FIDIS

Future of Identity in the Information Society

Title:	"D4.10: Specification of a portal for interoperability of identity management systems"
Editors:	James Backhouse (LSE)
	Bernard Dyer (LSE)
Reviewers:	Vashek Matyas (MU)
	Thierry Nabeth (INSEAD)
Identifier:	D4.10
Type:	Deliverable
Version:	3.0
Date:	March 2008
Status:	Final
Class:	Public
File:	fidis-wp4-del_D4.10_Specification of a portal for interoperability of identity management system.doc

Summary

This deliverable sets out a high-level specification for a portal to assist practitioners responsible for information management systems within different business sectors, such as e-Health, e-Government and e-Commerce, with the aim of supporting their activities in this field, particularly relating to interoperability between stakeholders.

The portal will provide managers and developers of identity management systems with a tool to aid in their navigation through the tricky issues that identity management technologies and systems engender. It brings together a wide range of materials that have been developed in FIDIS and elsewhere, which are required to reach good decisions on interoperable identity.

The approach has been built on earlier LSE research in the area of Flood Risk Assessment which is currently being implemented by the UK government within England and Wales.

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

Copyright Notice:

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

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	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 (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieked Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
1.0	10.03.2008	Continuous developments and discussions with partners. Initial release (James Backhouse and Bernard Dyer)
2.0	26.03.2008	Comments and contributions from the reviewers Thierry Nabeth (INSEAD) and Vashek Matyas (MU). Their contributions covered the content of the script and references to earlier work. It may be ambitious at this stage to indicate that the portal, and the proposed forum, will be well received and supported by many practitioners involved with identity management.
3.0	30.03.2008	Final version incorporating comments from the reviewers and discussions with FIDIS partners.

Table of Contents

1 Executive Summary 6

2 Introduction 7
2.1 Why is a portal needed? 8

3 Structure of the portal 9
3.1 Activity Chart 9
3.1.1 Identity Management Processes 9
3.1.2 Types of Identity 11
3.1.3 Identity Technologies 11
3.1.5 Identity Applications Domains 13
3.2 Application of the Activity Chart in Practice 13
3.2.1 Step 1: Identity Management Processes 15
3.2.2 Step 2: Specify Identity Types 17
3.2.3 Step 3: Specify Identity Technologies 18
3.2.4 Step 4: Specify Identity Lifecycle 19
3.2.5 Identity Applications 19
3.3 Support guidance 20
3.3.2 Information Tables 21
3.4 Additional Support 22
3.5 Home Page 22

4 Implementation and Exploitation 24

5 Conclusions 27

Appendix 1 28

1 Executive Summary

This deliverable sets out a high-level specification for a portal to assist practitioners responsible for information management systems within different business sectors, with the aim of supporting their decision making in identity management. The portal will act as a one-stop shop, by bringing together in one place a wide range of materials that are required to reach good decisions in this field, particularly on the interoperability of identity.

It will provide context and links to identity management material that is available in the public domain and will enable the user to find guidance and tools for performing applications relating to identity. A major aim of the portal is to provide a vehicle for establishing sustainability of the FIDIS project research after its completion.

Another aim is for a portal that can bring together practitioners, involved with identity management, by creating a forum in which they can participate by sharing or exchanging their knowledge and experience.

Chapter 2 introduces the rationale and concepts underpinning the portal and outlines the reasons why the portal will be beneficial to practitioners. Chapter 3 describes the proposed structure of the portal and its content, which will consist of three major parts, namely the Activity Chart, Support Guidance and Additional Support. It also describes how the portal will be navigated by hyperlinks which connect all of the elements of the portal together. Recommendations for implementing and exploiting the portal are discussed in Chapter 4 and the conclusions are stated in Chapter 5.

2 Introduction

This deliverable D4.10 proposes a specification of a portal for supporting the interoperability of identity management systems. The proposed portal has the aim of supporting management decision-making in identity management by making accessible the work of FIDIS, and other related projects throughout the world, to practitioners working in this area. Because of the variety of different disciplines used in applying identity management, including technical, legal and social activities the portal offers to practitioners involved with IM a way of bringing together, into one place, the many contributions in this field.

The portal draws on the several research areas addressed in FIDIS Work Packages, particularly the work performed in WP4, which is documented in four deliverables[4] that can be accessed on the FIDIS website.[5] Another important foundation of the proposed portal is the FIDIS website and it endeavours to take this work forward particularly in the application of the FIDIS research by practitioners within various business sectors. It is envisaged that the portal will further add to the sustainability of the FIDIS research after the completion of the project.

The approach, for the development of the portal, built on LSE research in the area of Flood Risk Assessment[6] which is currently being implemented by the UK government within England and Wales. A similar portal structure to the one applied in flood risk assessment has been adopted for the FIDIS portal.

It will be a web-based tool that will provide access, by hyperlinks, to all parts of the portal which contain identity management material such as:

- interoperability between stakeholders within sectors such as e-Health and e-Government
- related research fields such as profiling, high tech ID, privacy, and mobility
- research and development activities within projects such as FIDIS, PRIME, and the Identity Project, which deals with biometric identity and access research
- guidance documents such as Connected Health, European Interoperability for Pan-European e-Government Services, standards, statutes, and EU Directives
- application tools used within such areas as biometrics, RFID and profiling. Many of these tools are documented in the FIDIS database on identity management systems and tools

[4] Deliverable D4.6: Draft best practice guidelines
Deliverable D4.7: Review and classification for a FIDIS identity management model
Deliverable D4.8: Creating the method to incorporate FIDIS research for generic application
Deliverable D4.9: An application of the management method to interoperability within e-Health

[5] http://www.fidis.net/publications

[6] www.defra.gov.uk/environ/fcd/research

2.1 Why is a portal needed?

There are many guidance documents and tools available worldwide relating to identity management, and more are constantly being developed within R&D projects. One of the main considerations when dealing with identity management as a practitioner is to understand the whole picture.

It is intended that the portal will:

- provide context and links to identity management material that is already available in the public domain
- define a generic approach that can be applied in all contexts to determine how best to carry out identity management applications
- enable the user to find what they are looking for in the way of guidance and tools
- identify gaps in the guidance and tools, which may be addressed, by subsequent R&D projects
- to provide a tool for establishing sustainability after completion of the FIDIS project

3 Structure of the portal

Fundamentally, the portal consists of 3 major parts, the **Activity Chart**, **Support Guidance** and **Additional Support**, as shown in Figure 1:

3.1 Activity Chart

The Activity Chart, set out on a single web page, summarises the principles of identity management and how they may be applied in practice. The Activity Chart is divided into five parts, which in turn are divided into sub-parts, or elements, as illustrated in Figure 2, and described below. All of the sub-parts have been given a unique reference number, e.g. P1, T2, L3 etc, so that these can be found and accessed easily via hyperlinks or directly from within a directory structure.

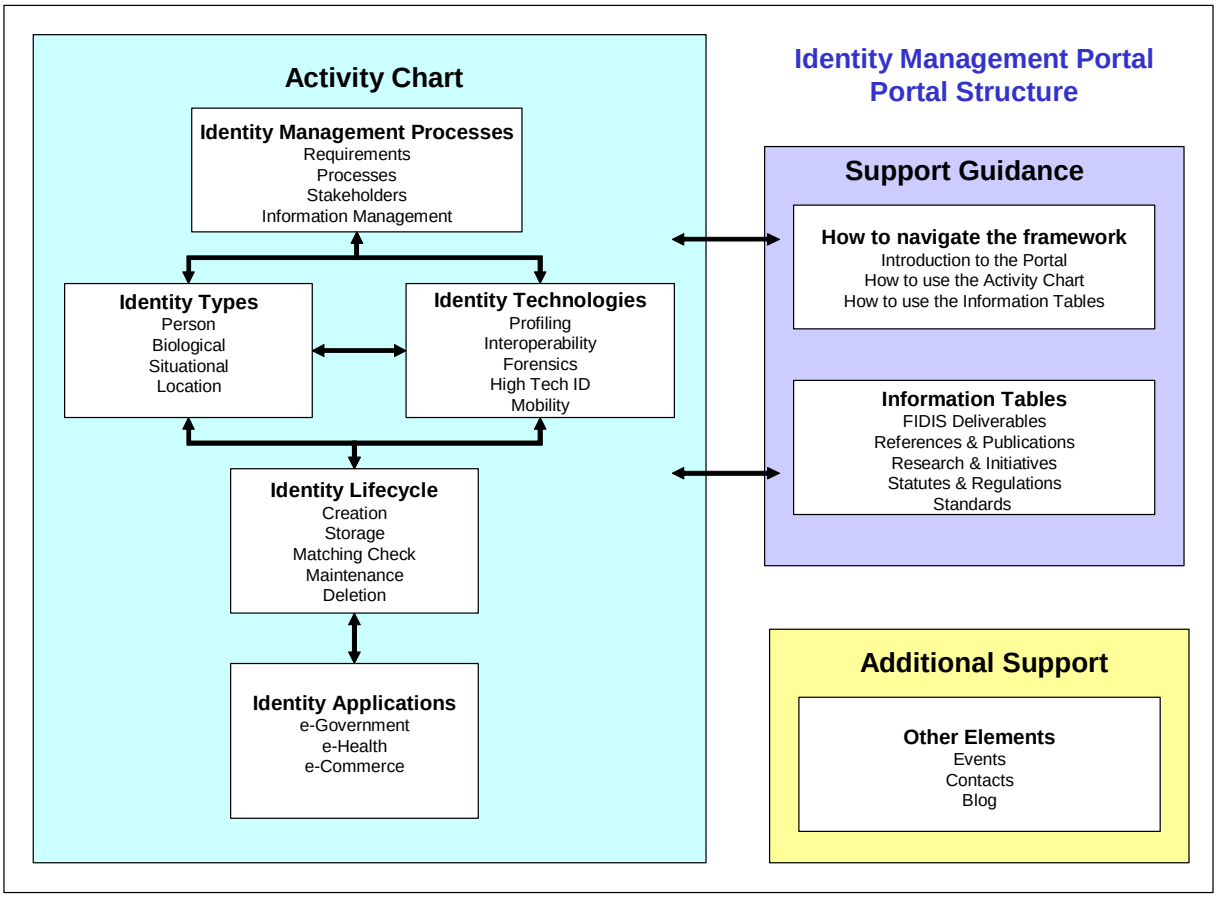

Figure 1: Portal Structure

3.1.1 Identity Management Processes

The identity management processes refer to the use of identities throughout their lifecycle in the many application areas such as e-Health, e-Government and banking systems. One

extremely important issue to be taken into account is that many of the systems share, or exchange, the same identity information so it vital that when an identity is created that it is completely accurate and cannot be changed without the approval of the responsible authority. The processes may be sub-divided into the following elements.

- **Requirements**
  The requirements should include what the scope of an application is, the number of individuals being stored on the identity database, the types of identity being used, the stakeholders involved and their roles in the system, and the processes to be applied by each of them.

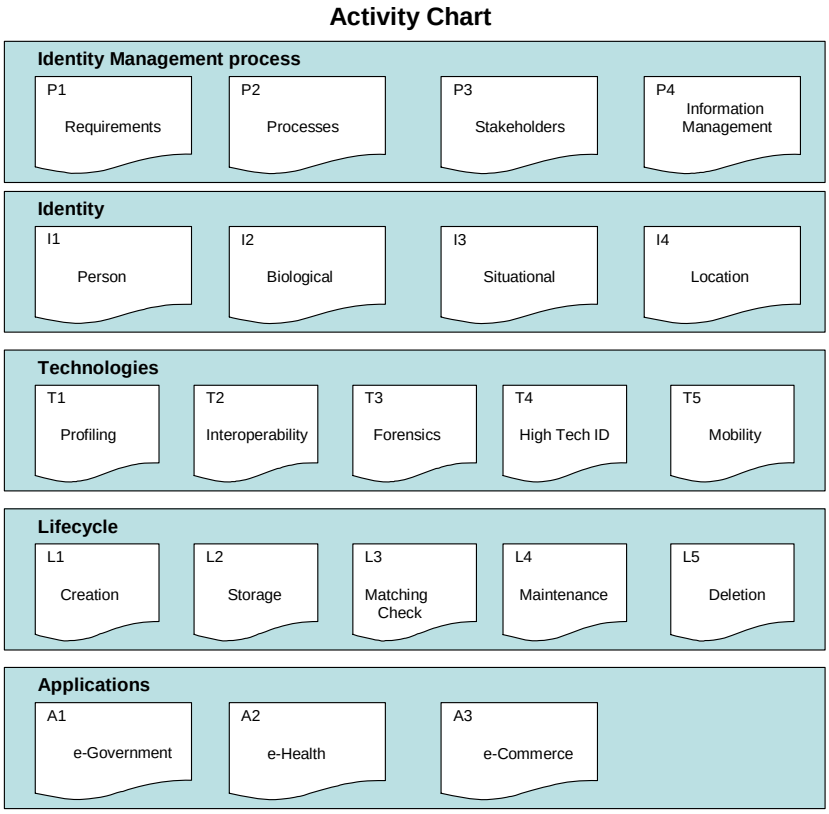

Figure 2: The elements of the Activity chart

- **Processes**
  Processes and information models should be developed to show how identities are managed within each stakeholder and how the identities are shared or exchanged with other stakeholders involved with the application system.

- **Stakeholders**
  The roles and responsibilities of each stakeholder involved with the application must be well specified in identity policy documents. Particular attention must be made to the roles and responsibilities of staff because in many instances, they are the cause of errors in systems, or illegal use of identities. Fraudsters such as money launderers and identity thieves are now infiltrating associates into financial

institutions, retail outlets and government sector organisations to perform illegal tasks on their behalf.

- **Information Management**
  In order to perform assignments in identity management it is necessary to recognise the role of effective information management. It is the skilful handling of knowledge to deliver the right information, to the right place, at the right time. Deliverable D4.6 recommended the Five Principles of Information Management namely Information Representation, Duty of Care, Processes and Procedures, Technologies and Audit for adoption for this purpose.

3.1.2 Types of Identity

The many types of identity, and their application, are documented in deliverable D4.7 and particular attention is given to the following identities:

- Personal
- Biological
- Situational
- Locational

When dealing with biological identities such as fingerprints, iris scans and face recognition methods confidence is needed in the reliability of the software and its ability to perform such tasks with the utmost accuracy.

3.1.3 Identity Technologies

Five of the FIDIS research themes cover identity technologies which are discussed below.

- **Profiling**
  Profiling is probably the only way that vast volumes of data about individual and group behaviour can be mined and analysed. This technique is being applied extensively in fighting crimes such as money laundering and terrorist financing. However, when applying profiling techniques privacy principles must be taken into account.

- **Interoperability**
  The question of interoperability in respect of identity and identity management systems is one of growing concern. The work of WP4 addresses this issue and the proposed portal attempts to assist organisations with managing interoperability within and between organisations that are cooperating with each other.

- **Forensics**
  Forensic technology is being applied to counteract ID fraud and is used to provide sufficient evidence for possible prosecutions when fraud cases have been taken to court. Forensics may also be considered as a particular form of profiling

- **High Tech ID**
  High Tech systems cover such technologies as Public-Key Infrastructures, biometrics, electronic signatures and mobile identity management. Radio Frequency Identification (RFID) systems are also being used in many application systems such as the tracking of people and assets, medical applications where patients are linked with key drugs, and supply chain automation.
- **Mobility**
  The work of FIDIS dealing with mobility and identity covers legal, technology and sociology aspects. It also investigates legal certainty and privacy protection with regard to Location Based Services (LBS).

3.1.4 Identity Lifecycle

The identity lifecycle covers the following stages:

- **Creation**
  Extreme care must be taken by public authorities when creating citizen identities, in particular that the representations in digital form, of the various types of identity, are accurate, complete, authentic and unique.
- **Storage**
  When dealing with vast amounts of data which are stored as millions of entries, it is important that adequate assurance against information risks has been developed. Databases are prone to error and if a database has errors within it, they are rapidly shared or exchanged with others multiplying the problems exponentially.
- **Matching Check**
  Real-time identification of individuals is extremely important particularly when dealing with law enforcement, border control and financial transactions from cash points. Any matching checks, say of the individual's fingerprints against those stored on a database must be extremely accurate and within well defined tolerances.
- **Maintenance**
  It is critical that all identity databases and processes are kept up to date and that all practitioners are informed of the latest versions. This is especially so when the information is used by more than one department or more than one organisation. The application of the five principles of management should assist in these tasks.
- **Deletion**
  As the active databases grow substantially, year on year, with new entries introduced to the systems, it is prudent that identities of deceased persons should be pruned from the database and transferred to archives.

3.1.5 Identity Application Domains

The research performed in WP4 has concentrated on interoperability within three areas of interest, namely e-Health, e-Government and e-Commerce. For each sector identity management requirements were specified, a stakeholder model was presented, followed by operational and application activities expressed in the form of the five principles of information management. This work was documented in deliverable D4.8.

- **e-Health**
  Identity management was studied in detail within the health sector and this was reported in deliverable D4.9. The study took into account the work of deliverable D4.11 which was concerned with the models underlying the health identity management of different types of welfare states in Europe.
- **e-Government**
  Identity management is being applied in many areas of government, including health services, vehicle registration and the supply of financial benefits. Further work is taking place within WP16 in developing a conceptual framework for e-government which will include privacy, data protection and identity management issues. The proposed framework is based on a survey throughout EU countries and one of the aims is to establish a common vocabulary for identity management. A major aspect of the work involves identity cards and the creation of national identity registers.
- **e-Commerce**
  E-Commerce consists primarily of distributing, buying, selling and marketing products over electronic systems such as the internet and other computer networks. The major part of e-commerce is concerned with performing financial transactions over banking systems. It is therefore vital that the electronic transfer of identities and information, relating to individuals and organizations, is assured to an appropriate level.

3.2 Application of the Activity Chart in Practice

The Activity Chart discussed earlier has been expanded into more detail as shown in Figures 5 and 6. Each part of the chart has been subdivided into Steps and Step 1 has been further divided into Processes. The steps are those that need to be considered when performing identity management activities.

If any of the boxes on these diagrams are selected on the digital version of the Activity Chart, a hyperlink will take the user to the appropriate part of the portal where support or guidance notes will be provide assistance to enable the user to complete a particular task. References will be made to the relevant parts of FIDIS deliverables.

Each process box has been given a unique reference, e.g. P1.1, which will enable cross-reference to a Check-list that will be provided.

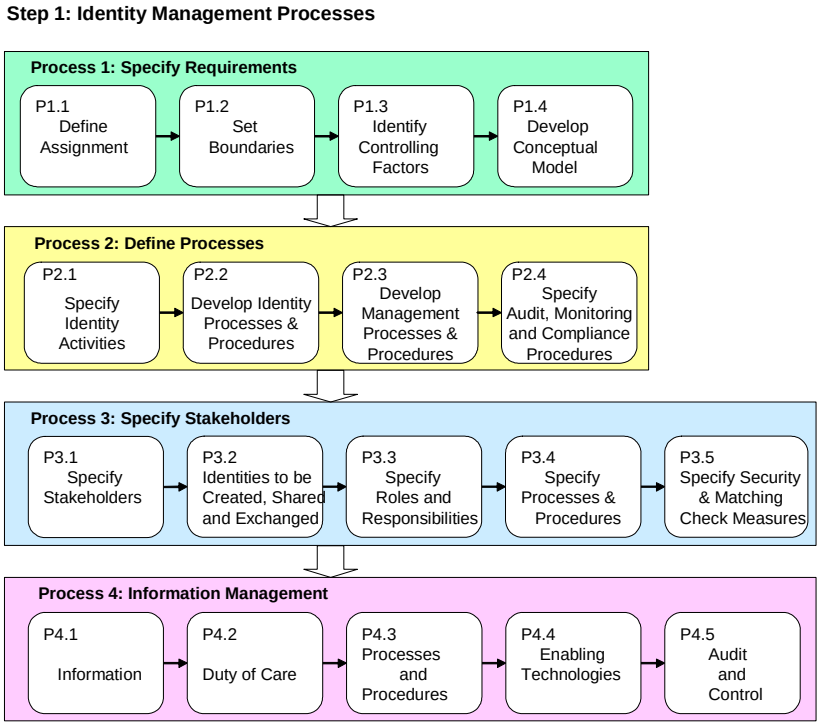

Figure 5: Step 1: Identity Management Processes

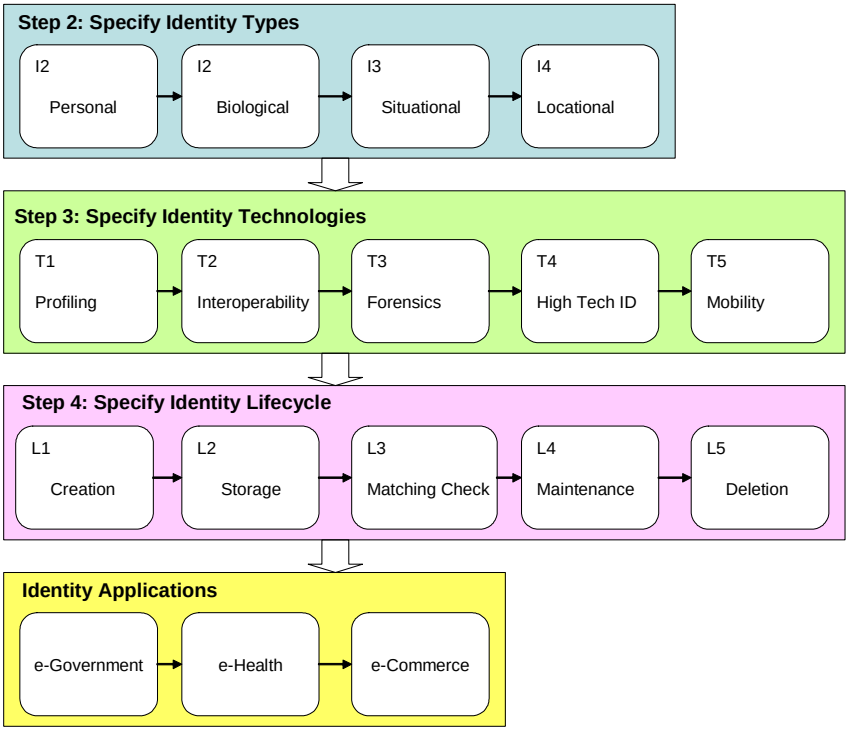

Figure 6: Steps 2 – 5

Brief descriptions of typical activities that need to be performed in each box are provided for each step in the Activity Chart. Where appropriate, examples have been taken from e-Health applications.

3.2.1 Step 1: Identity Management Processes

3.2.1.1 Process 1: Specify Requirements

P1.1: Define Assignment

- Specify e-Health or application of interest
- Specify aspects of identity that need to be included
- Describe other stakeholders involved
- Detail previous experience to be included

P1.2: Set Boundaries

- Define scope of assignment
- Define time-scale
- Determine resource requirements:
  - Personnel
  - Finance

P1.3: Identify Controlling Factors

- Check legislative requirements
- Determine financial limits
- Specify requirements of each stakeholder

P1.4: Develop Conceptual Model

- Prepare process models & information maps
- Specify security requirements
- Specify software requirements:
- Development of software with:
  - Links to internal software
  - Links to external software

3.2.1.2 Process 2: Define Processes

P2.1: Specify Identity Activities

- Patient lifecycle
- Healthcare delivery
- Medical records
- Relevant research projects

P2.2: Develop Identity Processes and Procedures

- Primary care
- Secondary care
- Tertiary care

- Interfaces between stakeholders
- Security procedures

P2.3: Develop Management Processes and Procedures

- Local governance
- Regional governance
- National governance
- EU international governance
- Within and between stakeholders

P2.4: Specify Audit, Monitoring and Compliance Procedures

- Select audit points
- Specify monitoring and auditing procedures
- Ensure compliance

3.2.1.3 Process 3: Specify Stakeholders

P3.1: Specify Stakeholders

- Health departments
- Health authorities
- Doctors' surgeries
- Hospitals

P3.2: Agree Identities to be Created, Shared or Exchanged

- Personal
- Locational
- Medical
- Biological

P3.3: Specify Roles and Responsibilities

- Ensure legal obligations
- Maintain all records
- Ensure security of information
- Perform staff training
- Manage procedures within and between stakeholders
- Ensure compliance

P3.4: Specify Processes and Procedures

- Identity procedures within & between stakeholders
- Rules, regulations, statutes & directives
- Investigation procedures
- Training procedures

P3.5: Specify Security and Matching Check Measures

- Specify security in all parts of software and manual systems

- Specify matching checks for all types of identity
- Specify tolerances

3.2.1.3 Process 4: Information Management

P4.1: Information
- Personal details
- Location details
- Next of kin details
- Medical details
- Biological details
- Stakeholder details

P4.2: Duty of Care
- Ensure legal obligations
- Maintain all records
- Ensure security of information
- Perform staff training
- Manage procedures within and between stakeholders
- Ensure compliance

P4.3: Processes and procedures
- Identity procedures within & between stakeholders
- Comply with rules, regulations, statutes & directives
- Investigation procedures
- Training procedures

P4.4: Enabling Technologies
- Profiling
- Interoperability
- Forensics
- High Tech ID
- Mobility

P4.5: Audit and Control
- Specify audit points
- Specify monitoring & auditing procedures
- Ensure compliance

3.2.2 Step 2: Specify Identity Types

I2: Personal identity
- Name
- Signature
- Insurance number
- Citizen Service Number

- Passport
- Nationality

I2: Biological Identity
- Gender
- Iris print
- Fingerprint
- DNA
- Voice

I3: Situational Identity
- Qualifications
- Profession
- Employment
- Travel

I4: Locational Identity
- Address
- Electoral Roll
- e-mail address
- Business address

3.2.3 Step 3: Specify Identity Technologies

T1: Profiling
- Vast amounts of data have to be processed
- Analysis of databases needs to be performed
- Protect privacy

T2: Interoperability
- Sharing & exchanging information
- Specify stakeholders and their roles and responsibilities
- Communication network
- Security

T3: Forensics
- Analysis of ID crimes
- Accuracy of tech devices
- Integrity of data
- Forensic profiling

T4: High Tech ID
- PKI
- Biometrics
- Electronic signatures

- RFID

T5: Mobility
- Law, technology & sociology aspects
- Mobile devices, smart phones, smart cards
- Location Based Services

3.2.4 Step 4: Specify Identity Lifecycle

L1: Creation
- Collection and correlation
- Digital representation
- Accuracy
- Completeness
- Authenticity
- Uniqueness

L2: Storage
- Devices
- Volumes
- Security
- Duplication & back-up
- Access
- Protect against copying for fraudulent activities

L3: Matching Check
- Digital Identities to be checked
- Accuracy of checks
- Verification
- Checking authority

L4: Maintenance
- Authorization of updates
- Updating all databases
- Ensuring synchronization

L5: Deletion
- Authorization of deletion
- Deletion from all databases
- Archive all deletions

3.2.5 Identity Applications

e-Government
Applications include:
- Vehicle registration

- Social benefits
- Passports

e-Health
Applications include:
- Medical records
- Medical insurance
- Healthcare provision

e-Commerce
Applications include:
- Banking services
- Online purchases
- Payment of bills

3.3 Support guidance

The **Support Guidance** and **Additional Support** are set out on a single web page and are divided into parts, which in turn are divided into sub-parts or elements, as illustrated in Figure 3, and described below. All of the sub-parts have unique references, e.g. N1, IT2, O3 etc, and all may be accessed by hyperlinks. It is envisaged that The Activity Chart will be used in conjunction with the **Support Guidance**, in particular the Information Tables, which will contain all types of knowledge that may be useful to the user when performing his/her work.

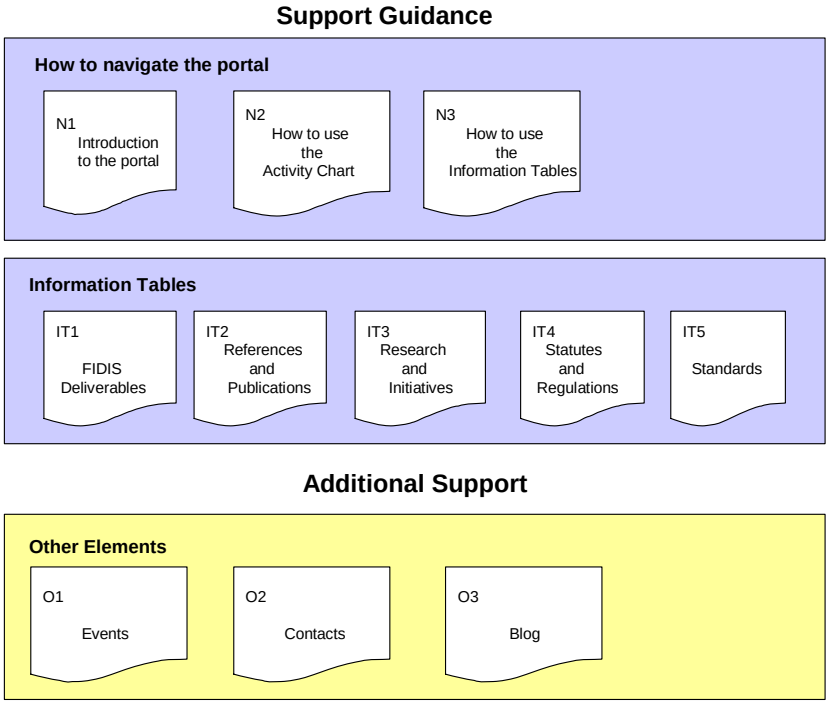

Figure 3: Support Guidance and Additional Support

3.3.1 How to navigate the portal

The portal will be set up as a framework of boxes, as shown in the figures, which when clicked on by the cursor will take the user through a series of levels, with each level providing more detail. This will enable the user to utilise hyperlinks to enlarged versions of the boxes, which in turn will provide hyperlinks to the **activity chart**, **support guidance** and **additional support**. Each box will provide text and diagrams to assist the user in applying the recommendations for the box's area of specific interest.

3.3.2 Information Tables

The purpose of the Information Tables is to provide a comprehensive list of information that may be referred to throughout IM applications.

The Information Chart is in the form of an Excel spreadsheet with 5 worksheets, documented in Appendix 1, which are specified as follows:

- Table 1: FIDIS deliverables
- Table 2: References / Publications
- Table 3: Research & Initiatives

- Table 4: Statutes, Regulations & Directives
- Table 5: Standards related to identity management

This information is in the following forms:

- **FIDIS deliverables** are listed in Table 1. They are referenced by the WP number and each deliverable has been classified in terms of the seven FIDIS Research Themes.
- **References and Publications** relating to identity which are published and documents of importance to be referred to in the guidance. If the document is available on the internet, the hyperlink to the site or the document itself will be provided.
- **Research projects and initiatives** of relevance to identity management. These will be either ongoing or recently completed. In some cases, the final documents may have been published and might also be included under References and Publications. The information provided will include completion dates and hyperlinks to websites for further information. Each project or initiative will be reviewed with respect to the FIDIS Research Themes. Therefore, it will be possible at a quick glance to determine which projects/initiatives might be of relevance to a particular user. Links to project descriptions will also be provided.
- **Statutes, regulations and directives** will list directives, statutes, acts, and regulations, etc. referred to in the guidance notes, with hyperlinks to websites for further information of the document itself.
- **Standards,** relating to identity management, will be tabled with the standard body e.g. ISO responsible for the document being stated.

3.4 Additional Support

Additional support relating to identity management will be provided by lists, and contact details of:

- **Events** such as exhibitions, conferences, seminars and workshops.
- **Contacts** for seeking further knowledge and experience. This will be a list of practitioners who are willing to share their knowledge and experience.
- **Blog or Forum** which may be used as a communication tool between practitioners. It will be organised by disciplines and business sectors.

3.5 Home Page

The home page of the portal shown in Figure 3, is the first page that is displayed on entering the website, which will have a dedicated URL. It will show the relationships between the following parts of the portal:

- **Welcome**

The welcome element will state what the intentions of the portal are and how the new entrant can gain most benefit from using it.

Background to the portal

The development of the portal will be explained, and how the work was carried out in the FIDIS project. Particular emphasis will be placed on interoperability and the work of WP4.

Other parts of the portal have been discussed earlier in this document.

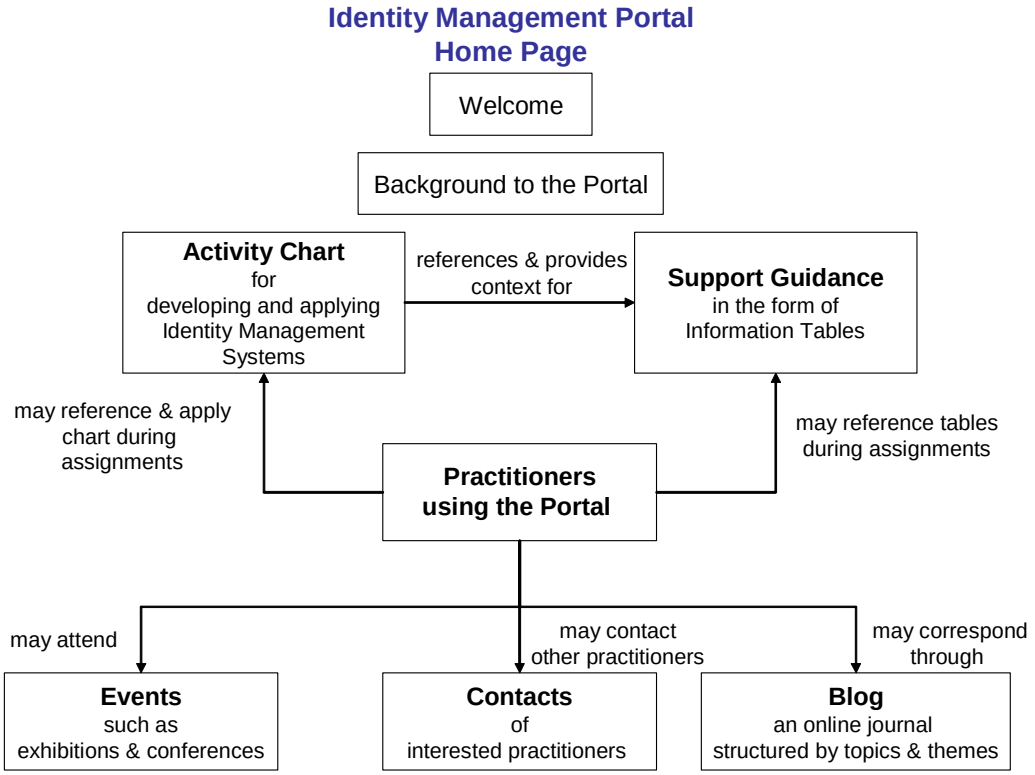

Figure 4: Home Page of the Interoperability Portal

All parts of the portal will interrelate and the point at which the user might commence navigation will depend upon their specific needs at the time. It is envisaged that the portal will be used by practitioners to assist them with their development needs by starting with the **Activity Chart** box followed by access to the **Support Guidance** box, as and when, to find various types of information they may require.

4 Implementation and Exploitation

The proposed development lifecycle for the portal website is shown in Chart 1. A major aim for implementing the portal is to provide a vehicle for establishing sustainability of the FIDIS project research after its completion. One or more partners may decide to develop the portal so that it can be exploited commercially, after the completion of the FIDIS project. If this is the case a business plan will need to be established.

Developing the Business Plan

An initial business plan should be prepared that focuses on the exploitation of the FIDIS research activities, through the application of the proposed portal, by interested FIDIS partners. The plan should be based on discussions with partners and answers from them to the following questions:

- What do partners want to do?
- Do partners want to exploit the FIDIS research commercially?
- Do partners only want to continue the research and transfer knowledge through the portal on their publications, conferences, courses, etc?
- Will partners be willing to support other organisations (either FIDIS partners or third parties) in exploiting the FIDIS results?
- How much effort in terms of personnel, equipment, finance and other resources are partners willing to commit and over what period?
- What is the "bottom line" for each partner?
- What are the issues concerning agreements on intellectual property?
- Who in the partner organisations will make the decisions?

Sales and marketing issues to be considered include:

- The need for performing a market survey on the implementation and application of an identity management portal
- How large is the European market for such a portal?
- What is the global market for such a portal?
- Financial considerations include:
    - What are the envisaged potential revenues for operating a portal commercially?
    - What fees, if any, should be charged for using the portal, possibly on an annual subscription basis?
    - Will organizations be willing to sponsor the portal?
    - What are the envisaged costs of developing and maintaining the portal over say a 5 to 10 year timeframe?

Issues relating to setting up and operating the portal include:

- Specifying the aims and objectives of operating the portal on a commercial basis
- Establishing a commercial organisation. Does any partner(s) wish to take on this role?
- Specifying technology requirements and establishing a website
- Managing the installation and exploitation strategy
- Managing the transition of the results of FIDIS to the portal

Portal Website Development Lifecycle

Phases	Guidelines	Duties	Personnel
Structure	• **Simplicity and coherency.** to allow ease of use to potentially diverse audience groups. • Complexity (given range and amount of info) should not be reflected in the structure presented (i.e., at GUI level, homepage /introductory pages) but instead by linking to **sub pages** ("behind the screen").	• Specify site map • Specify page types (templates + update requirements)	Practitioners (WP Leaders) and web designer
Content	• **Relevance and appropriateness.** A selective approach should be applied. Not "everything" should go in. • **Completeness and non-repeatability.** Content-wise, pages should be self-contained. similar info should not appear more then once • **Standardisation.** In terms of headings, language style etc.	• Review content • Proof read/ Rewrite content pages	Practitioners (WP Leaders)
Design	• **Optimal user orientation** (GUI) • **Clean, elegant look** • **Standardisation.** In terms of navigation mechanism, graphic elements, and overall style • **Enhancements in the future** ("smart" templates)	• Create a sketch for overall design (page layout, visuals, colours, fonts etc) to be approved by practitioners • Design all template pages according to spec (provided all content pages have been prepared)	Web designer
Programming	• Avoid limitations resulting from reliance on rigid ready-made templates	• Coding designed template • Upload site onto server	Programmers
QA	• Quality testing and corrections before release	• Content: spelling checks etc. • Graphic design: consistency check • Operational (technical) testing: check all links are working properly, correct URLs etc.	Practitioners (WP Leaders)
Maintenance	• Simple structure and selective approach to content should **minimize** maintenances requirements • Robust design of templates and inclusion of built-in editors should allow simple **updating** ability.		

Chart 1: Portal Website Implementation

5 Conclusions

This deliverable sets out a high-level specification for a portal to assist practitioners responsible for information management systems within different business sectors, with the aim of supporting their decision making in identity management. It brings together a wide range of materials, including FIDIS research, that are required to reach good decisions, particularly on interoperable of identity.

It provides context and links to identity management material that is available in the public domain and will enable the user to find in a one-stop shop what they are looking for in the way of guidance and tools. A major aim of the portal is to provide a tool for establishing sustainability after completion of the FIDIS project.

Another opportunity which may be achieved is that the portal may assist in the bringing together of practitioners, involved with identity management, by the creation of a forum in which they can participate by sharing, or exchanging, their knowledge and experience.

Appendix 1

Table 1: FIDIS Deliverables - Page 1

Fidis Ref	Title	Themes							General			
		T1	T2	T3	T4	T5	T6	T7	G1	G2	G3	G4
		"Identity of Identity"	Profiling	Interoperability	Forensics	Privacy & Legal-Social	High Tech ID	Mobility & ID	Workshops	Literature	Computing	Business Processes
D1.2	FIDIS Communication Infrastructure			•							•	
D1.3	Manual of the Extended Wiki System			•						•	•	
D8.3	Database on Identity Management Systems and ID Law in the EU•			•						•	•	
D8.5	Report on inter-disciplinary workshops			•					•	•		
D9.1	A Specification for a FIDIS Journal			•						•		
D3.1	Overview on IMS						•					
D3.2	A study on PKI and biometrics			•			•					
D3.3	Study on Mobile Identity Management						•	•				
D3.5	Workshop on ID-Documents						•			•		
D3.6	A study on ID documents						•			•		
D3.7	A Structured Collection on Information and Literature on Technical and Use of RFID						•			•		
D3.10	Biometrics in identity management						•					
D3.11	Report on the Maintenance of the IMS Database						•			•	•	
D12.1	Integrated workshop on Emerging AmI Technologies						•		•			
D12.2	Study on Emerging AmI Technologies						•			•		
D12.3	A Holistic Privacy Framework for RFID Applications					•	•					
D13.1	Identity and impact of privacy enhancing technologies					•	•					
D13.3	Study on ID number policies			•		•						

Table 1: FIDIS Deliverables - Page 2

FIDIS Ref	Title	Themes							General			
		T1	T2	T3	T4	T5	T6	T7	G1	G2	G3	G4
D13.6	Privacy modelling and identity			•		•						
D13.7	Workshop Privacy					•			•			
D14.1	Workshop on Privacy in Business Processes					•			•			•
D14.2	Study on Privacy in Business Processes by Identity Management					•				•		•
D11.1	Collection of Topics and Clusters of Mobility and Identity? Towards a Toxonomy							•		•		
D11.4	Workshop on Mobility and Identity							•	•			
D11.5	The legal framework for location-based services in Europe							•			•	•
D7.2	Descriptive analysis and inventory of profiling practices		•								•	
D7.3	Report on actual and possible profiling techniques in the field of AmI		•				•				•	
D7.4	Implications of profiling practices on democracy		•								•	•
D7.6	Workshop on AmI, Profiling and RFID		•				•			•		
D7.7	RFID, Profiling and AmI		•				•					
D7.8	Workshop on Ambient Law		•						•			
D7.9	A vision of Ambient Law		•									
D7.10	Multidisciplinary literature, with Wiki discussion on Profiling, AmI, Biometrics & ID		•				•			•	•	
D5.1	A survey on legislation on ID theft in the EU and ……..				•					•		
D5.2	ID Fraud Workshop				•				•			
D5.2b	ID-related Crime: Towards a common ground for interdisciplinary research			•	•							
D5.2c	Identity related crime in the world of films				•							
D5.3	A mutidisciplinary article on identity-related crime			•	•							
D5.4	Anonymity in electronic government: case-study analysis of governmnets' ID knowledge				•						•	•
D6.1	Forensic implications of Identity Management Systems				•						•	
D6.5	Second thematic workshop on forensic implications				•				•			
D6.6	Second thematic workshop on profiling		•						•			
D6.6b	Workshop on forensic profiling		•		•				•			

Table 1: FIDIS Deliverables - Page 3

FIDIS Ref	Title	Themes							General			
		T1	T2	T3	T4	T5	T6	T7	G1	G2	G3	G4
D2.1	Inventory of topics and clusters	•								•		
D2.2	Set of user cases and scenarios	•								•		
D2.3	Models	•										
D2.6	Identity in a networked world - user cases and scenarios	•								•		
D4.1	Structured account of approaches on interoperability			•								
D4.2	Set of requirements for interoperability of identity Management Systems			•								
D4.4	Survey on Citizen's trust in ID systems and authorities			•						•		
D4.5	Survey on Citizen's trust in ID systems and authorities			•						•		
D4.6	Draft best practice guidelines			•							•	•
D4.7	Review and classification for a FIDIS identity management model			•							•	•
D4.8	Creating the method to incorporate FIDIS research for generic application			•							•	•
D4.9	An application of the management method to interoperability within e-Health			•							•	•

Table 2: References / Publications (Examples)

Ref	Title	Authors	Themes							Reference / Web address
			"Identity of Identity"	Profiling	Interoperability	Forensics	Privacy & Legal-Social	High Tech ID	Mobility & ID	
P1	Identity as an Emerging Field of Study	Ruth Halperin			•		•	•		Datenschutz und Datensicherheit (DuD) 9/2006
P2	Identity of Identity	Thierry Nabeth	•				•			Datenschutz und Datensicherheit (DuD) 9/2006
P3	Interoperability of Identity and Identity Management Systems	James Backhouse			•		•			Datenschutz und Datensicherheit (DuD) 9/2006
P4	Three Tiers of Identity	Andre Durand					•	•		Digital identity World, March 16, 2002
P5	Connected Helath - Quality and safety for European Citizens	EC 2006			•		•		•	ISBN 92-79-02705
P6	European Interoperability for Pan-European e-Government Services	EC 2004			•		•	•		ISBN 92-894-8389-X
P7	The Ernst & Young Global Information Security Survey 2004	Ernst & Young					•	•		Ernst & Young, September 2004
P8	Communities of Practice: Learning, Meaning and Identity	Wenger Etienne	•							Cambridge University Press, Dec 1999
P9	The Identity Cards Bill: Bill 9 0f 2005-2006	UK House of Commons					•	•	•	Research Paper 05/43
P10	The challenge to individualism	A. Vedder	•				•			Ethics and information Technology 1 pp. 275-281,1999

Table 3: Research & Initiatives (Examples)

Ref	Title	Institution / Sponsor	Reference / Web address / Contact
R1	FIDIS – Future of Identity in the Information Society	European Commission	http://fidis.net
R2	PRIME – Privacy and identity Management for Europe	European Commission	https://www.prime-project.eu/
R3	Personal Identification and Identity Management in New Modes of E-Government	Oxford Internet Institute, University of Oxford	http://www.oii.ox.ac.uk Miriam.Lips@oii.ox.ac.uk
R4	The Identity Project	JISC: Cardiff University, LSE, Birkbeck, Imperial, Goldsmiths, Queen Mary and Royal Holloway Colleges	http://jisc.ac.uk
R5	Digital Footprints: Online Identity Management and Search in the Age of Transparency	Pew Research Center	http://pewresearch.org
R6	Identity Management and Privacy	HP Labs	http://www.hpl.hp.com
R7	Biometric Identity and Access Research Project	California State University	http://www.findbiometrics.com
R8	Identity in the Cyberspace	The University of Melbourne	http://www.dis.unimelb.edu.au
R9	Safeguarding Digital Identity	MITRE Corporation, University of Illinois, SRI International, Cornell University, Georgia Tech	http://www.thei3p.org

Table 4: Statutes, Regulations & Directives (Examples)

Ref	S/T/D	Title	Jurisdiction	Date	Reference
S1	Directive	Protection of individuals with regard to the processing of personal data	EU	1995	Directive 95/46/EC October 24, 1995
S2	Directive	Privacy and Electronic Communications	EU	2002	Directive 2002/58/EC July 12, 2002
S3	Statute	Data Protection Act	EU	1998	
S4	Statute	Human Rights Act	UK	1998	
S5	Statute	Public Records Act	UK	1958	
S6	Statute	Electronic Communications Act	UK	2000	ISBN 0 10 540700 3
S7	Directive	Third Money Laundering Directive	EU	2005	Directive 2005/60/EC, 2005

Table 5: Standards (Examples)

Ref	Title	Reference	Standard Body
ST1	A framework for Identity Management	ISO/IEC 24760	ISO/IEC
ST2	Privacy Framework	ISO/IEC NP 29100	ISO/IEC
ST3	Biometric template protection	IISO/IEC WD 2475	ISO/IEC
ST4	Information Security – An Ontology of Identity Credentials	NIST	NIST
ST5	Information technology – Code of practice for information security management	BS ISO/IEC 17799:2000	BSI ISO/IEC
ST6	Information and documentation – Records management - General	BS ISO 15489-1:2001	BSI ISO
ST7	Principles of good practice for information management	PD 0010: 1997,	BSI
ST8	Authentication context for biometrics	ISO/IEC CD 24761	ISO/IEC
ST9	Identity Web Services Framework		Liberty Alliance