FIDIS

Future of Identity in the Information Society

Title:	"D4.7: Review and classification for a FIDIS identity management model"
Author:	WP4
Editors:	James Backhouse (LSE) Bernard Dyer (LSE)
Reviewers:	JWG, VUB, ICPP, INSEAD, READING, KUB ALU-FR, MU
Identifier:	D4.7
Type:	[Deliverable]
Version:	3.0
Date:	Thursday, 26 April 2007
Status:	[Final]
Class:	[Public]
File:	fidis-wp4-del4.7.review_and_classification.doc

Summary

This deliverable is concerned with recommendations for establishing an identity classification system which can be incorporated into the best practice guidelines and the FIDIS identity management model, proposed in FIDIS Deliverable D4.6. It is paramount that the classification system may be readily applied in all areas of government, commerce and industry.

A review was made of the identity issues, being studied by FIDIS and other external bodies, which need to be represented in the classification system. The review concentrated on the work published in FIDIS Deliverable D2.1 "Inventory of topics and clusters", and in proposed standards by ISO and the U.S. Department of Commerce. It is hoped that this report may provide a basis for developing a global identity classification system, which can be shared by practitioners involved with identity management. The system will be continually enhanced throughout the duration of the FIDIS project.

It is recommended that the proposed inventory defined in FIDIS Deliverable D2.1, which categorises and defines the different terms used in the identity domain, should provide the core of the identity classification system.

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)*
1.0	December 2006	Preparation and initial release (James Backhouse and Bernard Dyer)
2.0	January 2007	Continuous development. Contributions to this document: VUB: Mireille Hilderbrandt and Els Soenens. Contributions to the key concepts, including the limitation principle, content of the tables. Other contributions will be included in D4.8 and D4.9. TILT: Bert-Jaap Koops. Contributions to the key concepts, structure and content of the tables. Masarykova universita: Vashek Matyas. Contribution on the content of the tables. JWG: Kai Rannenberg and Denis Royer. Contributions to ISO documentation.
3.0	February 2007	Final version incorporating comments from reviewers.

Table of Contents

1 Executive Summary

This deliverable is concerned with recommendations for establishing an identity classification system, covering all topics of identity, which can be incorporated into the best practice guidelines and the FIDIS identity management model, proposed in FIDIS Deliverable D4.6 "Draft best practice Guidelines". It is paramount that the classification system may be readily applied in all areas of government, commerce and industry.

A review was made of the identity issues, being studied by FIDIS and other external bodies, which need to be represented in the classification system, The review concentrated on the work published in FIDIS Deliverable D2.1 "Inventory of topics and clusters", and in proposed standards by ISO and the U.S. Department of Commerce. It is hoped that the proposed system may provide a basis for developing a global identity classification system, which can be shared by practitioners involved with identity management. This will probably be best achieved through the ISO organisation. The system will be continually enhanced during the life of the FIDIS project.

It is recommended that the proposed inventory defined in FIDIS D2.1, which categorises and defines the different terms used in the identity domain, should provide the core of the identity classification system. The inventory provides a comprehensive dictionary, which has been structured in such a way as to create a convenient map of the identity domain.

The proposed classification system has been incorporated into the proposed FIDIS development method and framework, which was described in deliverable FIDIS D4.6. An outline is provided, as to how the classification system may be applied to interoperability, within the FIDIS research, e-health, e-government, and e-commerce sectors.

2 Introduction

One of the objects of investigation for the FIDIS research community is the interoperability of identity management systems from the technical, policy, legal and socio-cultural perspectives. It looks at the limits on identity systems designed for one purpose being used for other purposes (inter-purpose interoperability: e-government, e-health, e-commerce systems), and sees the role of the market in generating interoperability (interplay of governmental regulation, self-regulation and no regulation: cross-border and cross-sector comparisons). It is important to stress that interoperability of identity management should strike a balance between the need to exchange data and the need to prevent threats against privacy and security.

The aim of the project is to develop integrated approaches for security, virtual identity management, and privacy enhancing technologies at application level, system level and infrastructure level. A fundamental aspect to be considered when applying identity management, involving many disciplines, within all areas of government, commerce and industry, is the creation of a common comprehensive classification system, which can be shared and applied by practitioners involved with identity management.

The proposed classification system endeavours to provide managers and developers with a system to manage effectively the vast amounts and forms of information and the many issues, such as security and privacy, which identity management technology and systems engender. The classification system brings together a wide range of topics that are required to reach good decisions on interoperable identity and its application.

2.1 Classification systems

A paper by Susan Irwin[1] states, "the need to organise large amounts of information has led to the development of classification theory and systems and other management tools. Regardless of the nature of the information resource, the need to express its content, describe its format, facilitate its access, and enable its use remains constant (Ref: Dillon & Jul, 1996 p.212-13). Library classification schemes have four main purposes. First they order the fields of knowledge in a systematic way. Second, they bring related items together in a helpful sequence. Third, they provide orderly access to the shelves either for browsing or via the catalogue. Finally, they provide an exact location for an item on the shelves (Ref: Dittmann and Hardy, 2000 p.8)".

It is recommended that the approach adopted by library classification schemes be used for the FIDIS identity classification system.

[1] Irwin, Susan; "Classification Theory and the Internet: A move toward Multidimensional Classification"; University of Denver; March 6, 2001

2.2 Aims of the deliverable

The aims of the deliverable are:

- To review the identity issues, being studied by FIDIS and other external bodies, which need to be represented in the classification system

- To propose a classification system that can be incorporated into the proposed FIDIS development method and framework described in FIDIS D4.6

- To outline how the classification system may be applied to the domains of FIDIS research, e-health, e-government and e-commerce

3 Review

The following documents, which cover a wide range of topics related to the classification of identity identifiers/credentials, were reviewed.

3.1 FIDIS Deliverable "D2.1: Inventory of topics and clusters"

This document is the most comprehensive one of those reviewed, as it deals with all aspects of identity management in great detail. All the material in the report is relevant to creating an identity classification system and the salient points covered within the report include:

- The concept and application of an ontology
- A conceptualisation of the identity domain conducted in the FIDIS project
- An inventory that categorises and defines the different terms used in the identity domain
- The definition of key identity topics and terms
- A structured approach to the inventory of identity terms
- Considerations relating to the characterisation of a person via a set of attributes, and their application in different situations and how they relate to the person
- Approaches, mechanisms and processes in disclosing identity information.
- Definition of a shared vocabulary to be used in the identity domain
- Setting up the conditions for the dynamic of exchange of this knowledge within the FIDIS community and external users

3.2 ISO/IEC WD 24760; "Information technology – Security techniques – Identity management framework".

The document is a working draft for an ISO International Standard that has been informally distributed for review and comment.

It defines and establishes a framework for identity management, and the management of information associated with the identification of an entity within some context. It concentrates on the use of the proposed framework in the context of Information Security.

The scope of the proposed standard is divided into chapters covering:

- Identity concepts
- Identity Management
- Identity management in the information society
- Identity Management and Information Technology
- Identity Management and information security
- Related IT security concepts

It references ISO/IEC 17799:2005 – "Code of practice for information security management as an indispensable document for the application of this proposed standard" (normative reference).

The draft standard covers much of the work discussed in FIDIS D2.1, but not in as much detail.

3.3 ISO /IEC JTC 1 /SC 27 N5530; "ISO/IEC JTC 1/SC 27 WG5 liaison statement to FIDIS on Biometrics, Identity Management and Privacy"

This document is the first liaison statement, from ISO/IEC JTC 1/SC 27 WG5 to FIDIS, as part of the liaison to collaborate on developing standards on Biometrics, Identity Management and Privacy.

The proposed standards will define concepts associated with identity and identity management, especially NP 24760 " A framework for Identity Management", and will provide a framework for the secure, reliable, and private management of identity information over the lifecycle of entity identities and identity information.

Besides NP 24760 there are four further standards, relating to identity management, being developed by ISO/IEC JTC 1/SC 27 WG5. All five projects are listed below:

- **Biometrics**
  - ISO/IEC WD 24745 Biometric template protection (Project 1.27.45)
  - ISO/IEC CD 24761 Authentication context for biometrics (Project 1.27.49)
- **Identity Management**
  - ISO/IEC 24760 A framework for Identity Management (Project 1.27.50)

  The glossary of terms defined in this proposed standard only covers a small proportion of those discussed in FIDIS D2.1.
- **Privacy**
  - ISO/IEC NP 29100 Privacy Framework (Project 1.27.54)
  - ISO/IEC NP 29101 Privacy Reference Architecture (Project 1.27.55)

3.4 NIST National Institute of Standards and Technology; "Information Security - An Ontology of Identity Credentials, Part 1: Background and Formulation"

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA of 2002, Public Law 107-347). It is a draft version that has been prepared for use by federal agencies. It may be used by non-governmental organisations on a voluntary basis and is not subject to copyright.

The scope of the proposed standard is divided into the following sections:

- Section 1, *Introduction*, provides the purpose, scope audience, and assumptions of the document and outlines its structure
- Section 2, *Overview of Identity Concepts*, identifies the characteristics or dimension of identity that can be used to categorise credentials
- Section 3, *The Structure of Credentials*, describes the structure and requirements for physical and logical credentials
- Section 4, *Survey of Identity Credentials*, this section categorises key credentials by their purpose e.g. documents for travel and discusses the properties, procedures and inherent issues in using these credentials
- Section 5, *Identity Credential Standards*, describes and provides references to the most important U.S. standards for primary and secondary identity credentials including some international standards
- Section 6, *Identity Credential System Models*, describes a typical model for a credential lifecycle and discusses the role of Information Technology in the lifecycle
- Section 7, *Trust and Security*, describes how the level of trust in identity credentials is related to the level of security applied to issue the credential, and to authenticate its use
- Section 8, *Case Studies of Identity Documents*, discusses properties and usage of common identity documents
- Section 9, Miscellaneous Topics, discusses related topics that potentially fall under several sections
- A *Glossary*, contains a list of key definitions referred to or pertinent to this document

The draft standard is comprehensive and covers much of the work discussed in FIDIS D2.1, but concentrates on the use of identity in the context of Information Security. As in the ISO documents, the glossary of terms defined in the NIST standard only covers a small proportion of those discussed in FIDIS D2.1.

4 Classification System

There is considerable overlap in the content of the reviewed documents, but the greatest detail relating to the classification of identity credentials is provided in FIDIS D2.1. It is recommended that the inventory, specified in FIDIS D2.1, is used as the basis for the classification system in FIDIS.

The structure and detail of the proposed FIDIS identity classification system are shown in the following tables. The classification system relating to the identity of a person has been divided into two classes

- Class 1: Factual/Physical/Material Attributes (Simple/Singular)
- Class 2: Abstract/Interpretational Attributes (Complex)

The vertical axis of the tables specifies the list of identities being included in the system and the horizontal axis represents the five principles of information management described in FIDIS Deliverable D4.6. The ordering of the principles reflects a cascade from the classification of information streams to responsibilities, and then on to technology and operational considerations.

The five principles of information management are stated below:

4.1 Five Principles of Information Management

4.1.1 Information

To ensure that the institution:

- Recognises, understands and controls data and information through its classification, structure and the way it is represented
- Chooses appropriate methods to capture, store and transmit data within the institution and across its boundaries to, and from, its business partners
- Evaluates the information that it holds and takes appropriate measures to protect its information resources
- Implements appropriate levels of security for managing its information.

4.1.2 Duty of Care

To ensure that the institution:

- Informs appropriate staff of pertinent legislation and regulations which apply to the way information and data is handled within their sector and business activities
- Executes its responsibilities under the duty of care principle.

4.1.3 Processes and procedures

To ensure that the institution:

- Identifies, documents and describes its processes and procedures
- Monitors and controls any change to standard procedures using the documented descriptions of its operations

4.1.4 Enabling technologies

To ensure that the institution:

- Identifies, assesses and applies appropriate technologies to support and enable its business processes and procedures
- Establishes procedures to monitor and control potential exposure to risks arising from the misuse or failure of its computer systems

4.1.5 Auditing

To ensure that the institution:

- Employs appropriate measures to monitor and document its operations and any deviations from its designated standards and methods of operation as established by its industry's regulatory bodies

4.2 Further description of the tables

- **Identity**

  The identity being specified in the classification system

- **Identifier / Credential**

  The identifier/credential being specified which relates to the identity

- **Importance**

  Level of importance of the identifier/credential, which may be *high, medium or low*; or *primary or secondary*, which will depend upon its application

- **Information held by person and other stakeholders**

  The identifier/credential, which is held by the person, and by other stakeholders such as an employer or government agency

Notes:

1. Where there may be more than one identifier/credential representing a particular attribute, such as Name or Address, they are stated as Name (n) or Address (n).

2. Most of the identifiers/credentials are documents that only relate to the person, which can be copied. They do not directly identify the person, as in the case of biological identifiers/credentials.

3. The identifiers/credentials, stakeholders, etc, stated in the tables are not exhaustive and will be extended as the work progresses.

4. It is envisaged that each country will have its own "names" for government departments, national ID numbers, etc.

5. The tables provide an overview of the five principles, applicable to most identifiers/ credentials, rather than detailed descriptions for each one.

- **Roles and responsibilities**

  The roles and responsibilities of all stakeholders such as:
  - Ensuring information is secure at all times
  - Ensuring that the practitioners managing the information are bona fide
  - Ensuring staff are aware of pertinent legislation and regulations

- **Processes and procedures**

  The processes and procedures of all stakeholders for managing the information, such as:
  - Ensuring that the identity lifecycle is managed correctly and effectively
  - Ensuring that the information is complete, accurate and authorised
  - Ensuring interoperability between stakeholders is secure, efficient and effective

- **Enabling technologies**

  Ensuring that the appropriate technologies, to support and manage, the identity information are in place, such as:
  - Card readers
  - Biometric scanners
  - RFID

- **Audit and control**

  To audit and control operations relating to identity management including:
  - The vetting of personnel
  - Compliance with statutes and regulations
  - Variances between actual and monitored information

Classification System

Stakeholder: Person Class 1: Factual / Physical / Material Attributes (Simple / Singular)

Identity	Principles of Information Management							
	Information				Roles & Responsibilities	Processes & Procedures	Enabling Technologies	Audit & Control
	Identifier / Credential	Importance	Held by person	Held by other stakeholders				
Person	Name (n)		Yes	All stakeholders	Secure and protect: Information Computer systems Destroy out of date information Ensure stakeholders & representatives are bona fide Protect: Credit card usage Passwords PIN numbers Delete unsolicited emails Monitor regularly: Information Computer systems Vetting of personnel Comply with statutes & regulations	Purpose for use Application Lifecycle: Input Storage Access Maintenance Deletion Accuracy Authentication Authorisation Confidentiality Security Interoperability Identification Matching checks	Paper Electronic Web E-mail Cards: Credit (n) Store (n) Licence (n) Membership (n) Etc Voice Face to face Camera (n) Scanner (n) RFID PET TET Databases	Ensure all items are bona fide: Person (n) Stakeholders & their representatives Documents and copies Scans match with originals Computer systems Compliance with statutes & regulations
	Signature		Yes	All stakeholders				
Location	Address (n)		Yes	All stakeholders				
	Electoral roll		Yes	Govn't (Local)				
	Business address (n)		Yes	Employer (n)				
	Location address (n)		Yes	All stakeholders				
	Phone Numbers (n)		Yes	All stakeholders				
	e-mail address (n)		Yes	All stakeholders				
Status	Birth certificate		Yes	Govn't (Records)				
	Marriage certificate (n)		Yes	Govn't (Records)				
	Divorce papers (n)		Yes	Govn't (Records)				
	Death certificate		Yes	Govn't (Records)				
	Passport (n)		Yes	Govn't (National Affairs)				
	Bio-implant (n)		Yes	Govn't (National Affairs)				
	Driving licence		Yes	Govn't (Vehicle Agency)				
	Citizenship		Yes	Govn't (National Affairs)				
	Nationality		Yes	Govn't (National Affairs)				
	Family		Yes	Govn't (National Affairs)				
	Wealth		Yes	Govn't (National Affairs)				
	Title		Yes	Govn't (National Affairs)				

Classification System

Stakeholder: Person Class 1: (Continued)

Identity	Principles of Information Management							
	Information				Roles & Responsibilities	Processes & Procedures	Enabling Technologies	Audit & Control
	Identifier / Credential	Importance	Held by person	Held by other stakeholders				
Education	School (n): certificates, diplomas, degrees		Yes	Govn't (Education)	Secure and protect: Information Computer systems Destroy out of date information Ensure stakeholders & representatives are bona fide Protect: Credit card usage Passwords PIN numbers Delete unsolicited emails Monitor regularly: Information Computer systems Vetting of personnel Comply with statutes & regulations	Purpose for use Application Lifecycle: Input Storage Access Maintenance Deletion Accuracy Authentication Authorisation Confidentiality Security Interoperability Identification Matching checks	Paper Electronic Web E-mail Cards: Credit (n) Store (n) Licence (n) Membership (n) Etc Voice Face to face Camera (n) Scanner (n) RFID PET TET Databases	Ensure all items are bona fide: Person (n) Stakeholders & their representatives Documents and copies Scans match with originals Computer systems Compliance with statutes & regulations
	University (n): degrees certificates, diplomas		Yes	Govn't (Education)				
Situational	Qualification (n)		Yes	Prof Body/Institution				
Medical	Doctor (n)		Yes	Govn't (Health)				
	Hospital (n)		Yes	Govn't (Health)				
	Medical records (n)		No	Govn't (Health)				
	Condition (n)		Yes	Govn't (Health)				
Biological	Gender		Yes	Govn't (Health)				
	Eye colour		Yes	Govn't (Health)				
	Height		Yes	Govn't (Health)				
	Fingerprint		Yes	Govn't (Health)				
	DNA		No	Govn't (Health)				
	Retina		Yes	Govn't (Health)				
	Iris		Yes	Govn't (Health)				
	Face		Yes	Govn't (Health)				
	Handwriting		Yes	Govn't (Forensics)				
	Voice		Yes	Govn't (Forensics)				
Banking	Bank (n)		Yes	Finance Institution (n)				
	Account (n)		Yes	Finance Institution (n)				
	Telecommunication (n)		Yes	Finance Institution (n)				

Classification System

Stakeholder: Person Class 1: (Continued)

Identity	Principles of Information Management							
	Information				Roles & Responsibilities	Processes & Procedures	Enabling Technologies	Audit & Control
	Identifier / Credential	Importance	Held by person	Held by other stakeholders				
	Transaction (n)		Yes	Finance Institution (n)	Secure and protect: Information Computer systems Destroy out of date information Ensure stakeholders & representatives are bona fide Protect: Credit card usage Passwords PIN numbers Delete unsolicited emails Monitor regularly: Information Computer systems Vetting of personnel Comply with statutes & regulations	Purpose for use Application Lifecycle: Input Storage Access Maintenance Deletion Accuracy Authentication Authorisation Confidentiality Security Interoperability Identification Matching checks	Paper Electronic Web E-mail Cards: Credit (n) Store (n) Licence (n) Membership (n) Etc Voice Face to face Camera (n) Scanner (n) RFID PET TET Databases	Ensure all items are bona fide: Person (n) Stakeholders & their representatives Documents and copies Scans match with originals Computer systems Compliance with statutes & regulations
Business	Employer (n)		Yes	Employer (n)				
	Address (n)		Yes	Employer (n)				
	Position (n)		Yes	Employer (n)				
	Salary (or Pension) (n)		Yes	Employer (n)				
	Period (n)		Yes	Employer (n)				
Domestic	Telephone bill (n)		Yes	Telephone co (n)				
	Electricity bill (n)		Yes	Electricity co (n)				
	Water bill (n)		Yes	Water co (n)				
	Council tax (n)		Yes	Government (Local)				
	Shopping bills (n)		Yes	Retailer (n)				
	Leisure, Travel, etc (n)		Yes	Leisure co (n)				
Government	Insurance Number		Yes	Govn't (National Affairs)				
	Citizen Service Number		Yes	Govn't (National Affairs)				
	Income Tax return (n)		Yes	Govn't (Inland Revenue)				
	VAT return (n)		Yes	Govn't (Inland Revenue)				
	Pension (n)		Yes	Govn't (Pensions)				
	Benefit (n)		Yes	Govn't (Benefit Agency)				

Classification system

Stakeholder: Person Class 2: Abstract / Interpretational Attributes (Complex)

Identity	Principles of Information Management							
	Information				Roles & Responsibilities	Processes & Procedures	Enabling Technologies	Audit & Control
	Identifier / Credential	Importance	Held by person	Held by other stakeholders				
Biological	Gait		Yes	Govn't (Health)	Secure and protect: Information Computer systems Destroy out of date information Ensure stakeholders & representatives are bona fide Protect: Credit card usage Passwords PIN numbers Delete unsolicited emails Monitor regularly: Information Computer systems Vetting of personnel Comply with statutes & regulations	Purpose for use Application Lifecycle: Input Storage Access Maintenance Deletion Accuracy Authentication Authorisation Confidentiality Security Interoperability Identification Matching checks	Paper Electronic Web E-mail Cards: Credit (n) Store (n) Licence (n) Membership (n) Etc Voice Face to face Camera (n) Scanner (n) RFID PET TET Databases	Ensure all items are bona fide: Person (n) Stakeholders & their representatives Documents and copies Scans match with originals Computer systems Compliance with statutes & regulations
	Gesture		Yes	Govn't (Health)				
Behavioural	Aspiration/attitude		Yes	All stakeholders				
	Cognitive style		Yes	All stakeholders				
	Interests		Yes	All stakeholders				
	Learning style		Yes	All stakeholders				
	Personality		Yes	All stakeholders				
	Relationships		Yes	All stakeholders				
	Lifestyle		Yes	All stakeholders				
	Profile (Psychological, social….)		Yes	All stakeholders				
	Reputation		Yes	All stakeholders				

5 Incorporating FIDIS research into the proposed identity classification system

The FIDIS research activities, represented in the tables below, need to be incorporated into the proposed FIDIS identity classification system. The tables indicate how the research can be integrated into the best practice guidelines described in FIDIS D4.6, by applying the five principles of information management.

The vertical axis of the tables specifies the FIDIS Work Packages and the horizontal axis represents the five principles of information management, which state information streams, roles and responsibilities, proposes and procedures, enabling technologies and audit and control.

The tables provide a level of abstraction above the classification system and illustrate what it needs to cover. They may be used as a checklist for completeness.

Integration of FIDIS research activities

Work Package	Principles of Information Management				
	Information	**Roles & Responsibilities**	**Processes & Procedures**	**Enabling Technologies**	**Audit & Control**
WP1	All FIDIS and external information	Manage infrastructural activity "Internal Communication Infrastructure"	Coordinate network activities Create templates Collect, correlate and disseminate work in progress and results. Maintain and backup all information Maintain and extend Web-Portals	Internal Communication Infrastructure IS & IT systems backups Maintenance External communications	Ensure information is complete and accurate Ensure systems and information are secure Ensure statutes and regulations are complied with Ensure all stakeholders & their representatives are bona fide
WP2	Wiki guidelines, structure & references Content – internal & external information Observatory, concepts & definition of terms	Establish the public FIDIS Identity Wiki	Define Wiki guidelines Define Wiki structure & references – internal & external Aggregate & Integrate	Wiki	
WP3	Mechanisms, methods & tools Protocols Biometrics Standards Models for privacy RFID	Execute activity "High-Tech IDs technologies to support identity and identification"	Establish technical solutions Analysis of network protocols Implementation of biometrics AmI, profiling and RFID Holistic privacy framework for RFID Maintain IMS database	Network Protocols RFID PKI IMS Database Biometrics	
WP4	All FIDIS and external information	Develop the "transversal" perspective across full spectrum of FIDIS work	Integrate research Interoperability Best Practice Guidelines Principles of Information Mgt	IS and IT systems Information infrastructure	

Integration of FIDIS research activities (continued)

Work Package	Principles of Information Management				
	Information	**Roles & Responsibilities**	**Processes & Procedures**	**Enabling Technologies**	**Audit & Control**
WP7	National and international sources of law (treaties, EU regulations, statutes and regulations, case law, doctrine, principles etc.) Profiling, AmI, Internet of Things Ambient law Profiling: classification, clustering, association rules etc. Autonomic profiling	Jointly execute research activity "profiling"	Social, legal and political implications Security, privacy, due process, fairness & equality	Profiling technologies AmI, RFID-systems, (Behavioural & Physical) Biometrics, Sensor technologies, multi-agent systems, Network Protocols	Ensure information is complete and accurate Ensure systems and information are secure Ensure statutes and regulations are complied with Ensure all stakeholders & their representatives are bona fide
WP9	All FIDIS and external information Journals	Perform the management activity "Dissemination"	Create & disseminate the journal	Internal & extermal communication infrastructure	
WP10	All FIDIS and external information	Perform the management activity "Network Management"	Quarterly phone conference Annual NoE plan Annual board and plenary meeting Strategic workshop	Internal communication infrastructure	
WP11	Mobile communication networks Data services Private & public access	Execute research activity "Mobility & Identity"	Study on private and public access Survey on Mobile ID management	Mobile communication networks Data services	
WP12	RFID Emerging AmI technologies Good practice Standards Holistic privacy framework	Execute research activity "Emerging Technologies"	Technological, social and legal issues Good practice Standards Holistic privacy framework	RFID Emerging AmI technologies	
WP13	ID number policies EU states' policies	Execute research activity "Privacy and Privacy Technologies"	Profiling techniques	IS & IT systems Privacy technologies	
WP14	Privacy requirements	Jointly execute research activity "Privacy"	Privacy business processes Trusted computing	IS & IT systems Privacy technologies	
WP15	All FIDIS and external information	Jointly execute "PhD Training in the NoE"	Exchange of knowledge Workshops & summer schools Interdisciplinary events	Internal & extermal communication infrastructure	

6 Application of the Classification System

This section shows examples of the stakeholders, within the FIDIS research, e-health, e-government and e-commerce sectors, who may apply the identity classification system in their interoperability processes.

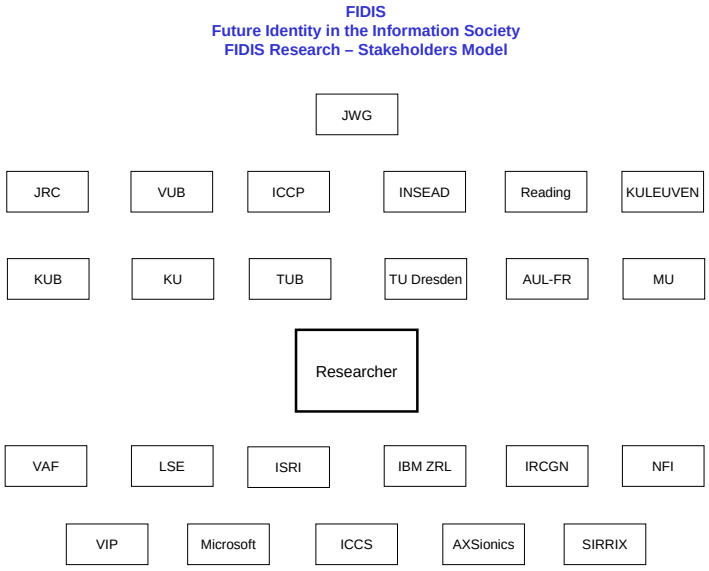
It is proposed that an ISO standard, or code of practice, is written for applying the classification system to interoperability of identity information within all sectors of industry, government and commerce. The standard may be structured in a similar way to that of a British Standard Institution "Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically" (BIP 0008), in which the LSE team played a major role in its publication. The structure of the BSI Code of Practice is based on the BSI "Principles of Good Practice for Information Management" (BSI DISC PD0010), written by the LSE team.

It is envisaged that the proposed code of practice for the identity classification system will include the following chapters:

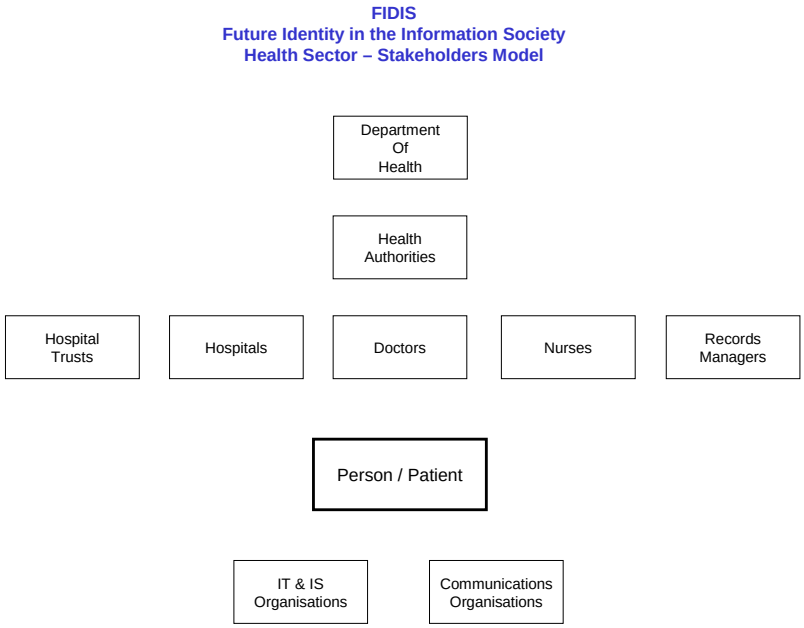
- Introduction
- Identity information policy
- Duty of care
- Procedures and processes
- Enabling technologies
- Audit trails
- Glossary of terms
- References

All the stakeholders in a particular business sector, including those shown below (they are not exhaustive), may then use the classification system to share and exchange information in a common way. The names of the stakeholders, in any sector, may vary from country to country.

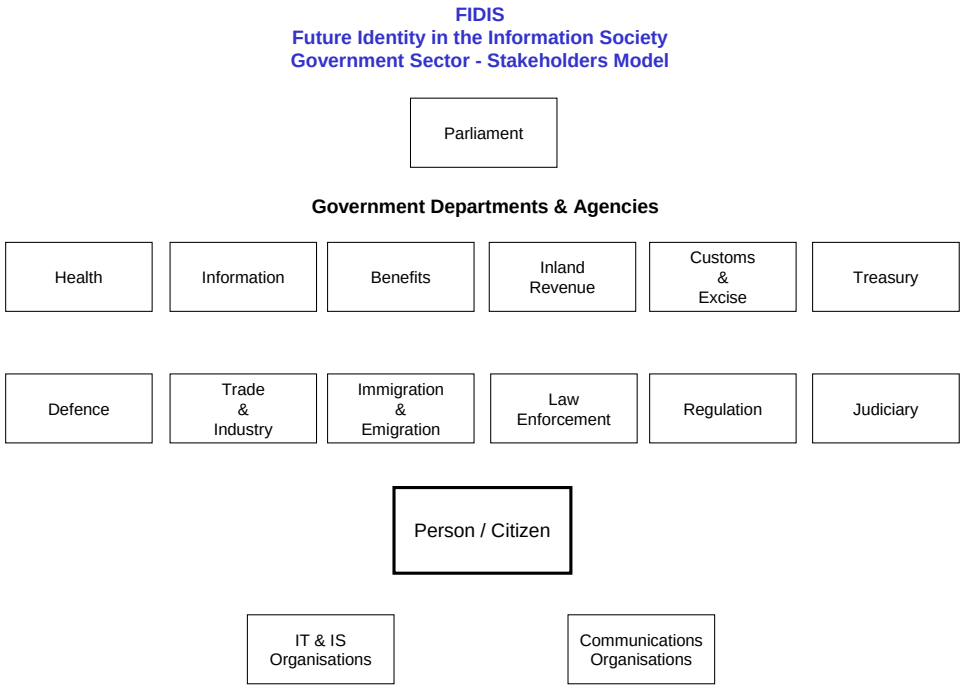
6.1 FIDIS Research Stakeholders



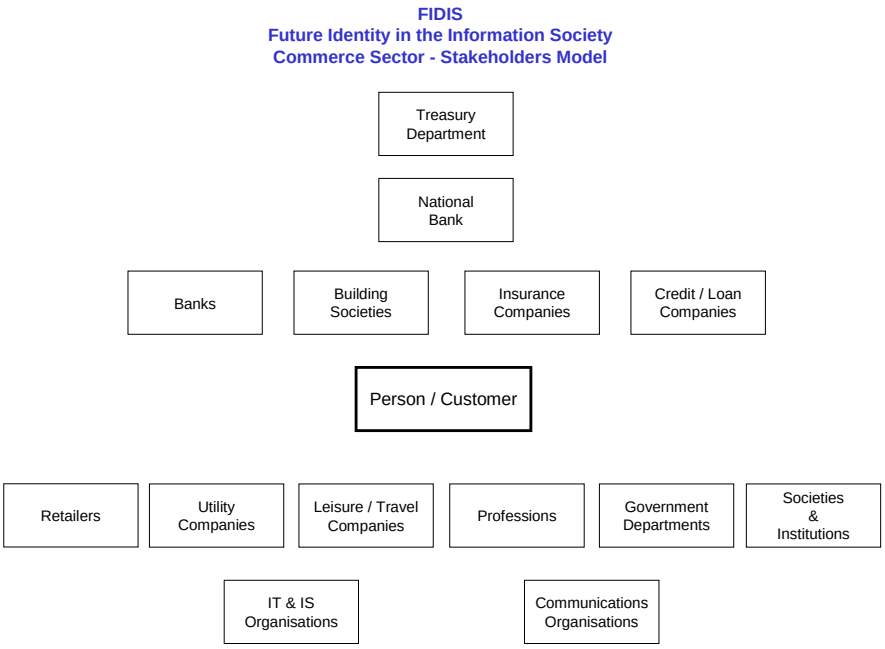
6.2 E-Health Stakeholders



6.3 E- Government stakeholders



6.4 E-Commerce Stakeholders



7 Conclusions and future work

This deliverable should only be considered as the start of a continuous process for developing the identity classification system, which it is hoped will contribute towards a global classification system. It concerns the recommendations for the structure, nature and content of a FIDIS identity classification system. From the review of FIDIS internal documents and external documents published by ISO and NIST, it is considered that FIDIS is at the forefront of research in identity classification.

It is hoped that the deliverable will stimulate participation of the FIDIS partner institutions in developing the classification system and its adoption in relevant organisations.

The classification system will be enhanced to create integration and interoperation, as far as possible, of all the FIDIS research findings, such as those in technologies, privacy, security; forensics, and profiling. The activities will include the application of identity classification to the interoperability between stakeholders and identifying the information, business processes, roles and responsibilities, technologies and audit/compliance issues. Emphasis will be on the delivery of a classification system that is easy to use, robust and complete.

7.1 Next steps in the 3rd Work Plan

The following actions are recommended:

- To use and develop the inventory, specified in FIDIS D2.1, as a basis for the classification system in FIDIS
- To pursue the liaison with ISO/IEC JTC 1/SC 27/WG 5, as stated in the Liaison Statement by the ISO organisation and FIDIS.
- To develop and extend a glossary of definitions and terms related to identity, so that they be may accepted and shared worldwide. This will probably best achieved through the ISO organisation, as ISO is the global standards creating body. We envisage the liaison between FIDIS and ISO will foster the adoption of FIDIS research on a worldwide basis.
- To liaise with ISO/IEC SC 27/WG in developing an identity management framework, which may be applied to all aspects of identity including, security, privacy and biometrics

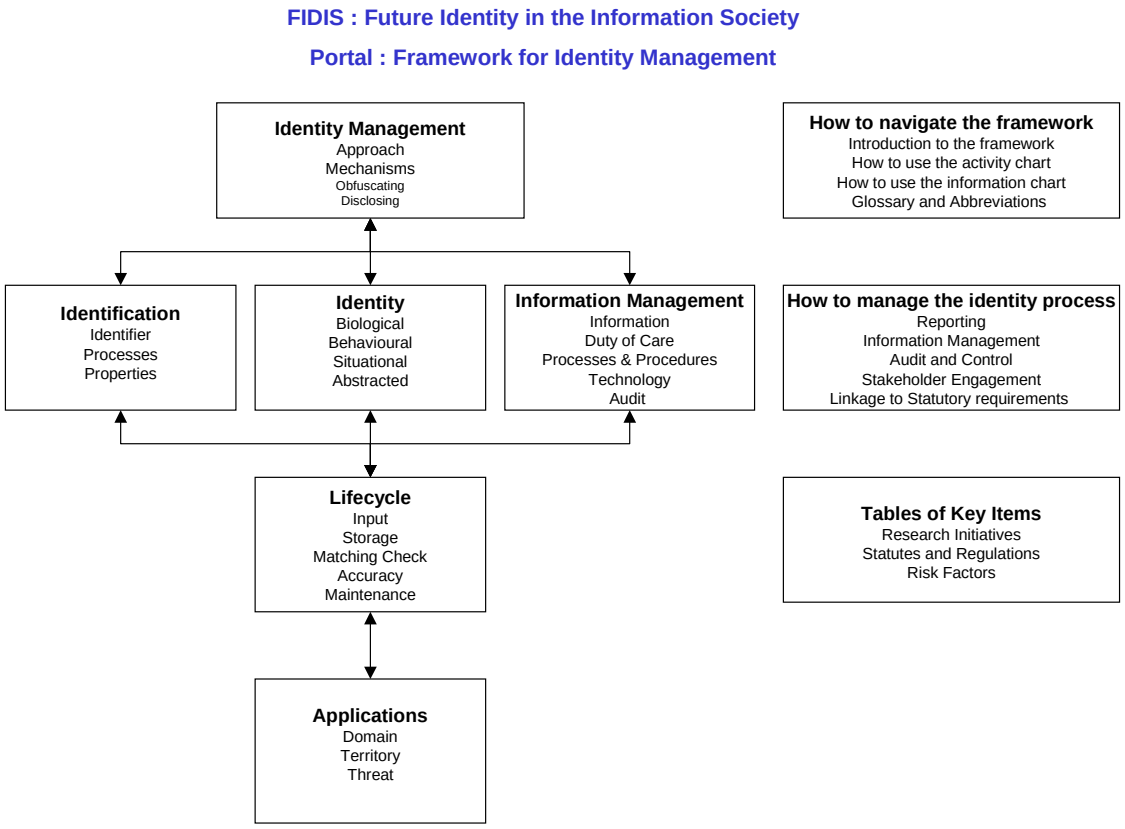
Deliverable D4.8: “Creating the method to incorporate FIDIS research for generic application” will apply in broad terms, the best practice guidelines, incorporating the proposed FIDIS method and classification system, to the FIDIS research, e-health, e-government, and e-commerce sectors. It will demonstrate how identity interoperability may be applied in those sectors. Emphasis will be on how the identity information is shared or exchanged between stakeholders.

Deliverable D4.9: “An application of the management method to an interoperability case study” will apply the method in detail to determine recommendations for best practice, relating to identity management, within the e-health sector.

7.2 4th Work Plan

Looking ahead to the 4th Work Plan, there is one further deliverable envisaged that will be used to develop this agenda:

Deliverable D4.10: "Specification of a portal for interoperability of identity management systems", will enable the practical adoption of the management method. The FIDIS portal, rooted in the constructs illustrated in the figure below, will be established to assist with the dissemination and exploitation of the FIDIS results.



8 References

BSI standards publications:

BIP 0008; "Code of practice for legal admissibility and evidential weight of information stored electronically"

PD 0010: 1997 " Principles of good practice for information management"

Dillon, Martin & Jul, Erik (1996); "Cataloging Internet Resources: The Convergence of Libraries and Internet Resources". Catologing and Classification Quarterly, 22(3/4), 197 – 238

Dittmann, Helena & Jane Hardy (2000): "Learn Library of Congress Classification"; Lanham, Maryland, the Scarecrow Press

Irwin, Susan; "Classification Theory and the Internet: A move toward Multidimensional Classification"; University of Denver; March 6, 2001

ISO/IEC WD 24760; "Information technology – Security techniques – Identity management framework"; Secretariat, ISO/IEC JTC 1/SC27, DIN, Germany; August, 2005

ISO /IEC JTC 1 /SC 27 N5530; "ISO/IEC JTC 1/SC 27 WG5 liaison statement to FIDIS on Biometrics, Identity Management and Privacy"; Secretariat, ISO/IEC JTC 1/SC27, DIN, Germany; November, 2006

ISO/IEC 17799:2005; "Code of practice for information security management"

NIST National Institute of Standards and Technology; "Information Security - An Ontology of Identity Credentials, Part 1: Background and Formulation"; Technology Administration, U.S. Department of Commerce; October 2006