FIDIS

Future of Identity in the Information Society

Title:	"D4.8: Creating the method to incorporate FIDIS research for generic application"
Author:	WP4
Editors:	James Backhouse (LSE) Bernard Dyer (LSE)
Reviewers:	Denis Royer (JWG,) Vashek Matyas (MU)
Identifier:	D4.8
Type:	[Deliverable]
Version:	3.0
Date:	April 2007
Status:	[Final]
Class:	[Public]
File:	fidis-wp4-del4.8.generic application.doc

Summary

This deliverable is concerned with the generic application of the best practice guidelines concerning interoperability, which incorporate an effective development method and framework. The guidelines presented in "D4.6: Draft best practice guidelines" have been applied, in broad terms, to four areas of interest relating to identity, namely the FIDIS research project and the sectors of e-Government, e-Health and e-Commerce.

The identity classification system, which was outlined in "D4.7: Review and classification for a FIDIS identity management model", has been applied in the report for each of the areas of interest.

It is envisaged that the proposed FIDIS interoperability framework will be suitable for performing the applications discussed in the EC reports:

- "European Interoperability Framework for Pan-European eGovernment Services"
- "Connected Health – Quality and safety for European Citizens"

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. Centre Technique de la Gendarmerie National (CTGN)	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	March 2007	Preparation and initial release (James Backhouse and Bernard Dyer)
2.0	April 2007	Continuous development. Contributions to this document: Masarykova Universita: Vashek Matyas. Contribution on the content of the script and tables. JWG: Denis Royer. Contributions on the content of the script.
3.0	April 2007	Final version incorporating comments from the reviewers.

Table of Contents

1 Executive Summary

This deliverable is concerned with the generic application of the best practice guidelines concerning interoperability, which incorporate an effective development method and framework. The guidelines presented in "D4.6: Draft best practice guidelines" have been applied, in broad terms, to four areas of interest relating to identity, namely the FIDIS research project itself and the sectors of e-Government, e-Health and e-Commerce. The identity classification system, which was outlined in "D4.7: Review and classification for a FIDIS identity management model", has been applied in the report for each of these areas of interest.

The emphasis is on the delivery of a practical approach, incorporating sound tools and techniques that may be applied in the project and within business sectors dealing with identity management. Imposing a method, that provides a framework and discipline, should assist with the development, dissemination and application of the FIDIS results.

The rationale for developing the method and framework to assist with the creation of the best practice guidelines is outlined in Chapter 2, together with the aims of the deliverable. Chapter 3 briefly restates the proposed FIDIS information management method and framework. The application of the method, to the FIDIS project, e-Government, e-Health and e-Commerce is described in Chapter 4. Chapter 5 discusses how the work will be progressed in the FIDIS 3rd and 4th Work Plans and outlines the method envisaged for disseminating and exploiting the FIDIS results.

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 of identity systems designed for one purpose being used for other purposes (e.g. inter-purpose interoperability: e-government, e-health, e-commerce systems), and sees the role of the market in generating interoperability (e.g. 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 FIDIS 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 development of a common comprehensive framework, which can be shared and applied by practitioners involved with identity management.

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

2.1 Aims of the deliverable

The aims of the deliverable are:

- To apply the proposed FIDIS generic framework, in broad terms, to four areas of interest namely the FIDIS research project and the sectors of e-Government, e-Health and e-Commerce
- To apply the proposed FIDIS classification system for each area of interest
- To demonstrate the application of the framework and models to support interoperability

3 The proposed FIDIS Information Management Method and Framework

In the FIDIS project, to meet the challenge of bringing together the many different disciplines of identity management, there is a need for recommending best practice guidelines, which incorporate a method and framework for providing effective governance and information management. To assist the reader, the method and framework are briefly re-stated below.

The method is separated into four domains, developed by the authors, as shown in Figure 1, namely the requirements domain; the business modelling domain; the information management principles domain; and the system specification domain. In FIDIS these domains cover all aspects of identity management.

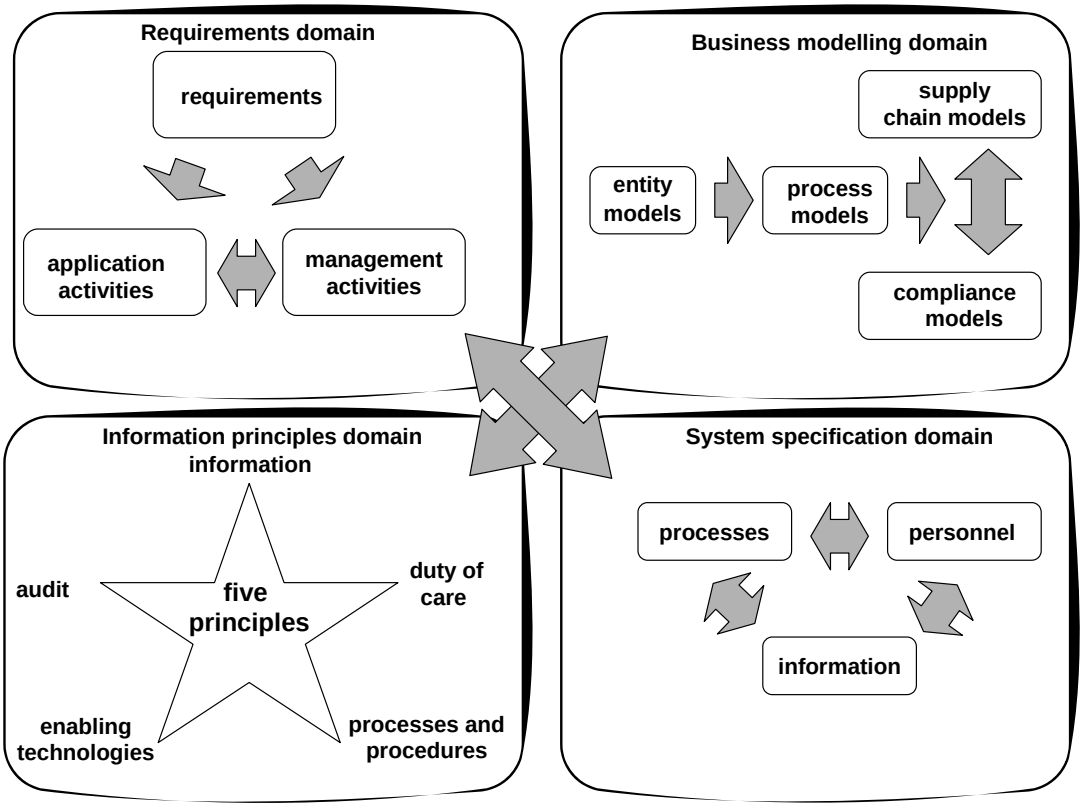

Figure 1: Domains of the Framework

3.1 Requirements domain

The requirements are divided into two main areas, those specifying the application activities and those specifying the management activities.

3.2 Business Modelling Domain

Business modelling of the activities is an essential prerequisite before information management can be implemented. Organisations should be able to analyse and anticipate the effects of processes, information flows, document management and enabling technologies, such as e-business, upon their operations.

3.2.1 Types of models

Business modelling takes many different forms and there are many techniques available. What is important is that fundamental processes should be modelled, and the way that this is done should maximise the generation of value for the institution.

3.2.1.1 Entity models

Entity models specify the relationships between such entities as people, objects, processes, and information within and between organisations. They are used to brainstorm, or when working from a fresh start, to specify and resolve business issues and to define the related corporate information.

3.2.1.2 Stakeholder models

Stakeholder models highlight the different stakeholders who are involved in the various activities of identity management throughout the supply chain. Stakeholder models may be created for particular business sectors, such as e-Government and e-Health, and they may be used as a basis for information flows within and between stakeholders.

3.2.1.3 Process and information flow models

Information flow models show the business processes, how they interact with each other and how information flows between them. They provide a functional overview of the operations and allow personnel to see the functions and processes of a business quite independently of the organizational chart.

3.2.1.4 Compliance models

A generic compliance model, (see D4.6: Section 4.2.1.4), has been developed in order to assess the degree to which institutions are fulfilling their obligations and their effectiveness in applying identity management.

3.3 Information management principles domain

The five principles[1] discussed below underpin the modelling and are intended to serve as guidelines for those involved with the design and operation of information systems, irrespective of the technology being deployed.

The principles bring together the high-level internal policy issues and the detailed operational levels of any business or organisation. They are intended to provide a framework within which managers and others can develop detailed operational procedures. Alternatively they may be used as a template to check for the completeness or adequacy of an existing set of procedures and job descriptions.

The five principles take the form of a set of statements of objectives for information management. These are intended to act as guidelines for a set of procedures that any institution should be capable of devising and operating as an extension of their current standard operating procedures, or of their quality management processes.

3.3.1 Five Principles of Information Management

The Five Principles are:

1 Recognise and understand all types of information
2 Understand the legal issues and execute "duty of care" responsibilities
3 Identify and specify business processes and procedures
4 Identify enabling technologies to support business processes and procedures
5 Monitor and audit business processes and procedures

The ordering of the principles also reflects a cascade from the high level classification of information streams to responsibilities, and then on to technology and operational considerations.

3.3.1.1 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.

[1] Mayon-White and Dyer (1997): Principles of Good Practice for Information Management, *British Standards Institution BSI PD0010*

3.3.1.2 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 industry and business activities
- Executes its responsibilities under the duty of care principle.

3.3.1.3 Processes and procedures

To ensure that the institution:

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

3.3.1.4 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

3.3.1.5 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.

3.4 System Domain

Applying all of the above domains and their components helps to create the specification and requirements of an application system, either manual or electronic, in terms of **processes, information** and **personnel.** (See D4.6: Section 4.5)

4 Application of the method

This section outlines how the proposed method and framework may be applied to interoperability within the four areas of interest namely, the FIDIS research project, e-Government, e-Health and e-Commerce.

4.1 FIDIS research project

4.1.1 Requirements domain (see D4.6: Section 4.1)

A requirements model for the FIDIS research project is shown in Figure 2.

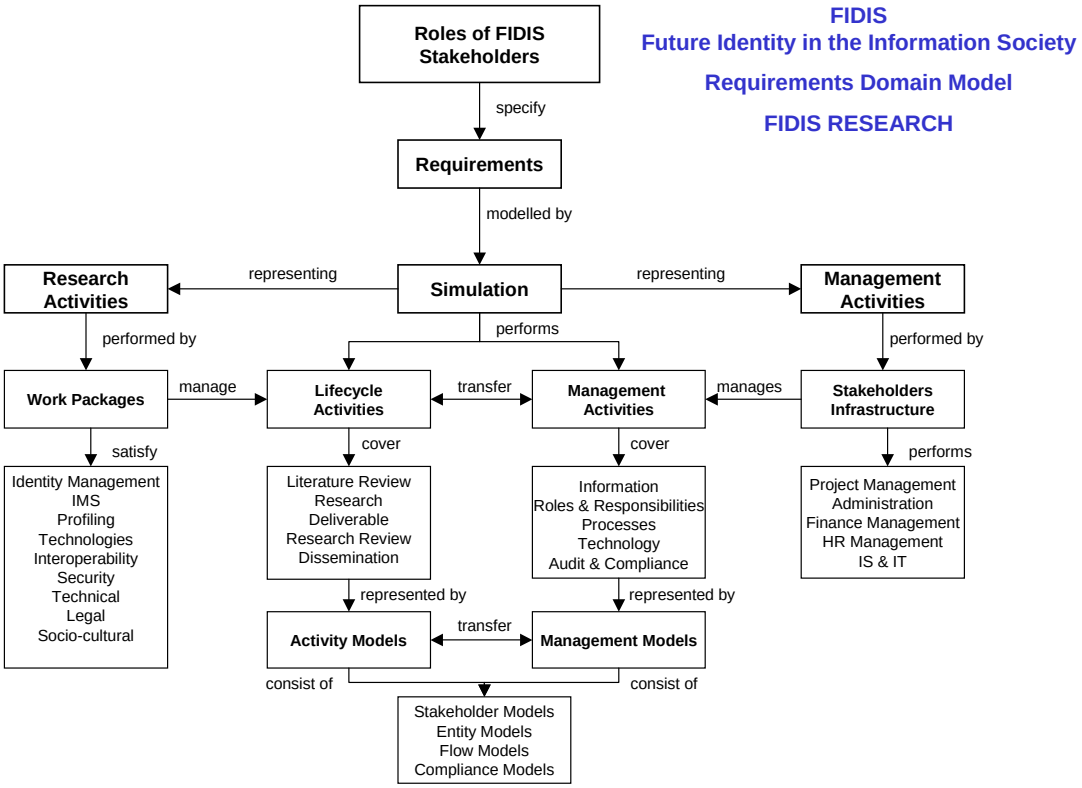

Figure 2 : FIDIS Project requirements model

Research activities

- Establish and maintain the “FIDIS Identity Wiki” to disseminate electronically the research (WP2)
- Execute research activities relating to “High-Tech Technologies” to support identity and identification (WP3)

- Develop the transversal perspective across the full spectrum of FIDIS work through "Interoperability" (WP4)
- Jointly execute the research activities relating to "Profiling"(WP7)
- Execute research activities relating to "Mobility & Identity" (WP11)
- Execute research activities relating to "Emerging Technologies" (WP12)
- Execute research activities relating to "Privacy and Privacy Technologies" (WP13)
- Jointly execute research activities relating to "Privacy" (WP14)

Management activities

- Manage the research activities through the "Internal Communication Infrastructure" (WP1)
- Manage the FCI Steering Committee
- Perform the management activity of the "Dissemination of the Research" (WP9)
- Perform the activity of the "Network Management" (WP10)
- Jointly execute the "PhD Training" in the NoE (WP15)

4.1.2 Business modelling domain

A stakeholder model for the FIDIS research project is shown in Figure 3 and represents the members of the FIDIS consortium. The information flows between them are performed by the internal communications infrastructure which is managed in WP1.

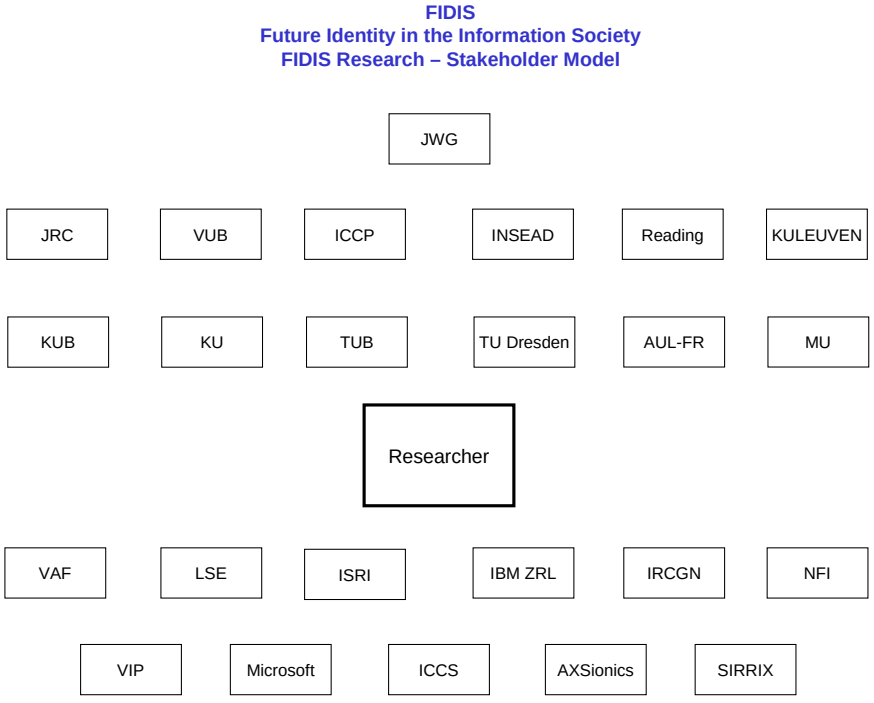

Figure 3: FIDIS Stakeholders

4.1.3 Information management principles domain

1. The principles of information management relating to the FIDIS project are shown in Tables 1 and 2

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	

Table 1

	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, teleconference system	
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 "Models for Privacy"; "Mechanisms, Methods, Tools"; "Protocols""	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	

Table 2

2. The principles of information management relating to all sectors are shown in Table 3

Personal Identifiers / Credentials used within all sectors

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 Ensure stakeholders & representatives are bona fide Protect: Credit card usage Passwords PIN numbers Comply with statutes & regulations	Purpose for use Application Lifecycle: Input Storage Access Maintenance Deletion Authorisation Confidentiality Security Interoperability	Paper Electronic Web E-mail Cards: Credit (n) Store (n) Licence (n) Membership (n) Etc RFID	Ensure all items are bona fide: Stakeholders & their representatives Documents and copies Compliance with statutes & regulations
	Signature		Yes	All stakeholders				
Location	Address (n)		Yes	All stakeholders				
	Location address (n)		Yes	All stakeholders				
	Phone Numbers (n)		Yes	All stakeholders				
	e-mail address (n)		Yes	All stakeholders				

Table 3

4.2 e-Government

It is envisaged that the proposed FIDIS interoperability framework will be suitable for performing the applications discussed in the report "European Interoperability Framework for Pan-European eGovernment Services"[2] which was published by the European Commission. The framework will be applied to D16.1: conceptual framework for Privacy-Friendly Identity Management for e-Government.

4.2.1 Requirements domain

A requirements model for e-Government is shown in Figure 4.

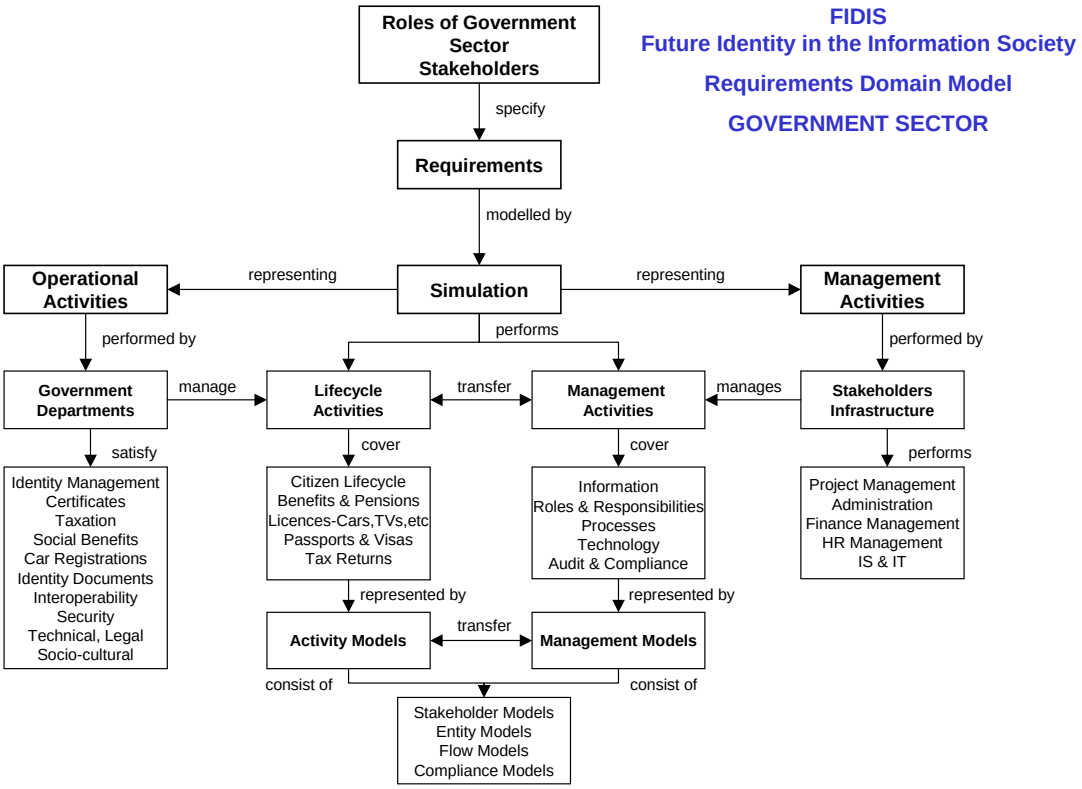

Figure 4: e-Government requirements model

Operational / application activities include:

- Manage the identity of the citizen to ensure that it is secure and strictly confidential to those who are authorised to see the information.

[2] European Interoperability Framework for Pan-European e Government Services, EC, 2004, ISBN 92-894-8389-X

- Request and receive certificates such as birth, marriage, death, residence, and nationality
- Apply for, and receive entitled unemployment benefits, family allowances, student grants and medical costs, which require identity items relating to Tax Registration, Status (married/single, dependents, disability registration, etc)
- Apply for and deliver electronic identity documents such as passports, visas, medical papers, etc
- Submit and execute tax returns which require identity items such as Insurance Number/Citizen Service Number and Tax Details
- Request and execute driving licences and car registrations (new/unused/imported), which require identity items such as Vehicle registrations, licences, insurances, roadworthiness
- Search and make reservations of library materials from public libraries
- Search for vacancies that correspond to qualifications, to obtain information about organisations and to enrol in professional training programmes
- Request building permits from their municipality, to file an appeal procedure and to make building permits decisions public

Management activities

The requirements for management activities should specify the management tools, techniques and procedures, which have to be employed to ensure that all the information, roles and responsibilities, processes and technologies are in place to manage identity activities. These should include the management of projects, finance, human and technology resources.

4.2.2 Business modelling domain

A stakeholder model for e-Government is shown in Figure 5, which might represent a "typical" structure of government. The government policies are determined by parliament and performed by the various departments and agencies. The proposed European Interoperability Framework is to "support the EU's strategy of providing user-centred eServices by facilitating the interoperability of services and systems between public administrations, as well as between administrations and the public (citizens and enterprises), at a pan-European level".

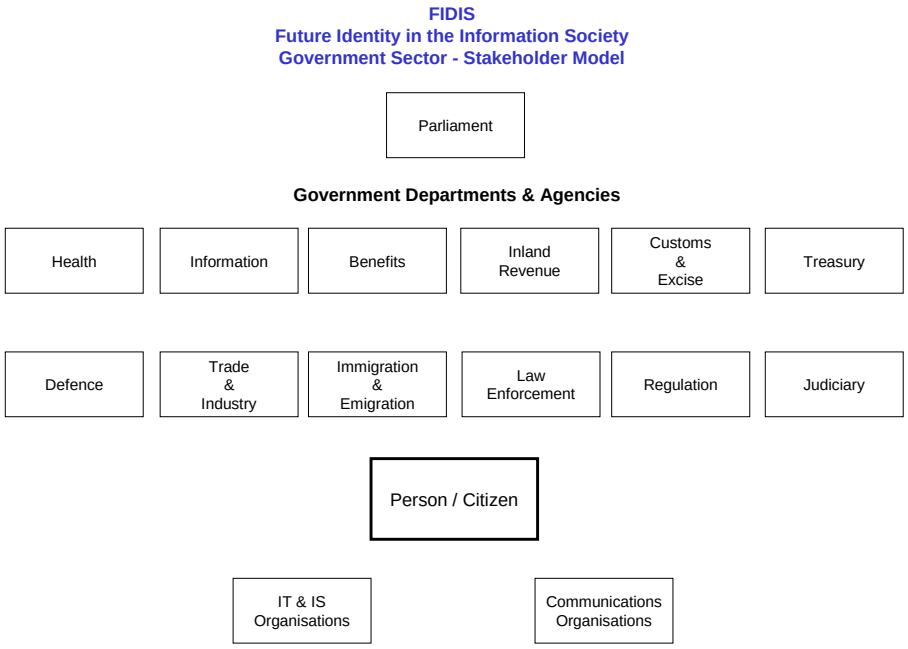

Figure 5: Typical stakeholders within Government sector

4.2.3 Information management principles for e-Government are shown below in Table 4

Identity	Principles of Information Management							
	Information				Roles & Responsibilities	Processes & Procedures	Enabling Technologies	Audit & Control
	Identifier / Credential	Importance	Held by person	Held by other stakeholders				
Status	Birth certificate		Yes	Govn't (Records)	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
	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)				
Education	School (n): certificates, diplomas, degrees		Yes	Govn't (Education)				
	University (n): degrees certificates, diplomas		Yes	Govn't (Education)				
Situational	Qualification (n)		Yes	Prof Body/Institution				
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)				

Table 4

4.3 e-Health

It is envisaged that the proposed FIDIS interoperability framework will be suitable for performing the applications discussed in the report "Connected Health – Quality and safety for European Citizens"[3] which was published by the European Commission.

4.3.1 Requirements domain

A requirements model for e-Government is shown in Figure 6.

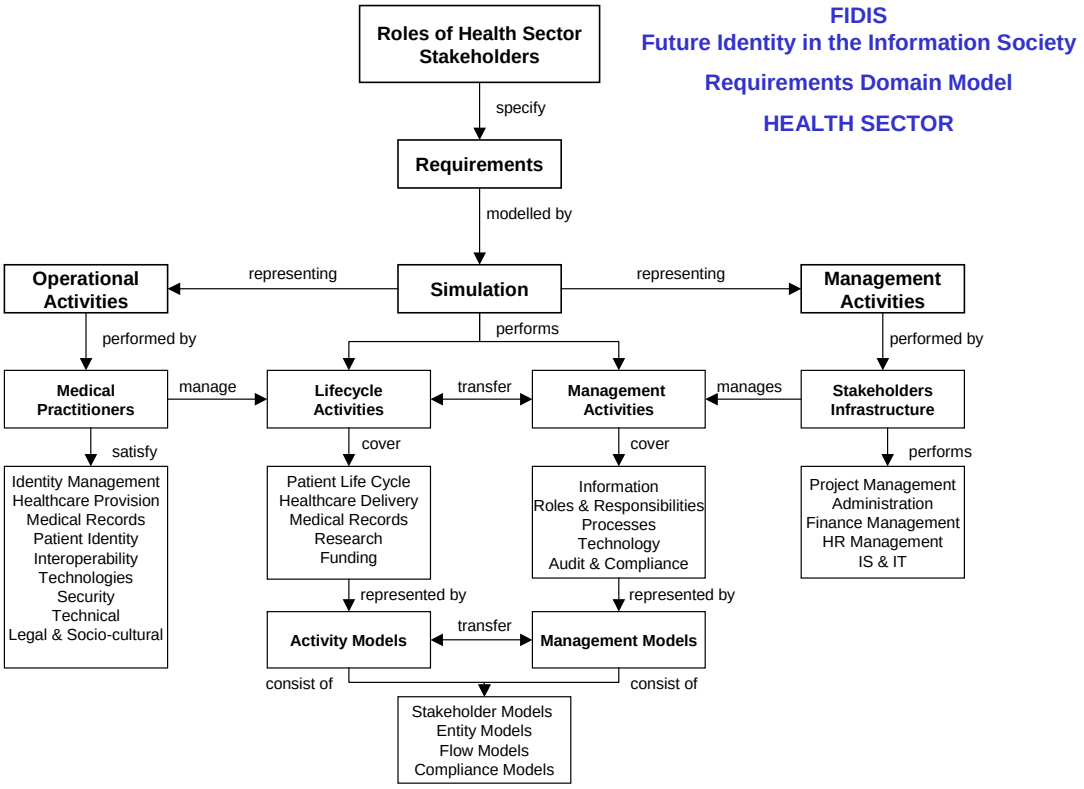

Figure 6 : e-Health requirements model

Operational / application activities include:

- Manage the identity of the patient to ensure that it is secure and strictly confidential to those who are authorised to see the information
- Provide health care to all citizens
- Manage professional medical institutions by verifying qualifications supported by certificates, diplomas, degrees, etc

[3] Connected Health – Quality and safety for European Citizens, EC, 2006, ISBN 92-79-02705

- Provide and manage medical practitioners by verifying qualifications and CVs of practitioners such as doctors, surgeons and nurses
- Supply and monitor funds
- Keep medical records up to date of doctors, patients, biological data, etc

Management activities

The requirements for management activities should specify the management tools, techniques and procedures, which have to be employed to ensure that all the information, roles and responsibilities, processes and technologies are in place to manage identity activities. These should include the management of projects, finance, human and technology resources.

4.3.2 Business modelling domain

A stakeholder model for e-Health is shown in Figure 7 which represents a "typical" structure of a national health service. The government policies are determined by parliament and performed by the various departments and agencies. The Connected Health initiative considers the "requirements of e-Health interoperability which aim to provide systems and services that are connected and can work together easily and effectively, while maintaining patient and professional confidentiality, privacy and security".

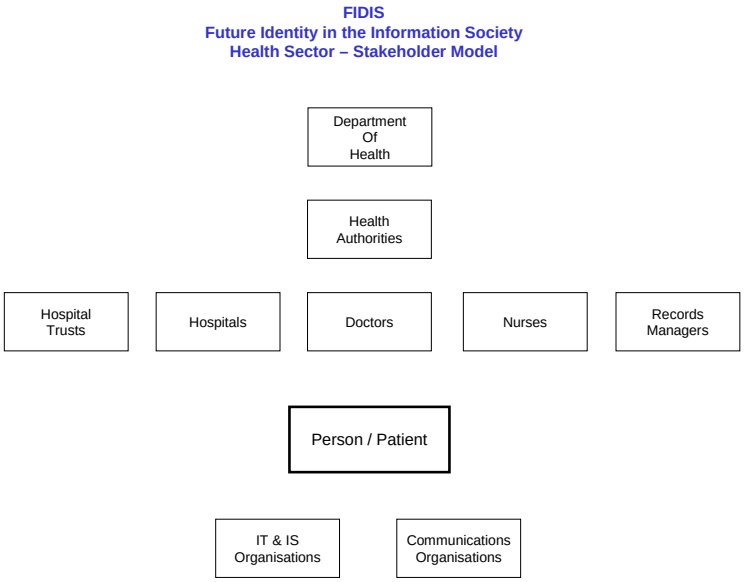

Figure 7: Typical stakeholders within health sector

4.1.3 Information management principles domain

The principles of information management relating to e-Health are shown in Tables 5

Health Sector – Identifiers / Credentials

Identity	Principles of Information Management							
	Information				Roles & Responsibilities	Processes & Procedures	Enabling Technologies	Audit & Control
	Identifier / Credential	Importance	Held by person	Held by other stakeholders				
Medical	Doctor (n)		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
	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		Yes	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)				

Table 5

4.4 e-Commerce

e-Commerce consists primarily of distributing, buying, selling, marketing and servicing products and services over electronic systems such as the internet and other computer networks. It is vital that the electronic transfer of identities and information, relating to individuals and organisations, are protected at an appropriate level.

An example of a security standard is the PCI Data Security Standard which is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including Visa, MasterCard, American Express, Discover Financial Services and JCB, to help facilitate the adoption of consistent data security measures on a global basis. The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organisations proactively protect customer identity and information.

4.4.1 Requirements domain

A requirements model for e-Commerce is shown in Figure 8.

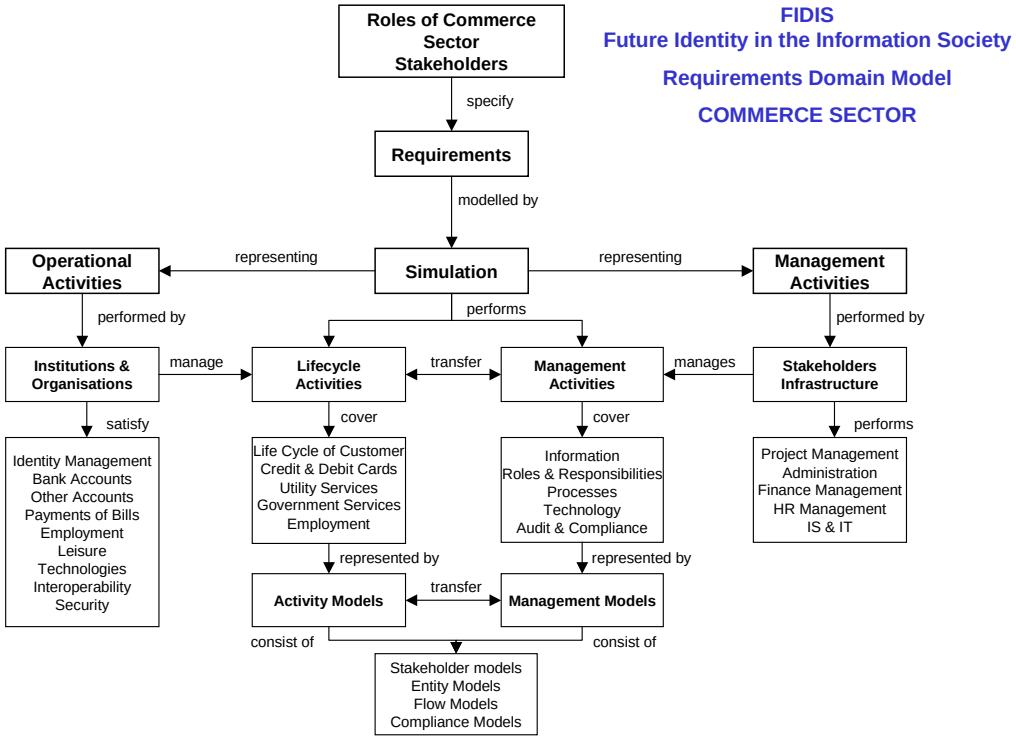

Figure 8: e-Commerce requirements model

Operational / application activities include:

- Manage the identity of the customer to ensure that it is secure and strictly confidential to those who are authorised to see the information
- Create and execute financial accounts with organisations such as banks, building societies, insurers and retailers
- Manage accounts within banks, building society and insurance companies, credit and debit cards
- Perform financial and other transactions with organisations and individuals using cheques and Internet payments of bills for services, products and taxes
- Apply for, and fulfil employment with organisations utilising application forms, CVs, qualifications, salary/pension details
- Carry out personal activities such as leisure and travel using such items as club membership cards and airline tickets

Management activities include:

The requirements for management activities should specify the management tools, techniques and procedures, which have to be employed to ensure that all the information, roles and responsibilities, processes and technologies are in place to manage identity activities. These should cover the management of project, finance, human and technology resources.

4.4.2 Business modelling domain

A stakeholder model for e-Commerce is shown in Figure 9 which represents a "typical" structure of a commercial sector. All types of information, documents, products and currencies flow, within and between organisations and customers, throughout supply chains within the commercial sector

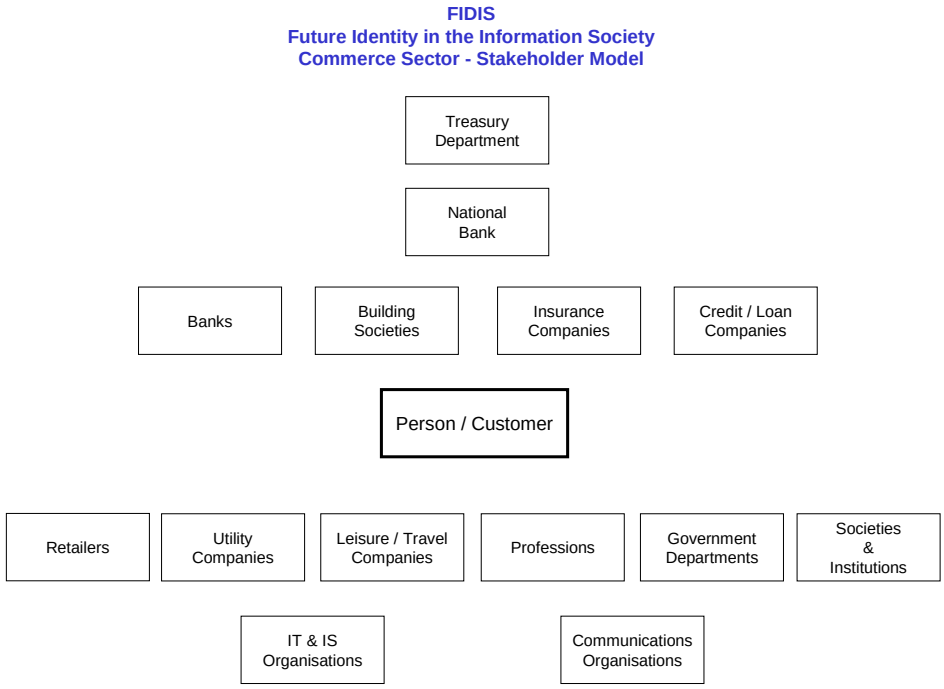

Figure 9: Typical stakeholders within commerce sector

4.4.3 Information management principles domain

The principles of information management relating to e-Commerce are shown in Table 6

Commerce Sector – Identifiers / Credentials

Identity	Principles of Information Management							
	Information				Roles & Responsibilities	Processes & Procedures	Enabling Technologies	Audit & Control
	Identifier / Credential	Importance	Held by person	Held by other stakeholders				
Banking	Bank (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
	Account (n)		Yes	Finance Institution (n)				
	Telecommunication (n)		Yes	Finance Institution (n)				
	Transaction (n)		Yes	Finance Institution (n)				
	Credit card (n)		Yes	Finance Institution (n)				
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)				

Table 6

5 Conclusion and future work

This deliverable should only be considered as the start of a continuous process for developing best practice guidelines. It is concerned with the generic application of the best practice guidelines concerning interoperability, which incorporate an effective development method and framework. The guidelines presented in "D4.6: Draft best practice guidelines" have been applied, in broad terms, to four areas of interest relating to identity, namely the FIDIS research project itself and the sectors of e-Government, e-Health and e-Commerce. The identity classification system, which was outlined in "D4.7: Review and classification for a FIDIS identity management model", has been applied in the report for each of the areas of interest.

It is envisaged that the proposed FIDIS interoperability framework will be suitable for performing the applications discussed in the EC reports:

- "European Interoperability Framework for Pan-European eGovernment Services"
- "Connected Health – Quality and safety for European Citizens"

5.1 3rd Work Plan

The next 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.

5.2 4th Work Plan

The generic best practice guidelines, which incorporate an effective development method and framework, will be applied in the following deliverables:

- ***D4.11:*** Overview of reflections and models underlying the health identity management of different types of welfare states in Europe
- ***D7.14:*** Report Where Idem meet Ipse
- ***D16.1:*** Conceptual framework for Privacy-Friendly Identity Management for e-Government

To enable the practical adoption of the management method, we are proposing for development in a further deliverable, a FIDIS portal, rooted in the constructs illustrated in Figure 10, established to assist with the dissemination and exploitation of the FIDIS results. It is envisaged that the final best practice guidelines will be established after the delivery of D4.10 "Specification of a portal for interoperability of identity management systems".

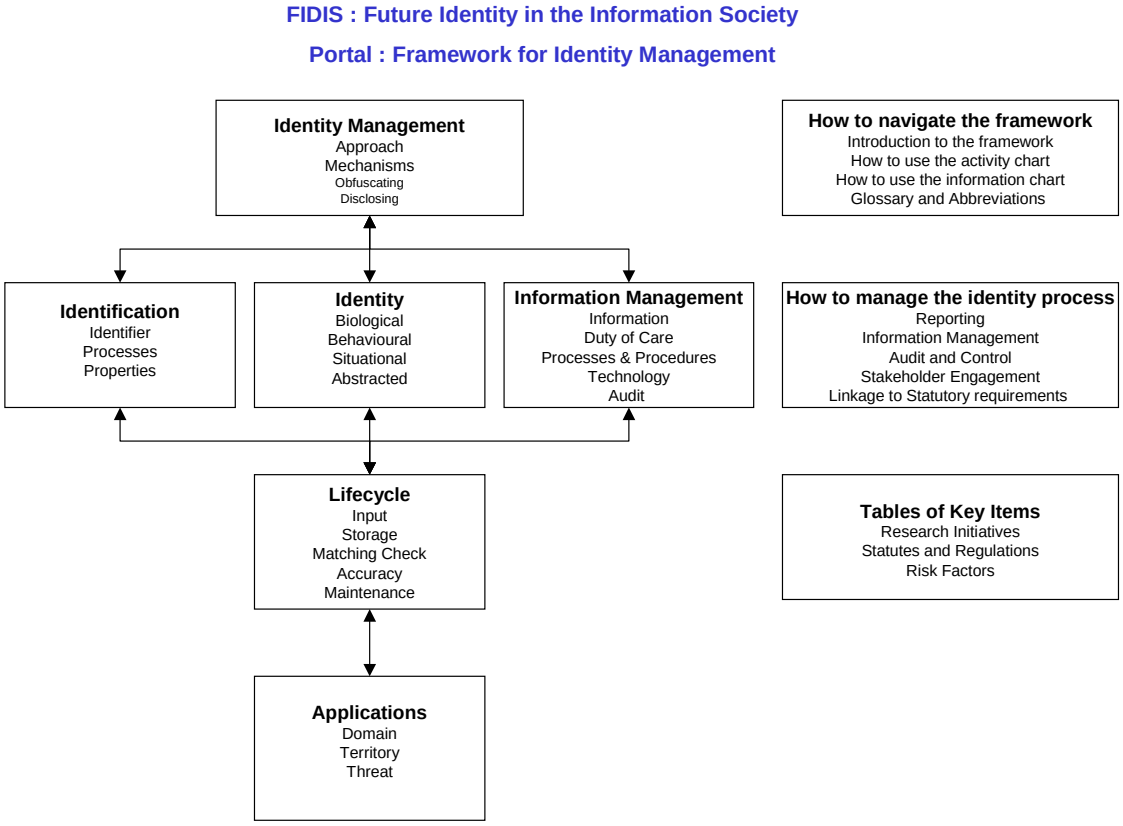

Figure 10: Structure of Portal for Interoperability