodicity of medical checks for professional drivers.

[16] This part does not concern the temporary passport.
[17] http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/20710B02C6C5B894C2256D1A0048E290

Two aspects of the interoperability in driving licences are: the technical specification for the microchip and the standards related to the medical requirements and training; for example, the validity of the licenses and the medical examination frequency.

8 Use of credentials systems in e-commerce

Michaël Vanfleteren and Els Kindt, K.U.Leuven R&D

The wider use of on-line credential and authentication services is emerging and changing the Internet landscape. Indeed, more and more websites require visitors to submit credentials[18] or to identify themselves, sometimes through a secure authentication mechanism. Such a mechanism is aimed at ensuring the integrity of certain electronic transactions, especially those involving on-line payments.

A credential system in the widest sense could be described as a system whereby information is submitted that attests to the truth of certain stated facts, e.g., the identity of a given person. Such a system could be a mechanism in which users can obtain credentials from internal or external organisations and demonstrate possession of these credentials in order to have access to particular applications, services or sites. This development inevitably raises a number of legal issues which must be addressed, including issues relating to data protection.[19] This section will focus on the restrictions imposed upon credential systems by the data protection legislation. Most credential systems will indeed contain directly or indirectly a link to an identifiable individual and, in this respect, raise privacy concerns.[20] For credential systems to be interoperable, these concerns must be dealt with and are likely to be a condition for its legality.

As an example of a credential system, the NET.Passport of Microsoft represents a good starting point. Microsoft .NET Passport was an Internet user-identity—management system that let Internet users use just one login name and password to sign in, access Web services, and shop on-line at all participating Web sites. Users could control what personal information they wanted to register in their accounts and what personal information they wanted to release to the Web sites that they visit. In addition to .NET Passport sign-in, the .NET Passport Service also included .NET Passport wallet and .NET Passport express purchase. .NET Passport used cookies whenever a user signed in to a .NET Passport participating site. .NET Passport stored a unique identifier, the time the user signed in, and whatever .NET Passport profile information the user had chosen to share with participating sites, in an encrypted cookie on the hard disk of the user. The cookie allowed the user to move from page to page at the participating site without having to sign in again on each page. Problems created by the .NET Passport system consisted of several threats to data protection which had to be dealt with by Microsoft. In Europe, the Article 29 Working Party[21]

[18] In the widest sense, a credential is a piece of information attesting to the truth of certain stated facts

[19] Other legal issues in connection with credential systems which need to be further researched include the regulation of intellectual property rights in the information society (see Directive 2001/29/EC of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society) and legal requirements relating to e-commerce transactions (see the Directive 2000/31/EC). Other relevant EU law instruments which have to be taken into consideration are the Directive 1999/93/EC on electronic signatures and the Directive 1997/7/EC on distance contracts.

[20] Article 2 (a) of the EU Directive of 1995 rules that an 'identifiable' person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

[21] The Article 29 Working Party is instituted by Article 29 of the data protection Directive 95/46/EC. The Working Party examines questions related to the application of the Directive and advises the European Commission.

released an opinion on on-line authentication services and especially analysed the .NET Passport system provided by Microsoft, asking it to comply with the EU data protection legislation
Since then, the Redmond's multinational made important changes in order to ensure the compliance of the .NET Passport system with the European Data Protection Directive.

At the same time, Microsoft is currently developing an Identity Metasystem. The Identity Metasystem is an interoperable architecture for digital identity that assumes people will have several digital identities based on multiple underlying technologies, implementations, and providers.[22]

Only so-called anonymous credential systems raise no privacy concerns. Anonymous credential systems may allow anonymous yet authenticated and accountable transactions between users and service providers. Such systems are anonymous in the sense that transactions carried out by the same user cannot be linked. An anonymous credential system is of significant practical relevance because it is the best means of providing privacy for users[23] [24]. As such, these systems represent a powerful technique for protecting users' privacy when conducting Internet transactions. However, most credential systems do not use such anonymizing tools, and as a result such credential systems will have to comply with the existing legal framework for data protection.

8.1 Legal & Regulatory Framework

The right to privacy is considered a core value of a democratic society. It is recognised as a fundamental right in all major international treaties and agreements on human rights and in the constitutions of most countries in the world, either explicitly or implicitly.

In Europe, the fundamental right to respect for privacy is recognised in, among other texts, Article 8 of the European Convention of Human Rights and Fundamental Freedoms. It states that everyone has the right to respect for his/her private and family life, his/her home and his/her correspondence[25].

The major relevant specific acts of European legislation are the Data Protection Directive 95/46 and the Directive 2002/58 on electronic communications. Directive

---

Documents issued by the Working Party are available at: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm, especially WP 60 and WP 68 on online authentication systems.

[22] For more information on the Metasystem, please see: http://msdn.microsoft.com/library/en-us/dnwebsrv/html/identitymetasystem.asp?frame=true#identitymetasy_topic1&_r=1 updated on May 2005

[23] Jan Camenisch, Anna Lysyanskaya, An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation available at http://www.zurich.ibm.com/~jca/papers/eprint.pdf

[24] For example, JAP helps to anonymize HTTP traffic (http://anon.inf.tu-dresden.de/) or remailers like mixmaster or mixminion could anonymize e-mail (See Fidis, D3.1 deliverable, v.1.0, p. 64).

[25] See also the EU Charter of Fundamental Rights of 7 December 2000 which confirms in article 8 that everyone has the right to the protection of personal data and that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

95/46 of 24 October 1995 aims at promoting the free movement of personal data within the European Union, while preserving the right to privacy (hereinafter the Directive 95/46/EC). Directive 2002/58/EC complements the principles of the Directive 95/46/EC in terms of specific rules for the electronic communications sector. Its provisions apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Community.

8.2 Relevant data processing principles applicable to credential systems

Several data protection principles must be respected when implementing credential systems. These principles are mentioned in the European Directives, and prior to these Directives, in the OECD Guidelines of 1980.

Finality and proportionality

One of the basic principles of data protection is embedded in article 6 of Directive 95/46/EC. It states that personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes (finality principle, also sometimes referred to as use limitation principle). In addition, the data should be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed (the proportionality principle).

The purpose(s) of the processing of personal data in a credential system should thus be defined at the moment of the collection and any further processing should not be incompatible with the purpose(s) initially defined.

When setting up interoperable credential systems, one should hence first determine the purpose(s) and the way the system will function. In particular, one must decide whether the system will be used to authenticate, identify or verify someone's identity, and hence which data are relevant and proportional to these purposes.

In addition, all other functional requirements of the credential system and ID-concept shall be clearly defined, for example, whether the system would also be used to conclude contracts.[26] The answer will not only determine which the relevant data are, but also which other legal rules have to be complied with.[27]

[26] E.g., Windows media Rights Manager, which contains a function to enter into licensing contracts.

[27] For instance, the choice for an authentication system will generally require the use of digital signatures and the operation of public key infrastructures ("PKIs")[27]. On the contrary, an identification system will normally do with a user ID and password only. For the use of electronic signatures, the Directive 1999/93/EC on a Community framework for electronic signature created a harmonised legal framework in the European Union which needs to be complied with.

Fair and lawful processing

Article 6 of the Directive 95/46/EC lists several other important principles relating to data quality. Firstly, any processing of personal data should be carried out in a fair and lawful way with respect to the data subjects (principle of fair and lawful processing). Further, data should be accurate and, where necessary, kept up to date. The last principle refers to the duration of storage of data and sets out that data may not be kept in a form permitting identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed.

'Owner' versus 'operator' of the credential system

Most obligations under the data protection legislation are imposed upon the so-called 'controller'. Article 2 (d) of the Directive 95/46/EC defines the 'controller' as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

Given that legal consequences are attached to the failure to respect these obligations, it is therefore of utmost importance to know precisely who is considered controller or owner of the data.

The function of controller or 'owner' is to be distinguished from the one of processor or 'operator' of the data processing. Article 2 (e) of the Directive 95/46/EC states that 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. Therefore, the relationship shall be confirmed in a written agreement between controller and processor.

Indeed, the two functions may not always be very clear. For example, in a public-private partnership[28] and therefore the designations may need attention. Both those who design and those who actually implement on-line authentication systems (authentication providers) bear distinct responsibility for the data protection aspects, although at different levels, and therefore it is advisable for the different players to have between them clear contractual agreements in which the obligations of each party are made explicit.[29]

[28] For example, the Privium service card for frequent flyers at Amsterdam Schiphol airport.

[29] There are typically several possibilities available for the credential system management: (1) The password management is delegated to the browser on the pc of the user, as is done for instance by the Mozilla password manager; or (2) the password management is delegated to a proxy-server on the Internet, possibly provided by the ISP; or (3) authentication is provided by a third party using a specific authentication protocol. This is done by Microsoft .NET Passport; or (4) authentication is done by a contract party within a "circle of trust". A specific protocol is used, like for instance the one of the Liberty Alliance project.

Legitimate processing.

The Directive explicitly lists in article 7 the cases in which personal data may be processed. This means that for each processing of personal data – collection, recording, storage, adaptation, alteration, retrieval, consultation, disclosure, dissemination, etc. – the controller has to verify if the processing falls under one of the criteria for making data processing legitimate.

The first case in which processing of personal data can be considered legitimate is when the data subject has unambiguously given her consent[30].

For credential systems, it is of particular relevance that the value and quality of the consent given by the users of these systems complies with the legal requirements.
The processing is equally legitimate when it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject for entering into a contract. In the third case, the processing is authorised when it is necessary for compliance with a legal obligation to which the controller is subject. For example, a person is obliged to communicate some personal data concerning the persons living with him to the unemployment agency in order to obtain a benefit. In the fourth case, processing of personal data is legitimate when necessary to protect the vital interest of the data subject. The processing is also authorised when it is necessary for the performance of a task carried out in the public interest pursued by the controller or by a third party or parties to whom the data are disclosed. Finally, processing personal data is legitimate when it is necessary for purposes of the legitimate interests pursued by the controller or by a third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Data minimisation principle
The processing of personal data should be limited to data that are adequate, relevant and not excessive (the principle of data minimization) (Article 6(1) c of the Directive 95/46/EC). This idea is further expanded by adding that data should only be kept in a form that permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. As a consequence, technical tools and Privacy Enhancing Technologies in particular, should be available to contribute to the effective implementation of these requirements.

Citizens need an identity to distinguish themselves from others and to benefit from a whole range of public services, such as e.g. health and other social services, or to fulfil certain obligations, e.g. taxation. Citizens are using their identity as 'evidence' for specific competences, roles, capacities, authorizations, rights, access to services[31]. However, although a basic data protection principle states that personal data should only be processed where necessary, people use their 'real' identity in most cases. This

[30] The data subject's consent is defined as "*any freely given specific and informed indication by which the data subject signifies his agreement to personal data relating to him being processed*."
[31] J. Dumortier and C. Goemans, *Privacy Protection and Identity Management* in Security and Privacy in Advanced Networking Technologies, NATO Science Series, Series III: Computer and Systems Sciences – Vol 193, IOS Press, 2004, p. 204.

use is often neither necessary nor desirable from a privacy perspective. In parallel with physical identity, the concept of 'digital identity' has indeed emerged as a whole set of digitized personal data (PINs, accounts, multiple user names, passwords, tokens, smart cards) and individuals can also perform different roles and accordingly adopt multiple virtual identities. Hence, each system shall determine whether the personal data collected are relevant and not excessive.

Information

Any collection of personal data implies prior supply of certain information to the individual concerned (Article 10 of the Directive 95/46/EC).

The person whose data is collected must at least be provided with information about the identity of the controller (which includes the name as well as the physical and electronic address) and the intended purpose(s) of the processing.

Therefore, it is vital to credential systems to provide adequate information to the users concerning the data protection implications of the system. This information should be provided in an easily accessible and user-friendly way.

Security

Article 17 of the Directive requires that controllers implement security measures which are appropriate to the risks presented for personal data in storage or transmission, with a view to protecting personal data against accidental loss, alteration, unauthorised access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Credential systems shall provide the required security. The level of security will differ from the application of the system. A personalised financial service site clearly requires a higher level of security than a general retail site.

Notification

Another important obligation of data controllers is the requirement in principle to notify the respective national data protection authority before any data processing operation is carried out, unless any exceptions or exemptions apply (Article 10 of Directive 95/46/EC).

Use of Globally Unique Identifier (GUID)?

Article 8.7 of the Directive 95/46 states that "Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed."

The use of one single identification number for accessing and using services could result in an important simplification both for citizens and administrations. However, the use of identifiers, whatever form they take, entails data protection risks as already analysed by the Art. 29 Working Party in its opinion on the use of unique identifiers[32]. Full consideration should be given to all possible alternatives. If user identifiers are indispensable, the possibility of allowing the user to refresh the identifier should be considered. Security plays a fundamental role in this context. The question will be how to incorporate guarantees from a data protection perspective.

National applicable law?

In the Data Protection Directive, article 4 provides that the processing of personal data is subject to the national law of the activity of an establishment of the controller.

Therefore, the national data protection law where the controller(s) is/are established, will apply to the processing of personal data by a particular ID - concept[33]. The place of the establishment of the processors will in principle not determine which law is applicable. However, the rules on the transfer of data will have to be complied with.

Transfer of data

The transfer of personal data may take place within the Member States of the European Union or in relation to third countries. The data protection Directive allows the transfers of personal data within the Member States of the European Union in principle. However, Member States shall only allow a transfer to third country if the third country in question ensures an adequate level of protection (article 25, paragraph (1) of the Directive 95/46/EC). The second paragraph explains that 'adequacy' should be assessed on a case-by-case basis 'in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations'. Where there is an absence of adequate protection, the Directive also envisages the possibility of *ad hoc* measures, notably of a contractual nature, which could result in the establishment of adequate safeguards on the basis of which the transfer in question could proceed (Article 26(2) of the Directive 95/46/EC). So far, the European Commission has issued decisions on the adequacy of the data protection on some third countries, including Argentina, Canada, Switzerland and the United States[34].

When personal data are to be transferred to third countries, authentication providers should work with service providers who take all necessary measures to provide adequate data protection or that it put in place sufficient safeguards to ensure the

[32] Cfr footnote 3

[33] However, see also the Electronic Commerce Directive which states that “each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field.” Under Article 3, providers of information society services (Internet site operators, for example) are subject to the legislation of the Member State in which they are established (originating country rule or "Internal Market clause"). The Directive defines a provider's place of establishment as the place in which a service provider effectively pursues an economic activity using a fixed establishment for an indefinite period. A different principle hence applies to the other legal aspects of credential systems, such as the rules relating to concluding contracts.

[34] See http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm

protection of the personal data of the users of the system, by using contracts or binding corporate rules.

Liability

The Directive 95/46/EC states that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national data protection legislation is entitled to compensation from the controller for the damage suffered (Article 23). The controller may be exempted from liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

It is clear that this provision may be applicable to credential systems. However, it seems unclear whether the credential system providers could be exempted from any other liability under the general liability system for electronic commerce[35].

8.3 Conclusion

In conclusion, there are several rules, not only about electronic commerce but also about data protection which must be respected in order to assess the validity of an identification/authentication system. In this section we have focused at the formal level of the TFI model presented in section 4. This overview is only a first step in the legal analysis of the interoperability of credential systems.

[35] The liability of Internet Service Providers is regulated in Directive 2000/31/EC on Electronic Commerce (Articles 12-14). The Directive on Electronic Commerce exonerates intermediary service providers from any liability when they have played a passive role in transmitting information from a third party (article 12). It also limits the liability of providers of other intermediary services such as the storage of information. In other words, providers of infrastructure services and access services cannot be held liable for the information transmitted, provided that they do not initiate the transmission and do not select the recipient of the transmission or the information it contains. Their activities are thus of a merely technical, passive nature and the service provider has neither knowledge nor control over the information that is transmitted or stored. However, on-line service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities. Member States may require website operators to inform the competent authorities without delay of alleged illegal activities on the Internet. Similarly, the Member States may require providers of hosting services to inform the competent authorities of information leading to the identification of the owners of the hosted pages.

9 Case study: eID projects, from capability to use

Paolo Spagnoletti, LSE and LUISS, Italy and Stephan Freh, LSE

We now review eID initiatives addressing their technical, formal and social/informal dimensions. We highlight issues of interoperability of eID projects in these dimensions.

9.1 Overview of eID projects

There are currently several projects on IMS, with differences in terms of objectives, scope, budget and policy. Most of these projects are not yet completed and in some cases, such as in Canada and Korea, eID projects failed because of budget and privacy issues.

This section aims to provide a high-level overview on the current status of international and European eID projects and of EU research projects. Furthermore, it analyses key projects and highlights drivers and obstacles that lead from capability to use. The research data of this chapter is primarily based on a working paper of the European Commission (CEN/ISSS 2004 [13]), a white paper of the Information Society Technologies (Ringwald 2003 [66]), a survey of a government advisory agency (Hayat et al. 2004 [27]) and on the information available from the links of the "eGoverment Observatory" area of the IDABC website (http://europa.eu.int/idabc/en/chapter/140).

To perform the analysis we reviewed the projects using three dimensions. These dimensions are related to the main issues of the development of ID management systems. First, we look at the issues in the adoption of different technical solutions, such as biometrics, smart cards, PKI, etc. Second, we introduce privacy concerns and the influence of local legislation in the decision-making process of government. Third, we focus on the possible roles of governments in driving the move from capability to use. A more detailed study on PKIs and biometrics, specifically from the legal and technological point of view, is presented in D 3.2.

9.1.1 Technological issues

The secure identification and authentication of the end-user of a smart card system remains one of the main technical issues of eID systems. The smart card is used mainly as a secure access mechanism to e-services. For all kinds of e-Government services it is of utmost importance that the identity of the card holder - who is not physically present in the offices or outlets of the government but at the other end of a network connection - may be verified with very high reliability. Simple passwords or PIN codes might very well be acceptable from a legal point of view and may well limit liability but form no 'real' proof that a person is indeed who he or she claims to be. This is because of the simple fact that passwords and PIN codes can simply be handed over from one person to another, either willingly or by loss or theft. This is

where biometrics comes in. Biometric characteristics (either physical or behavioural) cannot be transferred between persons.

Though the work on the development of a policy framework for European passport described in section 7.5.1 of this document, at this point in time only very few European countries are on their way of introducing biometrics for end-user verification in combination with the national ID card (See FIDIS deliverable D3.2). This is despite the fact that worldwide more than 70 countries are applying biometrics for card holder verification purposes.

The reasons for the European delay can be found both in the incomplete standardization in biometric technologies and in the complexity of risks that arise when using biometrics. In essence, a biometric is comparable to a PIN which can never be changed; hence, if it is ever compromised, it is compromised for ever. PINs are protected by ensuring that they never leave the secure PIN-pad at the ATM or EFT/POS terminal. Unless a similar approach is adopted with biometrics, and central storage of such identifiers precluded, individuals will be possibly subject to masquerade, identity theft and identity denial, not only by other people, but also by the State. Another area of threat is the application of location and tracking technologies to people (Clarke 1999 [18]). By combining the tracking of devices with authenticated identities of individuals, enormously powerful social control mechanisms would become available to corporations and governments alike. Furthermore, from a technological point of view, there are also issues on reliability and security of biometric data (see D 3.2).

9.1.2 Privacy and legal issues

From the point of view of regulations, the main issues lie in the ways to manage identities in different States. For example, in Austria or in Hong Kong, holding an ID card is mandatory for every adult, while in the UK or the US state-issued ID cards do not currently exist. Furthermore, the development of eID management systems becomes easier in a context where large database containing citizens information are already available. This is the case in Malaysia (CEN/ISSS 2004 [13]). In fact, the government, in order to issue a national eID systematically, has to gain access to all necessary information required for the registration process concerning its citizens and businesses. While for example most former Eastern European countries have a central registry of all their citizens, most common law countries do not have similar data marts. As a result nationwide eID solutions in common law countries require a greater number of interconnections, are of greater complexity and require a higher level of interoperability. However, this also means that a common law country would need considerable change to its laws and regulations in order to allow its government agencies to implement such national eIDs. This is probably one of the key reasons, why countries such as the USA, Canada or Australia do not have a national eID nor do they plan to issue one. In fact, only 3 common law countries worldwide have a national eID solution in comparison to 27 code law based countries where a national eID is in place or in preparation.

Examples of projects terminated for legal and privacy issues are the 1998 Argentina smart card project with fingerprint biometrics, the 2001 national eID card in Israel and the Korean eID card. In the latter case the Korean Government undertook a feasibility study in 1996 for a smart card based national ID card holding personal data, a national ID number, health insurance information and also a credit card as well as a public transport function.

Additional problems, in terms of interoperability, arise when the implementation of eID solutions have to face different national regulations. In fact, the legal assessment becomes more complex if, in addition to the various national areas of regulation, other geographical areas such as for example the US or Japan have to be implemented in the e-ID concept. The European Union clearly has the most regulated environment for data protection and electronic signatures. US regulation tends to be more pragmatic than EU regulation and hence more flexible. Other regions of the world do not match the level of US/European regulation in this area.

9.1.3 Business and political issues

In this section we describe national and international forces driving the process of adoption of eID solutions.

A brief scenario of the worldwide adoption of eID solution can be depicted as follows. The Anglo-American regions are not ID card minded. In Canada, a national ID project was withdrawn under public pressure and the same applies in Australia. On the other hand, electronic ID cards are booming in the Far East (Japan, China, Hong Kong, Malaysia etc) as well as in the Middle East.

Interestingly, China, Japan, Korea, Hong Kong and Singapore have agreed to concerted action to develop a cross border interoperable smart card (Silk Road Card).

The EC has considered eID so far as a political minefield where national interests and privacy issues are dominant and has therefore not stepped in. However strong external pressure – coming from the US VISIT program is rapidly changing this situation and has forced Europe to organise itself in the eID arena. This is already leading to the speedy introduction of biometrics in passports[36]. This will also influence the adoption of biometrics in the national eID cards domain although not necessarily using the same technical solutions.

In order to better understand the national level strategies driving the move from capability to use, we suggest an in-depth analysis of Asian countries where successful projects have been launched. An interesting aspect is the different role assumed by the governments.

[36] In this document we adopt the following definition of Electronic Identity (e-ID) systems given in (CEN/ISSS 2004: 68 [13]): "*Electronic identity solutions have the aim to guarantee the identity of a person (or a legal entity, e.g. a company) during the access to e-services and in order to provide the trust to the parties involved in the electronic transaction.*". In this sense e-ID solutions are all those mechanisms aimed to identify a person using digital technologies such as biometrics, electronic signatures, etc..

Whereas in China a mandatory policy has been adopted aimed to kick off the world's largest National Citizen eID system issuing what will be ultimately contactless chip cards to 900 million citizen, different approaches have been adopted by the Hong Kong and Malaysian governments.

The Hong Kong government leaves to the cardholders the free choice of deciding whether or not to include applications such as Post e-Cert in their smart ID card in order to promote awareness and growth of the service. Hong Kong expects this will also encourage and drive industry initiatives to develop new business applications or services relating to the use of e-Cert on smart ID cards. A different role has been played by the Malaysian government in the deployment of his Multi Purpose Card Project.

The Government Multi Purpose Card project is one of seven flagship applications deployed by the Malaysian government to attract leading edge technology development to Malaysia. One of the big advantages in support of the project was that the Malaysian government had already a very effective National Registration Department that was charged with the issuance and maintenance of a paper-based national identity card. The MyKad incorporates in the national identity card several function such as Passport application, Drivers License, health card, retail transactions, tolls on the highways and parking, payment on the urban transport network and a PKI based digital signature application. The card supports an Automatic Teller machine (ATM) application for cash withdrawal, e-debit transactions to pay for government services and to conveniently reload the e-purses. Further details on the Malaysian project can be found on (CEN/ISSS 2004: 57 [13]).

9.2 eID Interoperability Initiatives and Projects

Up to the 19th century, merchants, who moved to a new city where they were not personally known usually carried with them a "letter of recommendation" from their bank, monarch or any other trusted third party, which would assist them to be identified and integrated into their new community. When reference is made to pan-European identity and ID management, it is exactly this process which is discussed – verification and authentication of citizens and businesses to unknown European government agencies, and as referred before in this document eID, which is also known as Electronic Identity (CEN/ISSS2004 [13]).

We will use the Technical, Formal and Informal model as a lens to analyse the survey data. Firstly, we address the technical domain. It merges the results of three surveys and complements it with extensive online research. Secondly, we deal with the formal level of eID interoperability. Government agencies operate in a strictly defined legal environment. The legal framework aims to restrict the power for the purpose of preventing the citizen from government arbitrariness and ensuring their privacy (Stalder and Lyon 2002 [74]). In the case of eID interoperability projects, the formal level is represented by the legal framework in which the country is working. Thirdly, we address the informal level of eID interoperability. While the grounding data of the first two levels is primarily based on quantitative data, the informal domain is approached with a qualitative analysis of several eID interoperability research projects.

We now present the findings from an analysis of various surveys available and online research (CEN/ISSS 2004[13], Ringwald 2003 [66]; Hayat et al. 2004 [27]). While projects vary significantly in their objectives, scope, budget and policy, we emphasise identification of differences of interoperability in relation to the informal notion of efforts undertaken by the governments achieving interconnection. In order to do so it is therefore critical to understand the current eID interoperability status of the countries surveyed.

As an initial step, 67 countries were identified as requiring closer analysis. This number includes the EU 25 and all countries that were part of the eID surveys mentioned above. At this point, it should be stated that the level of information on eID projects in these surveys varied considerably from country to country. However, the information on the countries in these surveys quite often showed significant similarities in content, structure and length. In other words, it is anticipated that large amounts of information from previously published surveys were reproduced in later surveys with little further additional research being carried out.

Figure 12 shows the number of countries supporting various eID functionalities. 67% of the 42 countries (excluding the EU 25) have made the decision to introduce an eID, and an even higher percentage of countries (80%) are planning one but have not yet reached a formal decision. Several countries including Australia, New Zealand and the US, have made the decision not to introduce a nationwide eID in the near future.

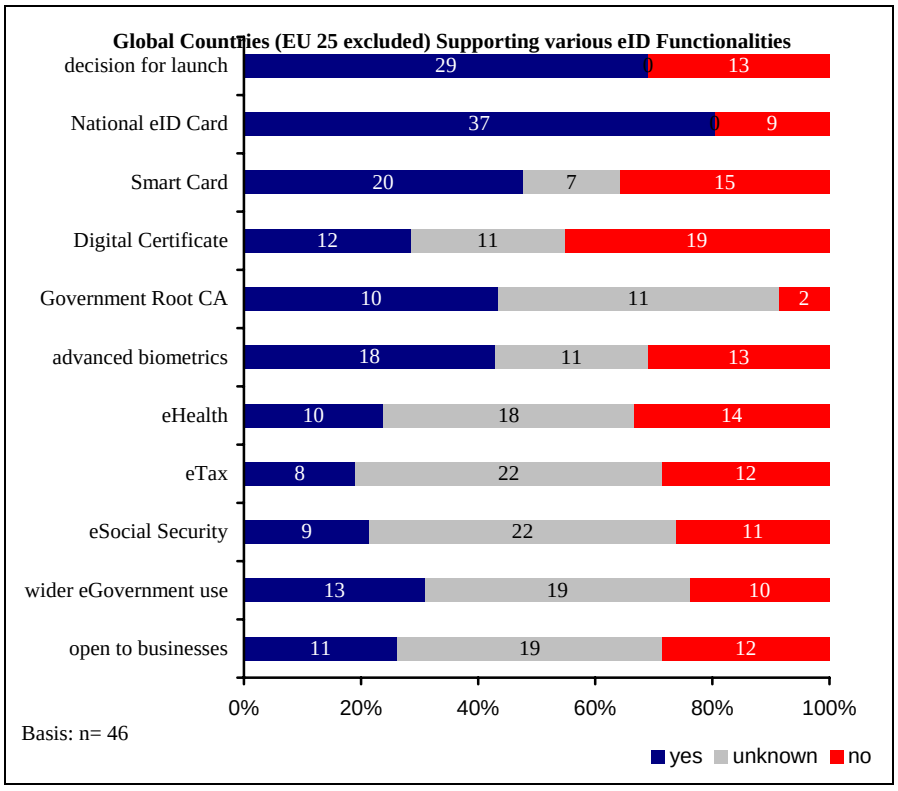

Figure 12: Number of Global Countries (EU 25 excluded) Supporting various eID Functionalities[37]

[37] In cases, where it was not possible to find any reliable information, whether the country would either plan or is already supporting a certain eID functionality, the data is classified as "unknown".

Multifunctional eID solutions can be used in a great number of different domains and require an even more complex interconnection, and these are therefore of special interest to us. Multifunctional eIDs are not necessarily but usually supported by smart card and digital certificate technology. Although, less than a third of the countries support or plan to support these features. In any case when digital certificates are used, the argument arises as to who will be the Root CA. This is closely linked to liability, privacy and most importantly to power issues. Apart from Norway and Singapore, all countries surveyed operate with a government agency controlled Root CA.

Advanced biometric solutions are usually linked with data and identity security. Technologies such as digital fingerprints, DNA codes, iris scans or facial recognition are classified as advanced in comparison to technologies such as photos, signatures or physical descriptions of individuals. Advanced technologies are primarily used for all types of fraud prevention. However, less than 50% of the countries which either have or plan eIDs are supporting any kind of advanced biometric technologies.

Interoperability from a customer focused point of view is often linked with convenience. Being able to use a single form of identity across different communication channels for corresponding with various parties is perceived as an enhancement of service and increased convenience, which should ideally result in a higher individual satisfaction. Government authorities therefore intend trying to interlink as many agencies as possible. Often this includes organisations from the private or commercial domain as well. In particular payment, transport and security control service providers are of special interest. Nonetheless, at present only a quarter of countries support or plan so support the use of a national eID in the private and commercial domain.

At the formal level, interoperability of eIDs is primarily seen through the lens of legal frameworks. In order to issue a national eID systematically, the government has to gain access to all necessary information concerning its citizens and businesses required for the registration process. While for example most former Eastern European countries do have a central registry of all its citizens, most countries based on a common law system do not have similar data marts. This is most probably one of the key reasons, why countries like the USA, Canada or Australia do not have a national eID nor do they plan to issue one. In fact, only 3 common law countries worldwide have a national eID solution in comparison to 27 code law based countries where a national eID is in place or in preparation (CIA 2003 [17]).

In Europe, the current situation with regard to national eID interoperability appears different. While only little more than half of the EU 25 countries have either already launched or are planning to issue a national eID, the projects seem to be quite ambitious in terms of interconnection complexity and use of advanced technology.

Whereas 14 countries plan an eID solution, Figure 13 shows a greater number than 14 countries are working on or are already supporting various eID functionality. This is the case as France and Italy have more than one national-wide eID project running and as multiple initiatives are reflected in the chart. Almost 80% of the EU 25 will offer a Digital Certificate service to its citizens and businesses by 2008 out of which Estonia, Luxemburg and Sweden do not have a government managed Root CA.

While a relatively high proportion of EU 25 countries are in favour of Digital Certificates, their willingness to work with advanced biometrics is rather limited in comparison with the rest of the world. Whereas, to date, 5 countries plan to use digital fingerprints, facial recognition and other similar advanced technologies, 8 countries have concluded that they do not believe that such high security measurements are needed.

Another significant difference is the collaboration approach of a majority of the European eID interoperability projects. While a high proportion of tax, health, social security and other government agencies will be able to use the national eIDs for identification and authentication purpose, more than half of the countries plan to open its eID solution to commercial organizations.

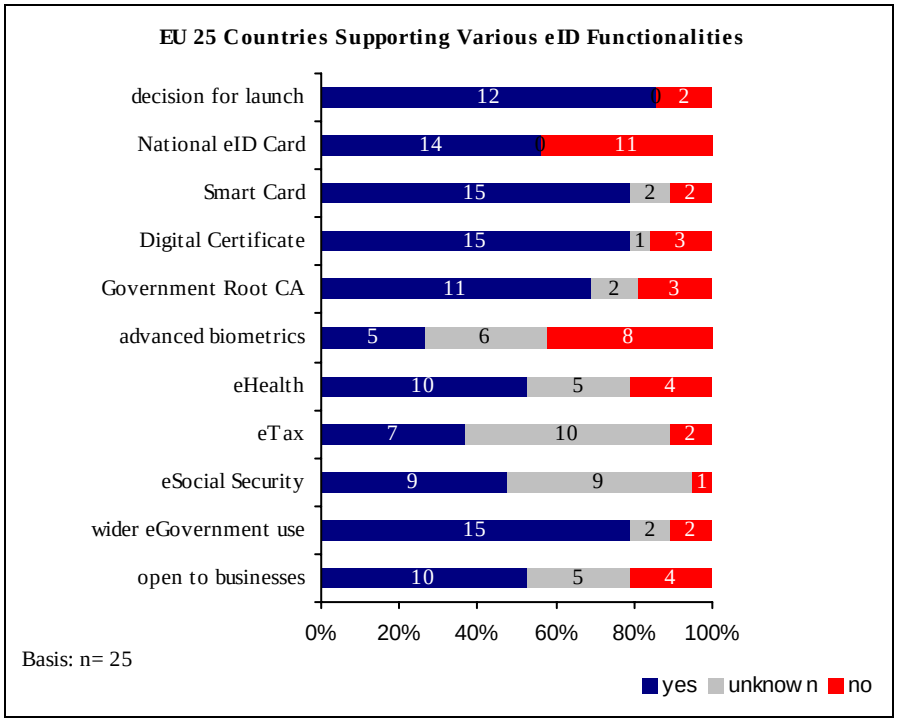

Figure 13: Number of EU 25 Countries Supporting various eID Functionalities[38]

An analysis of formal differences between countries based on their legal system (common law versus code law system) showed, on a global view, a considerable difference in level of adoption. However, a similar scrutiny among the EU 25 would not be of any relevance as the UK and Eire are the only countries within the EU with a common-law based legal system. Therefore by far the more challenging and pressing problem appears on a pan-European eID interoperability level, since the individual national legislation has to be harmonized in order to allow EU Member States to share, interconnect and use national versatile identities. Issues like data protection, privacy, information liability, access authority and the quality of authentication are heavily disputed issues.

[38] In cases where it was not possible to find any reliable information on whether a country is planning or already supports a certain eID functionality, the data is classified as "unknown".

9.3 EU Interoperability and Identity Related Programs

We now review various EU initiatives to establish pan-European eID solutions. As most research in Europe is fragmented into national programmes, the Information Society Technologies (IST) priority within the EU's Sixth Research Framework Programme (FP6) focuses on bringing universities, research institutes, small and large companies and governmental organisations together. FP6 can be seen as an umbrella program and it coordinates a great number of activities, which are scheduled for the period 2003-2006 (Information Society and Media DG 2005b [32]). Table 2 shows a rating of current FP6 funded interoperability eID related projects. The TFI model is used in identifying whether a project focuses at a technical, formal or informal level. A maximum combined score of 10 can be given to all 3 levels of the TFI model (1 being the lowest and 10 being the highest).

Project	eID Relevance	Interoperability Relevance	Technical	Formal	Informal	TFI Score
eTen	none	low	3	5	1	9
eMajor	low	medium	2	3	3	8
GUIDE	high	high	4	3	3	10
HOPS	none	medium	4	1	1	6
INTELCITIES	low	medium	5	1	0	6
TERREGOV	low	high	3	3	3	9
eEUROPE	high	high	4	2	4	10

Table 2: TFI Rating of FP6 Interoperability eID Related Projects

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 [34]). 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 (formal) 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.

The Electronic and Secure Municipal Administration for European Citizens (eMayor) project aims to provide secure, interoperable and affordable web services for small and medium sized government organisations (SMGOs) across Europe. The development of eGovernment web services in smaller municipalities is often hindered by lack of financial, political or legal support. Security and technical problems cannot be solved as the required expertise or infrastructure is not available. eMayor looks into the issues which are the main barriers to progress. By creating an eGovernment platform eMayor intends to help SMGOs overcome these barriers (Deloitte 2005) [20]. eMajor scored relatively well on the informal level as it considers cultural and regional related differences of eGovernment approaches. It is further rated as having a low and medium relevance to eID and interoperability.

The Government User Identity for Europe (GUIDE) program will create a European conceptual framework for electronic identity management for eGovernment.

Technologically, it will begin the development of an architecture for secure transactions between administrations, citizens and businesses as well as fostering back-office process integration. The social objective will start to create the institutional setting in Europe to endorse take-up of eGovernment services including social, ethical and legislative research (IST 2005 [37]). The project's approach is multi-disciplinary and includes technology, procedural and policy development across Europe. GUIDE consists of 23 organisations from 13 countries (GUIDE2005 [26]). This program has an extremely high relevance to eID interoperability. In addition, it pays comparatively great attention to the informal level.

The Intelligent Natural Language Based Hub for the Deployment of Advanced Semantically Enriched Multi-channel Mass-scale Online Public Services (HOPS) program is a three-year project focused on the deployment of advanced semantically enriched ICT voice-enabled front-end public platforms in Europe permitting access for European citizens to their nearest Public Administration (Inforamation Society Technologies 2005b [32]). The main objective is to address the mass-scale deployment of new online public services supported and accessible by voice channels. The project is based on the integration of voice technologies such as automatic speech recognition with natural language process technologies, complemented by a public administration sector-specific implementation of semantic web technologies (Montserrat 2005 [58]). HOPS understands semantic differently to the approach that is taken by this paper. HOPS's research concentrates on a rather technically driven view of semantic. When argued through a TFI lens, HOPS pays little attention to the formal and informal level. While it is rated as being not relevant to eID issues, it is of medium interest to interoperability.

The IntelCities (Intelligent Cities) project is focusing on eGovernment, ePlanning and eInclusion. It creates a shared, interoperable platform which will act as the basis for an eCity Platform which can deliver services and applications based on new and innovative forms of ambient intelligence. The eCity platform will collect information from many sources and present it through a virtual city that can be accessed by anyone who has access to a web browser, a mobile phone or other internet capable devices (IntelCities 2005 [36]). IntelCities is probably the most technically related project of all the seven examined in this paper. Its aim is to create a middleware solution and to outline processes for a successful implementation of it. Furthermore, its relevance to eID and interoperability is rated as low and medium.

The Impact of eGovernment on Territorial Government Services (TERREGOV) program addresses the issue of interoperability of eGovernment services for local and regional governments. The project integrates the dimensions of technological R&D, pilot applications involvement and socio-economic research in order to offer a European reference for the deployment of interoperable eGovernment services in local governments (Spy-Anderson 2005 [71]). TERREGOV shows a healthy balance of the technical, formal and informal level. It specifically focuses on semantic and social research in regards to interoperability. Moreover it is of great relevance to interoperability compared with little importance to eID issues.

Perhaps the most important initiative towards eID research among the EU 25 is eEurope (Malkom 2002 [52]). It is a political initiative that settles concrete action plans agreed by the European Council. In the area of eID the action plan settles a

roadmap for secure networks and smart cards as part of the main objective for a cheaper, faster, more secure internet (Iversen et al. 2004 [39]). The action plan highlights the need to accelerate, consolidate and harmonise the use of smart cards across the EU. eEurope contributes significant research to informal as well as technical issues and is of high relevance for both eID and interoperability.

10 Case study: the interoperable future of AmI Environments

Mark Gasson, Reading; Wim Schreurs, VUB; Sabine Delaitre, JRC

The scenarios described thus far have been limited to IMS technologies that are already established, in essence where issues of interoperability within the identity context have already been addressed, or are now causing problems because of a lack of co-operation in this area. However, in order to explore more fully the importance of interoperability, in this section we shall extrapolate existing technologies and consider a further scenario in which emerging technologies are prevalent.

10.1 Ambient Intelligence environments

The emergence of both the internet and wireless network technology, and with them the possibilities of distributed computing, i.e. using several computing devices that are not necessarily located in the same geographic location for a specific task, has had a profound effect on our way of life. Building on these advancements, Ubiquitous Computing (Weiser, 1991) is the next wave of technology, a paradigm shift from our current relationship with technology, whereby many thousands of wireless computing devices are distributed in the environment in everyday objects around us. Ubiquitous Communication will allow robust, *ad-hoc* networks to be formed by this broad range of mobile and static devices, forming a ubiquitous system of large-scale distributed networks of interconnected computing devices. By adding intelligent user interfaces and integrating sensing devices, it is possible to identify and model user activities, preferences and behaviours, and create individualised profiles. These key aspects are all required to achieve the idealised Ambient Intelligence (AmI) Environment, a concept which has been formalised by the European ISTAG[39].

The aim of the AmI environment is to provide a context aware system, using unobtrusive computing devices that will improve the quality of people's lives by acknowledging their needs, requirements and preferences and thus acting in some way on their behalf. To achieve this, the 'intelligent' environment, or rather an intelligent *agent* within the environment, needs to build up a profile of each individual, and be able subsequently to link the profile with the correct individual. In essence, the environment has become the interface to the distributed, seamless and invisible AmI. In a world where computing is truly ubiquitous, the environment will monitor direct interaction of people with objects and profiles will seamlessly follow the individual to whom they are linked.

The concept of AmI provides a wide-ranging vision of how the Information Society will develop. Certainly the emphasis of AmI is on greater user-friendliness, more efficient services support, user-empowerment, and support for human interactions. However, to achieve this, the differing facets of the AmI system need to be interoperable.

[39] *Information Societies Technology Advisory Group*

10.2 Interoperability issues

The issues relating to interoperability in AmIs have three key dimensions: Political/social (informal), formal and technical.

The AmI infrastructure is built on the notion that *ad-hoc*, complex, heterogeneous networks can function and communicate in a seamless and interoperable way. Only in this way can the broad range of services envisaged be offered to the individual. Essentially, the AmI is expected to embrace the *heterogeneity* arising from the different network technologies such that it appears *homogeneous* to the user. The vision is to allow for co-operation between networks on demand and without the need for offline negotiation between network operators.

The importance of this was underlined by the ISTAG, who identified three key breakpoints for AmI development [38]. Notably, the first of these is:

". . . under the requirement that AmI calls for a very flexible and seamless interoperation of many different devices on many different networks, it is a *key requirement that there is a set of common platforms or de facto standards to permit this interoperation to take place*."

The group felt that this would either be achieved through a deliberate effort to develop such open platforms or would arise from proprietary pacts between industrial suppliers.

Figure 14: The MultiSphere Reference Model [showing various layers of interaction desirable in the AmI scenario

The scale of this issue is highlighted by examining the levels of interaction that may occur between the user and technology within this AmI context. The 'MultiSphere Reference Model' is shown in Figure 14.

Although this model is aimed primarily at putting issues and ideas of wireless communication in context, from it, and similar models, the following interaction levels can be identified:

- Body area network (BAN) connecting sensors, chips or devices attached to the body/clothes or implanted in the body (distance: <1 meter)
- Personal area network (PAN) consisting of personal and/or shared devices or peripherals (distance: <10 meters)
- Local area network (LAN) for the nomadic access to fixed and mobile networks, and to the Internet (distance: <100 meters)
- Wide area network (WAN) for the access and routing with full mobility (worldwide access)
- The "Cyberworld" where users and intelligent agents interact (virtual)

Within an AmI environment, a seamless interoperability between these different network levels, by proprietary devices from varying manufacturers, needs to be realised. This is only possible if the network technology used is able to support systems integration (i.e. through standard protocols). Already a number of standards for open communication in sensor networks have been proposed. Efforts to make buildings smarter are focusing on cutting costs by streamlining building operations, such as lighting and air conditioning. The most common networks are the BACnet and LonWorks standards, developed for building automation. These standards are geared towards well-defined application areas, and are built on top of well defined network structures. The net result of being so application specific is that many of the visions for AmI cannot be implemented on such systems. In practice, from the technical viewpoint, this may indicate that the AmI scenario is already running into issues of interoperability.

To fulfil the full AmI vision, it is proposed that the AmI acts according to the user's preferences, needs and expectations, thus profiling is the key stone of this scenario (see FIDIS deliverable 7.3 for more information on this area). From an implementation perspective, the agent is the embodiment of the profiling aspect which attempts to build a comprehensive profile of the user by monitoring their interactions, behaviour, preferences, and essentially 'learning' by interpretation of these events in their context. From a purely pragmatic viewpoint, the agent needs to interact with or 'read' from the environment to retrieve data and with services to provide the user with the desired level of support. The key to successful development is the ability to offer interoperable systems such that the agent can 'data link' independent events or stored information with a specific profile. It is reasonable to note here that ultimately the price for such increased interoperability is likely to be borne by a decrease in potential user privacy as personal information becomes readily and widely linkable. In addition, a standardised and interoperable agent that is abstracted from the underlying hardware

such that it operates irrespective of the medium it is running on is required. Finally, the actual services the agent may need to access have to be useable by the agent with the data that it can acquire.

Whether people ultimately find this level of 'surveillance' acceptable is an interesting social question. Either way, it will only be possible provided legal and other interoperability agreements can be constructed. From a legal point of view, an important distinction exists between the notions of 'technical regulations' and 'technical standards'. Technical regulations are created by authorised public authorities and are in principle binding. Most problems of interoperability are however not solved via technical regulations, but via technical standards. Technical standards are prepared by all interested parties (companies, consumers, workers, public authorities) on the basis of a number of principles (e.g. consensus, openness and transparency)[40]. Although they can be very important to solve problems of interoperability, they are in principle not binding. To make these standards legally binding, they have to be included in legal acts. To this end, the most important EU legislative act is Directive 98/34 on technical standards and technical regulations in information society services.[41] This directive imposes a detailed information procedure for technical standards and regulations. However, to date the only related EU standard is laid down in the Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity[42]. Such standards directly relating to AmIs are still yet to be realised.

[40] An extended overview of the European Commission's standardisation policy can be found in the "Vademecum on European standardisation" of the European Commission, available at http://europa.eu.int/comm/enterprise/standards_policy/vademecum/index.htm

[41] Directive 98/34/EC of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society Services, *Official Journal L 204 , 21/07/1998 P. 0037 – 0048.*

[42] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, *Official Journal L 091 , 07/04/1999 P. 0010 - 0028*

11 Conclusion

James Backhouse, LSE

This report has ranged over a wide terrain of interoperability issues and a number of conclusions may be drawn.

- It has demonstrated the value of a relatively simple three level framework of technical, formal and informal aspects for reviewing interoperability issues of different types of IMS. The work of creating interoperability will certainly be aided by widespread adherence to common frameworks. It will be a recurring theme within WorkPackage 4 to search for frameworks that can simplify the task of developing the interoperability of identity management systems. The framework will need to incorporate elements for assessing the degree to which a given IMS performs on each of the three levels.
- While technical standards can remove much of the uncertainty surrounding the compatibility of such systems, developing and specifying such standards is but the first step in the process of interoperation.
- Further work lies in the task of reconciling the legislative and policy rules that govern the way that personal information and identity management is processed and exchanged. At this level there has been progress with the European Union developing its strategies to prepare the ground for electronic IDs for e-government and e-health. Of course there is uneven progress as different countries proceed at different rates – but this is nothing new.
- At the social and cultural level, considerable importance lies in understanding the different normative contexts in which IMS are built and operated. Different perspectives on identity prevail in different national and regional environments and these need to be understood and addressed before progress towards interoperability may be made. Where there is resistance to the untrammelled transfer of identity and personal information, riding roughshod over deeply held views will not necessarily resolve the issue. It may be necessary to enter into dialogues about the benefits that ensue in return for access. This means policymakers must assess public sentiment and the privacy impact of the IMS and act accordingly before pitching headlong into implementations that may arouse deep suspicions and resentment. In some contexts interoperability is seen as the enemy of privacy. Indeed, lack of interoperability may be seen as a bulwark against intrusion into the privacy of personal information. Privacy activists take comfort from the fact that different IMS may not be able to exchange identity information. In these contexts, regard must be had for the role and powers of the data subjects in consenting to their personal information being exchanged between systems.

The database of documents treating interoperability that has been created in this WorkPackage is seen as a significant development for FIDIS and aims to form a living and growing resource to support future research and inquiry.

WorkPackage 4 has a number of deliverables currently developed or under preparations:
In the First WorkPlan Months 1-18

1. D 4.1 Structured account of approaches on interoperability
2. D 4.2 Requirements for interoperability
3. D 4.3 Thematic Workshop (held March 2005)

In the Second WorkPlan Months 18-30

4. D 4.4 Survey on interoperable systems
5. D 4.5 A paper on findings of survey
6. D 4.6 Best Practice Guidelines

12 References

[1]. Backhouse, J. (2000) "Information @ Risk", *Information Strategy*, December/January pp. 33-35.
[2]. Backhouse, J., C. Hsu and A. McDonnell (2003) "Technical Opinion: Toward Public-Key Infrastructure Interoperability", Communications of the ACM, 46 (6), pp. 98-100.
[3]. Baecker, D., Organisation als System; Suhrkamp, Frankfurt am Main 1999.
[4]. Bellamy. Ch. & J. Taylor (1998), Governing in the information age, Open University press, Buckingham
[5]. Bernard, L. *et al* (2005) 'The European geoportal – one step towards the establishment of a European Spatial Data Infrastructure', *Computers, Environment and Urban Systems*, 29: 15-31.
[6]. Bauer Matthias, Meints Martin (ed.): Structured Overview on Prototypes and Concepts of Identity Management Systems; FIDIS Del. 3.1; available from http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.pdf
[7]. Beech D 1997 Data semantics on the information superhighway. In Meersman R, Mark L (eds) Database Application Semantics. Chapman and Hall.
[8]. Biometric Technology Today (BTT): Sept 2003.
[9]. Brodeur, J. *et al* (2003) 'Revisiting the Concept of Geospatial Interoperability within the Scope of Human Communication Processes', *Transactions in GIS*, 7, 2:243-265.
[10]. BTT: Biometric Technology Today Sept 2003.
[11]. Camenisch, J and Lysyanskaya, A. (2001) "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation", Eurocrypt, available at http://www.zurich.ibm.com/~jca/papers/eprint.pdf
[12]. CAP Gemini Ernst Young (2003) "Online Availability of Public Services: How Does Europe Progress?" Brussels.
[13]. CEN/ISSS (2004) "Towards an Electronic Id for the European Citizen, a Strategic Vision". in *CEN/ISSS Workshop eAuthentication*, Brussels,03.10.2004, pp. 1-71, CEN/ISSS Workshop eAuthentication.
[14]. Castells, M. (2001) *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford University Press: Oxford.
[15]. Chen, D. & Doumeingts, G. (2003) 'European initiatives to develop interoperability of enterprise applications – basic concepts, framework and roadmap', *Annual Reviews in Control*, 27: 153-162.
[16]. Choi, S-Y. & Whinston, A. B. (2000) 'Benefits and requirements for interoperability in the electronic marketplace', *Technology in Society*, 22: 33-44.
[17]. CIA (2003). "The World Factbook 2002." http://www.faqs.org/docs/factbook/index.html Accessed On 15.03.2005
[18]. Clarke R. (1999) "Privacy criteria for PKI" developed: http://www.anu.edu.au/people/Roger.Clarke/DV/PKI2000.html. Anonymity, pseudonymity and data minimsation in the context of public key infrastructures (KULRD)
[19]. Cowcher, R. (2005) *Current Issues on Interoperability* 09.03.05. (Personal communication).

[20]. Deloitte (2005). "eMayor Project." http://www.deloitte.com/dtt/section_node/0%2C2332%2Csid%25253D28578%2C00.html Accessed On 20.03.05
[21]. Dumortier, J. and Goemans, C. (2004) "Privacy Protection and Identity Management" in Security and Privacy in Advanced Networking Technologies, NATO Science Series, Series III: Computer and Systems Sciences – Vol 193, IOS Press, 2004, pp. 191-212.
[22]. Documents of the Article 29 Working Party, available at http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm and especially:
- Working document on on-line authentication services, WP 68, 2003
- Working document on first orientations of the Article 29 Working Party concerning on-line authentication services, WP 60, 2002
[23]. Enterprise DG (2005). "Networking of Public Administrations - the Ida Mission." http://europa.eu.int/idabc/en/document/78/25 Accessed On 07.03.2004
[24]. Etzioni, A. (1999) "Chapter 6" in The Limits of Privacy, (Etzioni, A. ed.) Basic Books, New York, pp. 183-215.
[25]. European Commission DGV (1999) Free Movement and Social Security: Citizens' Rights when Moving within the EU, Bulletin No. 2.
[26]. GUIDE (2005). "Creating a European Identity Management Architecture for Egovernment." http://istrg.som.surrey.ac.uk/projects/guide/ Accessed On 20.03.05
[27]. Hayat, A., H. Leitold, C. Rechberger and T. Rössler (2004) "Survey on Eu's Electronic-Id Solutions" *10.08.2004* Vienna.
[28]. Harvey, F. *et al* (1999) 'Semantic interoperability: A central issue for sharing geographic information', *The Annals of Regional Science*, 33: 213-232.
[29]. Homburg, V. & Bekkers, V. (2002) 'The Back-Office of E-Government (Managing Information Domains as Political Economies)', *IEEE*, proceedings of the 35th Hawaii International Conference on System Sciences.
[30]. IDABC (2005), 'European Interoperability Framework for Pan-European eGovernment Services', V 1.0.
[31]. Information Society and Media DG (2005a). "Egovernment Interoperability and Pan-European Services." http://europa.eu.int/information_society/activities/egovernment_research/focus/interoperability/index_en.htm#projects Accessed On 07.03.2005
[32]. Information Society and Media DG (2005b). "Information Society Policies at a Glance." http://europa.eu.int/information_society/policy/index_en.htm Accessed On 15.03.05.
[33]. Information Society and Media DG (2005c). "Search for Individual Research Projects Funded under Fp5 and Fp6 by the Ist Programme." http://www.cordis.lu/ist/projects/projects.htm Accessed On 07.03.2005
[34]. 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
[35]. Information Society Technologies (2005b). "Government User Identity for Europe - Creating an European Standard for Interoperable and Secure Identity Management Architecture for Egovernment." http://dbs.cordis.lu/fep-cgi/srchidadb?ACTION=D&SESSION=108972004-4-

14&DOC=165&TBL=EN_PROJ&RCN=EP_RCN:71101&CALLER=IST_UNIFIEDSRCH Accessed On 20.03.05
[36]. IntelCities (2005). "Project Summary." http://www.intelcitiesproject.com/wcm-site/jsps/index.jsp?type=page&lg=en&cid=5048&cidName=ABOUT&parentId=5046&from=child Accessed On 20.03.05
[37]. IST (2005) IST Information Desk.
[38]. ISTAG (2001), "Scenarios for Ambient Intelligence in 2010", Edited by Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J. & Burgelman, J-C., IPTS-ISTAG, EC: Luxembourg, ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf , ISBN 92 894 0735 2
[39]. Iversen, J. M. J., H. Kubicek, H. Westholm and R. Cimander (2004) "Reorganization of Government Back Offices for Better Electronic Public Service European Good Practices (Backoffice Reorganization)" *Danish Technological Institute and University of Bremens* Bremen.
[40]. Kesterling, A., Kommunikation unter Anwesenden – Studien über Interaktionssysteme; Frankfurt am Main, 2000.
[41]. Kesterling, A., (ed.), Luhmann, N., *Die Religion der Gesellschaft*, Suhrkamp Verlag, Frankfurt am Main, 2000.
[42]. Kinder, T. (2003) 'Mrs Miller moves house: the interoperability of local public services in Europe', *Journal of European Social Policy*, 13, 2: 141-157.
[43]. Kitiyadisai, K. (2004). *Bridging the Digital Divide from a Buddhist Perspective with Implications for Public Policy*. In Proc. Selected Papers from the Computers and Philosophy Conference (CAP2003), Canberra, Australia. Conferences in Research and Practice in Information Technology, **37**. Weckert, J. and Al-Saggaf, Y., Eds., ACS. 91-95
[44]. Klischewski, R. (2003) 'Top Down or Bottom Up? How to Establish a Common Ground for Semantic Interoperability within e-Government Communities', in Traunmüller, R., Palmirani, M. (Hrsg.) 'E-Government: Modelling Norms and Concepts as Key Issues, Proceedings of 1st International Workshop on E-Government at ICAIL 2003'. Bologna: Gedit edizioni, S. 17-26.
[45]. Köhntopp Marit and Pfitzmann Andreas (2004); "Anonymity, unobservability, and pseudonymity - a proposal for terminology". Draft v0.20., September 2004, available from http://dud.inf.tu-dresden.de/Literatur_V1.shtml (v0.5 and all succeeding versions).
[46]. Kraemer, K. L. & King, J. L. (1986) 'Computing and Public Organisations', *Public Administration Review*, Special Issue: 488-496.
[47]. Landsbergen, D. & Wolken, G. (2001) 'Realizing the promise: Government Information Systems and the Fourth Generation of Information Technology', *Public Administration Review*, 61, 2: 206-220.
[48]. Lee, J. L. & Siegel, M. D. (1996) 'An ontological and semantical approach to source-receiver interoperability', *Decision Support Systems*, 18: 145-158.
[49]. Luhmann, N., Die Form 'Person; in: Soziale Welt; 42 (2); p. 167-175, 1991.
[50]. Luhmann, N., Die Gesellschaft der Gesellschaft; 1st Edition; Suhrkamp, Frankfurt am Main 1997.
[51]. Luhmann, N., Organisation und Entscheidung; 1st Edition; Westdeutscher Verlag, Opladen/Wiesbaden 2000.
[52]. Makolm, J. (2002) "Best Practice in E-Government". in *Electronic Government*, EGOV 2002 Aix-en-Provence, Springer Verlag.

[53]. Mason J. & Lefrere, P. (2003) 'Trust, collaboration, e-learning and organisational transformation', *International Journal of Training and Development*, 7, 4: 259-270.
[54]. Meersman R 1997 An essay on the role and evolution of data(base) semantics. In Meersman R, Mark L (eds) Database Application Semantics. Chapman and Hall
[55]. Miller, B. *et al* (2001) 'Towards a Framework for Managing the Information Environment', *Information, Knowledge, Systems Management*, 2: 359-384.
[56]. Moen, W. E. (1994) 'Information Technology Standards: A Component of Federal Information Policy', *Government Information Quarterly* 1, 4: 357-371.
[57]. Moen, W. E. (2000) 'Interoperability for Information Access: Technical Standards and Policy Considerations', *The Journal of Academic Librarianship*, 26, 2: 129-132.
[58]. Montserrat, J. B. (2005). "Enabling an Intelligent Natural Language Based Hub for the Deployment of Advanced Semantically Enriched Multi-Channel Mass-Scale Online Public Services." http://www.bcn.es/hops/ Accessed On 20.03.05
[59]. Mulley, C. & Nelson, J. D. (1999) 'Interoperability and transport policy: the impediments to interoperability in the organisation of trans-European transport systems', *Journal of Transport Geography*, 93-104.
[60]. Ouksel, A. M. & Sheth, A, (1999) 'Semantic Interoperability in Global Information Systems: A brief introduction to the research area and the special section', *SIGMOD Record*, 28, 1: 5-12.
[61]. Pavlau, P. (2002) "Institution-Based Trust in Interorganizational Exchange Relationships: The Role of Online B2b Marketplaces on Trust Formation", Journal of Information Systems, 11 pp. 215-243.
[62]. Prokopiadou, G., Papatheodorou, C. & Moschopoulos, D. (2004) 'Integrating knowledge management tools for government information', *Government Information Quarterly*, 21: 170-198.
[63]. Realini, A. (2004) G2g E-Government: The Big Challenge for Europe.
[64]. Ringwald, A. (2003) "Electronic Identity: Eeurope Smart Cards / Trailblazar 1 "Public Indentity"" eEurope Paris.
[65]. Reffat, R. M (2003) 'Developing a Successful e-Government', *proceedings of the Symposium on e-Government: Opportunities and Challenge*, Muscat Municipality, Oman, pp. IV1-IV13
[66]. Ringwald, A. (2003) "Electronic Identity: Eeurope Smart Cards / Trailblazar 1 "Public Identity"" *eEurope* Paris.
[67]. Snoonian, D. (2003) "Smart Buildings", IEEE Spectrum, pp. 18-23.
[68]. Stalder, F. and D. Lyon (Eds.) (2002) Electronic Identity Cards and Social Stratification, (1) Routledge, New York.
[69]. Stamper, R. *et al* (2000) 'Understanding the roles of signs and norms in organisations – a semiotic approach to information systems design', *Behaviour & Information Technology*, 19, 1: 15-27.
[70]. Schnittger, B. (2005) "Introducing IDABC: European Integration by Electronic Means", *SYNeRGY,* **(01),** pp. 3-6.
[71]. Sheth A (1996) Data Semantics: What, Where and How? Paper presented at the 6th IFIP Working Conference on Data Semantics (DS-6), Atlanta, GA
[72]. Sheth A (1997, 3±4 December 1997). Semantic Interoperability in Infocosm: Beyond Infrastructural and data interoperability in federated information

systems. Paper presented at the International Conference on Interoperating Geographic Systems (Interop'97), Santa Barbara
[73]. Spy-Anderson, P.-J. (2005). "Terregov Project Synopsis." http://www.terregov.eupm.net/my_spip/index.php Accessed On 20.03.05
[74]. Stalder, F. and D. Lyon (Eds.) (2002) *Electronic Identity Cards and Social Stratification,* (1) Routledge, New York.
[75]. Threlfall, M. (2003) 'European social integration: harmonization, convergence and single social areas', *Journal of European Social Policy*, 13, 2: 121-139.
[76]. Verginadis, G. *et al* (2002) 'An Architecture for Integrating Heterogeneous Administrative Services into One-Stop e-Government, EGOV2002 Conference, Aix-en-Provence, September 2-6, 2002
[77]. Wavell, S. (1998) 'Your Very Good Health – in a Foreign Body', Sunday Times, 31 May: 11.
[78]. Weiser, M. (1991), "The computer for the Twenty-First Century", Scientific American 165, 1991, pp. 94-104
[79]. Wimmer, M. & von Bredow, B. (2002) 'A Holistic Approach for Providing Security Solutions in e-Government' *IEEE*.
[80]. Woodall, S. R. (2000) 'Self-jamming behaviour: Joint Interoperability, Root Causes, and Thoughts on Solutions', *Comparative Strategy*, 19: 309-317.
[81]. WWRF (2001), "The book of vision 2001", Version 1.0, Wireless World Research Forum,http://www.wireless-world-research.org/general_info/Bookofvisions/BoV1.0/BoV/BoV2001v1.1B.pdf

13 Acronyms and glossary

AmI	Ambient Intelligence
CA	The Certification Authority in Public Key Infrastructure
Compatibility	Correct exchange of information
Data Marts	Subsets of data resultant from queries to a larger database using specific parameters
eID	Electronic ID
G2C	Government to Citizen. Type of services offered by the Governments to their Citizens.
ICTs	Information and Communication Technologies
IMS	Identity Management System
Interconnectivity	Ability to exchange data between systems
Interoperability	Ability to exchange information between systems correctly and use that information appropriately
ISP	Internet Service Provider
PET	Privacy Enhancing Technologies
PKI	Public Key Infrastructure. Technical and legal infrastructure to issue, manage and revoke digital certificates
TFI	Technical, Formal and Informal. Framework that addresses information systems at the following three levels: technology artefacts; policy describing rules and regulations; and non written human behaviour

14 Appendix A

14.1 China

On June 28 2003, the Third Plenary Meeting of the 10th National People's Longstanding Committee approved "The National Citizen ID Law of the People's Republic of China", becoming effective on January 1, 2004. By now the Chinese government has officially kicked off the world largest National Citizen eID system issuing ultimately contactless chips card to 900 million citizen over the age of 16 to be completed by the end of 2008. Batson, 2003 China's ID-card law doesn't have any provisions controlling how the government or companies can gather and use personal information. Song Gongde, a legal expert at the National School of Administration in Beijing, says he was encouraged by a provision in China's ID law, passed in June, that strictly limits the kinds of data that can be put on the ID card, including name, birth date and the 18-digit citizen ID number. But the law does not give citizens the right to see or correct their personal information, whether it is stored on a card or elsewhere.

14.2 Hong Kong

In August 2003 the government of Hong Kong (Immigration Department) began issuing new multi application eID cards (SMARTICS) to its citizens. The government began issuing smart cards to new arrivals, children eligible for a juvenile ID card on reaching age 11, 18 year olds eligible for an adult ID, individuals applying for replacement cards and those changing data on their ID cards. Existing ID card holders have been called up through public announcements to attend the Smart ID Card Centres in groups, in accordance with their year of birth. Cardholders have a free choice to decide whether to include the applications in their smart ID card or not. Hong Kong residents are also given the option to apply for one year's free use of the Hong Kong Post e-Cert which will be embedded in the chip. Having a year's free use of e-Cert will promote awareness and growth of the service. Hong Kong expects this will also encourage and drive industry initiatives to develop new business applications or services relating to the use of e-Cert on smart ID cards. There are plans to add electronic cash in the future. In the introduction phase much effort was put to address the public concerns of privacy. As a result of these efforts the project now has broad support.

14.3 Malaysia

The Malaysian multi purpose electronic ID (MyKad, internet extension for Malysia + Malaysian word for card) is the most advanced and largest eID project in the world. The Government Multi Purpose Card project is part of the Malaysian Multi-media Super Corridor initiative. This project is one of seven flagship applications deployed by the Malaysian government to attract leading edge technology development to Malaysia. Conceived back in 1997 the MyKad project was awarded to a consortium in May 1999 with an official launch in July 2001. By May 2004 the card had been issued to 11 million people. It replaces the present paper-based identity card that is issued to every Malaysian citizen over the age of 12 years. It is mandatory for all Malaysian citizens (above 12 years old) to be in possession of an identity card. There are 17 million paper based identity cards in circulation on a total population of 21 million.

The government expects to have issued 18 million eID cards by the end 2005. This scheme is on target. The MyKad incorporates the Malaysian national identity card as one of its primary functions. This application is the foundation for the project and forms the basis for it being accorded such high priority by the government. Fraud is fairly high with the old paper based cards. By introducing chip cards the risk of fraud is largely reduced. Also the Malaysian Passport application, owned by the Malaysian immigration department is being incorporated in the MyKad. This should allow cardholders to pass through passport control desks more quickly, and will also eliminate the requirement of manually processing the cardholders' entry or exit. However the card does not replace passports for overseas travels.

The Drivers License application is also integrated in the card. A data file in the MyKad has replaced the existing paper based driving license. The Government wanted to realise a better management of driver records and more accurate tracking of errant drivers. There are currently approximately 7 million paper card-based driver licenses in the country. Both the immigration and driving license application are automatically loaded into the eID chip at the time of card application. The card is also positioned as a national health card, which enables Malaysian citizens the access the free or subsidized health care provided by the government. Personalised medical emergency data (allergies, medications, medical history) is also stored on the cards.

A second (contactless) Electronic Purse was recently added on the card. This complements the existing contact Proton purse and allows payments for retail transactions, tolls on the highways and parking. An upcoming use would be the payment on the urban transport networks. This will add to the convenience of the cardholders. The card supports an Automatic Teller machine (ATM) application for cash withdrawal, e-debit transactions to pay for government services and to conveniently reload the e-purses. This is a bank controlled application, the Malaysian government having developed a convenient methodology for the banks to capture and control this application on the MyKad. A PKI based digital signature application to enable users to conduct secure transactions and encrypt data over the Internet using the same PKI infrastructure. In 2004 the Malaysian Inland Revenue board (RIB) will launch an tax e-filing and stamping system. This will allow tax payers to apply for their tax returns and also get tax forms officially stamped in an on-line process. For this they have to use the digital signature facility on board the MyKad in the communication with the IRB. For cardholder verification the card holds the face (digital colour photograph) and a pair of thumbprint templates (500 bytes per print) of the cardholder. These are captured during the card application process using a specially designed system. The chip used in the MyKad was recently upgraded from an ATMEL 32K Bytes EEPROM micro controller device, to a compatible 64K device, both masked with a proprietary multi application Operation System. The card also holds a Mifare contactless chip for public transport purposes, this being the 2nd e-purse. Chipcard readers have been extensively deployed to police personnel (50,000 units) for checking driving license and ID. Banks, with the Malaysian government's permission, are also deploying devices to read and capture information from MyKad as it allows for the paperless registration of new account holders, the capture of the ATM application (and MEPS Cash e-purse) as well as the easy registration of new credit card holders. One of the big advantages in support of the project was that the Malaysian government had already a very effective National Registration Department that was charged with the issuance and maintenance of a paper based national identity

card. It was this agency that was chosen to lead the deployment of the MyKad project. From the onset of the project, the guiding rule was that, as much of the business processes for the existing identity card system would be retained as possible. This was a crucial element in the success and rapid deployment of the project. Malaysia is also very active in the domain of e-passports. 5 million passports have been issued since 1998 of different generations but all including biometric templates (2 thumbs). Malaysia is now on its way of adapting to the latest ICAO specifications and might very well become the issuer of the first fully ICAO compliant ePassport worldwide.

14.4 Thailand

The Thai Government has started in November 2003 the issuance of a smart card based multi-application national ID card to its citizens. The card is positioned as a communication tool between the Government and the citizen. It supports services from 34 Government bodies. The main purpose of the card is to bring the level of fraud down. Thais have now separate cards for tax, health, social security and the driver's license. The current plastic ID card is mandatory for all Thais over 15 of age. The new combination is called the 'e-card'. The card electronically holds the citizens' personal data, insurance information, healthcare data, social security details from the Labour Ministry, tax information from the Inland Revenue Department and drivers license information. All 61 million citizens of Thailand from the age of 1 year will receive the card, but the first batch of 16 million goes to farmers, government employees and citizens renewing their old ID cards. The Thai Bureau of Registration Administration as the principal went for an 'open platform' card, including Java Card, to allow to add applications post issuance. They choose Java-based chip cards with 52 kilo-bytes of free memory for applications. The cards include digital fingerprints for biometric verification of the cardholder. Nevertheless a government official has said that the first batch of cards did not cost more than 100 Thai baht apiece (US$2.40). Krisana Kitiyadisai [43] says "Buddhist concepts will be the framework for investigating whether the smart card scheme, its objectives, and implementation process are objectionable or acceptable from a Buddhist perspective."