FIDIS

Future of Identity in the Information Society

Title:	"D 8.3 Database on Identity Management Systems and ID Law in the EU"
Authors:	WP8
Editors:	Ioannis Maghiros, Sabine Delaitre (IPTS, Seville), Bert-Jaap Koops (TILT, Tilburg)
Reviewers:	Martin Meints (ICPP, Germany) Denis Royer (JWG, Germany)
Identifier:	D 8.3
Type:	[Deliverable]
Version:	1.07
Date:	Tuesday, 14 March 2006
Status:	[final]
Class:	[Public]
File:	fidis-wp8-del8.3.doc

Summary

This document consists of two parts. Part A puts forward a structure for a database of Identity Management Systems (IMS). Two designs for a database are laid out: a prototype with 29 fields (section 3) and an extended version with a total of 138 fields (section 4). The prototype has been implemented and is accessible online at http://www.jrc.es/projects/ims/imsintrodb.cfm. This document also includes a user manual (section 5) and the technical specifications for the database (section 6). Records will continue to be added to the database of IMS over the coming months and the document describes the next steps in the development process.

Part B introduces a database of ID laws, the Identity Law Survey (IDLS). Section 8 provides the context, and section 9 presents the initial structure of the law survey used to build a prototype, available at http://rechten.uvt.nl/idls/. Sections 10-11 outline a revised database structure, and sections 12-14 provide the interface requirements, user manual, and maintenance plan. The aim is to develop a simple and user-friendly database, providing the public with basic information and knowledge on ID-related laws in the EU and North America.

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

Copyright Notice:

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)*
1	25.07.2005	Initial release of merged deliverables 8.3.1 and 8.3.2 (IPTS) + improvements of part A (section 6 for instance.) (IM, SD)
1.01-1.03	27-31.07.2005	Various minor adjustments (IM, SD)
1.04	03.08.2005	Iterative step (improvement of part B) of the merged version (BJK, SD). Towards the final version.
1.05	04.08.2005	maintenance plan added in part B, some minor adjustments in part B (BJK)
1.06	08.08.2005	user manual part B added (BJK)
1.07	21.09.2005	several small changes to s. 1 and part B (BJK)
1.08	28.11.2005	Maintenance plan for IMS DB, some adjustments for referencing and annex (SD)
1.09 (vf)	12.01.2006	Update of the List concerning IMS in database, cf. annex (SD)
(vf)	19.01.2006	ICPP review
2.0	25.01.2006	Few modifications in order to take into account the ICPP comments.
2.01	24.02.2006	JWG review
3.0	03.03.2006	Integration of adjustments in part B (sent by BJK), revision part A and annex. Executive summary, mapping of database IMS and prototype.

Contributors

Chapter	*Contributor(s)*
1 (Introduction)	Ioannis Maghiros, Sabine Delaitre (IPTS)
Part A (IMS)	Ioannis Maghiros, Sabine Delaitre (IPTS)
Part B (IDLS)	Bert-Jaap Koops (TILT)
Annex	Sabine Delaitre (IPTS)

Table of Contents

Executive Summary

This document reports on the work done during the first period on constituting two data sets: on Identity Management Systems (IMS) and on Identity Law Survey (IDLS). The deliverable, which is made up of the pilot databases and the report that describes them, requires a multi-disciplinary approach, combining technical expertise and legal knowledge. Furthermore information had to be collected from Member States and countries outside the EU in order to provide an extensive set of data. The work was therefore well-suited for the FIDIS network, as partners come from a wide range of backgrounds and from many different countries.

Two data sets and the corresponding database prototypes have been developed: a database of Identity Management Systems and a database (ID Law) on identity with a special focus on legal aspects. The two prototypes were then made operational and this report was developed which provides all kinds of details (structure, user manual, links to prototypes, contents in annex and so on)

This work also serves indirectly as a means of strengthening the integration of the Network of Excellence as it draws on work done in other workpackages. The IMS database for example uses an IMS classification system developed in collaboration with deliverable 3.1 and extends this work. The structured archive of ID laws makes use of the information on identity theft laws collected in Workpackage 5 (deliverable D5.1).

Deliverable 3.1 is directed at an audience of academics, EU policy-makers, experts from technological, social science and legal disciplines and interested citizens. It gives an overview of existing identity management systems (IMS). Different types, classes and subclasses of IMS are identified, described and illustrated by example of existing IMS. More specifically there are three types of IMS that have been identified:

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

Additionally, a search on existing implementations of IMS including prototypes and concepts leads to three classes of solutions:

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

The document describing Deliverable 5.1, gives the first results of a survey on legislation on ID theft in EU member states and the US. Unlike the US, EU countries appear to have no specific legislation on ID theft or ID fraud. The survey of ID theft legislation started in December 2004, co-ordinated by Tilburg University with the help of the FIDIS network

members. Since then, a network of country correspondents has been set up of legal experts who provide information about the legal situation in their country. This network is still evolving, since only a minority of the 25 EU member states are represented in FIDIS. We have so far restricted ourselves to finding contacts in the countries with FIDIS members, and will extend the network with correspondents of the other EU countries in the second Workplan period.

Part A of this report puts forward a structure for a database of Identity Management Systems (IMS). Two designs for a database are laid out: a prototype with 29 fields (section 3) and an extended version with a total of 138 fields (section 4). The prototype has been implemented and is accessible online at http://www.jrc.es/projects/ims/imsintrodb.cfm. This document also includes a user manual (section 5) and the technical specifications for the database (section 6). Records will continue to be added to the database of IMS over the coming months and the document describes the next steps in the development process.

Part B introduces the corresponding database of ID laws, the Identity Law Survey (IDLS). Section 8 provides the context, and section 9 presents the initial structure of the law survey used to build a prototype, available at http://rechten.uvt.nl/idls/. Sections 10-11 outline a revised database structure, and sections 12-14 provide the interface requirements, user manual, and maintenance plan. The aim is to develop a simple and user-friendly database, providing the public with basic information and knowledge on ID-related laws in the EU and North America.

Two prototypes have been thus produced; one of a database of Identity Management Systems (IMS dB) and one of a database on identity with a special focus on legal aspects (ID Law dB). Future work foresees that the databases will be integrated within the FCI (FIDIS infrastructure) and that the two existing databases in IMS and ID Law dB will be maintained. All of this work will be reported in deliverable D8.6. The maintenance activity foreseen could be placed under WP8 or WP3 or WP5.

The Annex provides details of the records available in both databases that have an international scope. IMS database counts 32 IMS records mainly identified in Europe and USA and ID law database covers EU countries and the following countries MEXICO, CANADA and USA. For each country several records related to ID Law are available.

1 Introduction

The third deliverable of Work Package 8, "Integration of the NoE", is a Database on Identity Management Systems available in the EU and ID laws.

This document presents the work on this deliverable. It consists of two parts. Part A (sections 2-8) corresponds to deliverable 8.3.1: a database of Identity Management Systems (IMS). Part B (sections 9-15) relates to deliverable 8.3.2 on a structured archive of ID laws, searchable by country and by legal topic.

1.1 FIDIS Background

FIDIS objectives are shaping the requirements for the future management of identity in the European Information Society and contributing to the technologies and infrastructures needed. FIDIS work is structured into 7 research activities:

- "Identity of Identity"
- Profiling
- Interoperability of IDs and ID management systems
- Forensic Implications
- De-Identification
- HighTechID
- Mobility and Identity

As a multidisciplinary and multinational NoE FIDIS, appropriately, comprises different country research experiences with heterogeneous focuses, and integrates European expertise around a common set of activities. Additionally, all relevant stakeholders are addressed to ensure that the requirements are considered from different levels. FIDIS overcomes the extreme fragmentation of research into the future of identity by consolidating and fostering joint research in this area. Research results will be made accessible to European citizens, researchers and in particular to SMEs.

1.2 Background on Deliverable 8.3

As stated previously, deliverable 8.3 is comprised of two parts. The first is a database of Identity Management Systems. The purpose of this database is to collect the key information on all available and prototype IMS in one place. This can function as a means to enhance innovation, as users of the database can identify what attributes are missing from existing systems and which areas need further development. The public can also makes use of this information as electronic identity management becomes increasingly important and more and more identity information becomes digitalised. The second part of the deliverable is a

structured archive of identity laws, the Identity Law Survey (IDLS). This archive contains information on several kinds of ID laws and is searchable by country and legal topic.

The maintenance plans for both databases IMS and IDLS are different in vision for the future mainly due to the different nature of database in terms of objective, size and contents.

This deliverable requires a multi-disciplinary approach, combining technical expertise with legal knowledge. Furthermore information has to be collected from member states and countries outside the EU in order to provide an extensive survey of available data. The work is therefore well-suited for the FIDIS network, as partners come from a wide range of backgrounds and from many different countries.

This work also serves indirectly as a means of strengthening the integration of the Network of Excellence as it draws on work done in other workpackages. The IMS database for example uses an IMS classification system developed in deliverable 3.1 and extends this work. The structured archive of ID laws makes use of the information on identity theft laws collected in Workpackage 5.

The final aim for this deliverable is to develop two simple and user-friendly archives, one providing the public with an overview of all identity management systems and the other with information on ID-related laws in the EU and North America.

2 Part A – Introduction

Part A is an overview of the work that has been conducted for the database of Identity Management Systems. The starting point for this work is the information already available among partner organisations and in particular based on work performed by partner ICPP and IPTS which resulted in an in-depth study[1] on the IMS. This section explains what Identity Management Systems are, how they have been categorised and how the work on this deliverable is being conducted. Section 3 presents the prototype database structure. This is the functional specification for the actual database that has been developed by FIDIS partners. Section 4 is an extended version of the database design, with more than 100 additional fields. This is called the prospective database structure; some fields are not currently applicable, but it is expected that they might be in the future. As the database is updated, these fields may be incorporated into the design as necessary. Section 5 contains a user manual for the database that has been developed. Section 6 covers the technical aspects of the database and section 7 describing the maintenance plan concludes Part A.

2.1 Identity Management System: General Presentation

Identity Management Systems (IMS) are considered to be the citizen's gateway to the Information Society. Because of the growing number of services, IMS could even be presented as a critical tool for the citizen. Its utility as an almost unique access tool to many enhanced facilities of the Information Society will make it the "electronic" witness of a great part of the citizen's online life. An IMS will have to comply with the regulatory framework concerning the protection of the user privacy rights. Indeed, the acceptance of such systems will be based not only on their usability or ease of use but also on their effectiveness in respecting and preserving the privacy of their users.

IMS should enable the citizen to keep control or at least be aware (depending on the situation) of the nature and amount of personal data released. The most valuable IMS will be the one that allows multipurpose usage in order to preserve the privacy level of the user, while enabling multilateral and multi-channel security requirements.

Three of the main advantages of IMS are that they will:

- **Enable new services**: for example, they will allow a citizen to go to a single web site for (a) their health care needs, such as viewing their medical records, (b) paying doctors bills and (c) ordering drugs from the pharmacy. This example which illustrates the concept of "web services" shows the implication of the requirement to grant to several actors in the delivery chain different levels of access to a user's personal data.
- **Reduce the level of risk, and thus create a trustworthy environment**: in the digital world, identity is easy to fake. Indeed this environment is characterised by three enabling dimensions: (a) the ability to produce endlessly exact or true copies of information; (b) technologies that tend to facilitate the flow of personal information;

[1] ICPP, SBG: "Identity Management Systems (IMS): Identification and Comparison Study", September 2003, under contract from the IPTS.

and (c) cyber criminals who use exact copies of personal information to pretend they are someone else, thus effectively stealing someone else's identity. IMS will help guard the flow of personal information as well as impose authentication procedures to identify fake copies.

- **Help find an acceptable balance between privacy and security needs**: IMS will have to simultaneously (a) communicate the required personal data only and (b) respect the legal framework in which this service takes place by, for example respecting the requirements of law or taxation authorities.

2.2 Description of project target

The IMS database is being developed in two phases. Work on the first phase began in March 2004. Two versions of a functional specification for the database have been created. At first an extended database structure was developed with 138 fields in total. It was expected that the market would evolve rapidly and that many of these fields would quickly become necessary. In practice many of the products on which the initial analysis was based simply disappeared and so a second version was developed, the 'prototype database' which consists of 29 fields. These 29 fields cover the main features and attributes of IMS which are presently available and they leave scope for future developments.

The prototype database was developed using Microsoft Access which was later on moved on to an Oracle platform and is currently accessible via a web interface at http://www.jrc.es/projects/ims/imsintrodb.cfm. Ten full records have been introduced thus far into the database. For the remainder of the first 18-month period, which ends in September 2005, the FIDIS partners involved in developing the database will continue to add records.

In the second phase of development, the database will be made accessible to the general public. In particular, manufacturers and developers of IMS will be contacted in order to make them aware of the database and to request information on their products. During this phase, more records will be added to the database either by product developers themselves or by FIDIS partners. The classification of IMS according to type and class used and developed in D3.1 is also used in this database, so the information collected there will be re-used and extended for the IMS database. As developments in the field of IMS take place quickly, the database will need maintenance and updating throughout this second phase. This will be done by the IPTS in conjunction with the ICPP.

2.3 Examples of current IMS

The list of IMS below is taken from the Identity Management Systems (IMS): Identification and Comparison Study that was carried out by the Independent Centre for Privacy Protection (ICPP) and Studio Notarile Genghini (SNG) in 2003. As such there are some IMS that have emerged in the last two years that are missing from this list and there are certain IMS that no longer exist. Nevertheless, the list provides a good overview of the main systems available on

the market and furthermore it gives some indication of the main functionalities offered by each. The database will build on this existing expertise and add further information.

Name	Manufacturer	Nation	Available
DASIT	Fraunhofer Gesellschaft	Germany	C
DRIM	TU Dresden	Germany	C
idemix	IBM	Switzerland	C
Kerberos tickets	Div.	Div.	C
KeyNote Trust management	KeyNote	Div.	C
MiCircles	Midentity.com	UK	C
Midentity	Midentity.com	UK	C
OpenPrivacy	OpenPrivacy Initiative	USA	C
OTPW	University of Cambridge	UK	C
P3P	W3C	Div.	C
PRIMA DataManager / IJournal	TU Darmstadt	Germany	C
Privacy Network	ID-Vault	USA	C
Private Credentials	Zero Knowledge / Stefan Brands	Canada	C
Trusted Transaction Roaming Project	The Open Group	Div.	C
WS-Security	IBM	USA	C
ATUS	Uni Freiburg	Germany	P
IDMAN	TU Dresden	Germany	P
LibertyAlliance	Div.	Div.	P
Parkinsonpas	City of Alphen a/d Rijn	Netherlands	P
SAML	Div.	Div.	P
TrustBridge	Microsoft	USA	P
XNS	OneName Corporation / Public Trust Organisation	USA	P
Erreichbarkeitsmanager	Uni Freiburg / Gottlieb Daimler- und Karl Benz-Stiftung	Germany	SP
It's My Profile	Prosumer Corp.	USA	SP
Orby Privacy Plus	YouPowered	?	SP
Playboy Privacy Pass	Playboy	USA	SP
SafeZone	Incogno	USA	SP
TrueSign	Privador	Estonia	SP
AccountCourier	Courion	USA	A
Anonymizer Privacy Manager	Anonymizer	USA	A

AssureAccess	Entegrity	USA	A
Certification Authorities	Div.	Div.	A
ClearTrust	RSA Security	Ireland	A
Cookie Pal	Kookaburra Software	USA	A
CookieCooker	TU Dresden	Germany	A
Digital Handshake	iLumin	USA	A
Digital Identity	Ascio Technologies	Denmark	A
Digital Signature Certification	Verisign	USA	A
DigitalMe	Novell	USA	A
Dotomi	Dotomi	Israel	A
eBay	eBay.com	USA	A
eTrust	Computer Associates	USA	A
Every.one.name	Global Name Registry	UK	A
eWallet	Gator	USA	A
FINEID	Population Register Centre	Finland	A
Flirtmaschine.de	Matchnet	Germany	A
Freedom	Zero Knowledge Systems	Canada	A
Freever	Freever	France	A
GetAccess	Entrust	USA	A
Hushmail	Hushmail.com	Canada	A
ID2	Nexus AB	Sweden	A
iPrivacy	iPrivacy	USA	A
Keon	RSA Security	USA	A
Lotus Notes	Lotus	USA	A
ManageID Suit	Blockade	USA	A
Match	Match.com	USA	A
Meetup	Meetup	USA	A
Mozilla 1.4	Mozilla / Open Source	Div.	A
Netidentity	Netidentity	USA	A
NetKey	Kobil	Germany	A
NetPoint	Oblix	USA / UK	A
Outlook Express 6 (Internet Explorer 6)	Microsoft	USA	A
Passport	Microsoft	USA	A
Persona	Persona	USA	A
PGP / GnuPG	Div.	Div.	A
PingID	PingID	USA	A
Policy Manager	Omniva / Disappearing	USA	A
Privacy Companion	IDcide	USA / Israel	A
Privacy Manager	Tivoli Systems / IBM	USA	A
Private Payments	American Express	USA	A
Roboform	Siber Systems	USA	A
Secretmaker	Secretmaker.com	USA	A

SelectAccess	Baltimore Technologie	Ireland	A
SiteMinder	Netegrity	USA	A
Shibboleth	Open Source	USA	A
Spamex	SaferSurf.com	Germany	A
Speednames	Ascio Technologies / Speednames	Denmark	A
Sun One / Network Identity	Sun	USA	A
The Sims Online	Electronic Arts	USA	A
There	There.com	USA	A
Upoc	Upoc	USA	A
Vanquish	Vanquish	USA	A
v-Go Single Sign-On	PassLogix	USA	A
VigilEnt	netiQ	USA	A
Viral	Another.com	UK	A
Virtual ID Card	University of Texas	USA	A
X/MCARE	ICL/Simac/McKesson HBOC	Netherlands	A
Yodlee	Yodlee	USA	A

An updated and structured list is available in D3.1, chapter 4.3.

2.4 Database design and categorisation

In cooperation with deliverable 3.1 of WP3 of FIDIS and using definitions established in the FIDIS Network of excellence (deliverable 2.1), the proposed structure for the IMS database reflects the following **three types** of IMS:

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

Within each type of IMS there are **three classes** of solutions:

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

The IMS database is thus structured as follows. On the top level are the general data that pertain to all IMS (section 3.1); these include information on the evaluators, general identifiers, costs, platform and environment. The next level is section 3.2 which categorises the IMS according to **type** (Type 1, Type 2 or Type 3 as set out above) and according to **class**.

3 Prototype database structure

This section shows the structure of the database that has been developed. It is currently being tested and added to by FIDIS partners. It differs to the full structure outlined in the annex in a few key ways. First it has none of the detail on functionality that is seen in the full structure. Some fields are removed because at present data for most of the investigated IMS is simply not available. Other fields are removed because they are not relevant to currently available IMS. The result is an intentionally abbreviated structure, which removes many sections in order to provide ease of use.

As and when data becomes available, the database can be expanded to include more of the fields outlined in the full structure.

3.1 General Attributes

The general attributes describe the basic information of an IMS by a first set, which allows the IMS to be identified and by a second one dealing with the platform and the environment.

Remark: the last column Y/N of the tables indicates if yes or no the attribute effectively is in the prototype.

3.1.1 Evaluation of IMS

This section covers the basic details about the evaluation, i.e. the entry of the IMS in question into the database.

The general attributes describe the basic information of an IMS by a first set, which allows the IMS to be identified and by a second one dealing with the platform and the environment.

Attribute Label	Definition	Values	Y/N
Evaluators	Name(s) of the evaluator(s)	Text	Y
Evaluators' Organisation	Organisation(s) of the evaluator(s)	Text	Y
Date of evaluation **(Date of contribution)**	Date(s) of the evaluation of the IMS and of the contribution	Date	Y

3.1.2 Identification of IMS

This section of the database is for the purpose of providing a general overview. Users can search by name, by provider, by country or by state of development.

Attribute Label	Definition	Values	Y/N
Name	Name of the IMS	Text	Y
Version number	Version of IMS	Text	Y

Attribute Label	Definition	Values	Y/N
Manufacturer	Main manufacturer or provider of the IMS	Text	Y
Nation	Nation of the manufacturer's location	Text	Y
Sources of information (References)	Sources of information, links, etc. and the IMS version number to which references refer, if possible avoiding 'marketing information'.	Text (including hyperlinks)	Y
Supported languages		Possible values (more than one can be selected): Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Slovak, Slovene, Spanish, Swedish	Y
Open/Closed	"Open IMS" means that the identities work with several systems or applications outside the IMS. "Closed IMS" means that the scope of the identities is restricted to the IMS context.	Enumerated: Closed, Open	Y
State of deployment	Statement whether the IMS is an available product or a service on the market (Available) or if it is a Prototype, a Suspended prototype, or just a Concept.	Enumerated: Available, Prototype, Suspended prototype, Concept	Y
Regions (Geographical scope)	Regions where the IMS is available	Enumerated: National, European, Global	Y

3.1.3 Platform and environment

Attribute Label	Definition	Values	Y/N
Requirements (Hardware /	Description of the hardware, software, operating system and	Text	Y

Attribute Label	Definition	Values	Y/N
software requirement)	services the IMS requires		
Number of Users **(Installation base IMS)**	Number of users of the IMS	Text	Y
Standards **(Interoperability / standards)**	Description if the IMS can be used with other applications and systems. This could be achieved by using standards like protocols for communication. This field will include the standards that the IMS adheres to, e.g. Liberty Alliance	Text	Y
Server-side component(s)	Description of the server-side-components (data-storage and processing)	Text	Y
Client-side component(s)	Description of the client-side-components (data-storage and processing)	Text	Y
Description of Methods	Description of methods (e.g. encryption), how the control of the user over his identity-related data is established with respect to availability, integrity and confidentiality.	Text	Y
Functionality **(Description of functionality / features -client and server-)**	Trust metric system for online communities. (What is the characteristic / speciality? Handling of identities? Use of pseudonyms / roles? Support of anonymity? Use of electronic signatures / PKI? Storage of data? Handling of accounts? Password management? Security / encryption, etc.? Data protection? Privacy Enhancing Technologies? Data minimisation? Support of law enforcement? Usability? […])	Text	Y
Seals **(+ other field for the text: which seal)**	Privacy and other seals that certify that the IMS applies to law.	Boolean: yes / no + text	Y

Attribute Label	Definition	Values	Y/N
Third party **(Support by third parties)** **(+ other field for the text: which third party)**	Description of which third party or intermediary support is integrated, e.g., certificate providers, IMS providers, delivery services, payment services, ...	Boolean (yes/no) + text	Y
Nature (of provider / distributor)	Description of the nature of the provider of the system. (e.g. public, private, regional, national, international)	Text	Y
Flow chart	Shows how data is processed within the IMS, which parts are involved.	Picture	Y
Screenshot	One screenshot	Picture	Y

3.1.4 Cost

Attribute Label	Definition	Values	Y/N
Price **(Purchase/Licence)**	Purchase cost in EUR	Real	Y
Comment to the cost **(Purchase cost comment)**	Any additional information on the field above	Text	Y

3.2 Type and class of IMS

The types and classes of IMS are defined in section 2.4 of this document.

Attribute Label	Definition	Values	Y/N
Type of IMS	Type 1, 2 and/or 3 as per definition of types outlined in section 2.4	Enumerated: type 1, 2, 3 (more than one type can be selected)	Y
Class of IMS	Class 1, 2 or 3 as per definition of	Enumerated: type 1, 2 or	Y

Attribute Label	Definition	Values	Y/N
	types outlined in section 2.4	3	
Main functionality	The evaluator is asked to describe the main functionalities and is given a list of possible examples: account management (including auditing accounts), access management (including role-based provisioning), meta-directory, password management, form filling, reachability management (allow filtering of incoming communication), single sign-on.	Text	Y

4 Prospective database structure

The database structure outlined here proposes a full set of attributes, some of which are not to be found on existing IMS. The reason for this is that the design of the database aims to take a prospective approach and anticipate future developments. This will make it easier to update the database in the future and it may highlight areas where further development is needed in existing IMS.

It is only when available commercially IMS include one or more of the proposed data fields that a new version of the database will have to be produced.

It is not desirable however to have a cumbersome structure at present in the initial phase of the database's development; it would decrease the usability of the database and make it less likely that all IMS would be entered onto the system. For this reason, only certain key attributes out of the ones listed below have been selected for the prototype. The attributes included in the prototype structure are in bold. Additional fields which are not at present included are indicated with an asterisk.

4.1 General Attributes

The general attributes describe the basic information of an IMS by a first set, which allows the IMS to be identified and by a second one dealing with the platform and the environment.

4.1.1 Evaluation of IMS

This section covers the basic details about the evaluation, i.e. the entry of the IMS in question into the database.

Attribute Label	Definition	Values
Evaluators	Name(s) of the evaluator(s)	Text
Evaluators' Organisation	Organisation(s) of the evaluator(s)	Text
Date of contribution	Date(s) of the evaluation of the IMS and of the contribution	Date

4.1.2 Identification of IMS

This section of the database is for the purpose of providing a general overview. There are some attributes that may relate to later ones, but the objective is to gather all the information that serves to identify the IMS. Users can search by name, by provider, by country or by state of development.

Attribute Label	Definition	Values
Name	Name of the IMS	Text
Version number	Version of IMS	Text
Manufacturer	Main manufacturer or provider of the IMS	Text
Nation	Nation of the manufacturer's location	Text
References	Sources of information, links, etc. and the IMS version number to which references refer, if possible avoiding 'marketing information'.	Text (including hyperlinks)
Supported languages		Possible values (more than one can be selected): Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Slovak, Slovene, Spanish, Swedish
Closed/Open IMS	"Closed IMS" means that the scope of the identities is restricted to the IMS context. "Open IMS" means that the identities work with several systems or applications outside the IMS.	Enumerated: Closed, Open
Closed/Open Source (*)		Enumerated: Closed, Open
State of deployment	Statement whether the IMS is an available product or a service on the market (Available) or if it is a Prototype, a Suspended prototype, or just a Concept.	Enumerated: Available, Prototype, Suspended prototype, Concept
Distribution (*)	If the IMS is available, then this field should be filled in to state whether the IMS is sold commercially, distributed through shareware, freeware or is part of the public domain.	Enumerated: Commercial, Shareware, Freeware, Public Domain

Attribute Label	Definition	Values
Geographical scope	Regions where the IMS is available	Enumerated: National, European, Global

4.1.3 Platform and environment

This section would include data allowing users to search by hardware or software solutions and to search for IMS which adhere to a certain standard, e.g. Liberty Alliance.

Attribute Label	Definition	Values
Hardware / software requirement	Description of the hardware, software, operating system and services the IMS requires	Text
Installation base IMS	Number of users of the IMS	Text
Installation, maintenance, use (*)	Brief description of the installation process and use of the system if the system is a commercially available one.	Text
Modularity (*)	Modularity means that the routines are grouped into independent, distinct blocks (modules) within each service area defined by the system architecture. In addition, each block has a single function and well-defined parameters and interfaces.	Boolean: yes / no + text
Market availability (*)	Description of the system availability. The 'state of deployment' attribute in section 4.1.2 above is described here with text. For example, if the IMS is currently a prototype, this field might provide an estimate of when the system will be available.	Text
Interoperability / standards	Description if the IMS can be used with other applications and systems. This could be achieved by using standards like protocols for communication. This field will include the standards that the IMS	Text

Attribute Label	Definition	Values
	adheres to, e.g. Liberty Alliance	
Guarantee of trustworthiness (*)	Description of the guarantees for the trustworthiness of the system. This is not obtained to the single functionality, but to the entire system and mainly to the trustworthiness of the manufacturer. Seals of third parties may be described here.	Text
Legal and contractual framework (*)	Description by providing references of the legal and contractual framework of the IMS and the manufacturers.	Text
Server-side component(s)	Description of the server-side-components (data-storage and processing)	Text
Client-side component(s)	Description of the client-side-components (data-storage and processing)	Text
Description of Methods	Description of methods (e.g. encryption), how the control of the user over his identity-related data is established with respect to availability, integrity and confidentiality.	Text
Description of functionality / features (client and server)	What is the characteristic / speciality? Handling of identities? Use of pseudonyms / roles? Support of anonymity? Use of electronic signatures / PKI? Storage of data? Handling of accounts? Password management? Security / encryption, etc.? Data protection? Privacy Enhancing Technologies? Data minimisation? Support of law enforcement? Usability? […]	Text
Seals	Privacy and other seals that certify that the IMS applies to law.	Boolean: yes / no + text
Support by third parties	Description of which third party or intermediary support is integrated, e.g., certificate providers, IMS	Boolean (yes/no) + text

Attribute Label	Definition	Values
	providers, delivery services, payment services, ...	
Nature of provider / distributor	Description of the nature of the provider of the system. (e.g. public, private, regional, national, international)	Text
Flow chart	Shows how data is processed within the IMS, which parts are involved.	Picture
Screenshot	One screenshot	Picture

4.1.4 Cost

Only the first field has been included in the prototype as data is not available on the other fields and it would be difficult to provide reasonable estimates.

Attribute Label	Definition	Values
Purchase/Licence	Purchase cost in EUR	Real
Purchase cost comment	Any additional information on the field above	Text
Deployment (*)	Estimate of deployment costs excluding purchase/licensing costs included above	Real + text to describe costs included in this category
Maintenance (*)	Estimate of average maintenance costs	Real + text to describe costs included in this category
Training (*)	Estimate of costs of training users	Real + text to describe costs included in this category
Technical resource requirements (*)	Description of the technical resources that are necessary, pointing out the number of people needed for operation and the costs.	Text

4.2 Type and class of IMS

This is the first section where the prototype differs significantly from the full structure. The full structure suggests many detailed fields covering each type of functionality in detail. The

prototype just includes the three fields below. The full structure on the other hand has many additional sections.

Attribute Label	Definition	Values
Type of IMS	Type 1, 2 and/or 3 as per definition of types outlined in section 2.4	Enumerated: type 1, 2, 3 (more than one type can be selected)
Class of IMS	Class 1, 2 or 3 as per definition of types outlined in section 2.4	Enumerated: type 1, 2 or 3
Main functionality	The evaluator is asked to describe the main functionalities and is given a list of possible examples: account management (including auditing accounts), access management (including role-based provisioning), metadirectory, password management, form filling, reachability management (allow filtering of incoming communication), single sign-on.	Text

4.3 Type 1 IMS attributes

From this point, all further fields have been left out of the prototype. This section is aimed at all IMS that have type 1 functionality or any combination that includes type 1 functionality. These are covered in a high level of detail covering various topics:

- Functionality,
- Security Protection,
- Privacy Protection,
- Interoperability/Standards
- Usability.

The first two are a compound of sub-topics. In fact, Functionality topic deals with Identity Management, User/Account Management, Password Management and other operational areas. Security Protection encompasses Authentication, Authorisation, Accounting/Auditing, Encryption, Security Properties, Law Enforcement and Liability and Trustworthiness.

4.3.1 Functionality

4.3.1.1 Identity Management

Attribute Label	Definition	Values
Automatic choice of the identity (*)	Rule handling and context detection	Boolean: yes / no + text
Storage of identity data (*)	Statement whether identity data are stored on a system under main control of the user (Client), or whether the storage is on the foreign IT systems (e.g. from the provider), so that the user can access it only by the interfaces established by the provider (Server)	Enumerated: client, server
User-controlled Multiple identity store (*)	Provisioning identity information across multiple storage sides	Boolean: yes / no + text
Multiple identity store (*)	Mention whether multiple identity store happens under user control (e.g., when the user initiates it / knows about it)	Boolean: yes / no + text
User-controlled Identity synchronisation (*)	Associating identity information, automatically detecting updates, and synchronising the changes across systems	Boolean: yes / no + text
Identity synchronisation (*)	Mention whether identity synchronisation happens under user control (e.g., when the user initiates it / knows about it)	Boolean: yes / no + text
Federated identity (vs. Centralised identity) (*)	Federated identity is the set of mechanisms through which companies can share identity information between secure networks.	Boolean: yes / no
Federated identity standards (*)	If federated what standards does the system adhere to?	Text (referring to previous attribute)
Identity revocation	Statement whether the IMS is	Boolean: yes / no

Attribute Label	Definition	Values
(*)	endowed with identity revocation process. Revocation is the process of rescinding an identity that has been granted. (Lifetime of identity)	
Procedure for identity revocation (*)		Text (referring to previous attribute)

4.3.1.2 User / Account Management

Attribute Label	Definition	Values
Workflow-driven provisioning (*)	Example: a workflow may allow automatically collecting the correct data for each target system for driving the creation of account accordingly.	Boolean: yes / no + text
Create, modify, suspend, delete account (*)		Boolean: yes / no
Account purging (*)	Automatic deleting. When an account is not used during a long time, it is deleted. Text specifies the conditions under which this occurs.	Boolean: yes / no + text
Secure metadata storage (*)	The purpose of this metadata is to make security decisions concerning the storage of data i.e. metadata enable the sensitivity of data to be evaluated and therefore the most appropriate level of security (usage of encryption for example) can be chosen.	Boolean: yes / no + text
Allocation of an unused username (*)	Statement whether there is a mechanism to provide the user with a list of unused usernames to choose from (e.g. Hotmail, Yahoo Mail, which offer alternatives if the chosen username is unavailable).	Boolean: yes / no + text
Form filling (*)	Filling in form automatically /	Boolean: yes / no

Attribute Label	Definition	Values
	suggesting input values by storing user profile on the server side (e.g. airline booking services which fill in address details for a logged in user)	+ text

4.3.1.3 Password Management

Password management refers to support for complex password-policy creation and enforcement.

Attribute Label	Definition	Values
Password reset service (*)	Statement whether the IMS gives users a service to reset their own password.	Boolean: yes / no + text
Password expiration (*)	Statement whether the IMS automatically reminds users to change their passwords regularly or enforces regular changes.	Boolean: yes / no + text
Password policies enforcement (*)	Statement whether the IMS applies a site-defined set of password quality rules when users select a new password or change their password. Users are not allowed to select passwords that violate this policy.	Boolean: yes / no + text
Password histories (*)	Statement whether the IMS keeps password histories.	Boolean: yes / no + text
Password synchronisation (*)	Password synchronisation is defined as any process or technology that helps users to maintain a single password, subject to a single security policy, and changing on a single schedule, across multiple systems.	Boolean: yes / no + text

4.3.1.4 Other Operational Areas

Attribute Label	Definition	Values
Reachability	Statement whether the IMS enables the filtering of incoming	Boolean: yes / no

Attribute Label	Definition	Values
management (*)	communication.	+ text
Incidence Response Programme (*)	What happens in the event that an incident does occur (e.g. malicious intrusion, virus, etc.)? The IRP can be defined as both the process by which an incident is handled and the way in which that process is carried out.	Text
Other (*)	Any other operational areas that the evaluator wants to mention.	Text

4.3.2 Security protection

4.3.2.1 Authentication

In computer security, **Authentication** is the process by which a computer, computer program, or another user attempts to confirm that the computer, computer program, or user from whom the second party has received some communication is, or is not, the claimed first party.

Attribute Label	Definition	Values
Single sign-on (*)	Single sign-on lets a user log on once to a PC or network and access multiple applications and systems using a single password.	Boolean: yes / no + text
Credential base (*)	A credential base contains the set of permissions used by the access control process for the establishment of the authorisation.	Boolean: yes / no + text
Used techniques (*)	What techniques does the IMS support for the credential base? Password, PIN certificates, biometrics, key, smart cards etc.	Text
Multi-channel security (*)	Statement whether the user can authenticate himself and sign transactions using different security strategies – the most suited for the user when employing a certain channel.	Boolean: yes / no + text

Attribute Label	Definition	Values
Use of digital signature (*)	Indicates whether the IMS supports digital signatures or not and which types it supports (cf. European Electronic Signature Directive)	Boolean: yes / no + text
Use of PKI (*)		Boolean: yes / no + text

4.3.2.2 Authorisation

Once authenticated, users can access resources based on their entitlements through the process of authorisation. In security engineering, **Authorisation** is the process by which an entity attempts to confirm that another entity is allowed to access a resource.

Attribute Label	Definition	Values
Distributed authorisation (*)	Distributed authorisation is used as a mechanism of efficiency (as opposed to centralised authorisation).	Boolean: yes / no + text
Entitlement base (*)	An entitlement base contains attributes and values from the user registry or the user count. This generally is a shared library that is dynamically loaded during the authorisation initialisation process in order to deliver the access rights.	Boolean: yes / no + text
Digital rights management (*)	The digital management of the rights covers the description, identification, trading, protection, monitoring and tracking of copyrights.	Boolean: yes / no + text
Role-based provisioning (*)	Role-based Provisioning allows establishing user access to applications and resources based on their role within the organisation. Role-based provisioning ensures that the user only has access to information they need to do their job.	Boolean: yes / no + text

4.3.2.3 Accounting/Auditing

Attribute Label	Definition	Values

Attribute Label	Definition	Values
Security accounting (*)	User usage (usage management, tracking of the activity)	Boolean: yes / no + text
Processes for accounting (*)	What processes does the system support?	Text (see above)
Security auditing (*)	Network usage. Auditing verifies that processes are reasonable appropriate for expected results.	Boolean: yes / no + text
Processes for auditing (*)	What processes does the system support?	Text (see above)

4.3.2.4 Encryption

Attribute Label	Definition	Values
Encryption of stored data (*)		Boolean: yes / no
Encryption of transmitted data (*)		Boolean: yes / no
Technologies Used (*)	What technologies does the IMS support?	Text
Level of encryption (*)	Level relates to size of encryption key. Weak: 8-40 bits. Medium: 64 bits. Strong: 104/128/192/256 bits. Very strong: 448/512 bits	Enumerated: Very Strong, Strong, Medium, Weak

4.3.2.5 Security Properties

Attribute Label	Definition	Values
Confidentiality (*)	Describes how and how far confidentiality is ensured, i.e. protection against disclosure of information (without modification) from outside of the IMS.	Rate + text

Attribute Label	Definition	Values
Integrity (*)	Describes how and how far integrity and authenticity are ensured, i.e. the protection of data against modification (e.g. illegal destroying and manipulation). Manipulation could be prevented or identifiable, e.g., with use of digital signatures.	Rate + text
Availability (*)	Analysis of the availability of functions in case of unexpected incidents. The availability can be assured, e.g., with backup-solutions, redundancy, third persons, etc.	Rate + text
Non-repudiation (*)	Statement whether the IMS supports mechanism that seeks to prevent future false denial of involvement by either party. Non-repudiation with proof of origin provides the recipient of data with evidence that proves the origin of the data. Non-repudiation with proof of receipt provides the originator of data with evidence that proves the data was received as addressed.	Boolean: yes / no + text
Anonymity (*)	Statement whether the IMS provides a security service that prevents the disclosure of information that leads to the identification of the end users.	Boolean: yes / no + text
Rating (*)	Rating according to rules defined below	Integer

The following rules are used to determine a rating. The rating structure derives from the report on IMS by ICPP and SNG[2]. It is intended to be complementary to the fields described above. The final score is divided by **1.7** in order to normalise scores on a scale of 10.

- The stored data is encrypted: (by default: +2 / optional: +1)
- Transmitted data is encrypted: (by default: +2 / optional: +1)
- Data access and manipulation is only possible after authentication: (by default: +2 / optional: +1)
- There are known bugs which could be security-relevant: (-2)

[2] ICPP, SBG: "Identity Management Systems (IMS): Identification and Comparison Study", September 2003, under contract from the IPTS.

- There are patches / revisions (+1)
- There are immediately effective patches / revisions without side effects (+1)
- Stored data is signed with digital signature or comparable mechanism to prevent undetectable manipulation: (by default: +2 / optional: +1)
- Transmitted data is signed with digital signature or comparable mechanism to prevent undetectable manipulation: (by default: +2 / optional: +1)
- The availability is supported by redundancy and / or fault-tolerant mechanisms: (+1)
- Backup & restore of data is supported: (+1)
- Backup & restore of data is (manually) possible with adequate effort: (+1)
- Fall-back solutions and / or external services for security are provided: (+1)
- IMS informs completely about all processed and transmitted personal data: (+1)

4.3.2.6 Law Enforcement and Liability

Attribute Label	Definition	Values
Digital signature (*)	Digital signatures are a method of authenticating digital information often treated; digital signatures guarantee the integrity of the message.	Boolean: yes / no + text
Digital certificate (*)	Digital certificates are used to verify the identity of the sender.	Boolean: yes / no + text
History functions (*)		Boolean: yes / no + text
Data retention (*)		Boolean: yes / no + text
Data retention period (*)	Number of months of the data retention period and the description of the purpose for which data is stored.	Range + text

4.3.2.7 Trustworthiness

Attribute Label	Definition	Values
Multilateral security	Segregation of power, self-protection,	Boolean: yes / no

Attribute Label	Definition	Values
(*)	open source etc.	+ text

4.3.3 Privacy Protection

Attribute Label	Definition	Values
User empowerment (*)	Analysis if and how the IMS supports the user to discover his/her privacy rights for using them. The presentation of privacy could be with additional text messages, documentation or even external education. The user should be able to perform self-protection.	Rate + text
Transparency (*)	Describes the transparency of the function referring to the kind of user and his/her privacy rights. This means if and how the user can understand and reconstruct the activity of the investigated function.	Rate + text
Data minimisation (*)	Means the reduction of processed personal data by anonymity and pseudonymity procedures, minimising the linkability between a person and the personal data. Describes if more personal data is processed than necessary for the system / application.	Rate + text
Rating (*)	Rating according to rules defined below	Integer

The following rules are used to determine a rating. The final score is divided by **1.5** in order to normalise scores on a scale of 10.

- There is a privacy policy: (+1)
- Privacy issues (law etc.) are documented: (+1)
- Privacy issues are well documented inside the IMS (e.g., help function): (+1)
- There are warnings on the occasion of privacy-relevant behaviour: (+1)
- The user has freedom of choices concerning the identity management: (+1)

- The user is supported by privacy control functionality such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent: (+1)
- The IMS informs user about purpose of data processing or does not process personal data: (+1)
- The IMS informs completely about all used and transmitted personal data: (+2)
- The IMS adheres to EU privacy standard / privacy statements exist as postulated by the "Safe Harbor Principles" by the US Department of Commerce: (+1)
- Usage of pseudonyms / anonymity is possible: (+1)
- Usage of different pseudonyms is supported (+1)
- User is only asked for needed data overall: (+1)
- Only necessary data is processed (data minimisation): (+1)
- Unlinkability / anonymity of data are supported: (+1)

4.3.4 Interoperability / Standards

Attribute Label	Definition	Values
Incidence Response Programme standards (*)	What standards does the Incidence Response Programme use?	Text
Identity Revocation standards (*)		Text
User / account management standards (*)		Text
Password management standards (*)		Text
Authentication standards (*)		Text
Authorisation standards (*)		Text
Accounting standards (*)		Text
Auditing standards (*)		Text
Other standards (*)		Text

4.3.5 Usability

Attribute Label	Definition	Values
Reduction of legal/technology system's complexity (*)		Boolean: yes / no + text
Simulating common situations (*)		Boolean: yes / no + text
Rating (*)	Rating according to rules defined below	Integer

The following rules are used to determine a rating. The final score is divided by **1.5** in order to normalise scores on a scale of 10.

Usefulness (max. possible: 5 points):

- Application benefits usage several times a month: (+1)
- Application benefits every day usage: (+1)
- Time for first time adjustment is less than time for action without IMS: (+1)
- After first time adjustment the action is faster as without IMS: (+1)
- After first time adjustment the action is more than twice as fast as without: (+1)

Ease of Use (max. possible: 5 points):

- The help function is not needed for standard activities: (+0.5)
- The manual is not needed for standard activities: (+0.5)
- Help function, manual and support are not needed at all: (+1)
- After a period of vocational adjustment the user is able to use the function autonomously: (+1)
- It is not necessary to consult external support: (+0.5)
- No previous knowledge is needed: (+0.5)
- A complete and understandable help function is provided: (+0.5)

- A complete and understandable manual is provided: (+0.5)

Malfunction Understanding (max. possible: 5 points):

- The user can recognise that an error occurred: (+1)
- In case of a malfunction the function presents a complete and understandable description of the error: (+2)
- There are suggestions for what to do next: (+1)
- The function makes a sensible suggestion about what to do next: (+1)

4.4 Type 3 IMS attributes

This section is relevant for all IMS that are either type 3 or include type 3 functionality (e.g. a combination of 1 and 3).

The Type 3 IMS attributes cover various topics:

- Functionality
- Security Control
- Privacy Control
- Support
- Usability
- Trustworthiness

4.4.1 Functionality

Attribute Label	Definition	Values
IMS category (*)	Description of the purposes the IMS could be used for, and the operational areas such as access management, form filling, reachability management, automatic choice of identity and pseudonym management. Additionally interfaces to other systems or applications, protocols, plug-ins and gateways are listed.	Text
Representation of identities (*)	Description of mechanisms, which the IMS uses for showing the user his/her different kinds of identities, especially the one he/she is acting in or the most probable identities to choose from. This includes all possible forms of	Text

Attribute Label	Definition	Values
	identities, e.g., plain personal data, pseudonyms, credentials and their attributes.	
Handling of identities (*)	Description of the functionality of identity handling, meaning identity administration and choice. Identity administration comprises the definition of own identities and the verification of own or foreign identities. Identity choice consists of all possibilities for the user to choose explicitly his/her identities and decide on the re-use of identities and of everything where the IMS supports the user by seamless use of identities (implicit use) or giving information to help him/her.	Text
History management (*)	The history management applies to the logging of all transactions of the system. This includes details about what the system is logging and how this log file is represented to the user. In connection with the usability-category it is analysed how comprehensible this representation is and if it is useful.	Text
Context detection (*)	This functionality describes possibilities to detect the context of the user's environment and makes suggestions for further activities or executes them autonomously. It has to be described further which contexts the system can detect and how the user can affect them.	Text
Rule handling (*)	The rule handling affects the automatic decisions of the IMS. The analysis includes which parts of the system uses rules, which are default ones, how the user can influence them and if they can dynamically react in case of changing contexts.	Text
Identity recovery (*)	This functionality helps to recover an identity after a system crash or a malfunction. This could be useful	Text

Attribute Label	Definition	Values
	both for the user in case of using a deleted or destroyed identity again and for the law enforcement in case of prosecution. Identity brokers may play a crucial role for identity recovery.	
Digital evidence (*)	Description if the system helps to preserve evidence for legal proceedings. This could be important for users in case of prosecution of claim as well as for law enforcement and criminal prosecution. The analysis includes how powerful the evidence would be in a legal proceeding that comes along with the difficulty of manipulate the evidence. E.g., digital signatures and digital time stamps could help to increase the value of the evidence. Another relevant issue is whether the user is aware of the digital evidence functionality and may even influence the kind of digital evidence or whether this is a hidden functionality with no possibility to affect it.	Text

4.4.2 Privacy Control

Attribute Label	Definition	Values
Privacy control functionality (*)	The user could be supported by privacy control functionality such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent.	Text
Anonymity control (*)	Can the user choose to be anonymous or not?	Boolean: yes / no + text
Pseudonym control (*)	Can the user choose a pseudonym with which to operate under or not?	Boolean: yes / no + text

Attribute Label	Definition	Values
P3P (*)	Platform for Privacy Preferences (P3P) enhances user control by putting privacy policies where users can find them in a form users can understand and most importantly, enables users to act on what they see.	Boolean: yes / no + text
CPEX (*)		Boolean: yes / no + text
Others (*)		Text

4.4.3 Self-service

Attribute Label	Definition	Values
Change password (*)		Boolean: yes / no + text
View profile details (*)	Profiles can be changed without changing an account. Whereas the account details are private, the profile details may be public.	Boolean: yes / no + text
View account information (*)		Boolean: yes / no + text
Negotiation (*)	Statement whether the system provides mechanisms to negotiate protection goals and configuration of what data may be transmitted under which conditions	Boolean: yes / no + text
Choice of identity (*)		Boolean: yes / no + text

4.4.4 Support to the user

Attribute Label	Definition	Values
Identification of social situations (*)	Statement whether the IMS helps the user to identify social situations.	Boolean: yes / no + text

Attribute Label	Definition	Values
Adequate role taking (*)	Statement whether the system helps the user to identify what is expected from him. *Role taking is the process by which the individual person becomes linked with their relevant society.*	Boolean: yes / no + text
Adequate role making (*)	Statement whether the system helps the user to identify what he is doing. *Evolving notions of how the users themselves expect to act in a given position (role making).*	Boolean: yes / no + text

4.4.5 Usability

The usability aspect describes both the usability of the product and the documentation and external support.

Attribute Label	Definition	Values
Usefulness (*)	The degree to which a person believes that using a particular system would benefit his or her tasks. The construct of perceived usefulness means a person's perception of using an information system that benefits him or her in an organisational context.	Rate + text
Ease to use (*)	The degree to which a person believes that using a particular system would be free of effort. Perceived usefulness and perceived ease of use have influence on the actual use of the IMS.	Rate + text
Malfunction understanding (*)	The degree of the system ability to present the risk of faulty operation to the user to warn him and help him to avoid it. This could be an additional warning request that the user has to reply or the ability to undo a malfunction after the user understood that he did something wrong.	Rate + text

Attribute Label	Definition	Values
Rating (*)	Rating according to rules defined below	Integer

The following rules are used to determine a rating. The final score is divided by **1.5** in order to normalise scores on a scale of 10.

Usefulness (max. possible: 5 points):

- Application benefits usage several times a month: (+1)
- Application benefits every day usage: (+1)
- Time for first time adjustment is less than time for action without IMS: (+1)
- After first time adjustment the action is faster as without IMS: (+1)
- After first time adjustment the action is more than twice as fast as without: (+1)

Ease of Use (max. possible: 5 points):

- The help function is not needed for standard activities: (+0.5)
- The manual is not needed for standard activities: (+0.5)
- Help function, manual and support are not needed at all: (+1)
- After a period of vocational adjustment the user is able to use the function autonomously: (+1)
- It is not necessary to consult external support: (+0.5)
- No previous knowledge is needed: (+0.5)
- A complete and understandable help function is provided: (+0.5)
- A complete and understandable manual is provided: (+0.5)

Malfunction Understanding (max. possible: 5 points):

- The user can recognise that an error occurred: (+1)
- In case of a malfunction the function presents a complete and understandable description of the error: (+2)
- There are suggestions for what to do next: (+1)
- The function makes a sensible suggestion about what to do next: (+1)

In the first version of the database there will not be great detail on the third party support. So it is sufficient to have only a general description which kinds of third parties help in which way in managing identities. But later on this part may be extended, e.g. by describing the

protocols of data exchange with the third party, the security mechanisms and privacy controls applied, and evaluating usability aspects.

4.4.6 Trustworthiness

Attribute Label	Definition	Values
Multilateral security (*)	Segregation of power, self-protection, open source etc.	Boolean: yes / no + text
Seals (*)	Privacy and other seals that certify that the IMS applies to law.	Boolean: yes / no + text

5 User Manual

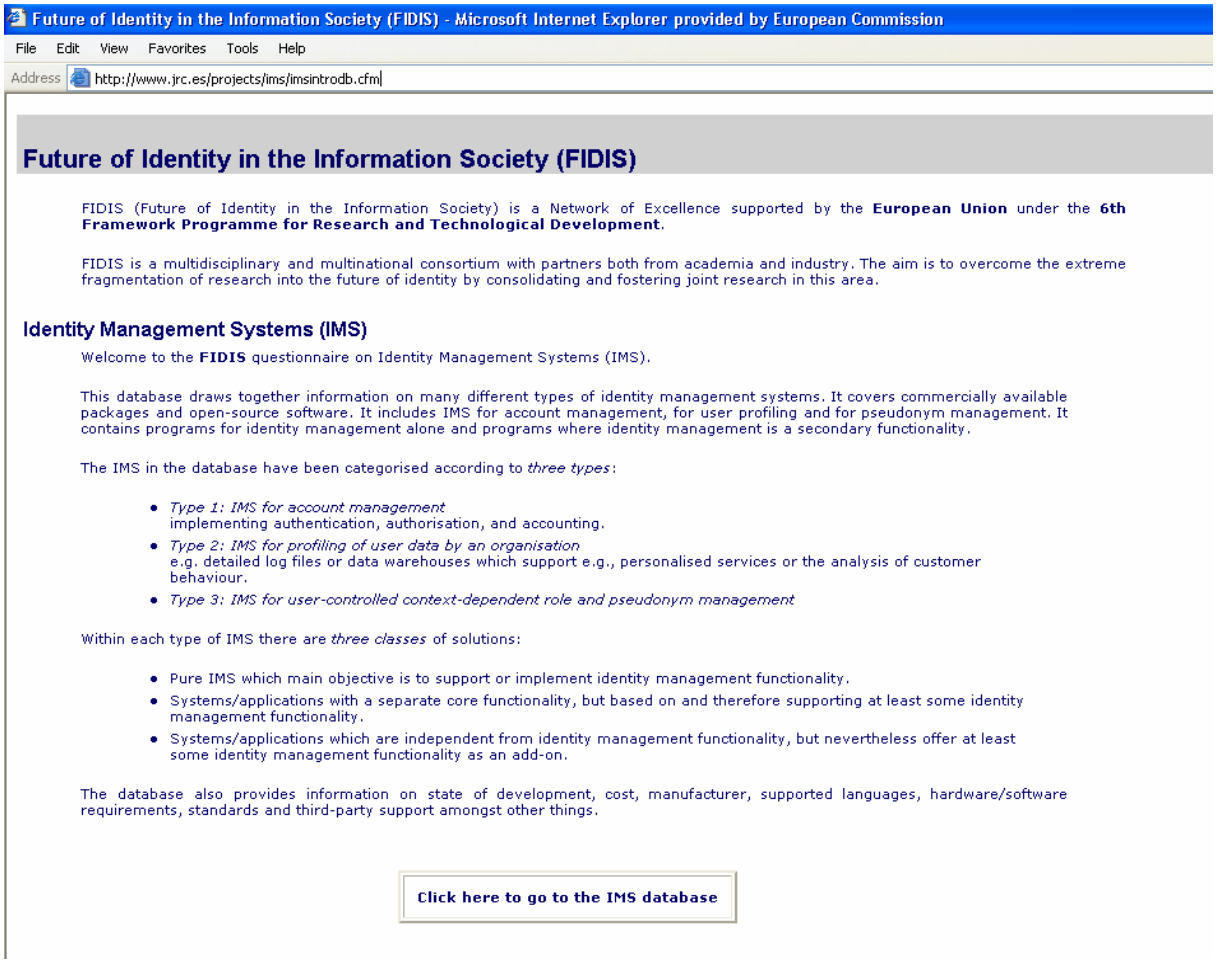
This section explains how the prototype database can be used in order to find out information on identity management systems and, furthermore, how records on new systems can be added to the database. Note that this prototype system will be transferred during the second FIDIS workplan to the FIDIS permanent infrastructure and that the links described below will seize to function then.

The introduction page for the database can be found at this address here: http://www.jrc.es/projects/ims/imsintrodb.cfm. Alternatively users can view the list of systems in the prototype database directly by following this link: http://www.jrc.es/projects/ims/imslist.cfm

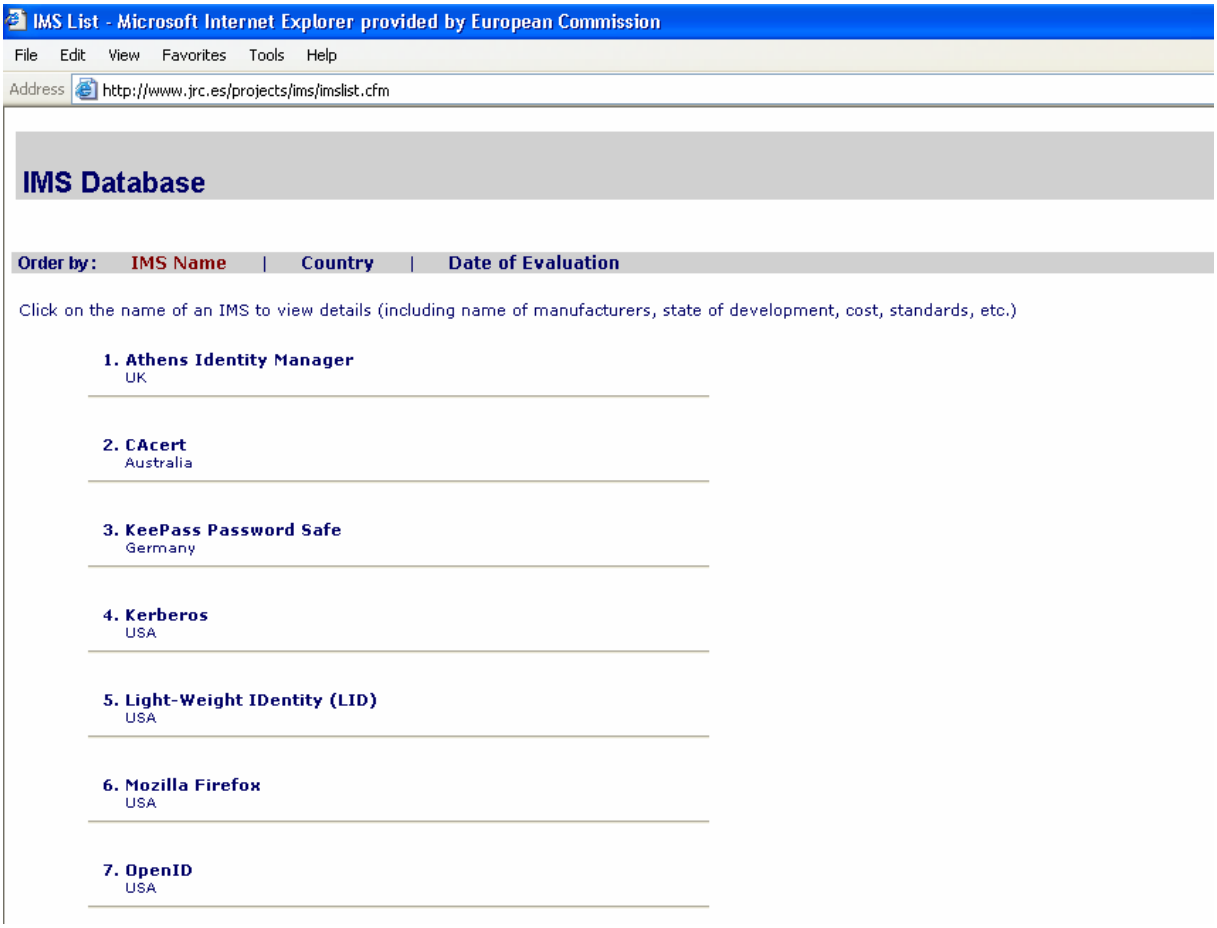
Evaluators (usually from the partners that are mostly updating the prototype) can introduce new records into the database by going to: http://www.jrc.es/projects/ims/imsintro.cfm. This is the introductory page which leads on to the actual questionnaire page (http://www.jrc.es/projects/ims/imsform.cfm). http://www.jrc.es/projects/ims/insertform.cfm

5.1 Using the database

The link http://www.jrc.es/projects/ims/imsintrodb.cfm takes the user to start page.

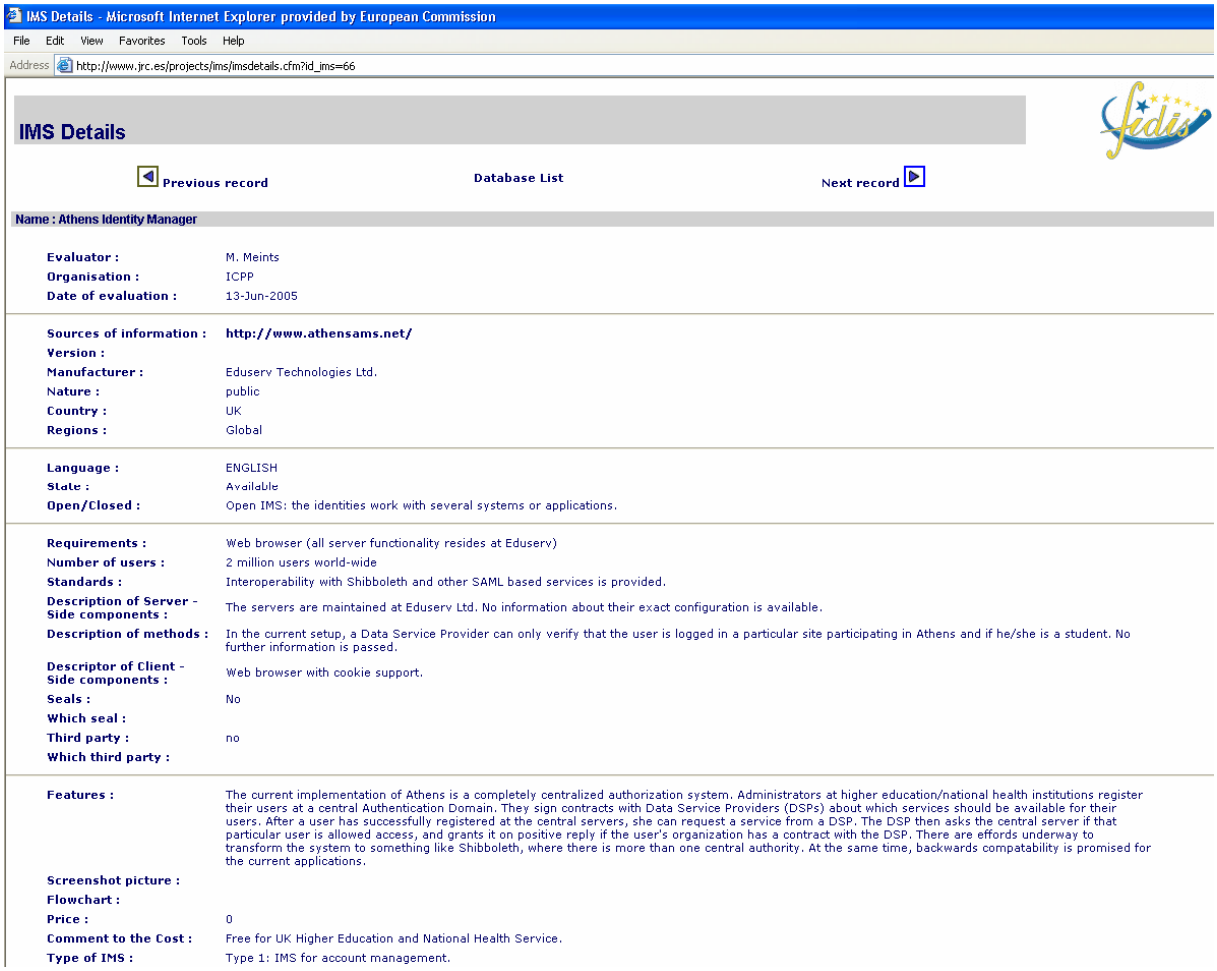


Following the link at the foot of the page leads the user to http://www.jrc.es/projects/ims/imslist.cfm. This is a list of all systems that have so far been entered into the database. An example screenshot is shown below.



The default ordering is by name of the IMS. The user can choose to reorder the systems alphabetically by country of origin or by date of evaluation. This is done simply by clicking on the desired ordering at the top of the page.

Individual records can be accessed by selecting the name of the particular IMS. For example, by clicking on 'Athens Identity Manager', the following page comes up:



Here the user can see all the information that has been entered on this IMS. The links at the top of the page can be used to navigate to the previous or next records or to return to the list of IMS.

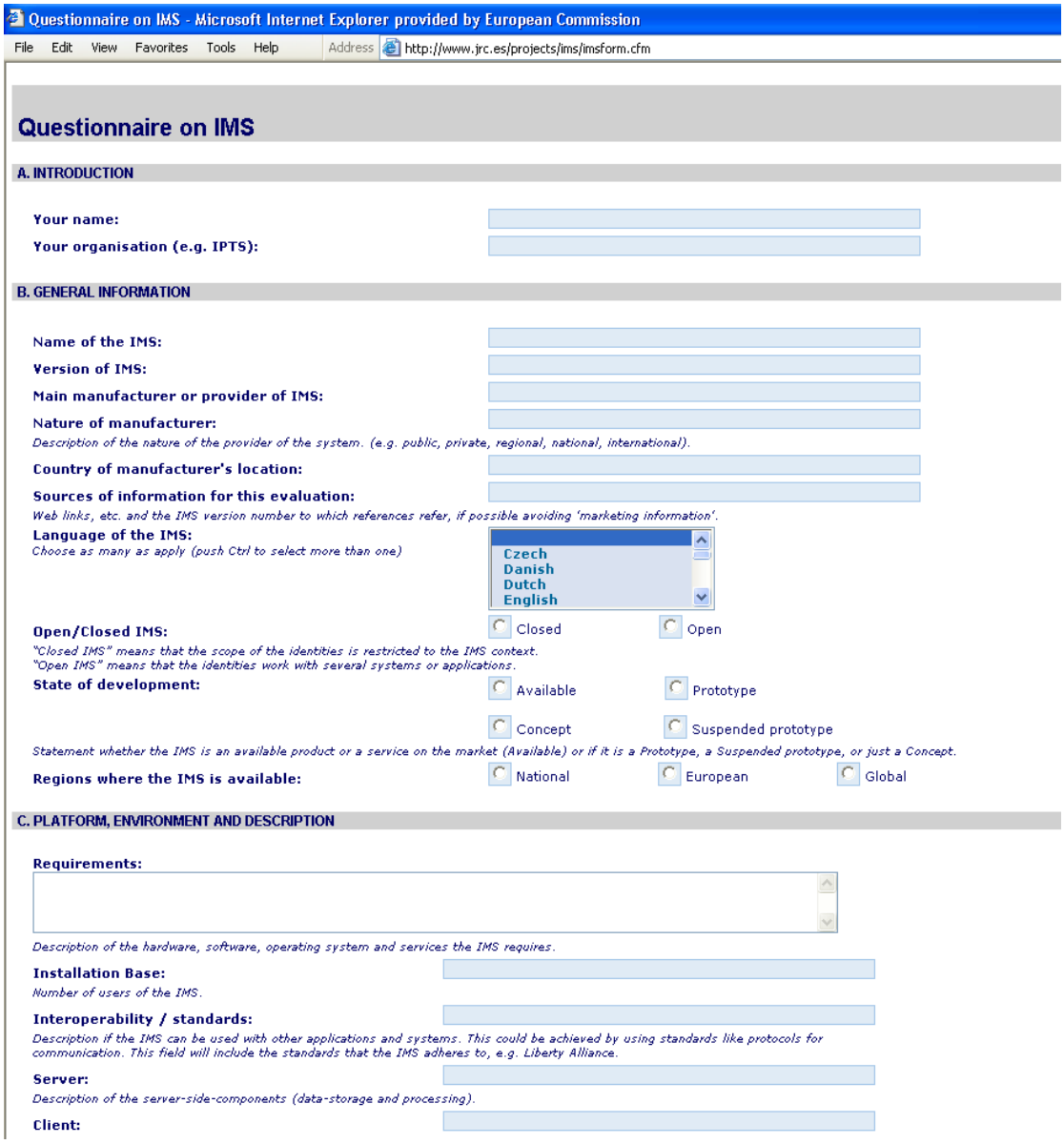
5.2 Entering a new record

Users who want to enter a new record into the database, can do so using the questionnaire (http://www.jrc.es/projects/ims/imsform.cfm) accessible via the introductory page[3]. A screenshot of the IMS questionnaire is shown below. Evaluators are asked a series of questions corresponding to the structure of the database presented in section 3 of this document. http://www.jrc.es/projects/ims/insertform.cfm

The questionnaire has six sections A-F including a section at the end where evaluators are invited to make any suggestions/further comments they may have.

[3] http://www.jrc.es/projects/ims/imsintro.cfm

Once the questionnaire has been submitted, the IMS enters into the database and appears in the list of systems on the home page of the database.



5.3 Modifying a record

At present only the IPTS can modify the records in the database. The information will be confirmed with the manufacturers in order to ensure it is correct. Nevertheless the webpage asks users of the database who identify an error in the data, to contact the IPTS IMS team so that they can correct it.

6 Technical specifications

6.1 Technical Details

These are the technical details of the database:

- Operative system: UNIX Solaris 7
- Server language: Coldfusion 4 / HTML / SQL
- Programming tool: Coldfusion Studio 4.5
- Database manager: Oracle 8i
- Web server: Apache Web Server 1.3.9
- Client pages: Plain HTML
- Web browser at IPTS: MS Explorer 6

6.2 SQL

```
CREATE TABLE "ICT"."IMS" ("ID_IMS" NUMBER(6) NOT NULL, "IMSNAME"
    VARCHAR2(255) NOT NULL, "EVALUATOR" VARCHAR2(255), "ORGANISM"
    VARCHAR2(255), "DATEOFEVALUATION" DATE, "REFERENCE"
    VARCHAR2(255), "VERSION" VARCHAR2(255), "MANUFACTURER"
    VARCHAR2(255), "NATURE" VARCHAR2(255), "COUNTRY"
    VARCHAR2(255), "GEOGSCOP" VARCHAR2(255), "LANGUAGE"
    VARCHAR2(255), "STATE" VARCHAR2(255), "OPEN_CLOSED"
    VARCHAR2(255), "REQUIREMENT" VARCHAR2(2000), "USERBASE"
    VARCHAR2(255), "STANDARD" VARCHAR2(255), "SERVER"
    VARCHAR2(255), "CONTROL" VARCHAR2(2000), "CLIENT"
    VARCHAR2(255), "SEALS" VARCHAR2(3), "WHICHSEAL" VARCHAR2(255),
    "VAL3RDPARTY" VARCHAR2(3), "WHICH3RD" VARCHAR2(255),
    "FEATURES" VARCHAR2(4000), "SCREENSHOT" VARCHAR2(255),
    "FLOWCHART" VARCHAR2(255), "PRICE" NUMBER(15), "TYPEIMS"
    VARCHAR2(255), "IMSCLASS" VARCHAR2(255), "IMSFUNCTION"
    VARCHAR2(255), "SUGGESTIONS" VARCHAR2(4000), "COSTCOMMENT"
    VARCHAR2(255),
    CONSTRAINT "SYS_C003268_1_1" PRIMARY KEY("ID_IMS")
    USING INDEX
    TABLESPACE "T_ICT"
    STORAGE ( INITIAL 10K NEXT 10K MINEXTENTS 1 MAXEXTENTS 121
    PCTINCREASE 50 FREELISTS 1 FREELIST GROUPS 1) PCTFREE 10
    INITRANS 2 MAXTRANS 255,
    CONSTRAINT "SYS_C003269_1_1" UNIQUE("ID_IMS"),
    CONSTRAINT "SYS_C003270_1_1" UNIQUE("IMSNAME")
    USING INDEX
    TABLESPACE "T_ICT"
    STORAGE ( INITIAL 10K NEXT 10K MINEXTENTS 1 MAXEXTENTS 121
    PCTINCREASE 50 FREELISTS 1 FREELIST GROUPS 1) PCTFREE 10
    INITRANS 2 MAXTRANS 255)
    TABLESPACE "T_ICT" PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS
    255
    STORAGE ( INITIAL 10K NEXT 24K MINEXTENTS 1 MAXEXTENTS 121
```

```
    PCTINCREASE 50 FREELISTS 1 FREELIST GROUPS 1)
    LOGGING
```

6.3 Example of Questionnaire response

insert into ims (IMSname, evaluator, organism, dateofevaluation, reference, version, manufacturer, nature, country, geogscop, language, state, open_closed, requirement, userbase, standard, server, control, client, seals, whichseal, val3rdparty, which3rd, features, screenshot, flowchart, price, costcomment, typeims, imsclass, imsfunction, suggestions) values ('#form.imsname#', '#form.evaluator#', '#form.organism#', '#dateofeval#', '#form.reference#', '#form.version#', '#form.manufacturer#', '#form.nature#', '#form.country#', '#GEO#', '#form.language#', '#ST#', '#OC#', '#requirement#', '#form.userbase#', '#form.standard#', '#form.server#', '#control#', '#form.client#', '#aresеals#', '#allseals#', '#are3rdparty#', '#all3rdparty#', '#features#', '#form.screenshot#', '#form.flowchart#', '#form.price#', '#form.costcomment#', '#TI#', '#CI#', '#form.imsfunction#', '#form.suggestions#')

Questionnaire on IMS

Response

Your response has been registered.

Thank you very much!

6.4 Example of IMS Record

select id_ims, imsname from ims order by imsname, id_ims select imsname from Ims where id_ims = #NextId# select imsname from Ims where id_ims = #PreviousId# select * from ims where id_ims=#url.id_ims#

IMS Details

Previous record **Database List** **Next record**

Name : #imsname#

Evaluator :	#Evaluator#
Organisation :	#Organism#
Date of evaluation :	#dateformat(Dateofevaluation, "dd-mmm-yyyy")#

Sources of information :	#Reference##Reference#
Version :	#Version#
Manufacturer :	#Manufacturer#
Nature :	#Nature#
Country :	#Country#
Regions :	#Geogscop#

Language :	#Language#
State :	#State#
Open/Closed :	Open IMS: the identities work with several systems or applications. Closed IMS: the scope of the identities is restricted to the IMS context.

Requirements :	#Requirement#
Number of users :	#Userbase#
Standards :	#Standard#
Description of Server - Side components :	#Server#
Description of methods :	#Control#
Descriptor of Client - Side components :	#Client#

Seals :	Yes: Privacy and other seals that certify that the IMS applies to law. No
Which seal :	#Whichseal#
Third party :	#Val3rdparty#
Which third party :	#Which3rd#

Features :	#Features#
Screenshot picture :	#Screenshot#
Flowchart :	#Flowchart#
Price :	#Price#
Comment to the Cost :	#CostComment#
Type of IMS :	Type 1: IMS for account management. Type 2: IMS for profiling of user data by an organisation. Type 3: IMS for user-controlled context-dependent role and pseudonym management.
Class of IMS :	Class 1: Pure IMS which main objective is to support or implement identity management functionality. Class 2: Systems/applications with another core functionality. Class 3: Systems/applications which are independent from identity management functionality.
Functionality :	#IMSFunction#
Suggestions :	#Suggestions#

Every effort has been made to check the information shown with the manufacturer. Nevertheless errors may remain.
If you would like to change any part of this record, please send your comments to the IMS team.

Previous record **Database List** **Next record**

7 Maintenance Plan

The maintenance plan will be launched soon after the database has been updated with the latest findings[4] and will carry on during the third Workplan period. The maintenance plan will be a loop composed of three stages: 1) identification of the IMS and gathering of the related data, 2) validation of the collected data and 3) updating of data. Therefore, an iterative way will be put in place between FIDIS members, maintenance team and external corresponding developers or responsible person of identified IMS.

The maintenance team must be able to modify contents of existing records, add new records, and change all data related to IMS records.

In addition, a validation phase is being implemented; this phase consists in sending the IMS data to the corresponding responsible of each identified IMS in order to verify the veracity of the information or to complement it.

Furthermore, a testing phase will start involving all FIDIS partners, where partners can use the database in order to give feedback but can also add additional records. In the next phase, via a validation stage, the IPTS will request additional information from Identity Management Systems developers. It is foreseen that the data entry and testing phase will last three months.

It is intended that the database, as amended by the testing phase with the FIDIS partners during the first trimester 2006 and will be made available to the general public in March 2006. This date coincides with the end of the 18-month period (second Workplan).

Another foreseen task will be to do the integration of the database into the FCI (FIDIS infrastructure) and the results will be reported in the deliverable D8.6.

And finally, a disclaimer concerning the non-exhaustiveness will be displayed on the website in order to inform that we do not pretend to provide an exhaustive IMS database.

8 Part A – Conclusion

Part A of this document has outlined two structures for a database of identity management systems (IMS). The first one is a structure for the prototype that has been developed. Several records have now been introduced into the database and the results are available to see at http://www.jrc.es/projects/ims/imslist.cfm. The second one is a structure which incorporates many elements that may be necessary for the database in the future but cannot be implemented at present.

The maintenance plan and specially the testing phase and the validation stage will ensure a high quality of the database. Furthermore, it is expected that data will feed into the database from deliverable 3.1 which has planned a questionnaire to be distributed amongst the relevant actors and which will enable classification of IMS according to type and class. This classification will play an important role when the database will become large since it will be possible to provide some searching options for helping the database consulting.

[4] In annex, the list of IMS and one example are presented.

9 Part B – Introduction

Part B provides a draft for the Identity laws database, the Identity Law Survey (IDLS). In the framework of FIDIS activities, this work is in line with Work Package 8, "Integration of the NoE", which relates to all integrating activities. One of the objectives of this WP is to develop a database on identity legislation in the EU and a selection of other countries. This is a counterpart to the database on Identity Management Systems (described in the first part of this document).

This second part of the deliverable describes the context for establishing the law survey in the first workplan of FIDIS (section 8.1). Next, the initial structure of the law survey, i.e. ID Law database that was used to build a prototype is described (section 9). Section 10 outlines the proposed new database structure, where the first findings of the collection of ID theft-related legislation were used to refine the initial structure. Section 11 gives a full overview of the database structure, whereas section 12 lists interface requirements (for use in deliverable D1.4) for the website that will open up the database to the public. Section 13 contains the user manual, and section 14 indicates how the ID Law Survey will be maintained.

9.1 Identity Law Survey

The objective in the first workplan period of FIDIS, April 2004 – September 2005, was to develop a database for ID-related legislation that is simple and user-friendly, in order to provide the general public with basic information on ID-related laws in the EU.

Such a database does not yet exist. On the contrary: there are some repositories of legislation, but these provide lists of laws, either laws in general – usually for a limited number of countries, or laws in specific areas, e.g., data-protection laws. However, there is no repository of ID-related laws on the web. Moreover, existing law databases typically provide legal texts, without comments or context, and they list entire laws where only one or two provisions may be relevant for the topic at hand. In contrast, the IDLS aims to provide added-value information on ID-related laws by selecting only those laws and legal provisions that are directly relevant for identity and identification, and by 'translating' the legal jargon into summaries in normal language understandable for interested lay-people. This gives the IDLS a unique position within the range of legal databases currently existing on the Internet.

To show how the database works and its interest, a prototype was to be built into which a sample of laws could be input. The sample chosen was a) legislation on official ID documents, and b) ID theft-related laws, which were collected within the framework of FIDIS workpackage 5, which has focused on ID theft.

Since it was known at the start that the United States have extensive specific legislation on ID theft, the starting point of the law survey was to incorporate not only European laws, but also the US legislation on ID theft and ID fraud into the prototype.

10 Initial ID Law database

10.1 Initial ID Law database structure

The two samples chosen for input into the prototype were:

a) legislation on official ID documents, and

b) ID theft-related laws.

For laws of type a), three major aspects were considered relevant:

A1. Which are the official documents designated by law?

A2. Is there a general obligation for citizens to show an ID?

A3. Is there a general obligation for citizens to carry an ID?

For laws of type b), the starting-point was the well-known United States law, the *Identity Theft and Assumption Deterrence Act of 1998*. This is the best-known – and, at the start, the only known – example of a specific law that criminalises ID theft. As a consequence, the initial structure that was decided to be used in the prototype was largely based on the US categorisation of criminal law, with the addition of some general criminal-law categories that were considered relevant to cover specific forms of ID theft or ID fraud.

B1. ID Theft

B2. ID Fraud

B3a. ID document Fraud

B3b. Immigration Document Fraud

B4a. General Fraud Provisions

B4b. Paper Fraud

B4c. Computer Fraud

B4d. Mail Fraud

B4e. Wire Fraud

B4f. Financial Institution Fraud

B4g. Internet Fraud

B5. Forgery of ID Documents

B6. General Forgery Provisions

B7a. Unlawful Data Collection

B7b. Unlawful Data Use

B8. Damage to ID documents

B9. Imposture

C. Private Law Provisions

10.2 Prototype

The structure was used by Tilburg University to build a prototype of the ID Law Survey, which was available in March 2005 and presented at the FIDIS General Meeting in Berlin of 17-18 March 2005. The prototype can be found at the following URL: http://rechten.uvt.nl/idls/. (After the structure of the prototype has been updated, see below, the prototype will be integrated in the FIDIS information infrastructure. Until that time, the prototype will for practical reasons remain located at Tilburg University's server.)

10.3 Content collected in the first year

In order to collect the samples to be input into the prototype, a network of correspondents was set up. This yielded the following correspondents (as of 30 April 2005):[5]

- *Belgium*, Hans Graux, KU Leuven
- *Canada*, Shaun Brown, Industry Canada
- *Czech Republic*, Vaclav Matyas, Masaryk University, Brno
- *Denmark*, Henrik Udsen, University of Copenhagen
- *Finland*, Tuomas Pöysti, Ministry of Finance and University of Helsinki
- *France*, Cyril Murie, Eric Freyssinet, Forensic Research Institute of the Gendarmerie Nationale, Engineering & digital technologies division (IRCGN/DCIN)
- *Germany*, Henry Kraseman, Independent Center for Privacy Protection, Schleswig-Holstein
- *Greece*, Vagelis Papakonstantinou, Drakopoulos Law Firm
- *Hungary*, Gábor Hontert, ISRI
- *Mexico*, Cristos Velasco, North American Consumer Project on Electronic Commerce
- *Netherlands*, Mark Dekker, Tilburg University
- *Slovakia*, Jozef Vyskoc, VAF
- *Sweden*, Helena Andersson, Stockholm University
- *United Kingdom*, Peter Sommer, LSE

[5] The inclusion of Canada and Mexico was not actively sought, but was caused by a fortuitous offer by two experts from those countries who showed interest in the ID Law Survey and offered to become country correspondents. This is a hopeful sign that in future, experts from other non-EU countries may also offer to become country correspondents once the ID Law Survey starts to gain some public recognition on the Internet.

In the next workplan period, an effort will be made to extend the network of country correspondents with other EU countries not represented in FIDIS.

Apart from the country correspondents, researchers at Tilburg University conducted a literature search for ID-related laws in other countries, including the US.

Both sources yielded information on official ID documents and some information on ID theft-related laws. However, since ID theft was not found to be a category used in EU legislation (see FIDIS deliverable D5.1), relatively little input could so far be given for the categories B1 and B2. The main conclusion to be drawn from the first year is therefore that the initial categorisation of ID theft-related laws, based on the US legal system, is not a particularly good one to present information about European legislation related to ID theft. In fact, the term 'ID theft' is contested and inappropriate (see FIDIS deliverable D5.1), and the closely related term 'ID fraud' is also not a category that features in European legislation as such. As a consequence, the initial database structure should be adapted. In the following section, we present a new categorisation that will be more appropriate for the ID Law Survey.

11 Proposed new database structure

11.1 Changes and extensions

Apart from the re-categorisation of the laws related to ID theft or ID fraud (see previous section), it will be useful to make some further changes to the database.

First, it is wise to add a general section, where information about the legal system (e.g., a common-law or a civil-law country) and where links to official legislation websites can be found, as well as a category of references for links and literature.

Second, the information on official ID documents should be extended with information about official ID numbers, since these are also the object of ID fraud. Moreover, given the focus of FIDIS on identification in the information society, a separate section about electronic ID instruments – at least as far as these are incorporated in legislation – will be interesting to include.

Third, the obligation to show an ID should be extended, since there is a wide variety of instances in which people (citizens, businesses, or consumers) have to identify themselves. Therefore, a new section on Identification Duties will be included, divided into sub-categories of criminal law, other public law, private law, and prohibitions of anonymity.

These changes and extensions lead to the following new structure. The current database prototype will be amended with this new structure. As soon as the new structure has been incorporated, the Identity Law Survey will be integrated in the FIDIS information infrastructure.

12 Full ID Law database structure

12.1 Overview

The ID Law database is structured as follows. On the **top level** are **countries**, including – if relevant – supranational law-making bodies (such as the EU), and for countries with a federal legal system, containing two country entries, one for the federal and one for the state level (cf. section 12.2).

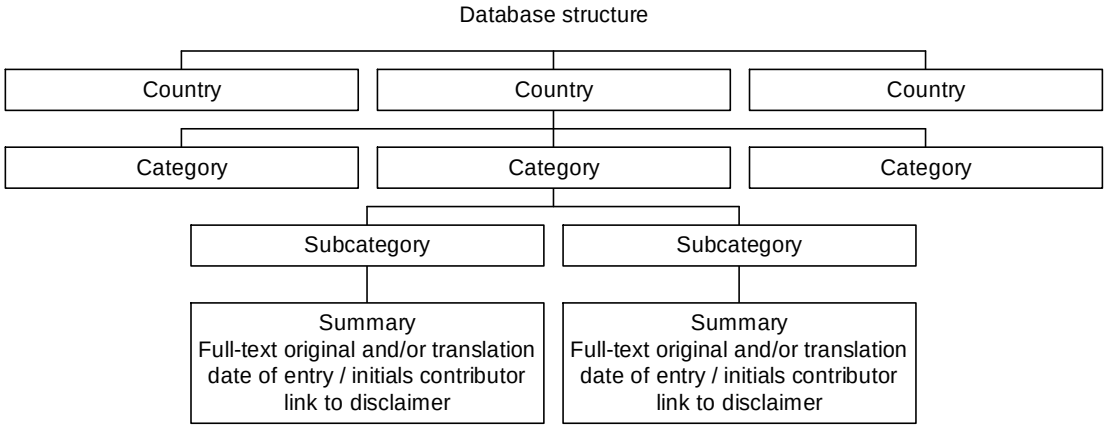
The **next two levels** concern the **categorisation of ID-related laws**, some of them subdivided in subcategories (see section 12.3).

The **fourth level** then gives the **content** of the laws, if available extended with the full-text of the law or legal provision(s), in an original language and/or in an English translation. Added to the content is a title, the date of entry or change, contributor initials, and a link to the disclaimer. Together, the fourth level thus represents the 'real' contents of each record that will be shown on the webpage (see section 13).

The structure therefore is as follows:

Level	Attribute Label	Definition	Value
1	**Country**	Name of the country (supranational body), if relevant extended with the attribute 'federal' or 'states'	Text
2	**Legal category**	Main category of ID-related legal area	Text
3	**Legal subcategory**	Subcategory of ID-related legal area, if relevant	Text
4	**Title**	indicates country and (sub)category; this is the text that shows up in search queries	Text
4	**Summary**	Summary of the law or legal provision(s)	Text
4	**Full-text original**	Full-text of the law or legal provision(s) in (one of) the original language(s), if available	Text
4	**Full-text translation**	Translation of the law or legal provision(s) in English, if available	Text
4	**Date of contribution**	Date(s) of the (last change of the) entry	Date
4	**Contributor**	Initials of the contributor(s)	Text
4	**Disclaimer**	Link to disclaimer	Hyperlink

Hierarchically, the structure looks as follows:



An example of a record is the following:

Level	Attribute Label	Example	Value
1	**Country**	Netherlands	Text
2	**Legal category**	C. Identification duties	Text
3	**Legal subcategory**	C1. Show ID – criminal law	Text
4	**Title**	Netherlands / C1. Obligations to Show ID	Text
4	**Summary**	The Compulsory Identification Act of 1993 designated several specific situations in which people have to show an ID, such as when riding in public transport without a valid ticket. On 1 January 2005, however, the law has been extended into a general obligation to show an ID to any police officer or supervisory official. The obligation holds for all people of 14 years and older. In the parliamentary documents, it was explained that the obligation to show an ID holds in situations in which the officer requires an ID as being necessary to fulfil his appointed duty.	Text
4	**Full-text original**	**Wet op de identificatieplicht** Wet van 9 december 1993, tot aanwijzing van documenten dienende ter vaststelling van de identiteit van personen alsmede aanwijzing van enige gevallen waarin de identiteit van personen aan de hand van deze documenten kan worden vastgesteld **Artikel 2** Een ieder die de leeftijd van veertien jaar heeft bereikt, is verplicht op de eerste vordering van	Text

Level	Attribute Label	Example	Value
		een ambtenaar als bedoeld in artikel 8a van de Politiewet 1993, een identiteitsbewijs als bedoeld in artikel 1 ter inzage aan te bieden. Deze verplichting geldt ook indien de vordering wordt gedaan door een toezichthouder.	
4	**Full-text translation**	--	Text
4	**Date of contribution**	14 Mar 05	Date
4	**Contributor**	BJK	Text
4	**Disclaimer**	disclaimer	Hyperlink

12.2 Countries

There is a pre-defined list of countries, which can be extended along the way. The current countries taken into account in the database are basically the EU member states and countries in North America:

- Austria
- Belgium
- Canada – federal
- Czech Republic
- Cyprus
- Denmark
- Estonia
- Finland
- France
- Germany – federal
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxemburg
- Malta
- Mexico
- Netherlands
- Poland
- Portugal
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- United Kingdom
- United States – federal
- United States – states

Note that not all EU countries are covered in the first stage; the prototype contains mainly the EU countries that are represented within FIDIS, and the US. The other EU member states will be added in stages (see section 15).

12.3 Categories of ID-related legislation

There is a pre-defined list of categories, some of them subdivided into subcategories, which can be extended along the way. The current categories are:

Category	Subcategory	Explanation
A. General		this includes relevant general info about the legal system (e.g., common-law or civil-law), official website where laws or case law are published, etc.
B. Official ID instruments		'official' means: specified by law as being a legally accepted means of identification; usually, this will refer to government-issued ID documents and numbers
	B1. Official ID documents	
	B2. Official ID numbers	e.g., social-security number, citizen number
	B3. Electronic ID	this will mention legislation that allows or establishes electronic forms or aspects of official identification means, such as an official citizen chip card, and biometrics in official ID documents
	B4. Obligations to Carry ID	
C. Identification duties		
	C1. Show ID – criminal law	e.g., general power for police to request an ID, to investigate crimes or to maintain public order
	C2. Show ID – other public law	e.g., in voting, marrying, applying for a passport, being a witness in legal case; only to be included

Category	Subcategory	Explanation
		where examples are readily available, as a sample
	C3. Show ID – private law	e.g., banking (know your customer), buying restricted goods, buying real-estate, car-rental; only to be included where examples are readily available, as a sample
	C4. Prohibitions of anonymity	in criminal law, e.g., hit-and-run offences, and in private law, e.g., ISP liability, distance selling (provider must publish address on website)
D. Identity-related crime		
	D1. ID-specific crimes	specific criminalisation of ID theft, ID fraud, or ID-document crimes (e.g., fraud, forgery, theft, damage, trade, receiving of official ID document or of unofficial ID document)
	D2. Fraud	general fraud, specific forms of fraud (e.g., paper fraud, mail fraud, wire fraud, computer fraud, Internet fraud, financial institution fraud)
	D3. Forgery	
	D4. Damage	damage to goods, damage to computer data
	D5. Data abuse	unlawful data collection, unlawful data use, data-protection law if specifically related to ID-related crime

Category	Subcategory	Explanation
	D6. Imposture	
E. Private-law infringements of identity		
	E1. Tort	
	E2. Personality rights	including portrait rights
Z. References		links to websites and documents; references to literature

The structure is flexible so that in future, new categories (F through Y) and subcategories (B5, B6, etc.) can be included if a FIDIS work plan decides it is useful to collect more information on ID laws.

12.4 Maintenance requirements

Since the ID Law Survey is a joint effort, several people (to be designated by the IDLS co-ordinator) should be able to update the ID Law database remotely after a login procedure. They must be able to modify contents of existing records, add new records, and change the name of or add new countries, categories and subcategories.

13 Interface requirements

The IDLS is a webpage that opens up the database to users. The webpage contains the following sections, which should be clickable buttons (titles in **bold**):

- **general**: introduction to the law survey, FIDIS context, disclaimer, etc.; this part is the default text that appears when someone enters the webpage
- **correspondents**: a list of all country correspondents
- **search**: a search mechanism
- **user help**: tips for searching
- **disclaimer**
- **contact**: contact information

The search mechanism is the most important feature of the webpage. It enables users to search in the following ways:

- by country (with a pop-up window listing all countries in the database); or
- by topic (with a pop-up window listing all categories and subcategories in the database); or
- by country and topic; or
- full-text search.

The database will be opened up through the search mechanism with pop-up windows enabling users to choose a country and/or a legal topic. The search gives the search results in the form of a list of clickable titles, each of which contains the country and legal topic of the record found. When the user clicks a title, the contents of the record are presented as follows:

Title
Summary
<line>
Full-text original
<line>
Full-text translation
<line>
Date of contribution (dd Mon yy)/ Contributor initials
disclaimer

The example of the record listed in 12.1 would show as follows:

Example

Netherlands / C1. Obligations to Show ID

Summary

The Compulsory Identification Act of 1993 designated several specific situations in which people have to show an ID, such as when riding in public transport without a valid ticket. On 1 January 2005, however, the law has been extended into a general obligation to show an ID to any police officer or supervisory official. The obligation holds for all people of 14 years and older.

In the parliamentary documents, it was explained that the obligation to show an ID holds in situations in which the officer requires an ID as being necessary to fulfil his appointed duty.

Full-text original

Wet op de identificatieplicht

Wet van 9 december 1993, tot aanwijzing van documenten dienende ter vaststelling van de identiteit van personen alsmede aanwijzing van enige gevallen waarin de identiteit van personen aan de hand van deze documenten kan worden vastgesteld

Artikel 2
Een ieder die de leeftijd van veertien jaar heeft bereikt, is verplicht op de eerste vordering van een ambtenaar als bedoeld in artikel 8a van de Politiewet 1993, een identiteitsbewijs als bedoeld in artikel 1 ter inzage aan te bieden. Deze verplichting geldt ook indien de vordering wordt gedaan door een toezichthouder.

Full-text translation

not available

Entry last changed 14 Mar 05, BJK/MD
disclaimer

14 User Manual

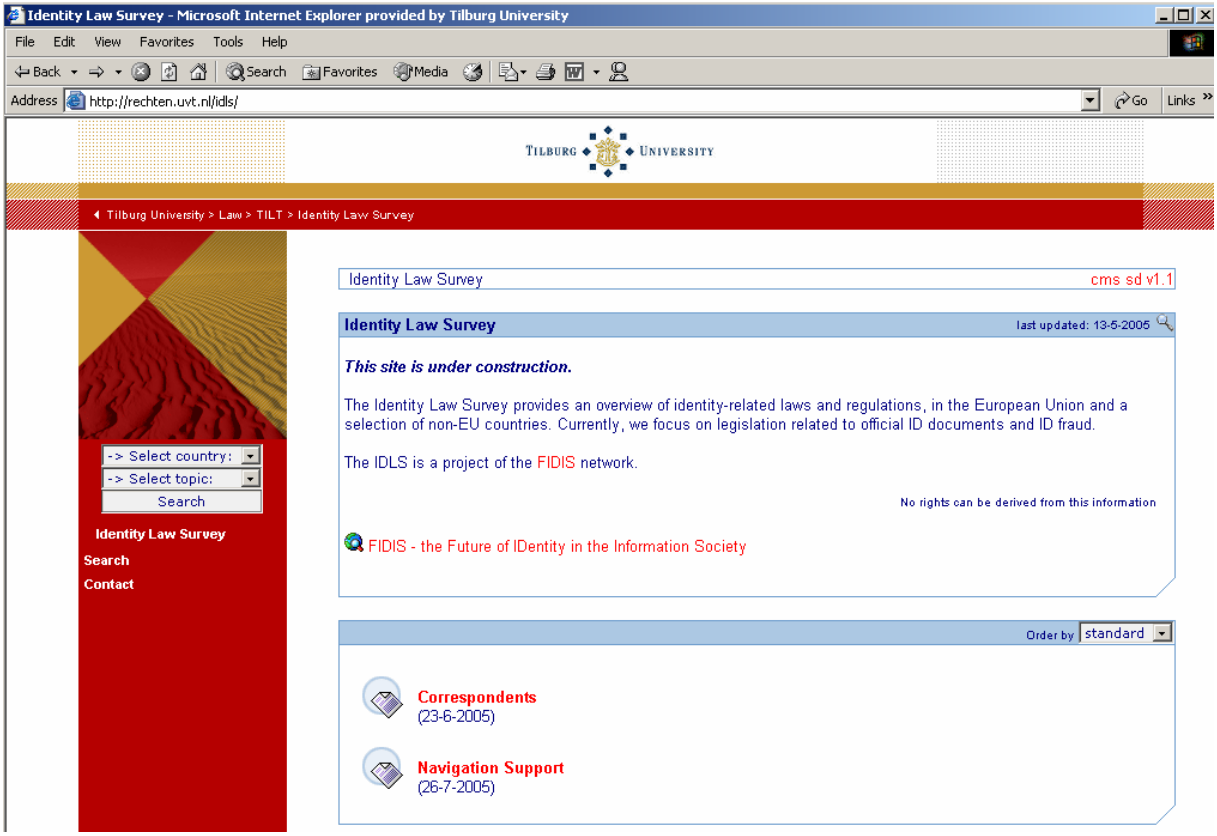
This section explains how the database can be used by end users (13.1) and administrators (13.2).

The introduction page for the database prototype can currently be found here: http://rechten.uvt.nl/idls/. The database will be transported to the FIDIS portal, but currently we base ourselves on the available prototype that is located at Tilburg. When the database is incorporated in the FIDIS portal, the user manual as given below will be adapted as far as is necessary. Since the functionality will be the same, there will be no major differences.

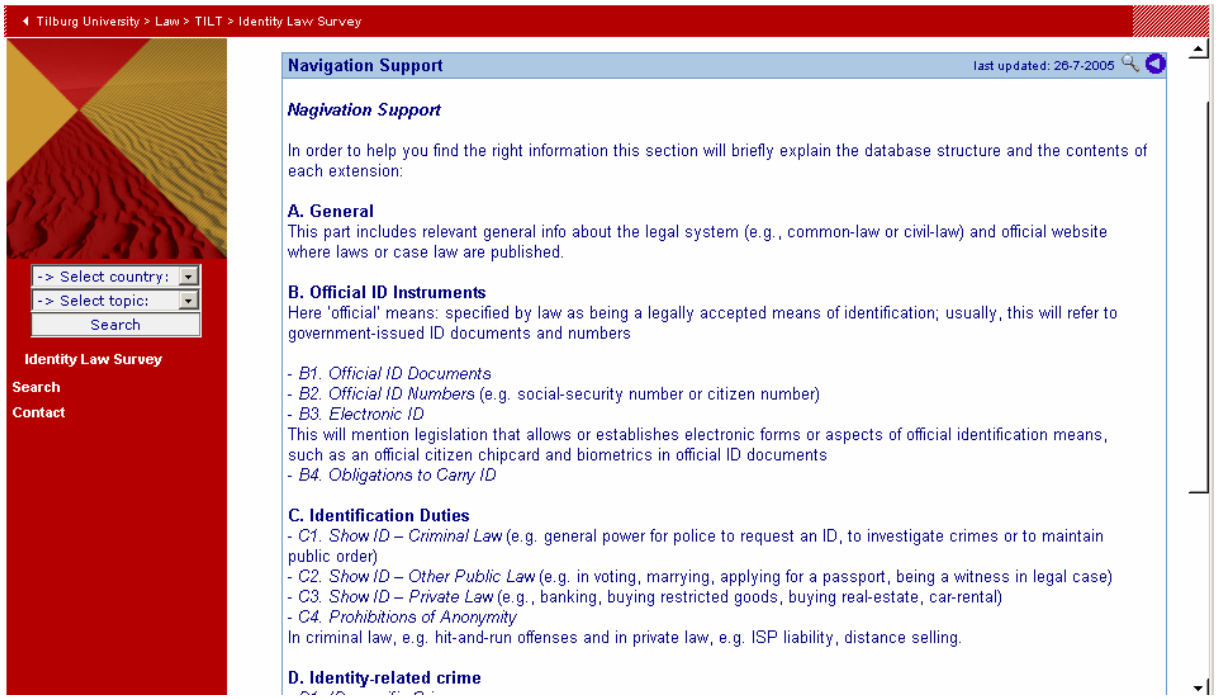
Please note that in the screen captures below, the old structure is still partly being used since the transition of all existing entries to the new structure was still taking place at the time of writing (see section 11).

14.1 Manual for end users

The link http://rechten.uvt.nl/idls/ takes people to the start page.



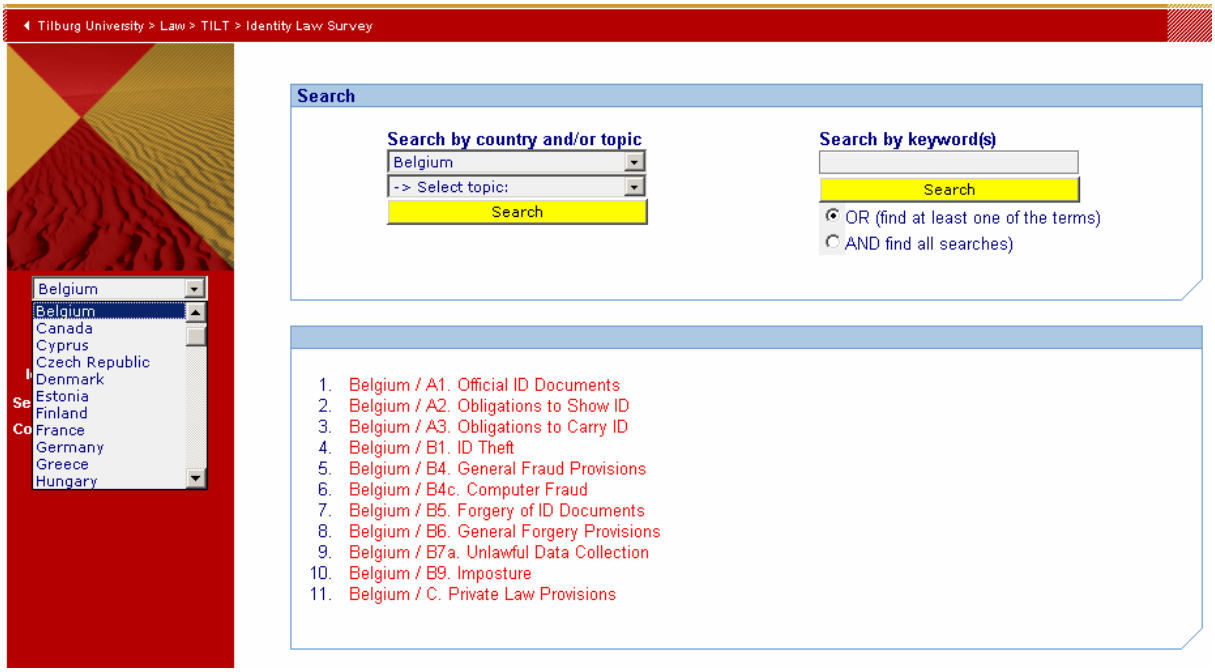
Here, users can click through to FIDIS (if they came in from somewhere else), view the list of Correspondents, and find Navigation Support. The Navigation support will help them, if necessary, to track the right topic that they want to find information about. It explains which type of laws is listed under which topic.



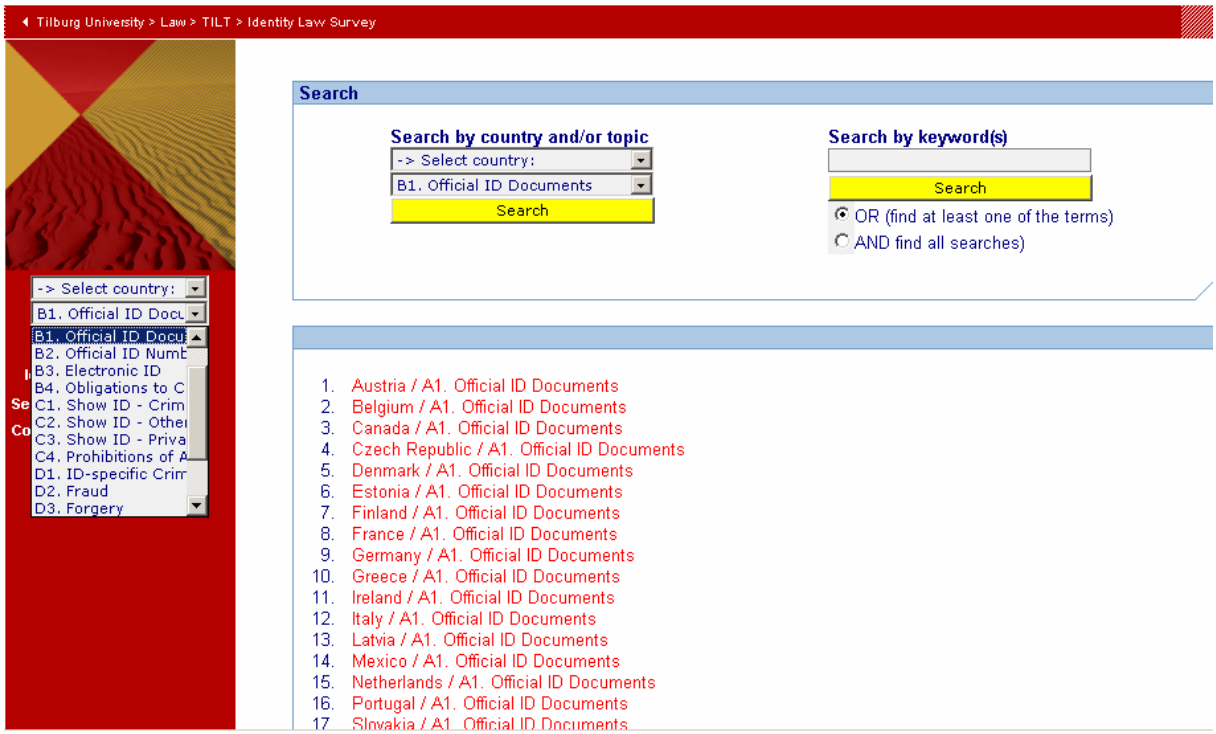
Users can search for information in four ways:

- by country (with a pop-up window listing all countries in the database);
- by topic (with a pop-up window listing all categories and subcategories in the database);
- by country and topic; or
- full-text search.

Searching **by country** shows a pop-up window from which a country can be selected; if the user selects a country and clicks search, a list is shown of all entries relevant to this country.

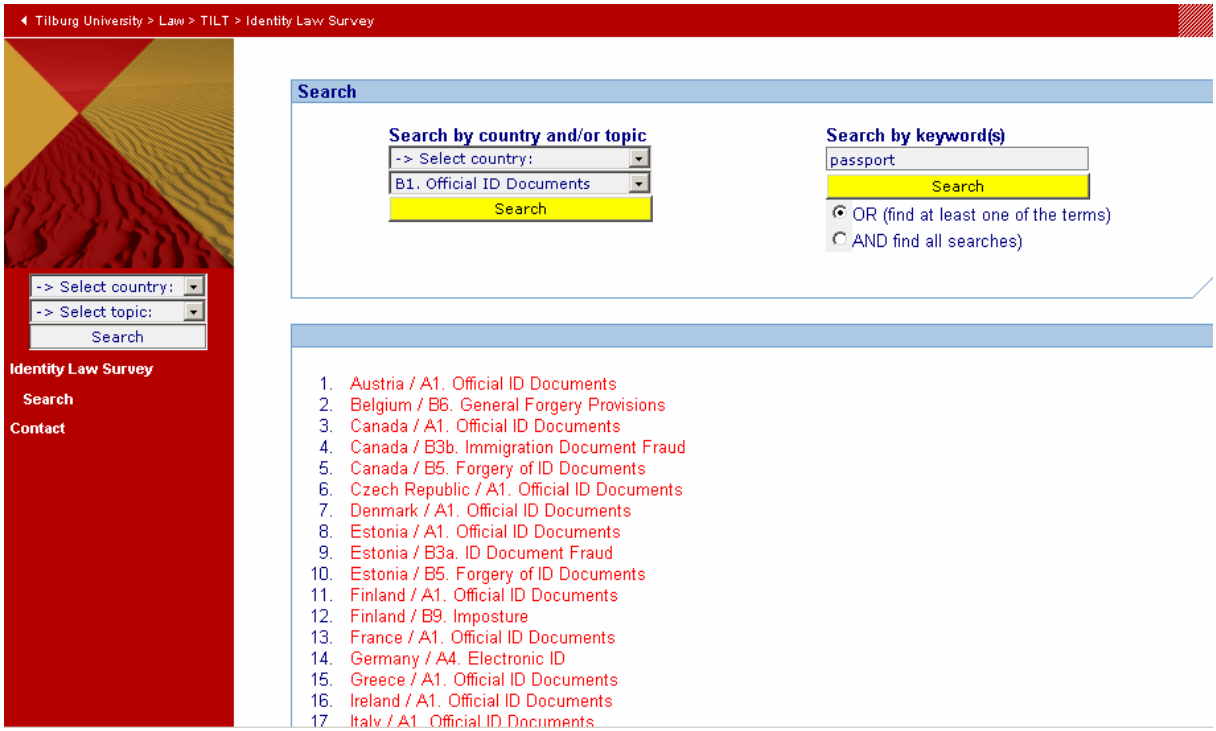


Alternatively, the use can search **by topic** to get a list of countries:



If searched **by country and topic**, only the resulting entry – if available – will show in the list.

Also, a **full-text search** on keywords is possible; in the example shown, a search on passport (right-hand box) yields all entries contain the word ‘passport’.



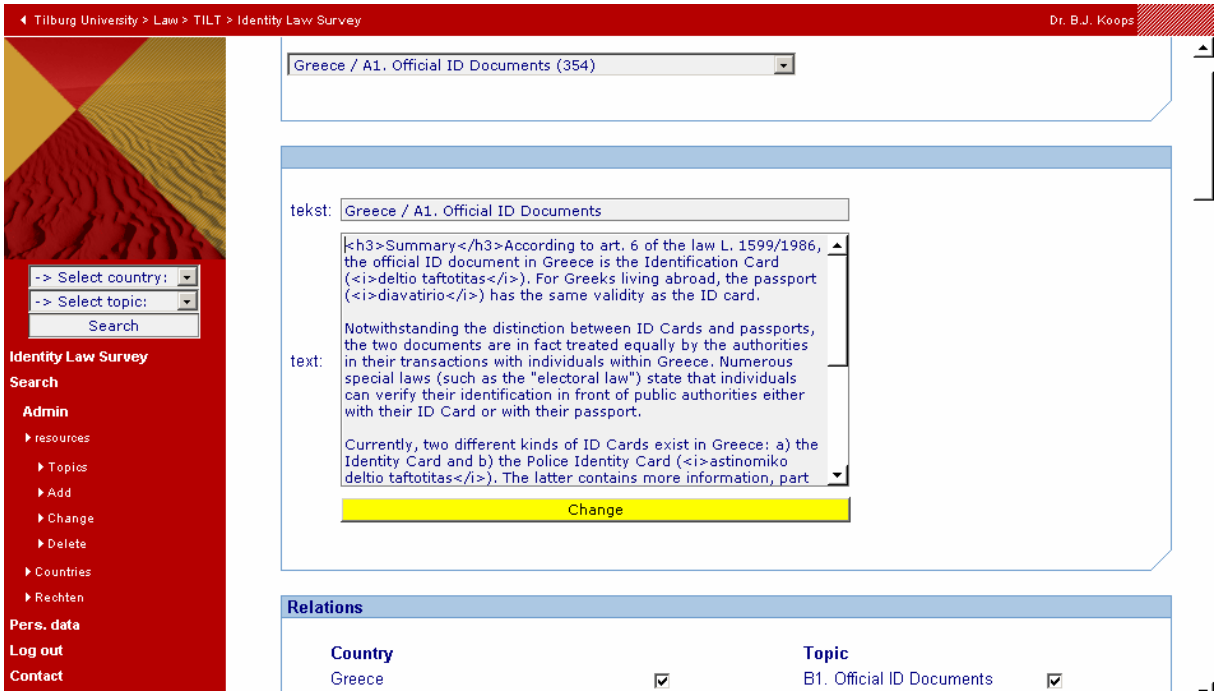
By clicking on an entry in the list, the contents are shown:

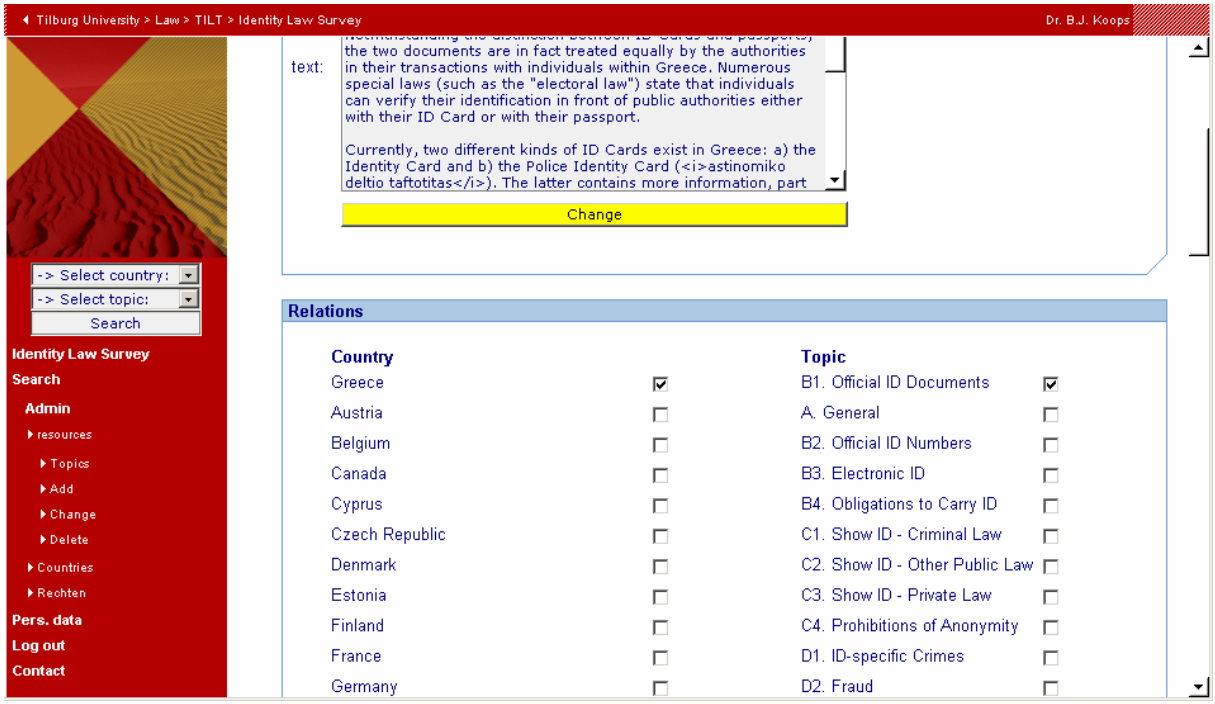
If users find gaps or incorrect information in the survey, they are invited to submit information to the IDLS team. By clicking on Contact, a message with the address of the IDLS team pops up.

14.2 Manual for administrators

Administrators can maintain the database basically through the same web interface. They can log in to the admin page by clicking on the dotted image in the upper right-hand corner and typing in their name and password (the administration of administrator rights is in the hands of the IDLS coordinator). Through the admin link that is now viewable in the left column, administrators can add, change and delete entries (here called resources). In the text field, they can change the html text (first screen capture below) or the labels (second screen capture below). (Currently, only subcategories are usable as labels in Topic; in the new structure as described in section 12.3, entries will be labelled with a category and, if relevant, a subcategory in Topic.)

Administrators can also add, change or delete countries or topics on the same page.





Administrators must take care to add to each entry the date of entry or last change, initials of the administrator and/or country correspondent (depending on whether the administrator simply inputs the information from a country correspondent, or whether he adds data or edits the text himself), and a link to the disclaimer.

15 Maintenance Plan

15.1 Extension in phases

In the first Workplan period, the prototype of the database was built and filled with a few legal categories to illustrate the working of the database. This concerned information about official ID documents, general obligations to carry or show an ID, and criminal provisions on ID theft and ID fraud.

In the second Workplan period, the content of the database will add to the entries in the initial categories (i.e., B1, B4, C1, C2 and D1), and will be extended with new categories of ID-related crime (subcategories D). Towards the end of the second Workplan period, the integration of the IDLS with the FCI will be instigated.

In the third Workplan, it is proposed that the work will be extended with categories B2, B3 and C3, if sufficient funding is allocated in the Workplan to achieve this. The remaining categories may be targeted in the fourth and fifth Workplan, if the consortium so decides.

15.2 Non-exhaustiveness and disclaimer

It will be stressed on the website that the ID Law Survey is not exhaustive. It is not possible – in the sense that it would require a collection of legally-trained people who together have knowledge of all the languages and legal systems of the EU members, as well as a continuous huge amount of time – within the framework of FIDIS to collect an exhaustive and up-to-date overview of all ID-related legislation in all EU member states. Such an exhaustive overview is not the goal of the ID Law Survey. The goal is rather to create a central information portal for the general public where information about ID-related legislation can be looked for. Tilburg University's experience of existing Law Surveys shows that there is great demand for such central information portals that provide legislation 'translated' into concise, understandable texts, even when these surveys are far from exhaustive and not necessarily always up-to-date.[6]

For this reason, a disclaimer will be put on the first page of the IDLS website, and each item will link to this disclaimer. The text of the disclaimer is:

> This survey of ID-related does not pretend to be exhaustive, nor can it be guaranteed to be up-to-date, since legislation continually evolves. The information provided should not be relied upon for legal advice.
>
> If you find any information to be incorrect or outdated, please inform us at idls@fidis.net.

[6] See the Crypto Law Survey, http://rechten.uvt.nl/koops/cryptolaw/, and the Digital Signature Law Survey, http://rechten.uvt.nl/simone/ds-lawsu.htm.

15.3 Management of the IDLS, correspondents, and funding

The IDLS will be maintained by a team of FIDIS people under the co-ordination of a Tilburg University co-ordinator (currently Bert-Jaap Koops). The IDLS team consists of Tilburg people specifically designated for this task (currently Mark Dekker, Sander Kriekaard, and Lydia Romme), extended with one or more other FIDIS people depending on allocation of specific funding for this within WP8.

As stated in the disclaimer, legislation continually evolves. Particularly with smaller countries and countries with official languages other than English, French, or German, legislative changes usually are not easily available, on the Internet nor in legal journals. Therefore, the best way to ensure the retrieval and updating of information in the IDLS is to create a network of correspondents who commit themselves to informing the IDLS team of new or changed legislation and legislative proposals. The creation and maintenance of a network of correspondents is a major task for the IDLS team throughout the full term of FIDIS.

As to funding of the efforts to maintain the IDLS, the IDLS team members are allocated funding within WP8, added for the Tilburg people with funding from Tilburg University's basic budget. Country correspondents from FIDIS members can fund their contribution with funding from their basic budget. External country correspondents work on a voluntary basis.

15.4 Maintenance after FIDIS

After five years, the ID Law Survey should be well-established and have gained renown on the Internet as the place to look for ID-related legal information. This aim can be fulfilled if a well-functioning network of correspondents is established and if FIDIS succeeds in creating a large basis of information to be stored in the database. The experience of existing Law Surveys (see note 6) shows that, once a Law Survey has been set up and contains a sufficient number of entries, and particularly once it shows that it is being updated on a regular basis, public recognition will follow. If this vision works out for the IDLS, it should be feasible to request funding to maintain the IDLS after FIDIS has ended, from public and/or from private funds. FIDIS will make an effort to request further funding in the fourth and fifth year of FIDIS. Should further funding not be (immediately) available, Tilburg University intends to make an effort to maintain the IDLS by requesting funding by itself and in the meantime will maintain the IDLS on at least a basic level so that the database is not becoming outdated too much until new funding is acquired.

16 Annex

16.1 IMS database overview

The 32 records in the IMS prototype database (December 2005) are being named in the following table. It is to be noted that the definitive list of IMS systems can only be found in the database that exists in the FIDIS infrastructure.

16.1.1 List of identified IMS

1. **Advogato**	n.a
2. **Athens Identity Manager**	UK
3. **CAcert**	Australia
4. **CIDAS**	Germany
5. **Cookie Pal**	USA
6. **Entegrity AssureAccess**	USA
7. **Friendster**	USA
8. **HiPath SIcurity DirX**	Germany
9. **Hushmail**	Canada
10. **JAP**	Germany
11. **Jabber**	n.a.
12. **KeePass Password Safe**	Germany
13. **Kerberos**	USA
14. **LOAF**	n.a.
15. **Leverage Sofware**	USA
16. **Liberty Alliance**	Federation of various corporations
17. **Light-Weight IDentity (LID)**	USA
18. **Mozilla Firefox**	USA
19. **Norton Password Manager**	USA
20. **OpenID**	USA
21. **OpenPrivacy**	USA
22. **Opera**	Norway
23. **Orkut**	USA

24. **PayPal**	USA and GB
25. **Roboform**	USA (Virginia)
26. **Shibboleth**	USA
27. **Spamgourmet**	n.a.
28. **Sxip Access**	Vancouver, BC, Canada
29. **Sxip Network**	Vancouver, BC, Canada
30. **Visible Path**	USA
31. **eBay**	USA
32. **iManager**	Germany, Freiburg i. Breisgau

16.1.2 Example of one IMS record: ROBOFORM (num. 25)

As an example all of the information held for one IMS systems is presented below:

Evaluator :	Christian Krause
Organisation :	ICPP
Date of evaluation :	13-Oct-2005

Sources of information :	**http://www.roboform.com/**
Version :	6.4.0
Manufacturer :	Siber Systems Inc
Nature :	private
Country :	USA (Virginia)
Regions :	Global

Language :	DANISH,DUTCH,ENGLISH,FRENCH,GERMAN,ITALIAN,SPANISH
State :	Available
Open/Closed :	Open IMS: the identities work with several systems or applications.

Requirements :	Browser, Windows OS
Number of users :	n.a.
Standards :	n.a.
Description of Server - Side components :	client-only product
Description of methods :	Roboform stores data related to different identities. These can automatically be written into any form on a web-page. Different username/password combinations to log in to different sites can be stored separately.
Descriptor of Client - Side components :	All data can be encrypted with a master password, using DES or 3DES.

Seals :	No
Which seal :	
Third party :	no
Which third party :	

Features :	Roboform can recognise parse forms in HTML-pages. As different identities can be stored, the user selects the desired profile and Roboform fills in the single fields automatically.
Screenshot picture :	**Fehler! Hyperlink-Referenz ungültig.**
Flowchart :	**Fehler! Hyperlink-Referenz ungültig.**
Price :	30
Comment to the Cost :	it is a maximum price
Type of IMS :	Type 3: IMS for user-controlled context-dependent role and pseudonym management.
Class of IMS :	Class 1: Pure IMS which main objective is to support or implement identity management functionality.
Functionality :	Form filling
Suggestions :	Roboform distinguishes Passcards and Identities. Passcards contain a URL combined with a username and password. Once stored, a passcard can log in the user automatically to the appropriate site. Even switching to that site is done by the tool. Identities contain much more information, like address, credit card number, bank accounts and a standard password to use with new accounts. The data stored with such an identity can be used to register with web sites or for online shopping. Multiple identities allow detailed role-management. The free version of Roboform is restricted to 10 passcards and 2 identities.

16.2 ID Law database overview

16.2.1 List of identified ID Law records

Herein, find the entire current list for the EU countries and the related ID Law records in the ID Law prototype; we do not intentionally present the records corresponding to the following countries MEXICO, CANADA and USA. The database on the FIDIS infrastructure is the full archive.

COUNTRY	Related ID law records
AUSTRIA	1. Austria / A. General 2. Austria / B1. Official ID Documents 3. Austria / B3. Electronic ID 4. Austria / D4. Damage
BELGIUM	1. Belgium / A. General 2. Belgium / B1. Official ID Documents

COUNTRY	Related ID law records
	3. Belgium / B3. Electronic ID 4. Belgium / B4. Obligations to Carry ID 5. Belgium / C2. Show ID - Other Public Law 6. Belgium / D1. ID-specific Crimes 7. Belgium / D2. Fraud 8. Belgium / D3. Forgery 9. Belgium / D4. Damage 10. Belgium / D5. Data Abuse 11. Belgium / D6. Imposture 12. Belgium / E1. Tort
CYPRUS	1. Cyprus / A. General
CZECH REPUBLIC	1. Czech Republic / A. General 2. Czech Republic / B1. Official ID Documents 3. Czech Republic / B4. Obligations to Carry ID 4. Czech Republic / C1. Show ID - Criminal Law
DENMARK	1. Denmark / A. General 2. Denmark / B1. Official ID Documents 3. Denmark / D5. Data Abuse
ESTONIA	1. Estonia / A. General 2. Estonia / B1. Official ID Documents 3. Estonia / B4. Obligations to Carry ID 4. Estonia / D1. ID-specific Crimes 5. Estonia / D2. Fraud 6. Estonia / D3. Forgery 7. Estonia / D5. Data Abuse
FINLAND	1. Finland / A. General 2. Finland / B1. Official ID Documents 3. Finland / D1. ID-specific Crimes 4. Finland / D2. Fraud 5. Finland / D3. Forgery 6. Finland / D6. Imposture
FRANCE	1. France / A. General 2. France / B1. Official ID Documents 3. France / D1. ID-specific Crimes 4. France / D2 Fraud 5. France / D3. Forgery 6. France / D5. Data Abuse 7. France / D6. Imposture 8. France / E1. Tort
GERMANY	1. Germany / A. General 2. Germany / B1. Official ID Documents 3. Germany / B3. Electronic ID 4. Germany / B4. Obligations to Carry ID 5. Germany / C1. Show ID - Criminal Law 6. Germany / D1. ID-specific Crimes 7. Germany / D2. Fraud 8. Germany / D5. Data Abuse
GREECE	1. Greece / A. General 2. Greece / B1. Official ID Documents 3. Greece / D1. ID-specific Crimes 4. Greece / D2. Fraud
HUNGARY	1. Hungary / A. General

COUNTRY	Related ID law records
IRELAND	1. Ireland / A. General 2. Ireland / B1. Official ID Documents
ITALY	1. Italy / A.General 2. Italy / B1. Official ID Documents 3. Italy / D1. ID-specific Crimes 4. Italy / D2. Fraud
LATVIA	1. Latvia / A. General 2. Latvia / B1. Official ID Documents 3. Latvia / D1. ID-specific Crimes 4. Latvia / D2. Fraud 5. Latvia / D3. Forgery 6. Latvia / D4. Damage
LITHUANIA	1. Lithuania / A. General
LUXEMBURG	1. Luxemburg / A. General 2. Luxemburg / B4c. Computer Fraud
MALTA	1. Malta / A. General 2. Malta / B4c. Computer Fraud
NETHERLANDS	1. Netherlands / A. General 3. Netherlands / A1. Official ID Documents 4. Netherlands / A2. Obligations to Show ID 5. Netherlands / A3. Obligations to Carry ID 6. Netherlands / B1. ID Theft 7. Netherlands / B2. ID Fraud 8. Netherlands / B3a. ID Document Fraud 9. Netherlands / B4a. General Fraud Provisions 10. Netherlands / B4b. Paper Fraud 11. Netherlands / B4c. Computer Fraud 12. Netherlands / B6. Forgery of ID Documents 13. Netherlands / B6. General Forgery Provisions 14. Netherlands / B7a. Unlawful Data Collection 15. Netherlands / B9. Imposture 16. Netherlands / C. Private Law Provisions
POLAND	1. Poland / A. General 2. Poland / B4c. Computer Fraud
PORTUGAL	1. Portugal / A. General 2. Portugal / A1. Official ID Documents 3. Portugal / B4c. Computer Fraud
SLOVAKIA	1. Slovakia / A. General 2. Slovakia / A1. Official ID Documents 3. Slovakia / A2. Obligations to Show ID 4. Slovakia / A3. Obligations to Carry ID 5. Slovakia / B1. ID Theft 6. Slovakia / B4c. Computer Fraud 7. Slovakia / B8. Damage to ID Documents
SLOVENIA	1. Slovenia / A. General 2. Slovenia / B4c. Computer Fraud
SPAIN	1. Spain / A1. Official ID Documents 2. Spain / A3. Obligations to Carry ID 3. Spain / B1. ID Theft 4. Spain / B2. ID Fraud 5. Spain / B4c. Computer Fraud
SWEDEN	1. Sweden / A. General 2. Sweden / A1. Official ID Documents 3. Sweden / B4a. General Fraud Provisions

COUNTRY	Related ID law records
	4. Sweden / B4c. Computer Fraud
SWITZERLAND	1. Switzerland / A1. Official ID Documents 2. Switzerland / A2. Obligations to Show ID 3. Switzerland / A3. Obligations to Carry ID 4. Switzerland / B4a. General Fraud Provisions 5. Switzerland / B4f. Financial Institution Fraud 6. Switzerland / B5. Forgery of ID Documents 7. Switzerland / B7a. Unlawful Data Collection 8. Switzerland / B7b. Unlawful Data Use
UNITED KINGDOM	1. United Kingdom / A1. Official ID Documents 2. United Kingdom / B1. ID Theft 3. United Kingdom / B4c. Computer Fraud 4. United Kingdom / B5. Forgery of ID Documents 5. United Kingdom / B6. General Forgery Provisions 6. United Kingdom / B7a. Unlawful Data Collection 7. United Kingdom / B7b. Unlawful Data Use

16.2.2 Example of one ID Law record: GERMANY, D1.ID-specific Crimes

Summary

Whoever falsifies or modifies a genuine document or uses a counterfeit or a falsified document, shall be punished with imprisonment for not more than five years or a fine.

Translated text in English

Criminal Code
Special Part
Title Four Common Provisions
Chapter Twenty-three Falsification of Documents

Section 267 Falsification of Documents
(1) Whoever, for the purpose of deception in legal relations, produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document, shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) In especially serious cases the punishment shall be imprisonment from six months to ten years. An especially serious cases exists, as a rule, if the perpetrator:

1. acts professionally or as a member of a gang which has combined for the continued commission of fraud or falsification of documents;
2. causes an asset loss of great magnitude;
3. substantially endangers the security of legal relations through a large number of counterfeit or falsified documents; or
4. abuses his powers or his position as a public official.

(4) Whoever commits the falsification of documents professionally as a member of a gang which has combined for the continued commission of crimes under Sections 263 to 264 or 267 to 269, shall be punished with imprisonment from one year to ten years, in less serious cases with imprisonment from six months to five years.

Source: Translation provided by the Federal Ministry of Justice, 13-11-1998, Criminal Code

Special Part
Title Four Common Provisions
Chapter Twenty-three Falsification of Documents

Section 273 Modification of Official Identification Documents

(1) Whoever, for purposes of deception in legal relations:

1. removes, renders unrecognizable, covers up or suppresses an entry in an official identification document or removes a single page from an official identification document; or
2. uses an official identification document altered in such a way,

shall be punished with imprisonment for not more than three years or a fine if the act is not punishable under Sections 267 or 274.

(2) An attempt shall be punishable.

Source: Translation provided by the Federal Ministry of Justice, 13-11-1998, Criminal Code

Special Part
Title Four Common Provisions
Chapter Twenty-three Falsification of Documents

Section 275 Preparation for Counterfeiting of Official Identification Documents

(1) Whoever prepares a counterfeiting of official identification documents by producing, procuring for himself or another, offering for sale, storing, giving to another, or undertaking to import or export:

1. plates, frames, type, blocks, negatives, stencils or similar equipment which by its nature is suited to the commission of the act; or
2. paper, which is identical or confusingly similar to the type of paper which is designated for the production of official identification documents and specially protected against imitation; or

3. blank forms for official identification documents,

shall be punished with imprisonment for not more than two years or a fine.

(2) If the perpetrator acts professionally or as a member of a gang which has combined for the continued commission of crimes under subsection (1), then the punishment shall be imprisonment from three months to five years.

(3) Section 149 subsections (2) and (3), shall apply accordingly.

Source: Translation provided by the Federal Ministry of Justice, 13-11-1998, Criminal Code

Special Part
Title Four Common Provisions
Chapter Twenty-three Falsification of Documents

Section 276 Procuring False Official Identification Documents

(1) Whoever:

1. undertakes to import or export; or,
2. with the intent of using it to make deception in legal relations possible, procures for himself or another, stores or gives to another

a counterfeit or falsified official identification document or an official identification document which contains a false certification of the type indicated in Sections 271 and 348, shall be punished with imprisonment for not more than two years or a fine.

(2) If the perpetrator acts professionally or as a member of a gang, which has combined for the continued commission of crimes under subsection (1), then the punishment shall be imprisonment from three months to five years.

Source: Translation provided by the Federal Ministry of Justice, 13-11-1998, Criminal Code

Special Part
Title Four Common Provisions
Chapter Twenty-three Falsification of Documents

Section 281 Misuse of Identification Papers

(1) Whoever, for the purpose of deception in legal relations, uses an identification paper which was issued to another, or whoever, for the purpose of deception in legal relations, gives another an identification paper that was not issued to that person, shall be punished with imprisonment for not more than one year or a fine. An attempt shall be punishable.

(2) Certificates and other documents which are used as identification documents in transactions shall be equivalent to an identification paper.

Source: Translation provided by the Federal Ministry of Justice, 13-11-1998, Criminal Code