FIDIS

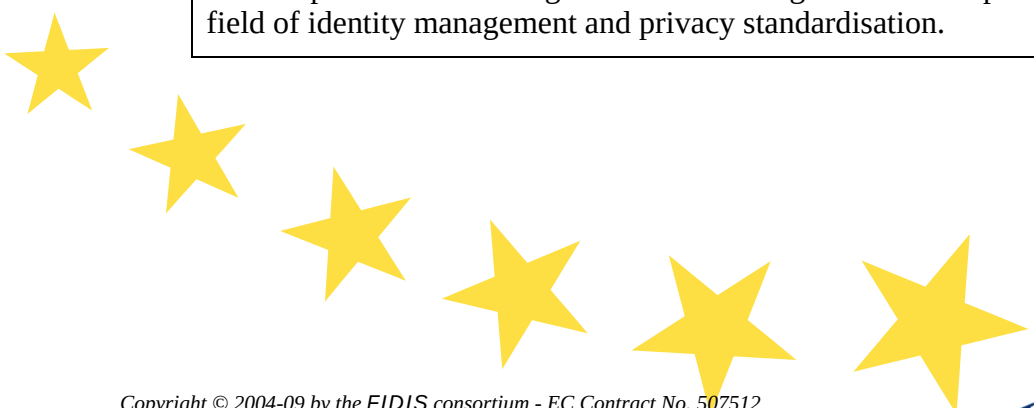
Future of Identity in the Information Society

Title:	"D19.3 Standardisation report"
Author:	WP19
Editors:	Hans Hedbom (KU), Brendan Van Alsenoy (KUL)
Reviewers:	Martin Meints (ICPP), Stefan Köpsell (TUD)
Identifier:	D19.3
Type:	[Report]
Version:	1.0
Date:	Monday, 20 April 2009
Status:	[Final]
Class:	[Public]
File:	D19.3_fidis_standardisation_report.wp19.v1.0.doc

Summary

As part of its dissemination activities FIDIS partners have participated in ongoing standardisation work. This report presents the work conducted within the FIDIS standardisation group from September 2007 to March 2009. It also describes the motivation for FIDIS involvement in standardisation and gives an overview of the IdM and privacy standardisation landscape for information systems. An overview of standards commented by FIDIS is given and as an appendix the comments made are presented.

Through this effort FIDIS has been able to spread its ideas and results in the standardisation area. The participation of FIDIS has been well accepted and also helped in establishing FIDIS as a recognised and respected actor in the field of identity management and privacy standardisation.



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 (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 Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	26.01.2009	• Initial release (Hans Hedbom, KU)
0.2	27.01.2009	• Added parts of section 3 and 5 (Hans Hedbom, KU)
0.3	28.01.2009	• Text from Jan added in 3.2 and incorporated suggested editorial changes (Hans Hedbom, KU)
0.4	16.02.2009	• Text on 24760 from Brendan van Alsenoy (KULeuven) and Hans Hedbom (KU) added to section 4. New text on 29115 added in section 4. • Chapter 5 expanded with introduction and the work process. • Added text from Kai on workshop. (Hans Hedbom, KU)
0.5	25.02.2009	• Comments from Brendan van Alsenoy (KULeuven) added and new text on Executive summary inserted (Hans Hedbom, KU)
0.6	03.03.2009	• Review comments from Martin Meints (TUD) addressed (Hans Hedbom, KU)
0.7	15.04.2009	• Document Partly updated to reflect the latest efforts for FIDIS Standardisation (Hans Hedbom, KU)
1.0	15.04.2009	• Document fully updated and finalized (Brendan Van Alsenoy, KUL and Hans Hedbom, KU)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Executive Summary)	Hans Hedbom (KU)
2 (Introduction)	Hans Hedbom (KU)
3 (The landscape of IdM and privacy standardisation)	Kai Rannenberg (GUF), Jan Schallaboeck (ICPP), Hans Hedbom (KU)
4 (Commented Standards)	Brendan Van Alsenoy (KUL), Hans Hedbom(KU)
5 (Other FIDIS activities within the Standardisation area.)	Hans Hedbom(KU), Kai Rannenberg(GUF)
6 (Conclusion and Outlook)	Hans Hedbom(KU)

Table of Contents

1 Executive Summary

As part of its dissemination activities FIDIS partners have participated in ongoing standardisation work. This report presents the work conducted within the FIDIS standardisation group from September 2007 to March 2009. ISO/IEC JTC1/SC27/WG5 was chosen as the most appropriate forum because of its global reach through ISO and its focus on identity management, privacy and biometry standards in the ICT area. As a result of this choice a liaison was established between FIDIS and ISO/IEC JTC1/SC27/WG5 in 2007. After the establishment of the liaison FIDIS has actively taken part in the standardisation work of WG5 by providing comments and input to the different standards elaborated in WG5. FIDIS has also actively participated in the discussions and presented our standpoints at the international meetings of WG5 held in Luzern, Berlin, Kyoto and Cyprus during the period and we will also attend the meeting in Beijing China in May 2009 (See appendix A. for details).

Through this effort FIDIS has been able to spread its ideas and results to the standardisation area. The participation of FIDIS has been well accepted by the members of WG5 and also helped in establishing FIDIS as a recognised and respected actor in the field of identity management and privacy standardisation.

2 Introduction

Standards are an important channel for achieving consensus and greater understanding of concepts and methods within industry, governmental bodies and other organisation. Realising this, FIDIS took the initiative to form a liaison with ISO/IEC JTC1/SC27/WG5[4]. FIDIS was given the status of a category_c liaison partner with WG5 in 2007 (at their spring meeting in Moscow). The reason why we chose to work with ISO/IEC JTC1/SC27/WG5 over any of the other organisations conducting standardisation was due to its global reach and its broadly applicable collection of standardisation efforts in the area of identity. Having limited resources, we also wished to concentrate on one area where we believed we could contribute the most and make the highest possible impact. This report presents the standardisation work conducted within FIDIS from September 2007 to March 2009.

Since the establishment of the liaison with WG5, FIDIS has made a significant number of comments and contributions to the different standards being developed within WG5. The FIDIS liaison also attended both the spring and autumn meetings of ISO/IEC JTC1/SC27 to motivate and defend these comments. At the same time we have had an opportunity to actively participate in the discussions and debates that accompany the different standards and thereby making FIDIS more visible and known within the standardisation community.

This report presents the work that has been done within the FIDIS standardisation group. It starts with a short overview of the landscape of standardisation activities in the identity management (IdM) and privacy area, though focusing mainly on ISO/IEC JTC1/SC27/WG5 (chapter 3). We then elaborate in more detail upon the different ongoing standardisation efforts for which we have provided comments (chapter 4). In chapter 5 we will describe the other activities (besides commenting) that have been conducted in the FIDIS standardisation group. This section also contains a short description on how the group has worked internally. Finally, the results of the efforts are summarized in the conclusions and outlook chapter.

Appended to the report are the liaison statements and full comment lists sent in to ISO/IEC JTC1/SC27/WG5 by FIDIS.

4 http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306

3 The landscape of IdM and privacy standardisation

3.1 ISO

The ISO/IEC standardisation system aims at developing globally accepted standards, by having National Bodies[5] (NBs) participate in Committees, Subcommittees and Working Groups, where the technical editing work is done. Consensus is built through a sequence of draft standard proposals, which are consecutively modified based on expert and NB comments and votes. The process is designed in such a way that NBs can discuss the drafts "at home", and return with their comments and votes. This is to enable global participation. Therefore the turnaround time between drafts is between 2 and 6 months, in the later stages getting more formal and with longer intervals.

A prospective new International Standard (IS) starts off as a New Work Item Proposal (NWIP) in either a Committee or Subcommittee. A majority of National Bodies must be found as supporters to start the (NWIP), together with a critical mass of experts actively pursuing the project. First rounds of editing are performed on a document in Working Draft (WD) status in the respective Working Group (by incorporating expert and NB comments). The next status level is Committee Draft (CD), on which only NBs and liaison organisations will be able to comment. After a vote on the Final CD (FCD), a last voting round takes place concerning the FDIS (Final Draft International Standard). If consensus is found at this stage, only editorial changes may be made before publication of the standard.

To enable cooperation with other bodies, e.g. FIDIS, the ISO/IEC system has introduced the concept of liaisons. Liaison organisations can comment at all stages, but they are not eligible to vote. They can however be quite influential, if they show competence in technical commenting and demonstrate relevant expertise in the area of the prospective standard.

Standardisation initiatives regarding security and privacy in information systems are handled by ISO/IEC JTC1 standard committee 27 (SC27). Within SC27, Working Group 5 (WG5) is responsible for the questions concerning identity management, privacy and biometrics. Most of the standards developed within WG5 are still in WD status or as NWIP, seeing as the working group has only known a relatively short existence.

The following standards currently under development within WG5 relate to privacy and IdM:

IdM Framework (24760): This standard aims to provide a framework for the definition of identity and the secure, reliable, and privacy friendly management of identity information. This framework shall apply to individuals as well as organisations of all types and sizes, in any environment and regardless of the nature of the activities they are involved in. This project is in the "Working Draft" stage.

A Framework for Access Management (29146): This standard aims to provide a framework for the definition of Access Management and the secure management of the process of accessing information. This framework is applicable to any kind of users, individuals as well as organisations of all types and sizes, and should be useful to organisations at any location

[5] The NBs are the ISO member organisations. Each country has one NB.

and regardless of the nature of the activities they are involved in. This project has just entered the “Working Draft” stage.

Entity authentication assurance (29115): This project aims at describing the guidelines or principles that must be considered in entity authentication, assurance and the rationale for why it is important to an authentication decision, especially: a framework for assessing "how close" an entity’s identity is to the one that is asserted, and this throughout an identity's life cycle. This project is in the "Working Draft" stage.

A Privacy Framework (29100): This Project aims at providing a framework for defining privacy safeguarding requirements as they relate to PII (Personally Identifiable Information) processed by any information and communication system in any jurisdiction. The framework is to be applicable on an international level and addresses system specific issues on a high-level. It is general in nature and puts organisational, technical, procedural and regulatory aspects in perspective. This project is in the "Committee Draft" stage.

A Privacy Reference Architecture (29101): This project aims at providing a privacy reference architecture model that describes best practices for a consistent, technical implementation of privacy safeguarding requirements as they relate to the processing of personally identifiable information in information and communication systems. This project is in the "Working Draft" stage.

Several of these standards are further described an analysed in section 4.

It should also be mentioned that WG 5 has decided to put forward two new Work Item proposals: One on “Privacy Capability Maturity Models” and one on ”Requirements on relative anonymity with identity escrow - model for authentication and authorization using group signatures".

3.2 ITU-T

ITU-T[6] is the standardisation branch of the International Telecommunications Union, one of the specialised agencies of the United Nations. It is structured as an intergovernmental private-public partnership organisation, comprising of 191 member states and more than 700 private or public sector companies. ITU-T's headquarters is in Geneva, Switzerland. Standards by ITU-T (called "Recommendations") are aimed at defining elements in information and communication technology (ICT) infrastructure. The standards only become mandatory in the event they are adopted as part of a national law. However, due to its affiliation with ITU, the United Nations and its broad membership base, ITU-T recommendations carry significant weight in practice.

ITU-T held a Focus Group on Identity Management during 2007[7], which resulted in a number of reports[8]. Of particular interest was the draft on Requirements for Identity Management Systems, which was intensively commented by FIDIS through their liaison with ISO/IEC JTC 1/SC 27/WG 5. Many of these comments are included in the Annex.

[6] http://www.itu.int/ITU-T/
[7] http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html
[8] Available at: http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

In October 2008 an ITU-T initiative proposed to evaluate the relevance of the Liberty Alliance Identity Assurance Framework (IAF) Specification for ITU-T X.eaa, a common text Standard Recommendation between ISO/IEC/JTC 1/SC27/WG5 (29115) and ITU-T SG 17, Question 6 (x.eaa), with a special focus on possible aspects of possible harmonisation of the aforementioned standards.

ITU-T for this purpose initiated a correspondence group (cg-eaa, E-mail-List at: http://www.itu.int/ml/lists/info/cg-eaa), with the following tasks outlined by the TOR:

1. Analyze and reformat the Liberty Alliance IAF into an ITU-T formatted Recommendation
2. Identify key differences between X.eaa and the IAF Specification and a possible new Draft ITU-T Recommendation.
3. Create harmonized scope statements for the x.eaa Draft Recommendation and the proposed New Draft Recommendation
4. Determine any potential impact on the ITU-T|ISO/IEC/JTC 1/SC27 joint work on entity authentication assurance.

An intensive discussion on the scope and the other aspects outlined above followed, with the final results still pending.

3.3 Other standardisation organisations of interest

3.3.1 Liberty Alliance

Liberty Alliance[9] is a consortium that was started in 2001 with the main focus to "establish open standards, guidelines and best practices for identity management." According to their own figures the consortium today encompasses more than 150 organisations globally. Their efforts within the standardisation arena are mainly centred around identity federation, authentication assurance and identity based web services. The standards ('open specifications') so far include the Liberty Aliance_FF (Federation Framwork)[1], the Liberty Aliance_WSF (Web Services Framwork)[2], the Liberty Alliance_IAF (Identity Assurance Framwork) [3] and the Liberty Alliance_IGF (Identity Governance Framework) [4]. They also produce best practice guides and whitepapers relating to identity and privacy.

3.3.2 Oasis

Oasis[10] (Organization for the Advancement of Structured Information Standards) originally started as SGML Open in 1993 and is a standardisation organisation that "drives the development, convergence and adoption of open standards for the global information society". The standardisation efforts in the field of identity and privacy are mainly focused on identification, authentication and federation services in the area of web services through the ws_security [6], ws_trust [7] and ws_federation [8] specifications (ws_federation is still work in progress). They are also the custodians of the SAML [5] standard which is used as a basic

[9] http://www.projectliberty.org/
[10] http://www.oasis-open.org/home/index.php

specification and transfer language in many other specifications such as Liberty Alliance and Shibboleth[11].

3.4 Harmonisation groups and Identification Software efforts

There exist a number of different groups and open source projects that either aim at harmonising existing efforts or at developing and promoting specific solutions for identity management. Because they currently cannot really be considered as standardisation organisations, we will not go into detail on these efforts here nor will we attempt to provide a complete list. However, seeing as some of them have an impact on standardisation, we will highlight a few of them.

On the harmonisation side, three efforts require mentioning: Project Concordia[12], OSIS[13] and Identity Commons[14]. Project Concordia is a consortium originally initiated by Liberty Alliance with the purpose of harmonisation and the provision of interoperability among identity protocols. OSIS aims at harmonising the development of software components for identity systems by creating an interoperable identity layer for the Internet. Identity Commons considers itself "an industry association for the collaborative development of the technical, social and legal aspects of a user-centric identity layer on the internet". OSIS is a part of Identity Commons.

With regards to software and implementation specifications, the best-known efforts are most likely OpenID[15], Yadis[16] and Higgins[17]. OpenID is an identification protocol suite that uses URIs (or XRIs) as identifiers. This identifier can be verified with any authentication mechanism as long as the verifying entity supports the protocol. Yadis is a service discovery mechanism that helps a service provider to determine what identity protocol to use. Currently Yadis only supports URI (or XRI) as identifier systems. Finally, Higgins is a software initiative within the Eclipse project that attempts to create a unified user interface for different identification systems by defining and implementing an API.

[11] http://shibboleth.internet2.edu/
[12] http:// projectconcordia.org/index.php/Main_Page
[13]http://osis.idcommons.net/wiki/Main_Page
[14] http://idcommons.net/
[15] http://openid.net/
[16] http://yadis.org/wiki/Main_Page
[17] http://www.eclipse.org/higgins/

4 Commented Standards

4.1 Sixth Working Draft ISO/IEC 24760 – Information Technology – Security Techniques – A Framework for Identity Management

ISO/IEC 24760 aims at providing a general framework for the management of identity information in IT systems. It focuses on those architectural and procedural aspects which apply regardless of environment or business activity. While it identifies the main requirements that need to be considered when setting up any identity management system, details and technical aspects are to be dealt with by other standardisation initiatives (or have already been standardised in the past). The framework is intended as guidance for any individual involved in the management of IT systems, particularly in the areas of access control, management of asset usage, and control of information linkage.

4.1.1 Current state of the draft

The identity management framework is divided into five main sections. The first section introduces and defines the core concepts of identity management. The next section describes the principles that need to be considered during implementation. The third section uses the core concepts to to delineate the lifecycles associated with an identity and the processes they typically involve. The fourth section identifies the components or building blocks that are commonly used to implement the aforementioned processes. Finally, the framework elaborates on how identity management processes and components can be implemented to meet the principles listed in the second section.

4.1.1.1 Basic concepts

ISO/IEC 24760 starts by attempting to clarify the main concepts surrounding identity, identity management and the relationship between them. ‘Identity’ is understood as ‘a structure[d] representation of an entity in a form of a defined collection of entity’s attributes in a relevant context, [which] allows this entity to be distinguished and recognized from other entities within that specific context’. In other words, the identity of an entity is considered to be the unique materialisation of that entity within a specific context. An identity can consequently only be a partial expression of the many possible manifestations of an entity.

Identification is defined as ‘the validation of provided mandatory evidences by an identity authority that an entity can be recognized with unique identity references within some context’. The identification process establishes the existence of the entity within a particular context. Among the attributes associated with the entity are one or more identity references. An identity reference is described as an attribute or combination of attributes of an entity that ensures unique representation of the entity within a specific context, and which can be used by an entity to make a claim that it is a previously identified entity.

Identity references are to be distinguished from identifiers. An identifier is defined as ‘a unique designation of an object an object that is used to represent the identity of entity within the specific context of the object’. Examples include account references in IT systems, passport numbers, credit card numbers, etc.

After discussing the relationship of identities to contexts and domains of applicability, ISO/IEC 24760 describes three major approaches to identity management: centralized, user centric and federated. It concludes this section by elaborating on the relationship between identity management and IT systems management, and the role identity management plays in the information society.

4.1.1.2 Identity management principles

In addition to policy, privacy, and legal requirements, ISO/IEC 24760 identifies several sets of principles relating to the management of identity management information, among which:

- the quality of identity information;
- the control of identity attributes;
- entity types and profiles;
- authoritative sources of identity information;
- identification processes;
- identity assurance;
- non repudiation assurances.

4.1.1.3 Processes for managing identity

Identity management is an integrated set of processes, policies and technologies which enable organisations and individual entities to facilitate the use and control of identity information. The framework discerns three major activities: identity life cycle management, entity authentication management and management of information associated with identification.

a) Identity life cycle management

Every identity has a lifecycle which needs be managed. First off all, every identity needs to be established for it to exist. This occurs during the identification process. It involves collecting and/or allocating sufficient attributes concerning the entity to distinguish it from any other entity in the context, and allocating a unique identity reference to the entity. During identification it will be verified whether the attribute values in question are correct with a degree of assurance proportional to the context (identity proofing). Once the appropriate level of assurance has been reached, the identity will be registered by storing the identity in a record of the identity management system. The identification process is often accompanied by provisioning (allocating one or more credentials to the identity).

Once the identity has been established, it needs to be activated. This will allow the entity to effectively interact with other entities in the context according to the policies of the context and its prerogatives. During its existence, it may become necessary to suspend or modify an identity (e.g. when attributes change or confidence in the identity is lost). Once there is no longer any need for the identity to exist it shall be terminated and possibly archived. Finally, identities can also be restored or re-activated from the suspended or archived state.

b) Entity authentication management

Identities need to be authenticated in various instances. They are initially authenticated during identification phase itself (proofing). Policies determine the checks and safeguards which need to be implemented to achieve the appropriate level of assurance during proofing.

Entity authentication will also occur frequently once the identity has been established and activated. 'Ongoing' identity authentication occurs when entities interact with one another; it is also described as the process whereby the validity of the credential given to an entity is verified.

Entity authentication can be either unilateral or mutual.

c) Management of identity information

Management of identity information in turn comprises three processes: establishing the original entity's identity, binding or unbinding information values, and then managing its changes over time. Identity information often is or needs to be certified by third parties, particularly in a federation.

4.1.1.4 Architectural components

This section discusses the possible components of an identity management framework and how they may interact. ISO/IEC 24760 distinguishes three major building blocks:

- a management system for identity information (IdMS), an identity authority;
- an identity registry, containing identity information, lists of attribute types and values, and a reference to the authoritative source of those attributes;
- identity providers, providing information on behalf of the authority and guaranteeing the interface to the registry;
- an identity reference generator, which ensures the provisioning of unique and reliable identity references.

Besides these technical components, each identity management framework should consider:

- a policy for use
- an authentication service
- a privacy consent service
- a personal profile service
- a discovery service
- a subscription/notification service.

4.1.1.5 Identity management framework in practice

In the final section ISO/IEC 24760 provides some guidance on how to apply the identity management framework in practice. It starts by elaborating the relationship between identity management and information security policies and access management. It then proceeds to explain how identity references and object identifiers can be used. This section also contains a relatively extensive description on aspects of privilege management and provisioning.

4.1.2 Summary of comments provided so far

ISO/IEC 24760 is the draft standard that has received the most comments from FIDIS. The reason for this is that it was the most mature work item at the time of our entry. The input from FIDIS ranges from suggested changes to terminology and clarifications of concepts, to

contributions of text in areas where this was required. With regards to the terminology, we have tried to promote and explain FIDIS understanding of the different terms used and our view on identity management. Similarly, with regards to the concepts that are elaborated, we have offered FIDIS' view on these concepts, but also pointed out inconsistencies in the proposed text in order to create a consistent and understandable document. Within this standard FIDIS has also actively taken part in "ad hoc" working groups created to advance the standard work further between WG5 meetings. In these groups we have provided textual input and suggestions for change primarily with regards to the sections concerning the identity life-cycle and requirements.

4.1.3 Conclusion and Outlook

From our view this standard is important in two aspects. First it is an effort to build consensus concerning the concepts and terminology. This process is important because it incorporates the different cultural and national views on identity and identity management systems. Second, once it is finished, it will serve as a reference in discussions and documents concerning identity management, as it defines the most accepted meaning of terms and concepts. The description of identity and the identification process will also help developers and others to understand the differences between the different aspects of identities and hopefully enable the understanding of relationships, limitations and risks involved in the identity concept. However, the document is still somewhat lacking in clarity and in some areas contains language and phrasings that are needlessly difficult to understand.

Future comments will in first instance be aimed at further improving the readability of the document and to simplify the text. We will also provide suggestions for additional text and clarification of concepts.

4.2 1st CD ISO/IEC 29100 – Information Technology – Security Techniques – A Privacy Framework

ISO/IEC 29100 seeks to provide a framework for defining 'privacy safeguarding requirements' when processing personally identifiable information (PII) through information and communication technologies. As a framework, it addresses issues from a high-level perspective, and is aimed at providing general guidance rather than prescribing a particular model. It is intended as a basis for possible further privacy standardisation activities, for example concerning the development of a technical reference architecture or the implementation of specific privacy technologies.

4.2.1 Current state of the draft

To achieve the aforementioned guidance, ISO/IEC 29100 puts forth a privacy terminology, a description of how privacy requirements are to be developed, a list of privacy principles, and provides examples as to how requirements may be implemented.

4.2.1.1 Terminology

When reviewing the list of terms and definitions, it immediately becomes apparent that ISO/IEC 29100 uses an autonomous set of concepts and terminology. Many of the terms that are defined differ from those defined under European data protection law. Although reference is made to the OECD Guidelines and Convention n°108 of the Council of Europe, the drafters had a clear intention to avoid making a 'euro-centric' framework and to ensure its international quality.[18] For example, the framework makes reference to 'PII' (personally identifiable information) and 'personal information' rather than to 'personal data', it defines the 'PII principal' rather than 'data subject', etc.

Even though there are great similarities and overlap between these concepts, there are also clear discrepancies. For instance, the notion of sensitive PII appears much broader than that of sensitive data under European Directive 95/46/EC. However, the definitions of PII and of 'personal information' in their current form seem as if they might be more restrictive than the European definition of personal data.

The list of terms is furthermore supplemented by concepts that are absent in laws, but which have been derived from IdM literature (pseudonymity, linkability, observability, …). Finally, the list of course also contains terms proprietary to this framework.

4.2.1.2 Development of Privacy Requirements

After providing an overview of the privacy framework, and some further guidance as to the concept of PII, the framework describes three main factors which an enterprise should take into account when it seeks to define privacy requirements for its operations:

a) privacy preferences;

b) business case or context;

c) legal and regulatory requirements.

a) Privacy preferences

Privacy preferences refer to the wishes and possible expectancies of PII principals towards the PII receiver. They are of course subjective by nature and depend on a multitude of factors that may create concerns for the individual providing his or her PII. Such factors include personal background, sensitivity of information, trust in communication partner, etc.

ISO/IEC 29100 does not attempt to standardise or even summarise the types of privacy preferences, but underlines the importance for service providers and developers to take them into account when identifying their customer needs and expectations.

b) Business case or context

Privacy requirements may be influenced by the nature of a business model or the context in which the processing of PII is to take place. The types of data processed and the potential for abuse may vary significantly according to each application. Some operations may pose

[18] Additional sources that were explicitly referenced include the Privacy Framework adopted by the Asia-Pacific Economic Cooperation (APEC), the Privacy Framework developed by the International Security, Trust & Privacy Alliance (ISTPA), and the 'Montreux Declaration' agreed by the International Conference of Data Protection and Privacy Commissioners.

specific threats due to the nature of the processing and actors involved, and may therefore demand additional safeguards. Of course, the purpose of the processing is also relevant for the actual implementation of certain privacy principles.

c) Legal and regulatory requirements

Legal and regulatory requirements are not only local data protection and privacy laws but also contractual obligations, professional or industry standards, binding corporate rules, company policies etc.

Based on these three factors, ISO/IEC 29100 provides an illustrative list of some potential privacy requirements:

- obtaining and recording the PII principal' knowledgeable, free and specific consent;
- identifying and communicating the purpose(s) for the collection, use, transfer, storage, archiving and disposal of PII;
- limiting the collection of PII to the identified purposes (collection limitation);
- implementing data minimisation procedures;
- destroying PII after the stated purpose has been fulfilled;
- providing individuals with access to information related to PII processing;
- checking the PII's accuracy and quality.

The framework also makes reference to ISO/IEC 27001:2005 and ISO/IEC 27002:2007 for defining additional requirements to safeguard or PII against loss or unauthorised access.

4.2.1.3 Privacy Principles

The privacy principles in ISO/IEC 29100 are an extracted 'set of overall commonalities' derived from fundamental privacy requirements found in the various regulatory instruments that acted as a source for this framework. These principles are considered to be the basis of ISO/IEC 29100, and their implementation is recommended regardless of social, cultural, economic or legal background.

The following eleven privacy principles are listed:

1. Consent and choice
2. Purpose specification
3. Collection limitation
4. Use, Retention and Disclosure limitation
5. Data Minimisation
6. Accuracy and Quality
7. Openness, Transparency and Notice
8. Individual Participation and Access
9. Accountability
10. Security Safeguards
11. Compliance

Many of these principles are quite similar to those identified by authors discussing the European data protection directive. There are exceptions however; 'data minimisation' for

instance has very specific meaning in the context of this framework. But despite some differences, most of the European data protection principles appear to be accounted for.

4.2.1.4 Implementation guidance

A first step towards achieving privacy assurance consists in embedding privacy compliance into an organisation's risk management. The framework provides several examples of potentially privacy-invasive activities (breach of confidentiality, harming data integrity, identity theft, loss of control, …) and underlines that they must be identified and adequately addressed by privacy and security safeguarding techniques. Privacy enhancing technologies (PETs) are considered a useful means to support the protection against the identified risks. The framework mentions a.o. the use of techniques to anonymise or pseudonymise PII, classifying data as PII and to associate it with specified purposes, use of encryption software, automated notifications, …

The framework goes on to emphasise the importance of adopting privacy safeguarding requirements in each phase of the data processing lifecycle. It starts by discerning six different phases (collect, use, transfer, store, archive and dispose), and subsequently elaborates on privacy aspects which need to be taken into consideration within these different phases of the lifecycle. The framework also provides a table overview of several 'safeguarding controls' which may be used to implement privacy requirements and how an enterprise can generate evidence of their implementation.

Finally, the framework describes how the privacy principles translate into responsibilities for PII receivers, and offers suggestions on how to establish a privacy management system.

4.2.2 Summary of comments provided so far

In first instance our comments have focused on the terminology and concepts that are used. As indicated earlier, ISO/IEC 29100 uses its very own terminology. Many of the terms that are defined differ from those on which we have a common understanding within FIDIS. This is true not only for those terms and concepts which have a particular meaning in Directive 95/46/EC, but also for other relevant terms which are discussed in IdM literature (pseudonymity, linkability, observability, …). We have attempted to constructively address inaccuracies and insufficiencies in order to render the framework as comprehensive as possible. In several instances we have also made suggestions for clarification and simplification.

As earlier working drafts of ISO/IEC 29100 were also lacking input of others, FIDIS also provided some text as tentative to fill these gaps.

4.2.3 Conclusion and Outlook

As a 'framework', ISO/IEC 29100 does not really serve as a standard but rather as an introductory basis, useful for comprehending basic privacy principles and requirements. It may be suitable as initial guidance for enterprises that are likely to come in contact with data protection regulations for the first time. Although the framework is quite elaborate regarding some of the measures that need to be taken, it remains vague towards others, and mainly works by way of example. The real value of ISO/IEC 29100 will therefore only become

apparent once the further standardisation initiatives it mentions (reference architecture, implementation of specific privacy technologies, …) are developed.

Positive elements of ISO/IEC 29100 are that despite its international scope, it seems to have accounted for practically all of the data protection principles under Directive 95/46/EC. As such the framework could help to remove boundaries and increase the chances of an adequate level of data protection on a global scale. Another positive element is that the framework clearly advocates consent and user choice as defaults. It recommends organisations to provide individuals with the option of providing specific consent and allowing them to express their privacy preferences (e.g. use for very specific purposes, data expiration times etc.).

Future comments will be aimed at further clarification of certain fundamental concepts, such as PII and data minimisation. We will also provide suggestions for additional measures to be included in the discussion of the data processing life cycle, as well as further elaboration of certain privacy principles.

4.3 Third Working Draft ISO/IEC 29101 – Information Technology – Security Techniques – A Privacy Reference Architecture

ISO/IEC 29101 is an extension to ISO/IEC 29100, the goal of which is to provide a 'privacy reference architecture model' and describing best practices for implementing privacy requirements. The result should offer system architects enough guidance to enable them to incorporate the requisite privacy safeguards into their system and facilitate the proper handling of PII across system platforms. Special emphasis is laid on: the various stages in data life cycle management, the roles and responsibilities of all parties involved, and combining privacy safeguards with existing security measures.

4.3.1 Current state of the draft

ISO/IEC 29101 is still in a very early stage of development. Most of the sections are still blank and therefore its final ambit is yet to be determined. In the following sections, we will provide a brief overview of the current outline of the draft, and discuss those elements which have already been elaborated.

4.3.1.1 Terminology

The defined terminology mainly supplements ISO/IEC 29100, providing additional definitions primarily related to consent and the processing of PII.

4.3.1.2 Basic elements of defining the Reference Architecture

The privacy reference architecture model has been adopted from the Common Criteria Target of Evaluation (ToE) development model set forth in ISO/IEC 15408. The premise is that the same workflow model can be used to assure the proper development or implementation of systems that process PII. The basic elements allowing the definition of a Privacy Reference Architecture are:

a) privacy requirements (as defined by ISO/IEC 29100);

b) functional requirements;

c) high-level design;

d) data processing model;

e) business process model;

f) IT model;

g) implementation.

4.3.1.3 Privacy design principles

This section should eventually elaborate on a basic set of design principles that ensure the safeguarding of the data subject's information privacy within each element of the data processing life cycle (collect, transfer, use, store, archive, dispose).

4.3.1.4 Integration of Privacy Safeguarding controls

This section seemingly will provide an overview of privacy safeguard mechanisms which may be adopted by organisations. It also lists a number of privacy-enhancing services and technologies, including:

a) anonymisation services;

b) pseudonymisation services;

c) limited show blind signatures;

d) biometric encryption;

e) secret sharing;

f) privacy preserving data mining;

g) unlinkable databases;

h) unobservable data management.

So far only the use of anonymisation services has been elaborated. The list is likely to be supplemented with other privacy-enhancing services and technologies.

4.3.2 Summary of comments provided so far

There have been only a very limited number of comments to ISO/IEC 29101 because the first working draft comprised practically nothing more than a table of contents. Our comments so far have consisted in suggesting some text where this was requested and possible additions to the list of privacy-enhancing services and technologies.

4.3.3 Conclusion and Outlook

Seeing as ISO/IEC 29101 is still in a very early stage of development, it is difficult to evaluate its merit. It is however apparent that this standard is still lacking in certain fundamental areas, which have not even been clearly referenced. These areas include:

- how PII principals' rights (e.g. right of access) may be accommodated;

- including privacy requirements in privilege management;
- adoption of security policies specifying use of encryption and data authentication protocols;
- authentication and assurance levels;
- possible need for contractual arrangements with PII receivers (including employees of the PII controller).

Future comments will consequently in first instance focus on including these areas and evaluating the further progression of this standard.

4.4 Fourth Working Draft ISO/IEC 29155 –Information technology – Security techniques – Entity authentication assurance

ISO/IEC 29155 is a joint text between ISO/IEC and ITU-T. The standard is aimed at providing guidelines and principles that should be taken into consideration when building assurance in the authenticity of an entity. Ultimately, the goal is to facilitate interoperability and federation of identity systems. It provides three basic building blocks:

- a framework for assessing "how close" an entities identity is to the claimed one

- guidelines for measurement of authentication strength

- the basis for a generally applicable set of authentication assurance measures.

4.4.1 Current state of the draft

In its current state the draft is still very immature. As with 29101, there are still many sections left blank, and some of the text is difficult to understand and unstructured. In the following sections, we will provide a brief overview of the current outline of the draft, and discuss those areas which have already been elaborated to some extent.

4.4.1.1 Terminology

The defined terminology mainly supplements ISO/IEC 24760, providing additional definitions primarily related to the authentication assurance process. However, there is some overlap of terminology between 24760 and 29155, and there are inconsistencies among these definitions. This is an area in which further updates to the draft most likely will harmonise the definitions towards a common understanding.

4.4.1.2 Entity Authentication Assurance Framework

This Section of the standard describes an open framework; with the components needed to fulfil the process of assessing "how close" a claimed identity is to the "real" identity throughout the identity life cycle. It consists of three basic framework components: Enrolment & Proofing, Credential Issuance and Identity Usage. Within each of these framework components, function areas and processes are described that are needed in order to fulfil the role of the framework components. Some of these function areas and processes serve an integration role or are needed in more than one of the components and thus span multiple

components. There are also sub groups within the functional areas and processes described. The following functional areas or processes are defined:

Transformation and Integration

Enrolment (including Proofing)

Identity Registry

Identity Data and Reputation Management (including Identity Management)

Credential Issuance and Personalization (including Trusted Credentials)

Physical Access

Logical Access

Identification

Credential Management

Monitor and Report

Infrastructure and Operations

The current text in this section is somewhat hard to follow and unclear, at least from the point of understanding the purpose and scope of the framework. It also seems to reflect more of a "sales pitch", making it more like an advertisement for a product rather than a description of a framework. This will, however, most likely change in future updates of the draft.

4.4.1.3 The rest of the document

The rest of the document is still very much under construction and development. It consists of five chapters (chapters 7-11) describing different aspects of authentication assurance. The first chapter discusses criteria for 'authentication effectiveness' and briefly addresses questions such as assurance levels, authentication principles and multifactor authentication. The following chapter addresses the threats related to authentication. The discussed treats are roughly divided into authentication protocol threats, authentication token threats and other authentication threats. Chapter 9 deals with other factors (besides the once mentioned in chapters 7 and 8) that influence authentication assurance. This section is still highly sketchy and discusses areas such as strength of credentials, communication paths, cost factors, usability and privacy. Chapter 10 is supposed to discuss threats versus control objectives. However, in its current form it is just one small section and thus in need of heavy revision. Finally, the last chapter highlights the need for common understanding of metrics and a need for mapping between the different assurances metrics used. The solution presented is to map towards one standard metric. However, no concrete mapping is suggested yet.

4.4.2 Summary of comments provided so far

We have provided very few comments to this document so far. This is because we judged the maturity level of the document such that it was difficult to get an overview of the document and where it was heading. Also time constraints played a part since we decided to prioritise the more complete documents in our review process. The few comments given are on structural issues and critique on what we believe to be factually erroneous descriptions.

4.4.3 Conclusion and Outlook

As with ISO/IEC 29101, ISO/IEC 29115 is still in a very early stage of development, and thus it is difficult to evaluate its merit. However, there are some elements already present that need to be addressed further. The framework needs to be elaborated and clarified further since it is an integral and quite important part of the standard. It is also this framework in the current draft that is the most mature.

The current document also lacks integration of the different parts. It is currently hard to grasp how the different sections relate to each other and to obtain a comprehensive overview. Finally, the privacy aspect is, beside a short note in chapter 9, more or less totally absent in the document. The current scope of the standard is in general somewhat disappointing.

Future comments will consequently in first instance focus on these areas and evaluating the further progression of this standard.

5 Other FIDIS activities within the Standardisation area

Sending in comments is just part of the work needed in order to disseminate FIDIS ideas and results to standardisation fora. The comments need to be collected, discussed, formulated and motivated, and after they are sent in, they must also be presented and defended. This section will discuss the work leading up to the comments and the work done in connection with the presentation and argumentation of our results and comments.

5.1 The work process

In order to facilitate the standardisation efforts within FIDIS, we created a mailing list to which interested partners in FIDIS could subscribe. This list has been used as the primary information channel for disseminating documents and views, as well as collecting comments and other input. Sessions in FIDIS general meetings and research meetings have been organised and used as small standardisation workshops, where new developments have been presented and proposed standards have been discussed (see annex A for details). On several occasions telephone conferences were organised to discuss matters that required immediate attention. The general work-cycle relating to comments and input for the different standards was organised as follows. The liaison officer first receives the documents and other information from the SC27 secretariat. He then sends these documents out on the mailing list, asking for comments from the FIDIS partners. The comments received and their motivation are collected and put into the correct format by the liaison officer and sent out again for consensus on the list (or discussed in a meeting if a FIDIS meeting was at hand). If there exists any controversy regarding the comments, or other issues in need of clarification, a telephone conference is used to resolve these issues. After consensus has been reached, the liaison officer constructs a liaison statement containing the approved comments. This statement is again sent to the mailing list for a quick review before it is sent into the SC27 secretariat as official FIDIS comment.

5.2 Standardisation meetings

FIDIS has actively participated in standardisation meetings on both international and national level. With regards to the international level, ISO/IEC JTC1/SC27 has held three regular meetings and ISO/IEC JTC1/SC27/WG5 has held one extra meeting in the period of the FIDIS liaison. FIDIS has been represented on all 4 meetings; actively participating in the discussions and, for the most part, successfully promoting and defending our viewpoints and concerns. There is also a meeting scheduled for May 2009 in Beijing where FIDIS will participate. The atmosphere of the meetings has been very open and friendly and FIDIS participants have been well accepted and integrated by the members in WG5. Besides attending these meetings, FIDIS has also been represented in ad hoc groups created by WG5 to facilitate forward progress in certain areas between meetings. All this, we believe, has helped to establish FIDIS internationally as an active player in the identity management and privacy arena.

On the national side, the FIDIS activities within ISO/IEC JTC1/SC27 have helped to facilitate cooperation with and participation in some European national standardisation bodies. This has had the effect that Sweden through SiS now is taking an active part in the WG5 work and that

other participants within the Swedish shadow committee of SC27 have expressed an interest in incorporating privacy aspects into already established security standards.

5.3 Workshops

As part of its liaison activities with ISO/IEC JTC 1/SC 27/WG 5 "Identity Management and Privacy Technologies", FIDIS co-organized a full-day workshop on Identity Management on September 30, 2007 in Lucerne (Switzerland). The 3rd organizer was ITU-T/SG 17. The workshop was placed directly after a meeting of ITU-T/SG 17 (in Geneva, Switzerland) and directly before a meeting of ISO/IEC JTC 1/SC 27/WG 5 and attracted more than 70 key players from these and other groups (such as Liberty Alliance). For FIDIS it was a perfect outreach activity with global attention by many relevant players, as FIDIS could not only present its approaches but also discuss the other approaches presented by the various groups.

The workshop is documented on:
http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306

and

http://www.itu.int/ITU-T/worksem/idmgt/index.html

The workshop program is also attached to this report.

6 Conclusions

This report has given an overview of the standardisation work performed within work package 19 of the FIDIS NoE. We have described the different efforts made in order to disseminate the results and views in FIDIS to the standardisation sector and specifically ISO/IEC JTC1/SC27/WG5. The report shows that we have actively managed to promote FIDIS ideas and results towards the ongoing work in WG5. It also shows that FIDIS, through our liaison with WG5, has been able to influence other standardisation efforts, particularly within ITU-T. The efforts presented have increased the knowledge of FIDIS and its work, and established FIDIS as a recognised and respected player within the field of international standardisation. The work has also in one case resulted in an active participation from a European country (Sweden) in WG5 and increased the national standardisation activities in the area of privacy and identity management.

Hopefully the work started within FIDIS can be successfully carried on by successor projects and by the different partners via their respective national bodies.

7 Bibliography

1. Liberty Alliance "Liberty Alliance ID-FF 1.2 Specifications " Available at: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications
2. Liberty Alliance "Liberty Alliance ID-WSF 2.0 Specifications" Available at: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_1_1_specifications
3. Liberty Alliance "Liberty Alliance Identity Assurance Framework (IAF) 1.1" Available at: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_identity_assurance_framework_iaf_1_1_specification_and_associated_read_me_first_1_0_white_paper
4. Liberty Alliance "Liberty Alliance Identity Governance Framework (IGF) 1.0" Available at: http://www.projectliberty.org/resource_center/specifications/igf_1_0_specs
5. OASIS, "Security Assertion Markup Language (SAML) V2.0 Technical Overview", Committee Draft 02, 25 March 2008. Available at: http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf
6. OASIS, "Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", OASIS Standard Specification, 1 February, 2006 Available at: http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
7. OASIS, "WS-Trust 1.3", OASIS Standard, 19 March, 2007 Available at: http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf
8. OASIS "Web Services Federation Language (WS-Federation) Version 1.2", Committee Draft 02, January 7, 2009 Available at: http://www.oasis-open.org/committees/documents.php?wg_abbrev=wsfed

Annex A. List of meetings and conferences

This annex lists the meeting sessions conducted by the standardisation group as well as ISO/IEC JTC1/SC27/WG5 meetings attended.

ISO/IEC JTC1/SC27/WG5 meetings attended:

- 3rd meeting of ISO/IEC JTC1/SC27/WG5 in Lucerne (Switzerland) 1– 5 October 2007
- 4th meeting of ISO/IEC JTC 1/SC 27/WG5 in Berlin (Germany), 13-14 February, 2008
- 5th meeting of ISO/IEC JTC 1/SC 27/WG5 in Kyoto (Japan), 14-18 April, 2008
- 6th meeting of ISO/IEC JTC 1/SC 27/WG5 in Limasol (Cyprus), 6-10 October, 2008
- 7th meeting of ISO/IEC JTC 1/SC 27/WG5 in Beijing (China), 4-8 May, 2009

Sessions conducted at FIDIS meetings:

- Session at the 2nd annual FIDIS Research Event 10-12 of September 2007 in Athens (Greece).
- Session at the 2008 general meeting 26-28 of March 2008 in Berlin (Germany).
- Session at the 3rd annual FIDIS Research Event 24-26 of September 2008 in Dresden (Germany).
- Session at the 2009 general meeting 25-27 of March 2009 in Frankfurt (Germany).

Annex B. Liaisons and Comments sent to ISO/IEC SC27/WG5

ISO/IEC JTC 1/SC 27 N5975rev2

ISO/IEC JTC 1/SC 27/WG 5 N55975rev2

REPLACES: N5972rev

ISO/IEC JTC 1/SC 27
Information technology -- Security techniques
Secretariat: DIN, Germany

DOC TYPE: meeting announcement

TITLE: **Notice of the Joint ISO/IEC JTC 1/SC 27/WG 5, ITU-T SG17/Q.6 & FIDIS Workshop on Identity Management Standards and Draft agenda on 30th September 2007**

SOURCE: WG 5 Convener (K. Rannenberg)

DATE: 2007-09-24

PROJECT:

STATUS: National Bodies and Liaison Organizations of JTC 1/SC 27 are requested to forward a copy of this document to each delegate planning to attend the above-mentioned meeting. The meeting will take place at the HSW in Lucerne (in the main train station), where also the SC 27 WG meetings will take place. So www.sc27.ch is the location for logistics information also in this case. Please note the information on registration procedures. **Especially, the attention is drawn to the extended due date for returning the workshop registration form (see Attachment 2) directly to the SC 27 Secretariat by 2007-09-20.**

Delegates are kindly requested to make their hotel reservations directly with the hotel of their choice. Some practical information and hotel list are provided in **Attachment 1** to this document. Two web sites, both freely accessible have been developed by JTC1/SC27 and ITU-T to support the workshop. This document and any further updates and logistic information regarding this workshop can be found at the SC 27 public web site at: www.jtc1sc27.din.de/sue/ws_idm. The power point presentations of the various speakers are available from the ITU-T dedicated website at: www.itu.int/ITU-T/worksem/idmgt/index.html.

ACTION ID: **FYI**

DUE DATE: **2007-09-20**

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chair
M. De Soete, SC27 Vice Chair
E. J. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 2 + 4 (Attachment 1) + 1 (Attachment 2)

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

Joint Workshop
ISO/IEC JTC 1/SC 27/WG 5, ITU-T SG17/Q.6, and FIDIS on Identity Management Standards in Lucerne
30th September 2007

General Information

A joint workshop on standardization activities in the area of identity management had been agreed between ISO/IEC JTC 1/SC 27/WG 5, ITU-T SG17/Q.6, and FIDIS. The date and venue of the joint meeting are September 30, 2007 in Lucerne, Switzerland, from 09.00 till 18.00. This document provides more details on the objectives, desired outcomes, and proposed agenda of the proposed workshop.

Objectives of Workshop

1. Information sharing between the ITU-T/SG17, FIDIS, JTC 1/SC 27/WG 5 and invited representatives from other groups attending.
2. Understanding of the ITU-T/SG17, FIDIS, and JTC 1/SC 27/WG 5 identity management initiatives, their focus, roles, and activities as well as other organizations' initiatives that participate in the Workshop.
3. Working towards a collaborative ITU-T SG17, FIDIS, and JTC 1/SC 27/WG 5 understanding and model for one or more common text on identity management standards.
4. Avoiding duplication of IdM work among the organizations represented at the workshop
5. Leveraging resources available to ITU-T/SG17, FIDIS, and JTC 1/SC 27/WG 5 in the standardization of IdM.

Desired Outcomes

1. A shared understanding of Identity management standardization, especially for JTC 1/SC 27/WG 5, ITU-T SG17/Q.6, and FIDIS.
2. Identification of potential joint ITU-T recommendations and ISO standards concerning IdM

Agenda (09.00 – 18.00)

09.00 Welcome (Kai Rannenberg, SC 27/WG 5; Richard Brackney, ITU-T; Hans Hedbom, FIDIS)

09.05 Greetings from our local host (Carlos Rieder, HSW Luzern)

09.15 - 10.45 Introduction by the organizers

- 09:15 ISO/IEC JTC 1/SC 27/WG 5 Activities (Kai Rannenberg and available Project Editors)
- 09:45 ITU-T Activities (Richard Brackney)
- 10:15 FIDIS Activities (Hans Hedbom)

10.45 Break

11.00 - 12.00 Stakeholders in Identity Management

- 11.00 Identities: Building blocks of telco business and organization (Ingo Friese, Deutsche Telekom Laboratories)
- 11.30 The view of the Montreal Conference of Data Protection and Privacy Commissioners on standardization in the area of identity management and privacy technologies (Steven Johnston, Office of the Canadian Privacy Commissioner)

12.00 Lunch Break

13.30 - 15.40 Standardisation Bodies in Identity Management

- 13.30 The Open Group Perspectives on Identity, Identifiers, and Identity Management (Ian Dobson, Director - Security Programs, The Open Group)
- 14:00 Liberty Alliance Identity Assurance Expert Group: Producing a Trust Framework for Global Inter-federation (Brett McDowell, Director, Liberty Alliance)
- 14.30 Break
- 14.40 NGN and its role in IdM from a security perspective (Scott Cadzow, ETSI Security Expert, Director Cadzow Communications Consulting Ltd, UK)
- 15.10 The W3C view (Rigo Wenning, W3C)

15.40 Break

15.55 - 16.55 Research Projects on Identity Management

- 15.55 Identity Management − The DAIDALOS view (Amardeo Sarma, NEC-E)
- 16.25 Privacy and IdM − Findings of the PRIME-Project (Jan Schallaböck, Independent Centre for Privacy Protection, Germany)

16.55 Break

17.00 Panel on future work and collaboration (Kai Rannenberg, Christophe Stenuit, SC 27/WG 5; Richard Brackney, Tony Rutkowski, ITU-T; Hans Hedbom, FIDIS)

ISO/IEC JTC 1/SC 27 N6107

ISO/IEC JTC 1/SC 27/WG 5 N56107

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: liaison statement

TITLE: FIDIS liaison statement to SC 27/WG 5 in response to SC 27 N5886

SOURCE: FIDIS Liaison Officer (Kai Rannenberg)

DATE: 2007-09-17

PROJECT: 24760
29100

STATUS: This document is being circulated for consideration at the 3rd SC 27/WG 5 meeting in Lucerne (Switzerland) on October 1st - 5th, 2007.

ACTION ID: **ACT**

DUE DATE:

DISTRIBUTION: P, O, L Members
W. Fumy, SC 27 Chair
M. De Soete, SC 27 Vice Chair
E. J. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners
R. Garcia Ontoso, Ch. Sténuit, Project Co-editors
S. Weiss, Project Editor

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 6

FIDIS liaison statement to SC 27/WG 5 containing comments on WD 24760 and WD 29100

FIDIS would like to thank ISO/IEC JTC 1/SC 27/WG 5 for its liaison statement from May 2007 and for the consideration of the FIDIS comments on WD 24760 and the updated documents received.
FIDIS attaches comments on the 3rd WD of Project 1.27.50 (24760) "A framework for identity management" and on the 2nd WD of Project 1.27.54 (29100) "Privacy framework".

FIDIS welcomes September 30, 2007 as the date for the joint identity management workshop and has nominated Hans Hedbom (Karlstad University) as speaker.

Attachment 1 to SC 27 N6107

[FIDIS[1]] comments on ISO/IEC 3rd WD 24760

Date: 2007-09-17	Document: **SC27 N5877**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
[FIDIS] 1	3.12	Bottom paragraph	te	It may possible to identify an entity with a high degree of certainty without knowing the unique identifier that is being employed in that particular context. Usage of some form of unique identifiers is most often a necessity in identity management systems, This is clearly illustrated in for instance medical and governmental contexts. It is an essential component of risk management. The general comment remains however that regardless of the context it may be possible for another entity to identify a particular entity without knowing the unique identifier(s) that is (are) being used in that particular context - albeit that this would require additional processing.	Replace: "… with unique identity references and additional information that characterizes the entity" by "… with unique identity references *and/or* any additional information that characterizes the entity.	
[FIDIS] 2	3.26		te	There is a discrepancy with other document (working draft 29100): use of "personally" vs. "personal" with regards to PII. Seeing as it concerns PII, the intended term is probably 'personally' (this is the term used in the USA Privacy Act of 2005).	Change: "personal" to "personally"	
[FIDIS] 3	3.27	2nd to last paragraph	te	Trust is a concept that crosses many disciplines as well as domains, so the focus of the definition differs. In identity management, trust is typically understood in its operational sense. Operational definitions of trust require a party to make a rational decision based on knowledge of possible rewards for trusting and not trusting. Based on this we propose the following definition: "An entity can be said to trust a second entity or a system when it makes the assumption that the second entity or system will behave exactly as trusting entity expects. This assumption is generally shared by all	"An entity can be said to trust a second entity or a system when it makes the assumption that the second entity or system will behave exactly as the trusting entity expects."	

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				those in an exchange."		
[FIDIS] 4	4 Symbols (and abbreviated terms)	3rd abbreviation	ed	The acronym provided does not correspond with its definition.	Replace HIPPA by HIPAA	
[FIDIS] 5	4 Symbols (and abbreviated terms)		te	There is a discrepancy with other document (working draft 29100): use of "personally" vs. "personal" with regards to PII. Seeing as it concerns PII, the intended term is probably 'personally' (this is the term used in the USA Privacy Act of 2005).	Change: "personal" to "personally"	
[FIDIS] 6	5-10		ed	Based on comments relating to 3.26	Replace : personal identifiable information" to "personally identifiable information"	
[FIDIS] 7	5.11 Context prerogatives and entity privacy preservation	First paragraph under 5.11	te		Replace: "The sharing of an entity's attributes between contexts when entities are people or groups of people has to be coherent with applicable privacy laws, regulations and principles and especially the privacy preservation of the entity." With: The sharing of an entity's	

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
					attributes between contexts when entities are people or groups of people has to be coherent with privacy principles and especially the privacy preservation of the entity and consistent with applicable laws and regulations."	
[FIDIS] 8	7.3 Legal and regulatory aspects	EU Data Protection of personal data directive and Privacy in electronic communications directive	te	EU Data Protection Directive = 95/46/EC EU Privacy in Electronic Communications Directive = 2002/58/EC	Specify: (95/46/EC) (2002/58/EC)	
[FIDIS] 9	7.3 Legal and regulatory aspects	1st paragraph	te		Add: "… rights to the data protection of personal data in the European Union and under the Convention n° 108 are currently primarily based on …"	
[FIDIS] 10	7.3 Legal and regulatory	** Need additional	te	In reference to information society, privacy is often understood as the freedom of a natural person to sustain a personal space, free from interference by other	Add: In reference to information society,	

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
	aspects	text here ***		entities. Others authors understand it as the right of a natural person to decide –in certain circumstances– for itself when and on what terms elements of its identity or attributes should be revealed.	privacy is often understood as the freedom of a natural person to sustain a personal space, free from interference by other entities. Others authors understand it as the right of a natural person to decide –in certain circumstances– for itself when and on what terms elements of its identity or attributes should be revealed.	
[FIDIS] 11	9.5.4			There are settings in which use of non-repudiation mechanisms, such as electronic signatures, is a necessary component of risk management in order to ensure a high level of accountability and/or to offer an appropriate probability value to the logs	Add the following after the first paragraph: “There are settings in which use of non-repudiation mechanisms, such as electronic signatures, is a necessary component of risk management in order to ensure a high level of accountability and/or to offer an appropriate probability value to the logs”.	
[FIDIS] 12	9.6.5. Digital certificates	First paragraph	te	It seems appropriate to reference X.509 Digital Certificates as an *example*; the current text seems to imply that this is the only form digital certificates may take	Change: “ It is also known as a PKI Certificate or an X.509 Digital Certificate.” To “It is also known as a PKI Certificate with X.509 Digital Certificates being prominent examples”	
[FIDIS] 13						

Attachment 2 to SC 27 N6107

[FIDIS[1]] comments on ISO/IEC 2nd WD 29100

Date: 2007-09-17	Document: **SC 27 N5881**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
[FIDIS] 1	5.3	Last paragraph		The sentence “If a user enters PII into a field that warns against doing so, it is reasonable to treat the information as though it were anonymous data.." is problematic, as data should not lose its qualification of PII nor of personal data just because of the circumstances under which it is being processed. It is quite possible that the law may place the responsibility on the data subject itself if it chooses to enter PII into a field that warns against doing so. However, once the PII comes under the control of another entity, and that entity continues to process that data according to its own purposes and its own means, that entity becomes accountable for those processing operations.	Delete this sentence “If a user enters PII into a field that warns against doing so, it is reasonable to treat the information as though it were anonymous data."	

ISO/IEC JTC 1/SC 27 **N6361**

ISO/IEC JTC 1/SC 27/WG 5 **N56361**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: liaison statement

TITLE: **FIDIS liaison statement to SC 27/WG 5 containing comments on ITU-T SG 17 Focus Group on Identity Management's draft reports in response to SC 27 N6264**

SOURCE: FIDIS Liaison Officer (H. Hedbom)

DATE: 2008-01-08

PROJECT:

STATUS: This document is being circulated for review and response by the 4th SC 27/WG 5 meeting scheduled to be held in Berlin (Germany), February 13th – 14th, 2008.

ACTION ID: **ACT**

DUE DATE:

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-chair
E. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 1 + 28 (Attachment)

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

FIDIS

Future of Identity in the Information Society

FIDIS liaison statement to SC 27/WG 5 containing comments on ITU-T SG 17 Focus Group on Identity Management's draft reports

FIDIS would like to thank ISO/IEC JTC 1/SC 27/WG 5 for its liaison statement from December 2007 and for the consideration of the FIDIS comments on WD 24760 and WD 29100 and for the updated documents received.

FIDIS would also like to thank ISO/IEC JTC 1/SC 27/WG 5 for its cooperation and support in organizing the joint SC 27/WG 5, ITU-T, and FIDIS workshop on Identity Management in Lucerne on September 30 and shares ISO/IEC JTC 1/SC 27/WG 5 view regarding the outcome of the workshop.

More over FIDIS would like to let SC 27/WG 5 know, that Hans Hedbom (Karlstad University, Dept of Computer Science, SE-651 88 Karlstad, Sweden. E-mail: Hans.Hedbom@kau.se) is its new liaison contact to SC 27/WG 5.

As input for the WG5 meeting on February 13/14 and the WG 5 liaison statement to ITU-T FIDIS attaches detailed comments on the draft documents from ITU-T SG 17 Focus Group on Identity Management and would like to make two general comments regarding the documents.

1. Single communication flow model too restrictive
Requirement 1 in the report on Requirements mandates a single communication model "User-Relying Party (RP) – Identity Provider (IdP)". This model is rather restrictive and may not be preferable from a privacy perspective, since it allows for extensive profiling on the side of the IdP. Representatives of both Liberty and Microsoft have assured us, that they would also support a scheme following a distribution of credentials through the User, without the requirement of direct communication between IdP and RP.
One possible approach to the problem could be to give the user full control over the IdP (i.e. the User is the IdP). The Interoperability Framework does not explicitly prohibit this, but on several places mentions the possibility of the RP being the IdP. Consequently we propose to at least include the possibility that the User also is the IdP.

2. General perspective on PII not comprehensive
Although there is a notion of the need for privacy protection in several parts of the document, there are chapters that seem not to have taken into account that PII is involved in most cases. This is a fundamental problem throughout the documents, which could not be solved just based on commenting, but may need a rewrite. Furthermore, the definition of PII used in the reports is unknown to us and appears to be somewhat misleading. We suggest using the definitions of ISO WD 29100 and WD 24760 as a base instead.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment** [2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**

ITU FG IdM Global Interoperability FRAMEWORK:

[FIDIS] 1	p.6 "ongoing authentication"	End of paragraph	Ge	Phishing is not synonymous with identity theft, rather it is a (fraudulent) activity which may lead to identity theft.	Consider revising	
[FIDIS] 2	P7 5.6 Unbinding of attributes from identities	End of paragraph	Ge	Report states: "This may be needed if a requesting/asserting entity has lost a certain property, status, or credential" → <u>suggestion</u>: add "… or in order to comply with data protection regulations". cfr. data minimization under Data Protection Directive: data may not be kept in form which permits identification for longer than necessary to achieve the purposes of the processing; or the "usage directives" with regards to traffic data under the Privacy in Electronic Communications Directive.	Add "… or in order to comply with data protection regulations"	
[FIDIS] 3	p.10 Credentials		Ge	Credentials are explained in the paragraph, but in some parts of the text authenticator is used as a synonym to credential this makes the explanation confusing.	Replace authenticator with credential throughout the paragraph.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment** [2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
[FIDIS] 4	p.10 5.9 Identity Relationships	First paragraph		Report states: "(a) an requesting/asserting entity Bob Smith can have an identity bsmith (as identifier) in Acme and bsmith (as identifier) and those two can be related" This sentence does not make sense.	Consider revising.	
[FIDIS] 5	p.10 5.9 Identity Relationships	Last paragraph		The whole paragraph hints towards a high level of linkability which is highly undesirable from a privacy perspective. We do see the need to get a unified view of an identity within an enterprise. Or for the requesting/asserting entity to keep track of the linkability of its different identities. However, we do not see the general need for anybody except the requesting/asserting party to get a unified view of the entity between enterprises (that are not in the same corporation)or between an enterprise and the outside world.	Please explain further why this would be needed.	
[FIDIS] 6	p.18 8.13 Identity Relationship Service			See [FIDIS] 6		
[FIDIS] 7	p.19 8.14 Identity Transformation and Bridging Service	Last paragraph		The text mentions five functional blocks for the IdM BF, however only four are shown in Figure 6. There are also only four blocks explained in the following sections.	Consider revising.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 1 to SC 27 N6361
[FIDIS] comments on ITU-T liaison documents

Date: 2008-01-08	Document: **SC27 N6264**

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment [2]**	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
[FIDIS] 8	Appendix A A-4/5 Credential issuance	Top of page	Ge	The report states: "Typically, there is no personally identifiable information (PII) data in the credential to compromise the privacy of that entity […]" But on the next page goes on to say: "This credential *represents* a digital identity as issued by the authority governing this framework." Strictly speaking, the two statements may be reconcilable [when considering that a "digital identity" in fact maps with a "partial identity", and that an identifier may in fact be meaningful for one transaction only]. However it may nevertheless be useful to underscore, e.g. after listing X.509 as an example, that a credential may be anonymous or pseudonymous in IMS where "full-blown" identity verification is not required. Additionally, it seems that there are quite a few credentials (in particular X.509 certificates) which do in fact contain PII (name and other attributes) in the certificate/credential.	Delete first sentence OR Leave the sentence but make it a normative statement, rather than a descriptive one: "Typically, there *should be no* PII ….") Add (at the end of the paragraph in question): "Credentials can also be anonymous or pseudonymous however, which might desirable for certain applications In order to reduce the PII that is being exchanged.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**

ITU FG IdM Report on Interoperability Requirements:

[FIDIS] 1	P3	Para a) middle	ge	In several places throughout the document notion is given to the fact, that the the RP can also be the IdP, whereas no reference is given to the fact that also User/Entity can be the party providing the Identity service, which should be default from a privacy preserving perspective to avoid profiling.	Change “which may be the relying party itself or another party” to “which may be the relying party itself, the requesting or asserting entity or another party”	
[FIDIS] 2	P6	Fig 2.	te	The figure may be misleading, since it draws one single box for “identity providers”, which may lead to the assumption, that there is only one such provider, where it is stated in several places, that there should be a choice of several providers. Therefore the figure should provide several boxes.	Replace box titled “Identity providers” with three boxes titled “Identity provider”	
[FIDIS] 3	P7	Brackets in last para	ge	See [FIDIS] 1	See [FIDIS] 1	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
[FIDIS] 4	P8	Figure 5, 1st para, and R1	ge	Following the OECD-Privacy-guidelines' principle of data minimization the described Common Structured Identity Management Model should be accompanied by a model following the communication scheme: Requesting Entity <-> IdP <-> Req. Identity <->RP, which should be recommended as default to avoid and reduce the possibility of profiling for the IdP. Sec. 6 of the use case shows that there are other communication flows in use. Liberty as well as Cardspace specifications also allow for a different setup.	New figure 5 showing: Req. Entity <-> IdP <-> Req. Entity <->RP. Current Figure 5 becoming figure 6 Delete first para and replace. Figures 5 and 6 show different possible communication flows in IdM. The first of the two is preferable as it minimizes the possibility for profiling on the side of the Identity provides, thus allowing a higher trust for the user, with regard to the protection of his PII. Only in those cases. Only if policy requirements do not allow is recommended. Replace R1: It is recommended that Identity Management Specifications and implementations follow the Model shown in figure 5. It is recommended that it supports the scheme in figure 6 and applies this scheme, where the one in figure 5 ist not applicable due to policies in place.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment** [2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
[FIDIS] 5	P8 3rd paragraph	End of paragraph	ge	The report states: "Anonymity and pseudonymity are frequently manifested where the kind of activity involved is so trivial that any kind of identity management overhead is not needed or desired". Although this may be true as a matter of fact, it should made be clear that anonymity and/or pseudonymity may be required by law as well (e.g. when processing data for purposes of statistical/historical analysis or in accordance with the principle of data minimization). Such operations may very well be non-trivial in nature and/or have considerable IdM overhead in place (both during as well as prior to the anonymization or pseudonym management). Furthermore, it seems more correct to say an assertion is anonymous or pseudonymous (rather than "an assertion may also be one of anonymity or pseudonymity").	Replace entire paragraph by the following: "An assertion may also be anonymous or pseudonymous. Whether or not anonymity or pseudonymity is used, depends much on the level of identity assurance that is required or desired. Anonymity and pseudonymity are frequently manifested where the kind of activity involved does not functionally require actual verification of the identity that is "behind" the digital identity (e.g. where the activity is so trivial that any kind of identity mangement overhead is not needed). Anonymity and/or pseudonymity may also be desirable in light of PII considerations (e.g. specific legal provisions or general data protection requirements)	
[FIDIS] 6	P8	Third para	ed	Following the principle of data minimization and purpose limitation anonymous approaches should be followed wherever a purpose for identification is not given. Pseudonymous approaches can help even in those cases where identification is necessary to avoid unwanted linkability, and to enhance the security of PII.	Replace last sentence: Anonymous solutions should be default. If identification is necessary for the purpose of a service, as much data as possible should be dealt with using pseudonyms, storing the linkage rule detached.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
[FIDIS] 7	P9	Figure 6 (old) and R2	ge	The described concept of an Identity plane concentrates all strati to one Identity Management system, whereas identification is in most cases only necessary on the application layer. To avoid unnecessary identification and thus the emergence of PII without a purpose, identification management should strictly only be applied where such purpose is given, in other cases anonymization techniques should be default	Fig. 6: add a star on the connections between the stratus and the Identity Management block, add a comment for the star reading "identification only where a purpose is given otherwise anonymize"	
[FIDIS] 8	P11	First para, 4th line	ed	Grammar	Delete "are"	
[FIDIS] 9	P11	4th para	ed	Grammar	Replace "for" by "of"	
[FIDIS] 10	P11	R4	ge	The concept of entity does not appear to be concise	Supplement by a structured concept of what an entity is, and what types of entities there are	
[FIDIS] 11	P12	R8	ge	A clear understanding and definition of object in the context is missing	See above [FIDIS] 10	
[FIDIS] 12	P12	R11	ed	Appears to be the same as R5	Delete	
[FIDIS] 13	P12 R15			There seems to be a cut and paste error here. In its current wording there are no apparent differences between R14 and R15	Change …. to access / modify /monitor its own Identity information on an Object… in R15 To … …. to access / modify /monitor Identity information on an Object under its authority..	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
[FIDIS] 14	P12	R15	ed/ge	Sentence does not make sense (eg. a child is usually not referred to as an object of its parents, information that lawful interception is granted to is not information that belongs to the authorities). It should be noted, that the recommended functionality may pose a built-in security threat, that poses significant liability risks on some identity providers. A recommendation with regard to the applicable security mechanisms should be considered.	Delete “its own” Consider revision	
[FIDIS] 15	P12	R17	ed	Grammar	Insert “an” between “at” and “Identity provider”	
[FIDIS] 16	P12	R18	ed	A definition of “Terminal Object” is lacking, rendering the requirement hard to understand	Consider explication	
[FIDIS] 17	P12 R18	Towards bottom of page	ge	The report states: “It is required that Identity Providers be able to support an Attribute that describes the preferred Terminal Object used for a particular service”. Although this may be desirable for certain applications from a security perspective, it should be noted that such information of course also relates to the “transactional” privacy of individuals, and thus should not be enabled “by default”; unless there is a clear justification in the purpose or security of the processing.	Add (also here) “… subject to applicable policy”	
[FIDIS] 18	P13 5.2.2	4th para	ge	Rapid verification and revocation is a functionality that must be carefully weighed against the possibility for profiling on the side of the IdP. Only where other mechanisms do not work this should be taken into account	Consider reviewing	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment** [2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
[FIDIS] 19	P13	R21	ge	See [FIDIS] 18	Replace second half of sentence by: "including deletion of credentials where the purpose of the processing has been fulfilled as well as rapidly checking the current status of a credential, where this is needed in accordance with applicable policies"	
[FIDIS] 20	P14	R22-24	ed	The term "chain of Authentication Assertions" is not included in the definitions, therefore the requirement is not easy to comprehend.	Either define or better replace "chain of" with "derived" and define this	
[FIDIS] 21	P14 5.2.3	Whole section including R25 and R 26	ge	The use of credentials may be preferable to using a combination of otherwise used identifiers such as URL, IMSI and the like, as credentials may at the same time serve as pseudonyms, whereas the other identifiers also may reveal additional information on the object and increase linkability without a given purpose. We would also like to underline that only where there is a specific legitimate purpose to further process these identifiers, and the processing complies with the overall data protection framework, may the processing referenced in R25 take place. There are clearly many instances in which such processing may take place, as is well illustrated by the examples listed. Due to its 'sweeping' language however, the section suggests little or no limitation to the exchange and further processing of identitifers in general (e.g. by not more clearly specifiying the purposes). Trusted intermediaries such as Identity Brokers also deserve explicit mentioning in this section.	Consider reviewing entire section Should at least include, "subject to applicable policy" where appropriate	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment** [2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
[FIDIS] 22	P15 R32 –R36			It seems strange that the requirements are recommended and not required. These requirements are essential when adhering to the privacy principles Stated by the OECD as well as to the EU-privacy law. Furthermore they are need to assure a secure and auditable transfer of identity information as well as verifying the validity of the request. Besides, an insecure transfer of attributes to non-validated receivers would diminish the trust in the verification of the entity.	Change recommended to required and possibly add "… subject to applicable policy" where needed.	
[FIDIS] 23	P15	R35	ed	For the sake of completeness it should be noted, that a mechanism for access of the attributes is to be included	Insert "to access," before "to store"	
[FIDIS] 24	P15	R37	ed	As stated in the accompanying text, patterns may have implications when involving PII. Following the OECD Guidelines, those patterns may only be stored under certain conditions and are recommended to be deleted otherwise. For clarification this should be explicitly mentioned in R37	After "including" insert mechanisms for secure and non repudiable deletion of the data if PII is involved and no pupose exists, and"	
[FIDIS] 25	P15	Whole Section	ge	Assurance mechanisms do not only differ by a quantitative means, but also qualitatively. Depending on the needed assurance different types of mechanisms should be considered, including different types of communication flow.	Replace "levels" by "types"	
[FIDIS] 26	P18 R46			It seems strange that the requirement is recommended and not required. The requirement is needed when adhering to the privacy principles Stated by the OECD as well as to the EU-privacy law.	Change recommended to required and possibly add "… subject to applicable policy" where needed.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
[FIDIS] 27	P12 R18	Towards bottom of page	ge	The report states: "It is required that Identity Providers be able to support an Attribute that describes the preferred Terminal Object used for a particular service". Although this may be desirable for certain applications from a security perspective, it should be noted that such information of course also relates to the "transactional" privacy of individuals, and thus should not be enabled "by default"; unless there is a clear justification in the purpose or security of the processing.	Add (also here) "… subject to applicable policy"	
[FIDIS] 28	P19 R48 and R50			See [FIDIS] 27	See [FIDIS] 5.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**

ITU FG IdM Report on Identity Management Ecosystem and Lexicon (Please consider these as revisions or additions to the Lexicon and the Living List):

[FIDIS] 1	p30 Anonymity	Bottom of page	ge	Last definition of "anonymity" in IDEM and FIDIS: "Anonymity refers to the quality or state of being not sufficiently identifiable to an attacker, within the set of all possible subjects that could cause an action or might be acted upon (the anonymity set)." Based on [Pfitzmann 2007b] (version November 26, 2007)	Replace definition iii. of anonymity by "iii. the quality or state of being not sufficiently identifiable to an attacker, within the set of all possible subjects that could cause an action or might be acted upon (the anonymity set)."	
[FIDIS] 2	P31 Assertion	Top of page	ge	Our (IDEM and FIDIS) current definition of an assertion is: "An assertion is a digital representation of a claim. An entity may assert an attribute, authentication or authorization, and present a credential as proof, to enable authentication, to validate a user's identity, or to identify what the user is authorized to do." Definition based on http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci839675,00.html (SAML).	Consider replacing	
[FIDIS] 3	P31 Attribute	Bottom of page	Ge	We currently define an attribute as: "An attribute is a physical or abstract named property belonging to an entity. An attribute typically has a value." (Based on [MODINIS IDM 2005], p.5	Suggest replacing (or at least integrating with) meaning iii. of attribute (which is based on WSIA Glossary)	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment** [2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
[FIDIS]4	P32 Authentication	Middle of page	Ge	We currently define authentication (and derived terms) as follows: "Authentication is the process of corroborating a claimed set of attributes or facts with a specified, or understood, level of confidence. 3.13.1 Data (origin) authentication Data (origin) authentication is a technical process which gives assurance, through corroborative evidence, of the identity of the entity from which a message originates, to the entity which receives a message. It serves to verify that a claimed attribute corresponds to the actual attribute held by an entity. [note: data origin authentication is separate definition in the ITU Lexicon, p.35] 3.13.2 Entity authentication Entity authentication is a process that provides assurance of the claimed identity of an entity, as it corroborates the (claimed) partial identity of an entity and a set of its observed attributes. 3.13.3 Authentication protocol An authentication protocol is a protocol used to authenticate data or entities. When relating to entities, it usually exists in the presenting of an identifier (e.g. a 'user-ID') and verifying the proof of something (e.g., the knowledge of a secret)." (Based on [MODINIS IDM 2005], p.7 and 9; [IDA Glossary 2002], p. 2 and [MENEZES 1997], p. 25.)	Consider adding 2nd meaning to authentication: "ii. the process of corroborating a claimed set of attributes or facts with a specified, or understood, level of confidence."	
[FIDIS]5	P33	Top of page	Ge	We currently define authorization as:		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
	Authorization			"Authorization is the process or act of determining the permissions of an entity, through the evaluation of applicable access control information, to perform a defined action on a defined controlled or protected resource. The set of defined actions corresponds to the set of possible uses of the controlled or protected resources for which the authorization authority is responsible (typically 'read', 'modify', 'create' and/or 'delete' resources). In the operational sense, authorizations are granted or denied based on the result of data or entity authentication, and on the policies defined within the system." (Based on NABETH 2005a], [HODGES 2006], [SLONE 2004]and [ROBBEN 2005b]) + Consider definition of "authorization profile": "Authorization profile The authorization profile of a user says which kind of resource an entity may access, in what situation and for what period of time depending on the capacity in which the entity is registered" (Based on ROBBEN 2005c], slide 6 and [ROBBEN 2005b], slide 8.)		
[FIDIS] 6	P33 Certificate	Middle of page	Ge	We currently use the following definition of certificates "A certificate is an affidavit whereby an accredited certification body attests to the truth of certain stated facts. In identity management, the term is often used to refer to a public-key digital certificate. X.509 Digital Certificates are a prominent example thereof. 3.18.1 Attribute Certificate		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
				Attribute certificates are digitally signed (or certified) bindings of an entity to a set of attributes, and may be used in various security services, including access control, data origin authentication, and non-repudiation. 3.18.2 Public-key digital certificate A public-key digital certificate consists of a data part and a signature part: • The data part consists of the name of an entity, the public key corresponding to that entity, possibly additional relevant information (e.g., the entity's street or network address, a validity period for the public key, and various other attributes). • The signature part consists of the signature of the CA over the data part." (Based on [FARELL 2002], [MENEZES 1997], p. 67 and the workshops held in the context of IDEM and FIDIS).		
[FIDIS] 7	P33 Circle of Trust	Bottom of page	Ge	A circle of trust is a group of entities, usually service providers, that federate (partial) identities and have pertinent business agreements in place regarding how to do handle identities within this circle. (Based on Based on [RÖSSLER 2002], p. 29.) Note: See also federation		
[FIDIS] 8	P34 Context	Towards bottom of page	Ge	We are developing the following definition of a "context": "A context can be described as a particular setting of an entity's environment. It can, for example, be a sphere of activity, a geographic region, a communication platform, a		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
				logical, or physical (security) domain. In identity management the term 'context' is typically used to refer to a (1) communicational context or (2) a (security) domain: (1) A communicational context is defined by roles and behavioral schemes assumed by the participants in the communication. In organizational systems communicational contexts in most cases map with sectors defined by the organization; (2) A security domain is an environment that is defined by security models and a security architecture, incorporating a set of resources and set of system entities that are authorized to access some or all of the resources. The traits defining a given security domain typically evolve over time." (Based on [HODGES 2005], p.10, [DE COCK, MODINIS], slide 3 and the workshops held in the context of the IDEM FIDIS)		
[FIDIS] 9	P34-35 Credential	Bottom – top of page(s)	Ge	We are developing the following definition: "A credential is a set of data or a piece of information, mainly an attribute or a set of attributes attached to the entity that makes use of it, attesting to the integrity of certain stated facts (e.g. the claimed identity of an entity). The production of adequate credentials can, but need not involve disclosure of identity." (Based on [BAUER 2005], p. 76 and [MODINIS IDM 2005], p. 11.)		
[FIDIS] 10	P35 Data origin	Middle of page	Ge	We have been developing the following definition: "Data origin authentication is a technical process which		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
	authentication			gives assurance, through corroborative evidence, of the identity of the entity from which a message originates, to the entity which receives a message (or a third party)." More generally speaking, it serves to verify that a claimed attribute corresponds to the actual attribute held by an entity.		
[FIDIS] 11	P35 Digital Identity P38 Federated Identity P40-41 Identity			We have been developing the following definitions: "Identity The identity of an entity is the dynamic collection of all of the entity's attributes. An entity has only one identity. As such, the identity of an entity this is more a fluid and evolving ("philosophical") concept, rather than a practical one. An entity has only one identity, but it is neither possible nor desirable for an information system to gather all the attributes of a specific entity. Information systems focus on a specific subset of relevant attributes, commonly referred to as 'partial identities'. 3.46.1 Identity data Identity data or identity attributes are identifiers and/or attributes specific to the entities' physical, physiological, mental, economic, cultural or social identity. 3.46.2 Partial identity A partial identity is a subset of the identity of an entity, that comprises one or more attributes of that entity. These attributes are not necessarily unique to that entity and therefore do not necessarily uniquely identify the entity in all contexts. 3.46.3 Digital identity A digital identity is a partial identity in an electronic form.		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
				3.46.4 Federated identity A federated identity is a partial identity which is the result of federation, and which usually implies that the entity to which this identity corresponds is recognized by several service providers or applications that are part of the federation. See also federated identity management; federation; identity federation; circle of trust." (Based on Based on [MODINIS IDM 2005], p. 9 and 12, [HODGES 2006], p. 6, [ITU LEXICON 2007], p38 and [ISO WD 24760] (concerning 'federated identity'), p. 8.)		
[FIDIS] 12	P37 Entity	Middle of page	Ge	We have developed the following definition of an entity: "An entity is an item of interest, inside or outside a system, such as an automated process, a subsystem, a device, a person or group of persons that incorporates a specific set of attributes." (Based on [SHIREY 2000], [MODINIS IDM] and the workshops held in the context of the IDEM and FIDIS projects)		
[FIDIS] 13	P38 Federated Identity			See FIDIS 11		
[FIDIS] 14	P38 Identification	Towards bottom of page	ge	The term "identification" is used in various ways in IDM literature: • identification in terms of registration: identification as the process of using claimed, observed or assigned attributes of an entity to establish a partial ["digital"] identity of that entity ; • identification as entity authentication:		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
				identification as the verification of the link between an entity and the asserted (partial) identity ; • identification in terms of identifiability: identification as the process of "individualizing" a particular entity within a set of subjects . (See e.g. [MODINIS IDM 2005], p. 9; [OPEN GROUP], p. 27 and [PFITZMANN 2006a], p. 21)		
[FIDIS] 15	P40 Identifier	Middle of page	Ge	With regards to meaning .v: We have further refined the MODINIS definition as follows: "An identifier can be defined as a non-empty set of attributes of an entity which uniquely identifies the entity within one or more specific contexts or sectors. Note: It should be noted that under this definition a set of attributes can include exactly 1 attribute."		
[FIDIS] 16	P40-41 Idenitity			See FIDIS 11 Additional comments: All meanings/definitions, except v. + vi. correspond with our notion of a "partial identity" Meaning v. in ITU lexicon refers to "identification", not "identity".	Move/delete meaning v.	
[FIDIS] 17	P41 Identity context	Middle of page		See previous comments wrt identity and our (developing) definition of context (FIDIS 8)		
[FIDIS] 18	P41	Towards		Similar to our concept of "identity data":		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
	Identity information	bottom of page		"Identity data or identity attributes are identifiers and/or attributes specific to the entities' physical, physiological, mental, economic, cultural or social identity."		
[FIDIS] 19	P42 Identity management	Top of page		Definitions developed in the context of FIDIS and IDEM: "Identity management (IDM) refers to the definition, designation and administration of identity attributes and the management of access to and the usage of applications, services and resources. It includes the management of identity attributes by their owners ('user-side IDM')) and/or by those parties with whom the owners interact ('service-side IDM'). 3.47.1 Identity management system An identity management system (IMS) is a system that consists of the organizational and technical infrastructure used for the definition, designation and administration of identity attributes. 3.47.2 Federated identity management The term federated identity management is used to refer to a setting in which rules are established or agreements are made with regards to the creation and management of (partial) identities within the federation. Such a framework generally incorporates several identity management systems that are run by distinct organizations, who have subsequently reached an agreement on how to exchange entity information among each other. These organizations are said to form a circle of trust." (Based on [MODINIS IDM 2005], p. 11-12, [LEENES 2006a], p. 12, http://en.wikipedia.org/wiki/ Identity_management and[ISO WD 24760], p. 8		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment** [2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
				(concerning 'federated identity').		
[FIDIS] 20	P43 Identity registration	Middle of page		We have been developing the following definition of registration: "Registration is the process of collecting and corroborating a specific set of attributes of an entity, which typically relate to the partial identity (e.g., the age), a characteristic or a mandate of that entity, with sufficient certainty, before putting at the disposal means by which the entity can be authenticated, or the characteristic or mandate can be verified." (Based on [MODINIS IDM 2005] and [ROBBEN 2005b], slide 5.)		
[FIDIS] 21	P44 Non-repudiation	Bottom of page	Ge	We have been developing the following definitions: "Non-repudiation refers to the concept of ensuring that a commitment or action cannot later be denied by one of the entities involved. 3.61.1 Non-repudiation of origin Non-repudiation of origin protects against any attempts by an acting entity to deny having sent a message or having performed a particular action. 3.61.2 Non-repudiation of delivery Non-repudiation of delivery protects against any attempt by the recipient to deny or falsely having received a message." (Based on [MODINIS IDM 2005], p. 12 and http://www.esat.kuleuven.ac.be/cosic/intro/#intro)		
[FIDIS] 22	P45 Object	Top of page	Ge	We have been developing the following definition: "An object is a non-acting entity that contains or receives data or information, to which access is controlled. An		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment** [2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
				object is for example a file, a program, a document, an area of main storage (such as a database)." (Based on Based on ISO/TC 215/WG 4 Glossary, which refers to the ISO Standard ISO/IEC 2382-08 on Information processing systems (Part 08: Control, integrity and security).		
[FIDIS] 23	P46 Policy	Top of page	Ge	We have been developing the following definitions: "Policy A policy is one or more definite goals, courses or methods of action to guide and determine present and future decisions. Policies are implemented or executed within a particular context (such as policies defined within an organization or business unit) or across contexts (e.g., in the case of an identity federation). Common examples of such policies are security policies, privacy policies, access control policies, registration policies etc. 3.75.1 Policy rule A policy rule is a set of actions to a set of conditions, where the conditions are evaluated to determine whether the actions may be performed. 3.75.2 Policy condition A policy condition is a representation of the necessary state and/or prerequisites that define whether a policy rule's action should be performed. 3.75.3 Policy action A policy action is the definition of what is to be done to enforce a policy rule when the conditions of the rule are met. A policy action can therefore also be considered as the result of policy enforcement. See also policy enforcement point.		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
				3.75.4 Access control policy An access control policy is the set of rules that define the conditions under which an access may take place. It is a set of rules to administer, manage, and control access to network resources. 3.75.5 Privacy Policy A privacy policy is a policy which is based mainly data protection and privacy considerations It may specify, among others, what personal data is being collected, for what purpose the collected personal data is being used, how long the data is being retained, how a person may access and correct data relating to him/her, how and whether a person can opt-put; and what security measures are being taken by the entities that process and/or control the data. 3.75.6 Security Policy A security policy is a set of rules and practices that specify (or determine) how a system or organization should protect (or protects) data exchange, data storage, sensitive and/or critical system resources, and the use and provision of security services and facilities." (Based on [WESTERINEN 2001], [ITU-T 2005], p. 3, referring to the X.812 recommendation. Based on [IDABC 2002], p. 15 and [SHIREY 2000], p. 101.)		
[FIDIS] 24	P46 Privacy	Middle of the page		Comments with regard to privacy definition: (based on FIDIS and IDEM workshops/discussions): "3.77 Privacy The term privacy is a term that is used in a generic way and therefore not susceptible to exhaustive definition. It is mainly used in reference to the following concepts:		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
				3.77.1 The (fundamental) right to privacy The right to privacy is understood as the (relative) fundamental right of a natural person to respect for his private and family life, his home and his correspondence. 3.77.2 Informational privacy In the information society, privacy is often understood as the right of a natural person to decide for itself when and on what terms its attributes should be revealed. 3.77.3 Privacy enhanced identity management system (PE-IDM system) An IMS has been said to be 'privacy enhanced' if the user is empowered to decide on the release of personal data and on the degree of linkage or linkability to/among his or her personal data within the boundaries of legal regulations. The more recent approach(es) no longer seems to imply user control, stating that an IMS is privacy enhanced if it, given the restrictions of a set of applications, sufficiently preserves unlinkability (as seen by an attacker) between the partial identities and corresponding pseudonyms of a natural person (Based on Article 8 ECHR, PRIME D14.1.A], p. 28, [MODINS IDM 2005], p. 14, [APES], p.10, [PFITZMANN 2006], p. 23, footnote 68 and [PFITZMANN 2007], p. 31.)		
[FIDIS] 25	P46-47 Privacy policy	Bottom – top of page	Ge	Cf. supra ("Privacy Policy A privacy policy is a policy which is based mainly data		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
				protection and privacy considerations It may specify, among others, what personal data is being collected, for what purpose the collected personal data is being used, how long the data is being retained, how a person may access and correct data relating to him/her, how and whether a person can opt-put; and what security measures are being taken by the entities that process and/or control the data.)		
[FIDIS] 26	P47 Provisioning	Towards bottom of page	ge	We have been developing the following definitions with regards to provisioning: 3.80 Provisioning Provisioning can be defined as the automation of all the steps required to manage (setup, amend and revoke) user or system access entitlements. 3.80.1 Resource provisioning Resource (or user) provisioning is the process of providing users with access to the (computing and non-computing) resources they are authorized to use. 3.80.2 Resource de-provisioning Resource de-provisioning (or decommissioning) is the process of the termination of the access rights to resources, and their (possible) reallocation. 3.80.3 Account provisioning Account provisioning is the process of providing entities with accounts, the appropriate access to those accounts, all the rights associated with those accounts, and all of the resources necessary to manage the accounts. 3.80.4 Account de-provisioning		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
				Account de-provisioning (or decommissioning) is the process of the termination of the access rights to accounts, and their (possible) reallocation.		
[FIDIS] 27	P47 Pseudonym	Bottom of page		We have been developing the following definitions: 3.81 Pseudonym A pseudonym is an identifier of identifiable entity, that is (1) either self-chosen by this entity or (2) or assigned by a provider, to identify this entity to a relying party for a period of time. 3.81.1 Persistent Pseudonym A persistent pseudonym is a pseudonym used for an extended period of time that spans multiple sessions. 3.81.2 Transient Pseudonym A transient pseudonym is a pseudonym used for a relatively short period of time that need not span multiple sessions. 3.81.3 Person Pseudonym A person pseudonym is pseudonym or identifier that serves as a substitute for the holder's name, which is regarded as the representation for the holder's (civil) identity. It may be used in multiple, if not all contexts, e.g. a number of an identity card, the social security number, the Belgian National Registry Number, a nickname etc. 3.81.4 Role Pseudonym A role pseudonym (or role identifier) is a pseudonym that is limited to specific roles, such as a customer pseudonym or an internet user name. It can be an assigned or a chosen identity. 3.81.5 Relationship Pseudonym		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
				A relationship pseudonym means that for each communication partner a different relationship pseudonym is used, but the same relationship pseudonym could be used in different roles for communicating with the same partner (e.g., nicknames). 3.81.6 Role-Relationship Pseudonym A role-relationship pseudonym means that for each role and for each communication partner, a different role-relationship pseudonym is used. The communication partner does not necessarily know, whether two pseudonyms used in different roles belong to the same holder. Two different communication partners who interact with a user in the same role do not know from the pseudonym alone whether it is the same user. 3.81.7 Transaction Pseudonym A transaction pseudonym is a pseudonym that is used for only one transaction. It is unlinkable to any other transaction pseudonyms and is (at least initially) unlinkable to any other item of interest (e.g., randomly generated transaction numbers for online-banking). 3.81.8 Sector-specific pseudonym A sector-specific pseudonym (or 'sector-specific identifier') is an identifier that has only meaning to the communication partners within a specific sector. 3.81.9 Context -specific pseudonym A context-specific pseudonym (or 'context-specific identifier') is an identifier that has only meaning to the communication partners within a specific context.		
[FIDIS] 28	P48 Relying	Bottom of page		We have been developing following definition:	See in particular meaning iii.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
Liaison [1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment** [2]	**Comment (justification for change) by the Liaison**	**Proposed change by the Liaison**	**Resolution on each comment**
	party			3.86 Relying party A relying party is used to refer to an entity which trusts the results of an authentication protocol to establish the identity or an attribute of an entity; e.g. for the purpose of enabling subsequent transactions. (Based on [IDA Authentication 2004], p. 14.)		
[FIDIS] 29	P49 Role	Towards bottom of page		We have been developing the following definition: "A role encapsulates the organizational functions/duties of an entity, while removing the direct link between the authorizations and the entity itself. It is group of authorizations (or authorization groups) related to a specific service." (Based on [YAGÜE 2005], slide 29 and [ROBBEN 2005b], slide 8.)		
[FIDIS] 30	P49 Security domain			We have been developing the following definition: "A security domain is an environment that is defined by security models and a security architecture, incorporating a set of resources and set of system entities that are authorized to access some or all of the resources. The traits defining a given security domain typically evolve over time." (Based on [HODGES 2005], p.10) See definition of context.		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

ISO/IEC JTC 1/SC 27 N6503

ISO/IEC JTC 1/SC 27/WG 5 N56503

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: liaison statement

TITLE: Liaison Statement from FIDIS to JTC 1/SC27/WG 5 in response to SC 27 N6264

SOURCE: FIDIS Liaison Officer (H. Hedbom)

DATE: 2008-03-01

PROJECT: 24760
29100

STATUS: This document is circulated for review and response by the 5th SC 27/WG 5 meeting in Kyoto (Japan), 14th – 18th April 2008.

ACTION ID: **ACT**

DUE DATE:

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-chair
E. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 1 + 14 (Attachment 1) + 14 (Attachment 2)

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

FIDIS

Future of Identity in the Information Society

FIDIS liaison statement to SC 27/WG 5 containing comments on the 4th WD of Project 1.27.50 (24760) "A framework for identity management" and on the 3rd WD of Project 1.27.54 (29100) "Privacy framework".

FIDIS would like to thank ISO/IEC JTC 1/SC 27/WG 5 for its liaison statement from February 2008 and for the consideration of the FIDIS comments for the liaison statement to ITU-T SG 17 on ITU-T SG 17 Focus Group on Identity Management's draft reports and the updated documents received.

FIDIS would also like to thank ISO/IEC JTC 1/SC 27/WG 5 for the nomination of Hans Hedbom as acting liaison officer from ISO/IEC JTC 1/SC 27/WG 5 to FIDIS.

FIDIS attaches comments on the 4th WD of Project 1.27.50 (24760) "A framework for identity management" and on the 3rd WD of Project 1.27.54 (29100) "Privacy framework".

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 1	General		Te	Although much reference is made to concepts identity federation, "the" identity, partial identities, entity profile etc which can span multiple contexts/domains, certain sections and definitions seem to be describe these terms from the point of view of 1 organisation and their meaning within the internal IMS of the organisation (in particular due to the exhaustively of e.g. "identity" and "entity profile") (→ "monolithic" view of identity). In 5.10, a more nuanced view is given which maps more with our understanding of these terms. See also e.g. p.18 section 5.7 when describing entity profile: although this term was originally defined rather exhaustively in 3.29 ("A list of all identity attributes associated with an entity and the location of the authentic source for the value of each attribute"), section 5.7 leads the reader to believe that there may be different entity profiles for different partial identities (and this is quite right from a normative point of view, when considering that a context may span multiple domains of applicability and therefore the entity profile need not necessarily be exhaustive in every domain, particularly when taking into account e.g. data minimization). Either definition of entity profile should be qualified as 'in a particular context or domain of applicability' or as relating to a partial identity of that entity (compare e.g. with 5.12 at bottom of p. 21-22 pdf). Although we do not embrace an "exhaustive" view on the notion of identity within FIDIS (we define "the" identity as a		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				"fluid" concept and consider each representation in a particular IMS or subsystem as a partial identity), we can appreciate that it might be important for conceptual clarity in an international standard to be able to refer to both partial identities and the identity as such (the latter which is understood to cover all attributes of an entity at a given time). However, at many points, e.g. in the discussion of context prerogatives and domains of applicability (5.8), 24760 still refers to "the identity" (as an exhaustive and/or monolithic concept, covering all attributes of an entity) where in fact we believe it should refer to partial identities, as they are well elaborated under 5.10.		
FIDIS 2	General		Te	There is a lot of confusion/overlap/contradiction between identifier and identity reference as currently defined (compare e.g. respective definitions and 5.4 with 6.3 and also the text in section 9)	The use of identifier and identity reference needs to be made consistent throughout the document.	
FIDIS 3 [	3.4 Source of authentic informatio n p10	Top	Ed	Grammar	Replace "a recognized point where authentic information originates" By "a recognized point from which authentic information originates"	
FIDIS 4	3.5 Authorizat ion	Top	Ed	Authorization goes beyond mere access control. We have been developing the following definition of authorization: "Authorization is the process of determining the	Replace "process of granting permissions to an entity to access a resource based on resource policy rules"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
	p10			permissions of an entity, through the evaluation of applicable policies, to perform a defined action on a controlled or protected resource."	By "process of determining the permissions of an entity, through the evaluation of applicable policies, to perform a defined action on a controlled or protected resource."	
FIDIS 5	3.6 Context P10	Top	Ed		Replace "help to fix" By "determine" or "contribute to"	
FIDIS 6	3.11 Identification P11	Top		24760: "process of an entity providing evidence to a level of confidence to an identity authority that this entity can be recognized within some context with unique identity references and/or any additional information that characterizes the entity" → this sounds like identity proofing / enrolment / registration process The term "identification" is used in various ways in IDM literature: • identification in terms of identity proofing / registration / enrolment: identification as the process of using claimed, observed or assigned attributes of an entity to establish a partial identity of that entity ; • identification as entity authentication: identification as the verification of the link between an entity and the asserted (partial) identity ; • identification in terms of identifiability: identification as the process of "individualizing" a		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				particular entity within a set of subjects . If 24760 limits “identification” the way it has in its definition 3.11, it imposes upon itself a most significant restriction for the duration of the document. We would suggest either revising this definition (allowing it to incorporate multiple settings in which “identification” in fact takes place), or adding additional terms such as identity proofing in order to avoid so unduly restricting the meaning of this fundamental term. See also FIDIS 23		
FIDIS 7	3.12 identifier		Te	In the definition (3.9), an entity can be an object. We totally agree. Therefore, an entity can be in particular "an object that is used by an entity" as in definition 3.12. We believe that the concepts of "identifier" and "identity reference" are both identifying information. Both concepts are of the same nature; their difference is according to their direct or indirect aspects. In particular, we believe that an "identifier" is an "identity reference" of the object used by the entity. In other words, "identifier" is a special type of "identity reference" (as long as we accept that "identity reference" can refer to an entity that is an object). In the definition of "identifier", the indirection is very similar to the one instaured by a pseudonym. From what precedes, we propose that: Definition 3.12 essentially becomes the definition of the concept of "pseudo-identifier" Definition 3.22 becomes the definition of "identifier"	Change: "an object that is used by an entity" To: "an entity used by another entity" replace **3.12** by **Pseudo-identifier** A pseudo-identifier, for an entity, is the identifier of an object used by this entity and representing this entity within a specific domain or process; the purpose of a pseudo-identifier is to provide entities with means of representation independent of the entity's identity in a given context without necessarily revealing the entity's identity; the validity of the pseudo-identifier is limited to the object life cycle	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				(which is now equivalent to "Identity reference")		
FIDIS 8	3.13 Identity	Middle	Ed Ed	Definition is too “static”; needs to take into account fluctuation / evolutive nature of identity (see also later comments wrt “identity” and “partial identity”)	Insert “the total (and possibly dynamic) …” or Add: “… at a given moment” Replace: “… that provides recognition to the entity in that specific context” By “… that characterize the entity in that specific context” Or “… that are associated with the entity in that specific context”	
FIDIS 9	3.29 (entity) profile p13		Ge	Why normative statement (“and the location of the authentic source for the value of each attribute”). Although this may very well be desirable from an accountability and data accuracy perspective (and thus also from a privacy perspective). Why is profile defined as something exhaustive? (“list of all identity attributes” See general comment [FIDIS 1]		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 10	5.2 The notion of identity	Middle	Ge	"The identity of an entity materializes the uniqueness of that entity in a specific context." Not even partial identities necessarily imply uniqueness it's the presence of an identity reference that makes the identity unique	Consider revising.	
FIDIS 11	5.4 Identifier and identity reference P16 3rd sentence	Middle	Ed	Typo/grammar	Replace "one must recognized that there are managed" By "one must **recognize** that **they** are managed"	
FIDIS 12	5.4 Identifier and identity reference P16	Middle	Ge	24760: "As an example, a system account identifier may use as alias a person's identity information contained in the person's identity card and use the associated credential. The state authority may then decide to change the person's identity reference or the associated credential and the person will not be able to access the system account until the authority has provided another set of identity information. This example is one good reason why another domain's identifier should not be used in a different domain. Another reason is that an individuals privacy is exposed as information applicable to one domain is used in another." Comments:		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				This section tackles issues such as unwanted re-registration and data accuracy problems. It however incorporates many different interests at once, which might seem competing at first, and is somewhat confusing due to ways in which terms such as 'identifier', 'alias' and 'identity reference' are used. On the one hand this section seems to advocate "stability" in identifier usage, both internally for account management purposes (allocating) as well as in external interactions. → Section switches from normative to descriptive, which makes it difficult to understand. It might therefore benefit from a rewrite or some additional insertions, such as ("in practice …" or "should" or …) → the term alias is not defined (it seems to be used either as initial identification mechanism or as IR prior to conversion to / association with identifier) → Perhaps IR should be plural here		
FIDIS 13	5.5 Identity and identification p16	Middle	Ge	This section demonstrates overlap between definition of identifier and identity reference Preceding sections allow us to believe that when assigned for later identification / authentication or account management purposes, 24760 speaks of an identity reference (IR's are generally thus used for identification/authentication of "active" entities); Whereas the identifier is reserved for objects under 24760.	-Remove typo ("identification refers is	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				Last sentence of this paragraph: "Identification refers is based on data that help in recognizing and discriminating the entity from another within a particular context. This information may be based on the biological characteristics of a human being (such as fingerprints or blood type), or a person's biographical history (date of birth or name of spouse), or an assigned unique identifier such as a vehicle identification number or company registration number, or any other useful distinguishing characteristic(s). The set of attributed used in a particular context will depend on the group of entities that need to be distinguished within that context." This makes clear that identifiers are still attributes (or at least can be) Compare last sentence 3rd paragraph of 5.4 (Identity and identity reference) "If the IT account identifier represents a unique entity on the system it can be used for accountability and traceability purposes, *but is not an attribute of this entity*." See also cryptographic keys as possible attribute of an entity. This should be further clarified. (either in 5.4 or in 5.5)	based on …") -replace "discriminating" by "distinguishing"	
FIDIS 14	5.6 The multiple facets of an entity	Middle	Ge	Identity and identification provide legitimacy for being recognized for acting in the context because the entity is legitimately present as a result of the proven affiliation to the group (country, company, social group).	Replace "Identity and identification provide legitimacy for being recognized for acting in the context because the entity is legitimately present as a result of the	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
	in different contexts P17			--> Mixture of normative and descriptive. → mixes of authorization and identification (even proposed changed might merit further revision along those lines: affiliation to a group is generally a criterion when applying a policy (e.g. access control) and is also constitutive of the entity's identity. However, authorization is not granted based on the "mere" identity of an entity as such, but rather based on the authorization policy and the finding that this entity displays the prerequisite attributes. (the "because" is particularly ambiguous here) See also FIDIS 16	proven affiliation to the group (country, company, social group)." By something along the lines of "Identity and identification provide a means for the entity to be recognized as acting in a context or domain because the entity's identity is generally established within a context or as a result of the proven affiliation to the group (country, company, social group)."	
FIDIS 15	5.7			-1st sentence of second paragraph could be formulated more clearly -typo 2nd sentence third paragraph	Replace "Entities are characterized by a number of attributes that describe them over time." By "Entities are characterized by a number of attributes that can by used to describe them over time." Replace by "Each of these attribute sets or profiles represent a different (or partial) identity of the entity and may **include** attributes such as …"	
FIDIS 16	5.8	Bottom	Ge	"An entity must be recognized with a valid membership of		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
	context prerogatives and domains of applicability p17			the context that legitimates that entity to conduct activities in the context community” This section serves to emphasize fact that an entity needs to be reliably identifiable and must be able to be authenticated as a prerequisite to allow the entity to perform a certain action in accordance with the applicable policy rules It also hints to the fact that it is not so much identity as such, but rather certain attributes of an entity (e.g. qualification of doctor or other proofs of competence) that determine the permissions of an entity in light of the applicable policy rules. Mere recognition of an entity (i.e. providing it with a means to identify itself) does not necessarily imply any permission to perform an action, thus the term ‘legitimates” is confusing. It is correct to the extent that a certain attribute which is shared by other entities (e.g. qualification of being a doctor) may be a determinative criterion when allowing an action to take place. It is however misleading to the extent that it suggests that mere membership of a group determines this, where it is in fact the outcome of the applicable policy rule.		
FIDIS 17	5.8 context prerogatives and domains	Top	Ge	24760: “The entity possesses an identity provided by the context that will be recognized and trusted in all the domains of applicability of the context.”	Replace “The entity possesses an identity provided by the context that will be recognized and trusted in all the	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
	of applicability p18			We believe that what is trying to be elaborated is: A certain ("digital") identity (i.e. and identity according to 3.13) is associated with an entity in a particular context. A particular digital identity (and particularly the associated identifiers) generally only has meaning within a context. It is however not the context as such leads to the result that certain identifiers, identity references, (other) attributes etc. are associated with an entity but rather: -a particular identity authority or other service provider assigns an identifier or identity reference and associates certain attributes with this entity's account; (the identity can of course also be self-asserted if the IMS allows it) - this digital identity might (as a matter of fact) be relevant outside of 1 particular enterprise or subsystem, which leads to the situation that this digital identity is recognized by other entities (e.g. other service providers, all together forming the "domain of applicability" of that (*partial*) identity) Therefore it is not the context as such which "provides" the identity, but rather any IdP within that context to the extent that this IdP is trusted and recognized by other actors in the context [or rather: for each domain of applicability within the context; see below]. The context is determinative, but not constitutive of the identity (see also second paragraph on p18) Furthermore, a context spans multiple domains of applicability. See also definition 3.27 of a partial identity – therefore the monolithic view of identity (1 identity – 1 context + one and the same identity that is recognized	domains of applicability of the context." By "The entity possesses an identity [according to 3.13] which is determined by the context in which it has been established. This identity will be recognized and trusted among one or more domains of applicability of the context"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				and trusted among all the domains of applicability) as implied here is contradictory. We therefore believe that this sentence would be more clear and more accurate if it were to read as follows: "The entity possesses an identity [according to 3.13] which is determined by the context in which it has been established and will be recognized among one or more domains of applicability of the context"		
FIDIS 18	5.8 context prerogatives and domains of applicability p18	Top	Ge/ed	"Each identity in each domain of applicability is …" We believe that according 3.27 (i.e. partial identity as "one attribute or a combination of attributes of an entity that are meaningful in a specific domain of applicability …") what you are seeking to refer to in fact is a partial identity rather than just an identity "full stop" (comp. exhaustive nature of identity in 3.13) The following section might also need a further rewrite: "A social security agency or a plate registration agency will benefit from a notional of federal notional registry authority and not being forced to verify the entity identity." -typo national / notional -"and not be forced to verify the entity identity": compare definition of (entity/identity) authentication 3.3: during authentication protocol or in an offline environment these entities (SS agency or plate RA) might still need to "verify" the identity of an entity when the entity is asserting it, even though it has been registered / enrolled in a national	Replace "Each identity in each domain of applicability is …" By "Each partial identity in each domain of applicability is … " Rewrite: "A social security agency or a plate registration agency will benefit from a notional of federal notional registry authority and not being forced to verify the entity identity."	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				registry. The benefit these entities might enjoy however, is that they do not have to go through the identification process in the meaning of identification as currently defined in 3.11. The subsequent sentence demonstrates this: "The identity of an entity in each domain of applicability may be, in return, combined to reduce further the effort of identification" – which we believe is correct under your current definition of identification. Last sentence second paragraph on p18: "Identity and identification apply therefore to a network of domains of applicability within one context. All of these domains are federated within a single identification scheme. The entity is legitimate in all domains of applicability of a context by the identity acquired at that context level." → assimilation context with a Network / Circle of Trust? → however, even in a CoT there are different partial identities and not necessarily 1 (monolithic) identity.		
FIDIS 19	5.9.1-5.9.3 Authorities and federation of authorities p19-20		Ge	"Identity federation is a relationship established between identity authorities." Identity authority is not defined. Many reports however refer to "identity providers" (IdP's) in general. The term "identity authority" might however be useful to refer to identity brokers, or the those IdPs that are considered (trusted) to manage the authentic data repositories on identity information. If identity authority is meant as an IdP performing these		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				types of roles, there is no issue with the text in 5.9.1. 5.9.3 however hints to the fact that "identity authorities" also cover IdPs that do not (yet) have this special status (see e.g. "Identity authorities in a federation are usually requesting to be recognized and trusted by each other before communicating")		
FIDIS 20	5.9.3 p20	Last sentence (under figure)	Ed		Replace "truth relations" By "trust relations" or "trust relationships"	
FIDIS 21	5.11 P21	Middle	Ge	"Identity Management solutions must implement consistent controls in relation with applicable laws, regulations and principles. Specifically, Identity Management solutions require minimum common controls of: □ the manner in which attributes of an entity are passed from entities in one context to entities in another context □ the manner in which an entity may have the ability to infer attributes of another entity (for example, based on knowledge of attributes and identities in other contexts)." → Comment: Identifiers and identity references deserve explicitly mentioning here (seeing as in certain sections identifiers are considered not to be attributes of an entity in 24760 (see e.g. 3rd paragraph of 5.4 (Identity and identity reference:		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				"If the IT account identifier represents a unique entity on the system it can be used for accountability and traceability purposes, *but is not an attribute of this entity*.") Proper management of identifiers under this meaning is also essential both to reduce certain privacy threats and to ensure data accuracy. Similar considerations apply to identity references.		
FIDIS 22	6. Identity managem ent		Ge	"Identity Management includes the accurate identification of entities in some context, and the secure, privacy aware and user centric management of information associated with that identification" We suggest to remove "user centric" because some people understand this as "user control". Although quite desirable from a privacy preserving point of view for certain applications, it should not be generalized as to be inherent in every type IdM. If by "user centric" the text simply means "taking into account (privacy) needs / preferences of the users", the comment is retracted (but would recommend including definition).	Simply drop "user centric"	
FIDIS 23	6.4 Identity authentic ation p26	Bottom	Ge	Recommend keeping clear conceptual (and terminological) distinction between identity proofing etc (what 24760 considers the identification process), and entity authentication during e.g. a authentication protocol.		
FIDIS 24	7.5 Identity managem	Last		"An IdMS provides: • A compliance control assurance for measure	Change: An IdMS provides:	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
	ent control objectives			such as data integrity control and • A guarantee of process accuracy when dealing with social security or medical records." This statement implies that an IdMS always will do this. However we believe that this is highly dependent on the design, administration and implementation of the system.	To: An IdMS should provide:	
FIDIS 25	9.1 Identity management and the information security policy	Last		"The preservation of third party entity's identity may also be required…." From both a security and a privacy perspective the protection of an entity's identity is equally (or even more) important as the preservation.	Change: "The preservation of third party entity's identity may also be required…." To: "The preservation and protection of third party entity's identity may also be required…."	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 26	3.2 Appropriation p9	Top of page	ge	Meaning? Definition should not use verb derived from term being defined.		
FIDIS 27	3.3 Data administrator p9	Middle	ed	Current definition data administrator: "entity that has the responsibility for processing data according to a pre-specified contractual arrangement such as a service level agreement, security policy or agreed upon procedures" ------- ➢ Use "charged with" instead of "has the responsibility": From a data protection perspective the data administrator is most likely to be acting under the authority of the legally responsible entity (i.e. controller). Although contractual arrangements will bind him (and thus also make him "responsible"), primary responsibility may fall on a different entity; who must seek recourse vis-à-vis the entities acting under his instructions). ➢ justification wrt "contractual *or other* arrangements: Certain obligations (policies, procedures to be followed) might be imposed unilaterally (e.g. through legislation) or not form part of an explicit contractual provision (e.g. standard industry practices) ➢ "… or agreed upon procedures" is not very eloquent	Replace text by: "entity charged with responsibility of processing data according to a pre-specified contractual or other arrangement, such as a service level agreement, a security policy or otherwise established policies"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				at end of this sentence + it in fact refers to policies.		
FIDIS 28	3.4 Data controller/ personal information controller p9	middle	ed	29100: “individual, entity, or enterprise who, according to local data protection and privacy legislation, controls the collection, transfer, modification, usage, storage, archiving, or disposal of personally identifiable information (PII)” Justification: -entity also comprises individuals and enterprises -possibility of multiple controllers needs to be accommodated	Replace by: “entity (or entities) considered responsible for the processing operation(s) according to the applicable legislation. Such qualification generally follows upon a finding that this entity controls the collection, transfer, modification, usage, storage, archiving, or disposal of personally identifiable information (PII)”	
FIDIS 29	3.5 3.6	Middle		Data owner is vague and ambiguous concept as it is used here. Data protection rights primarily relate to the manner in which certain information is being processed (in addition to rights of notification, objection etc). These claims of the data subject are generally not considered commodifiable (whereas property rights are). The definition of data owner might seem useful for purposes of user-controlled data processing, but is still misleading even in that context. It emphasizes that this is the “entity in control”, but this entity is still not necessarily the “owner” of the bits and bytes associated with the processing. Why not limit reference to controller, processor, data subject and third party. Less “european-centric” terms may of course be used, but we believe these roles should be reflected in the definitions, and that the standard should refrain from the use of the term “data		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				owner" (because it is misleading if the reader were to associate this with a property right; consider for instance also the intellectual property rights relating to databases → are much closer to concept of data "owner").		
FIDIS 30	3.7 Data processor P9	Middle	Ed Ed Ge	Current definition: "entity that processes personally identifiable data on behalf of the personal information controller and acts on privacy safeguarding requirements pre-specified in a contractual arrangement such as a service level agreement, security policy or agreed upon procedures" -move "controller" to before personal information -Replace end of definition by: "… or otherwise established policies" Request for clarification: is information treated synonymous with data? Some say that data becomes information once it has been interpreted. If there is no intended distinction, is it not advisable to always speak of PII for consistency? May also be advisable to explicitly clarify data vs. information in 29100 if different meanings are in fact intended.	"entity that processes personally identifiable data on behalf of the controller of the personal information controller and is obliged to implement the privacy requirements pre-specified in a contractual arrangement such as a service level agreement, security policy or otherwise established policies" Or (if there is no intended distinction data – information) "entity that processes PII on behalf of the controller and is obliged to implement the privacy requirements pre-specified in a contractual arrangement such as a service level agreement, security policy or otherwise established policies"	
FIDIS 31	3.8 Data subject	bottom	ed	Current definition: "individual whose personally identifiable data is collected, transferred, used, stored, archived, or disposed"	Replace by "Individual whose PII is being processed"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
	P9			-there should be no limit on types of processing operations in order to qualify as data subject (note: processing is not defined in 29100) -consistency wrt PII NOTE: comment only applies to the extent that personally identifiable *information* is in fact considered as synonymous with personally identifiable *data*.		
FIDIS 32	3.13 Identifier p10	Top	Ge	Current definition "reference to a unique object used to uniquely represent and identify an entity within a specific domain or process" See comments to 24760 regarding identifier vs. identity reference. Is 29100 considered consistent with 24760 with regard to identifiers vs. identity references?		
FIDIS 33	3.14 Identity p10	Top	Ge	See comments to 24760.		
FIDIS 34	3.15 Linkability p10	Top	Ed	Input needed	"the extent to which two items of interest (typically sets of personal data) appear related upon observation without taking into account a priori knowledge." [Based on ANON's definition of unlinkability]	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 35	3.16 Observability p10	Middle	Ed	Input needed	"the extent to which one or more items of interest are detectable or distinguishable from other items of interest" [Based on ANON's definition of unobservability]	
FIDIS 36	3.18 Opt-out p10	Middle	Ge	"affirmative request" is questionable here. Opt-out implies that default is consent unless user explicitly indicates otherwise; but that possibility for not giving consent (i.e. "opting out") is provided		
FIDIS 37	3.19 PII P10	Bottom	Ge	See earlier comment [FIDIS 5-6] regarding data vs. information		
FIDIS 38	3.20 PII provider P10	Bottom	Ge	Data owner is vague and ambiguous concept as it is used here. See FIDIS 4.		
FIDIS 39	3.21 PII receiver p11	Bottom	Ge/ed	29100 states "individual person, entity, enterprise, application provider, data controller, data administrator, or data collector who is receiving PII from the PII provider" -"Data processor" should be added to the list of possible PII receivers.	"an entity, such as a service provider, data controller, data administrator, or data processor who acquires PII from another entity"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				-All enumerated types of recipients fall under notion of entity -verb "receive" in definition of "receiver" should be avoided -seeing definition of PII provider (i.e. data subject), this definition does not accommodate possibility that entity might be receiving data from an entity other than directly from the data subject (e.g. in a federation).		
FIDIS 40	3.28 Privacy violation p11	Bottom	Ed	29100: "situation when personally identifiable data on an individual is collected, transferred, modified, used, stored, archived, or disposed without having the permission to do so according to applicable local data protection and privacy laws or according to policies set up by an enterprise -margin for simplification -NOTE: this definition assimilates privacy and data protection. Is this intended?	"event where PII processed in violation of the applicable data protection and privacy laws or otherwise established policies relating to PII"	
FIDIS 41	3.29 Profile p11	Bottom	Ge	Not entirely clear whether this definition is intended refer to noun, verb, or process?		
FIDIS 42	3.30 Pseudonym	Bottom	Ed	We have developed the following definition of a pseudonym: "A pseudonym is an identifier that is either self-chosen or	Replace definition by: "A pseudonym is an identifier that is either self-chosen or assigned, to	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
	P11 P12 P12		 Ge Ge	assigned, to identify that entity to one or more relying parties within a context or sector." Wrt 1st NOTE: Although etymologically correct, connotation pseudo = false should be avoided – this should be clarified as such Possible replacement for 2nd NOTE: "NOTE: Under certain conditions, pseudonyms (and identifiers in general) can be managed to improve privacy features of an IMS, in which case it is typically being used to reduce the linkability." REMARK: this comment does not take into account the discussion with regards to identity references – identifiers in 24760. The term "pseudonym" as it is used here by FIDIS maps primarily with what 24760 currently defines as identity references.	identify that entity to one or more relying parties within a context or sector."	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

ISO/IEC JTC 1/SC 27 **N7060**

ISO/IEC JTC 1/SC 27/WG 5 **N57060**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	liaison statement (defined)
TITLE:	FIDIS' liaison statement to ISO/IEC JTC 1/SC 27/WG 5 in response to SC 27 N6742
SOURCE:	FIDIS Liaison Officer (H. Hedbom)
DATE:	2008-09-29
PROJECT:	24760 29100 29101 29115
STATUS:	This document is being circulated for consideration at the 6th SC 27/WG 5 meeting in Limassol (Cyprus) 6th – 10th October 2008.
ACTION ID:	**ACT**
DUE DATE:	
DISTRIBUTION:	P-, O- and L-Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice-Chair E. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners
MEDIUM:	Livelink-server
NO. OF PAGES:	1 + 1 + 5 (Attachment 1) + 2 (Attachment 2) + 2 (Attachment 3) + 1 (Attachment 4)

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

FIDIS

Future of Identity in the Information Society

FIDIS liaison statement to SC 27/WG 5 containing comments on the 5th WD of Project 1.27.50 (24760) "A framework for identity management", on the 4th WD of Project 1.27.54 (29100) "Privacy framework", on the 3rd WD of Project 29115 “Entity authentication assurance” and on the 2nd WD of Project 1.27.55(29101).

FIDIS would like to thank ISO/IEC JTC 1/SC 27/WG 5 for its liaison statement from August 2008 and for the consideration of the FIDIS comments for the ISO/IEC JTC 1/SC 27/WG 5 liaison statement to ITU-T FIDIS attaches detailed comments on the X.idmreq document from ITU-T SG 17.

FIDIS attaches comments on the 5th WD of Project 1.27.50 (24760) "A framework for identity management", on the 4th WD of Project 1.27.54 (29100) "Privacy framework", on the 3rd WD of Project 29115 “Entity authentication assurance” and on the 2nd WD of Project 1.27.55(29101).

Attachment 1 to SC 27 N7060

[FIDIS] comments on ISO/IEC 5th WD 24760

Date: 2008-09-29	Document: **SC 27 N6730**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 1	5.4	First paragraph	Ed	Misspelled word	Change: "An entity has one identity in any particular context but may have several identity references (IR) that identities that entity within this context." To: "An entity has one identity in any particular context but may have several identity references (IR) that identitifies that entity within this context."	
FIDIS 2	5.5	Fourth paragraph	Ed	The sentence :" The assignment of the unique identifier may be by an identity manager or generator through or not the identity authority." seems strange.	Consider revising the sentence.	
FIDIS 3	5.9.2		Te	Relying party is not defined.	Consider defining relying party	
FIDIS 4	5.9.2	Third paragraph	Te	The section is highly looked into the Requester<->RP, RP<->IdP communication pattern and thus the requester is totally excluded from the RP<-> IdP loop. There should at least be some discussions on alternative data flows that are more privacy friendly like a IdP<->Requester<->RP dataflow and also to make the Requester and the IdP the natural points for discovery mechanisms rather than the RP.	Consider revising the section	
FIDIS 5	5.11	Figure 5	Te	According to the definitions in chapter 5 the term IT Account Identifier is incorrect either it is an IT Account Identity Reference or an IT Entity Identifier.	Change the picture to be consistent.	
FIDIS 6	6.2	Last	Te	There seems to be one party missing in the sentence	Change the sentence to the following:	

Attachment 1 to SC 27 N7060

[FIDIS] comments on ISO/IEC 5th WD 24760

Date: 2008-09-29	Document: **SC 27 N6730**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
		paragraph		"Identity management is relevant in all situations where information or service delivery depends on the identity of the accessing entity and is a prerequisite for holding users and identity authorities accountable for their actions.	"Identity management is relevant in all situations where information or service delivery depends on the identity of the accessing entity and is a prerequisite for holding users, service providers, and identity authorities accountable for their actions.	
FIDIS 7	6.3.5	Third paragraph	Ed	This paragraph seems to be missing something. Its construction is rather strange and it ends quite abruptly.	Consider revising the paragraph	
FIDIS 8	7.2	First paragraph	Ed	Strange choice of word in the first sentence. We do not consider privacy to be a peculiar aspect possibly a specific or particular.	Consider revising the sentences.	
FIDIS 9	7.3.2	Fourth bullet point	Te	There might also be limits in how much information that is allowed to be used and there might also be the question on the purpose for using the identity.	Change: "in which situations and for which processes is identity information needed and how much information has to be presented" To: "in which situations and for which processes and purposes is identity information needed and how much information has to or is allowed to be presented"	
FIDIS 10	7.3.2	Fifth bullet point	Te	There might also be the question on the purpose when acepting the identity.	Change: "in which situations and for which processes and an identity is accepted" To:	

Attachment 1 to SC 27 N7060
[FIDIS] comments on ISO/IEC 5th WD 24760

Date: 2008-09-29	Document: **SC 27 N6730**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
					"in which situations and for which processes and purposes an identity is accepted"	
FIDIS 11	7.4.10		Te	This section takes the view one entity one and only one identity references. This might be true in specific circumstances but is generally not desireable both from a privacy and division of role perspective. It furthermore contradicts section 5 and section 8 where it is stated that an entity can have multiple identity references within a context or domain of application. The section also introduces the organisation as a context instead of using the general terms DoA and context.	Consider revising the section	
FIDIS 12	7.4.15	Last bullet point	Te	Same general comments as in FIDIS 4	See FIDIS 4	
FIDIS 13	7.5	Third paragraph	Te	This section discusses control criteria based on risk assessment. However, we are missing the mentioning of Privacy Impact Assessment in this context.	Consider revising the paragraph	
FIDIS 14	9.3.3.3		Te	Inconsistent use of identifier.	Change: "The IT account is specific to each system and is associated to an identifier that uniquely identify the IT account on the accessed system." To: "The IT account is specific to each system and is associated to an identity reference that uniquely identify the IT account on the accessed system."	

Attachment 1 to SC 27 N7060
[FIDIS] comments on ISO/IEC 5th WD 24760

Date: 2008-09-29	Document: **SC 27 N6730**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
					Change: "As IT accounts are usually own by single entities IT account identifiers may therefore be considered as a pseudonym of an entity's identity within the context of an information system." To: "As IT accounts are usually own by single entities IT account identity references may therefore be considered as an identifier of an entity's identity within the context of an information system."	
FIDIS 15	9.4.3		Te	This section seems to mix identity references and identifiers under the term identifiers.	Consider revising for consistency reasons.	
FIDIS 16	9.4.4		Te	This section only presents a limited view of pseudonyms among others it states that they where originally used for likability which might very well be true, however, their main use in PETs today is for unlinkability reasons. It also mentions that pseudonyms where no re-identification is possible (e.g by one-way cryptography) generally creates anonymised data. This is only true if the anonymisation set is big enough and that all data tied to the pseudonym is anonymised (c.f. the discussion on anonymising services in 29101). Further one could mention the fact that data that is considered as PII is still PII under a pseudonym unless they are anonymised in many regulatory frameworks and according to 24760 definition	Consider revising the section.	

Attachment 1 to SC 27 N7060
[FIDIS] comments on ISO/IEC 5th WD 24760

Date: 2008-09-29	Document: **SC 27 N6730**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				of PII.		
FIDIS 17	9.5.1		Te	Inconsistent use of identifier	Change: "IT Account identifiers are associated with credentials provided to users to prove they can use this IT account when accessing a resource on an information system. The authentication process validates the pairs IT account identifier - credential, called sets of authentication means" To: "IT Account identity references are associated with credentials provided to users to prove they can use this IT account when accessing a resource on an information system. The authentication process validates the pairs IT account identity reference - credential, called sets of authentication means"	

Attachment 2 to SC 27 N7060

[FIDIS[1]] comments on ISO/IEC 4th WD 29100

Date: 2008-09-29	Document: **SC 27 N6734**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 1	Whole document		ED	Most pictures have to low resolution and are fuzzy and therefore hard to read.	Include pictures of better quality	
FIDIS 2	Whole document		ED	The use of gender is inconsistent in the document. Some parts uses he and his others he/she and her/his.	Chose one version and make the document consistent.	
FIDIS 3	5.2	Table 1	TE	In the “other sensitive information” row Health status is mentioned as an example. In some regulatory framework Health status is always considered as medical or health information.	Move health status to the “Health Information” or make a double entry and make a foot note indicating that it could be considered as both.	
FIDIS 4	5.5.1.6	Bullet list	TE	Many regulations allow the withdrawal of consent and the following deletion of data. Therefore, we believe that, the user should have this ability as well.	Add a bullet point: d. provide the ability for the individual to withdraw his/her consent and/or delete his/her PII where such a function is not prohibited by legislation	
FIDIS 5	5.6.1	Last paragraph	TE	“When the consent given is based on a true understanding of the implications of the data processing, the consent would be called ‘informed consent’.” As far as we understand it the concept of informed consent encompasses three main requirements: 1. The existence of a true choice 2. The consent is freely given. 3. is based on a true understanding of the	Change the paragraph to : “When the consent is based on a true choice, freely given and is based on a true understanding of the implications of the data processing, the consent would be called ‘informed consent’.”	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				implications of the data processing,		
FIDIS 6	6.2	Bullet list	TE	Even if the list is just meant as an example we are missing tools for user transparency (or what in this document is referred to as user participation)	Add a bullet point with the following text: Tools to support transparency and user participation or that in other ways help the users to exercise their legal and/or contractual rights.	
FIDIS 7	6.6.4	Third paragraph	ED	There seems to be something wrong with this sentence: "Third parties often times have very critical roles in handling PII for an enterprise."	Change to: "Third parties many times have very critical roles in handling PII for an enterprise."	
FIDIS 8	A.2	Table 6	ED	The last paragraph under "IT Security Measures" in the Consent and choice row seems to be missing something.	Consider revising this paragraph.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N7060
[FIDIS[1]] comments on ISO/IEC 2nd WD 29101

Date: 2008-09-29	Document: **SC 27 N6736**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 1	5.2		Ge	Providing new text	This Reference Architecture addresses those challenges specific to the protection of PII. This encompasses supporting the privacy principles (cf. Table 2 in ISO/IEC 29100) such as transparency, accountability, purpose specification and collection limitation. The standard describes mechanisms builds a basis for compliance with the variety of national legislation in this field. As legislation differs this Reference Architecture uses a high protection scheme for PII, allowing for compliance with the multitude of legal requirements. The processing of PII often entails a trust problem for the principal of the information. In a specific context or for a specific purpose he or she understands that it is necessary to provide a set PII. Often the principal will have a high interest, that the information is used only within this context or for the specific purpose. Accordingly national and international legislation recognize this interest and as a general rule allow processing only within preassigned purposes. However, the principal often	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

3 Subject to the concurrent JTC 1 endorsement of the NWIP 27035 (see SC 27 N6430)

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
					has little to no control over the data once it is released. If the data is used beyond the purpose, there is little chance that he or she will even take notice.	
FIDIS 2	7.2		Ed	Proposition	We are proposing to add two new subsections to 7.2: 7.2.9 Privacy Enhanced Identity Management. 7.2.10 Transparency services	
FIDIS 3						

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

3 Subject to the concurrent JTC 1 endorsement of the NWIP 27035 (see SC 27 N6430)

Attachment 4 to SC 27 N7060

[FIDIS[1]] comments on ISO/IEC 3rd WD 29115

Date: 2008-09-29	Document: **SC27 N6728**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 1	6	First paragraph	Te	The sentence “The entity authentication assurance framework is a process for assessing "how close" an entity is to the claimed one throughout an identity's lifecycle.” does not make sence	Change the sentence to “The entity authentication assurance framework is a process for assessing "how close" an entities identity is to the claimed one throughout an identity's lifecycle.”	
FIDIS 2	9.12		Te	This section introduces biometrics as the overall solution to repudiation (and implicitly to authentication assurance). We believe that the description here is highly biased and do not discuss the drawbacks concerning privacy and safety risks as well as the legal considerations of using the technology as well as the current impreciseness and other drawbacks of the technology.	This paragraph should be revised.	
FIDIS 3	10		Ed	The whole section 10 seems to be a copy of section 8	Merge 10 and 8 into one section.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

ISO/IEC JTC 1/SC 27 N7374

ISO/IEC JTC 1/SC 27/WG 5 N57374

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: liaison organization contribution

TITLE: Late FIDIS comments received on SC 27 N7109 -- Revised text of ISO/IEC 5th WD 24760 -- Information technology -- Security techniques -- A framework for identity management

SOURCE: FIDIS Liaison Officer (H. Hedbom)

DATE: 2009-01-15

PROJECT: 24760

STATUS: This document has been sent to the relevant Project Co-editors for review and implementation when preparing the text for the 6th WD 24760 to be circulated as SC 27 N7237 for study and comment (according to WG 5 resolution 8 contained in SC 27 N7097rev1).

ACTION ID: **ACT**

DUE DATE:

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
E. J. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners
R. Garcia Ontoso, Ch. Sténuit, Project Co-editors

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 9

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-1723; E-mail: krystyna.passia@din.de
HTTP://www.jtc1sc27.din.de/en

ISO/IEC JTC 1/SC 27 N7379

[FIDIS[1]] comments on revised text of ISO/IEC 5th WD 24760

Date: 2009-01-07	Document: **SC 27 N7109**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS1	10.4.3.4	First para	Te	Terminology needs to be consistent throughout the document. Creating a whole new terminology for the IT account Identity makes it hard to follow and understand.	Replace text with: As for the identity, provisioning can be seen within a process and have a lifecycle as they are established and terminated. For instance, the IT accounts associated to an IT entity identity must be managed, as it is established, activated, sometimes suspended, and finally archived or deleted. The IT account which was terminated once is sometimes reused to another identity while it is usually unlikely that reuse may be permitted in most situations. In the case that reuse is not permitted, the IT account needs to be archived instead of terminated. Any provisioning is valid for a period of time has a start date and an end date related to the IT entity identity existence in the context. The provisioning associated an to an IT entity identity may persist after the IT entity identity ceases to exist	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
					e.g. when it is archived . In these cases identity information still needs to be managed for the account. The relevant states of an IT entity identity are : ▪ 'Not Established': an identity is not yet recognized in a context. ▪ 'Established': an identity is recognized in a context. ▪ 'Terminated' : an identity is no longer recognized in a context. The possible associated statuses of a provisioning (e.g., an IT account identity) are the following: ▪ ''Established' status: an IT account is just associated with an identity. ▪ 'Activated' status: an IT account is recognized as valid to identify an	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
					identity. It is also called as 'unlocked' status. ▪ 'Suspended' status (optional): an IT account is recognized as not valid to identify an identity. It is also called as 'locked' status. ▪ 'Archived' status (optional): an IT account is no longer associated with any IT entity identity but the record of the IT account may be required to remain available to determine whether or not the IT account has in the past been associated with a particular identity. ▪ 'Terminated' status: an IT account is deleted from IT account repository. The following figure is showing a status transition model indicating the status of IT account which is	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
					associated to an identity along with its lifecycle:	
FIDIS2	10.4.3.4	Figure	Te	See FIDIS 1	Replace with figure in Annex1	
FIDIS3	10.4.3.4	Second para	Te	See FIDIS 1	Replace text with: Initial provisioning facilitates the introduction of a new entity as actor of an organization. The possibility to activate an initial provisioning process will safe unnecessary waiting time required from the privilege provisioning process. The initial provisioning of privileges to entities requires the provisioning to the entity of an appropriated initial IT account and credentials for accessing the minimal required information services relevant to the business roles and functions of the job assignments. Initial provisioning process will usually take place before the business need. It can start once the identification process of the IT entity is	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
					successful and it is activated when the business need occurs. Subsequent provisioning will occur during the user existence to reflect the additional business needs of the entity in the context. All provisioning are tied to the existence of the entity and cease to exist when the entity quits. Provisioning may, however, have shorter lifecycle than the associated entity's identity IT account creation will be carried out in due time in respond to business needs. They will be provisioned to the entity and associated to the entity's identity and will also ends when the business need ceases to exists.	
FIDIS4	10.4.3.4	Fifth para	Te	See FIDIS 1	Replace text with: Under certain circumstances, it may be required that provisioning should be suspended (i.e., person on long	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
					vacation leave). In this situation, it does not represent that the entity is leaving the context or the domain of applicability, but only a temporary revocation of rights. A provisioning or an IT account is being suspended when ▪ the business need disappears ▪ if the associated IT entity identity ceases to have interactions in the context according to a predefined pattern (e. g. a person doesn't use a service for a long period), or if there is period of time when no interactions will occur (e. g. when a person takes a holiday). ▪ confidence of the IT entity identity is lost. The process of suspension commonly requires a check to ensure that the correct IT account is subject to suspension. IT accounts are commonly	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
					suspended by changing an attribute such as the end of validity period or information on its status.	
FIDIS5	10.4.3.4	Sixth para	Te	See FIDIS 1	Replace text with: Reactivation from the suspended state is sometimes required (e.g. when returning after a period of unavailability). Prior to reactivation it may be required to proof the identity anew. Reactivated provisioning will usually have the same identity associated that was used previously.	
FIDIS6	10.4.3.4	Eight para	Te	See FIDIS 1	Replace text with: Inactivation may take the form of archiving when the associated IT entity identity is no longer active in the context but when the possibility exists that the associated IT entity identity may in future become active again in the context or if there are some other needs or requirements to keep IT account information . The reactivation takes then the form of "restoration".	

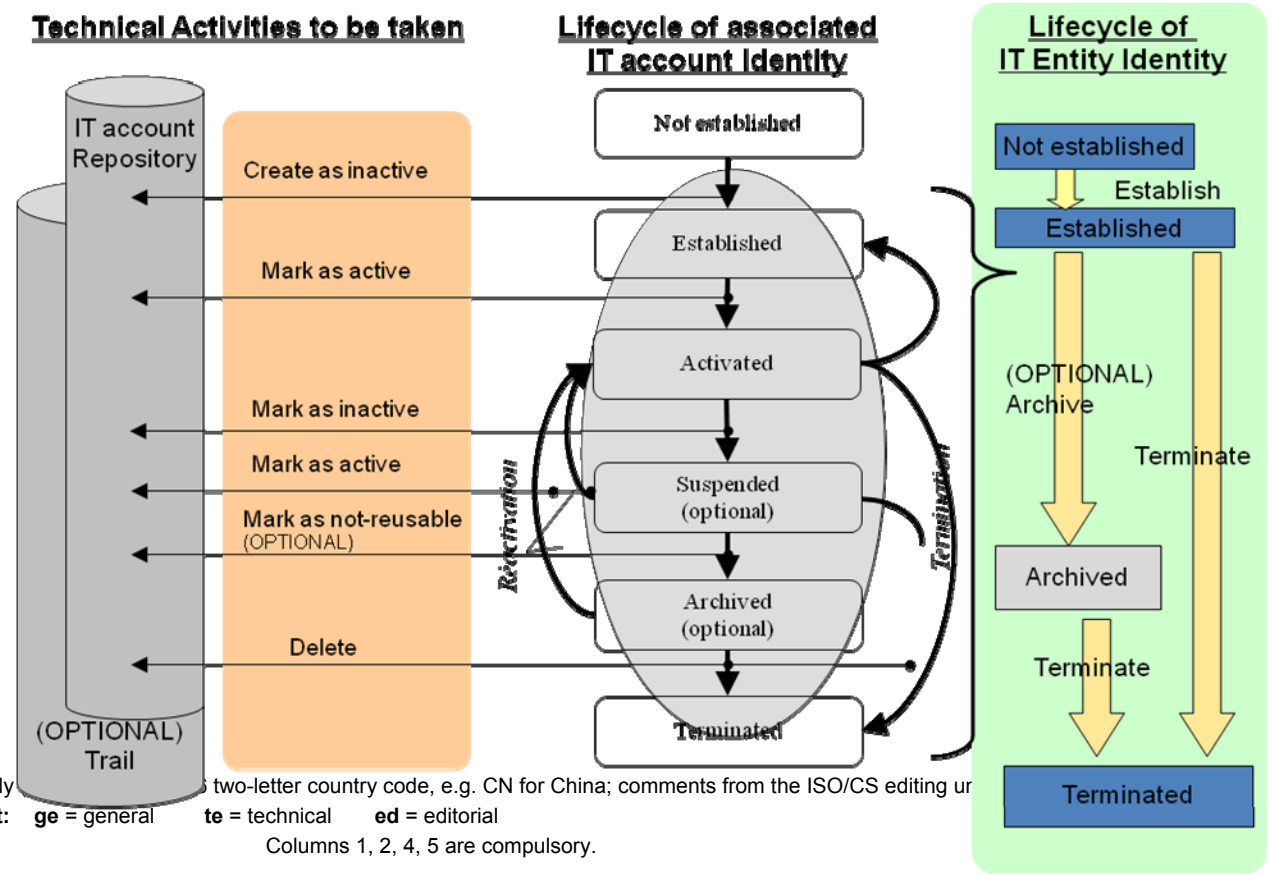
1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**

Annex 1



1 **MB** = Member body two-letter country code, e.g. CN for China; comments from the ISO/CS editing ur

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

ISO/IEC JTC 1/SC 27 **N7543**

ISO/IEC JTC 1/SC 27/WG 5 **N57543**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: liaison statement

TITLE: **Liaison Statement from FIDIS to JTC 1/SC27/WG 5 on WG 5 Projects (24760, 29100, 29101, 29115) (in response to SC 27 N7102)**

SOURCE: FIDIS Liaison Officer (H. Hedbom)

DATE: 2009-04-06

PROJECT: 24760
29100
29101
29115

STATUS: This document is being circulated for consideration at the 7th SC 27/WG 5 meeting in Beijing (China) on 4th – 8th May 2009.

ACTION ID: **ACT**

DUE DATE:

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-chair
E. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners
D. Brackney, R. Garcia Ontoso, Ch. Sténuit, S. Weiss, Y. Nyuo Shin, Project Editors

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 1 + 11 (Att. 1) + 3 (Att. 2) + 2 (Att. 3) + 8 (Att. 4)

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

FIDIS

Future of Identity in the Information Society

FIDIS liaison statement to ISO/IEC/JTC1 SC 27/WG 5 containing comments on the 6th WD of Project 1.27.50 (24760) "A framework for identity management", on the 1st CD of Project 1.27.54 (29100) "Privacy framework", on the 4th WD of Project 29115 “Entity authentication assurance” and on the 3rd WD of Project 1.27.55(29101).

FIDIS would like to thank ISO/IEC JTC 1/SC 27/WG 5 for its liaison statement from February 20089and for the consideration of the FIDIS comments for the ISO/IEC JTC 1/SC 27/WG 5 liaison statement to the 6th meeting of ISO/IEC/JTC 1/SC 27/WG 5 in Limasol (Cyprus)

FIDIS attaches comments on the 6th WD of Project 1.27.50 (24760) "A framework for identity management", on the 1st CD of Project 1.27.54 (29100) "Privacy framework", on the 4th WD of Project 29115 “Entity authentication assurance” and on the 3rd WD of Project 1.27.55(29101) .

Attachment 1 to SC 27 N7543

[FIDIS[1]] comments on ISO/IEC 6th WD 24760

Date: 2009-04-03	Document: **SC 27 N7237**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 1	3.8 credential p2	Note 1	Ed	Note 1 states: "the validity of credential may depend on a number of factors (e.g. context, time)" While time-constraint may cause a credential to expire, the context in which an entity attempts to use a credential does not. If used outside context, it will merely be ineffective, but this will generally not affect validity when the credential is later used in the context for which it was intended	Either delete 'context' Or change 'validity of' to 'effectiveness of a'	
			Ed	2nd Note 2: credential as claims do not necessary require to be validated / authenticated → confusing	Delete second note 2 Or -call it note 3 and -change 'necessary' to 'necessarily' -rephrase 'credential as claims'	
FIDIS 2	3.12 Identification (process) p3		Ed	Current definition of identification is ambiguous → are you referring to more to proofing, registration etc (1) or ongoing authentication (2): (1) if you are referring to proofing etc, which will enable later recognition and authentication of the entity, insert 'so' into definition (2) if you are referring to scenario where entity is identified after it already has an existence: then the current definition is misleading and perhaps redundant	'validation of provided mandatory evidences by an identity authority so that an entity can be recognized …'	
			Ed	Current text note 3: "the process validate an identity	Replace by:	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				proofing and can include identity registration"	The process of validating evidences of an identity is also referred to as 'proofing' and is part of the identity enrolment process	
FIDIS 3	3.13 Identifier p3		Ed	Wrt NOTE 2: same remark as FIDIS1 (validity – context)	Either delete 'context' Or change 'validity of' to 'effectiveness of a'	
FIDIS 4	3.19 Identity authority p4		Ed	Note 1 is ambiguous: does this mean that an identity authority is always a "subcontractor" of the information owner? Information owner is defined nowhere in the document. Is this the PII principal or data subject?	Delete Note 1	
FIDIS 5	3.23 Identity proofing p4		Ge	Explain link / difference between identification (process) (3.12) and identity proofing (3.23)		
FIDIS 6	6.3 Identity and identificatio n p7		Ed	1st sentence "Identification is the process that will recognize the entity …"	Replace by "Identification is the process that ensures that entities shall be recognizable in the future (future) by assigning …"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
	p8 (last sentence 6.3)		Ge Ed Ge/ed	Relationship to registration is mentioned ; but what about relationship to enrolment (defined as combination of proofing and registration); or proofing? Especially distinction or similarities with identity proofing should be clarified “Identification is based on data that help in recognizing and discriminating the entity from another within a particular context” → ‘discriminating’ has very negative connotation “Identity and identify provide the entity legitimacy and rights to exist in a context” → while it is highlighted earlier that the identification is often ‘tied together’ with the provisioning of credentials, the two are not synonymous. Furthermore, identification is not always constitutive for the rights of an entity “to exist” in a context. The conceptual difference between the identification and (the often closely related)	Replace ‘discriminating’ by ‘distinguishing’ Rephrase or delete	
FIDIS 7	6.6 Context prerogative		Ge	“An identity provided for a particular context is recognized and trusted by all domains of applicability within that context”	Rephrase or delete	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
	s and domains of applicability p9 2nd par			→ won't this only be so in the case of federation among the various domains of applicability? (see p. 10) Or is it an automatically assumed that within every context identity federation takes place? This would seem to go a bit too far. (if it were the case, why introduce the notion of a 'context' at all and not simply refer to a CoT?)		
FIDIS 8	6.10.2 Federation of identity authorities / Circle of Trust 1st par p12		Ge	"A federated identity management framework may help the establishment of federated perspective through the recognition of a single identity reference and the maintenance of common entity information" → CoT does not imply that all members refer to a particular entity by using a single identity reference but rather supports the use of multiple pseudonyms and different 'opaque handles' => sentence is misleading / erroneous in this regard	Delete sentence	
FIDIS 9	6.10.3 Discovery of identity sources 3rd par p13		Ge	"The discovery mechanisms should include dynamic registration and de-registration of federation relationships, identity authority authentication, privileges assignment, and attributes maintenance" → Could benefit from further elaboration & clarification (particularly the last two elements are relatively vague / ambiguous). E.g. -what determines entity privileges when using a discovery service? -what is meant by "attributes maintenance"? Sync?	Consider elaborating and replace: "privileges assignment" By "authorization management"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 10	6.12 Identity management and privacy p17		Ge/Ed	"The understanding of privacy results sometimes an detrimental effect on the process of identity management" → which "understanding of privacy" are you referring to here? One in which no accountability mechanisms exist? Accountability mechanisms are generally accepted as standard requirements under privacy & data protection regulations (art. 16-17 Directive 95/46/EC; K.U. v. Finland (ECHR)) The text on p22 is better (but not quite there yet - see comment 16). Other potential source of inspiration for rewrite: p27 Liberty ID-FF Guidelines v1.2	Rephrase	
FIDIS 11	7.2.4 Authoritative sources of identity information p19		Ge	"The following criteria may be relevant when selecting an authoritative source: -…" → no mention is made of the protection of these databases against unauthorized manipulation or proper authentication of the data that is being fed into these databases, whereas this directly impacts the trustworthiness of an authoritative source. There may also be legal and contractual obligations in connection with authorative sources	Add the following bullets to the list: -security of the databases against unauthorized manipulation (e.g., authorization management, integrity protection) -security of the protocols governing data to these sources (e.g., data origin authentication) -legal and contractual obligations	
FIDIS 12	7.2.5 Merging contexts or		Ed	"Controls should ensure, within the merged context or domain, that: -[…]	Replace by -it is not possible to associate an identity with the wrong entity"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
	domains p19			-it is not possible to incorrectly associate an identity with the wrong entity" → double negative		
FIDIS 13	7.2.6		Te	"Different types of entities require different identification processes..." The identification process it not based solely on the entity type but also on the context, privileges, roles and responsibilities of a specific entity.	Change: "Different types of entities require different identification processes..." To: "Different entities may require different identification processes..."	
FIDIS 14	7.2.8 Identity references p20		Ge	No mention is made of the fact that their or privacy arguments (and sometimes even specific legal restrictions) against using an identifier assigned outside the context, e.g.: -In Belgium, use of national registry number requires prior authorization by Data Protection Authority -if every SP uses the same IR, it creates a linkability nightmare	Insert some text referring to possible restrictions / disadvantages on using IR assigned outside the context	
FIDIS 15	7.2.8 Identity reference			"care shall also be given to ensuring that the entity may only possess one identity reference in the context (i.e., bank card identity references cannot be used as one entity may possess several)." This implies that an entity only can have one identity within a context something that contradicts the description earlier in this document and that is an unnecessary restriction leading to likability.	Change: "care shall be given to ensuring the uniqueness of that identity reference for each different entity, and" "care shall also be given to ensuring that the entity may only possess one identity reference in the context (i.e., bank card identity references cannot be used as one entity may possess	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				We suggest that it is important that an identity only have one and unique identity reference.	several)." To: "care shall be given to ensuring the uniqueness of that identity reference for each different identity, and" "care shall also be given to ensuring that the identity may only possess one identity reference in the context (i.e., bank card identity references cannot be used as one entity may possess several)."	
FIDIS 16	7.2.12 Access to identity information p21		Ge	"IF access to identity information needs to be controlled …"1 "what identity access needs to be recorded" → where identity information relates to natural person, it amounts to PII and consequently access control + logging are standard requirements (current phrasing is too "optional")	Specify (at least in the accompanying footnote) that were identity information amounts to PII, access control + recording of access are standard requirements	
FIDIS 17	7.2.13 Revocation of identities and identity attributes p21		Ge	Other possible instances which create need for revocation: -abuse of credentials associated with particular entity (ID theft) -if "entity or identity attributes" also include the privileges associated with an entity (cf. definition term 3.1), than change in role of entity within organization would also require change in privileges	Replace "an entity or identity attributes" by "an identity or identity attributes" AND Consider elaborating list or narrowing scope (if broad scope is maintained 'revocation' might not be right term, but	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				-…	rather “updating” or “managing”)	
FIDIS 18	7.3.1 Privacy p22		Ed/.Ge	“requirements for privacy and data protection may conflict” “Similarly, requirements to minimize the amount of personal information […] at the expense of operational cost and inconvenience […]” → data accuracy is not only question of privacy, but in turn also impacts operational risk. By verifying data in real time with authoritative source of information, who has policies in place to keep it accurate and up to date, the operational cost might be more limited in the long run	Replace by: “requirements for privacy and data protection may seemingly conflict” or “may appear to conflict at first sight” Delete	
FIDIS 19	7.2.4 Suspension p26		Ed	“An identity is suspended when assurance to the entity is lost” → confidence / assurance is not necessarily lost wrt the entity as such, but rather wrt digital identity associated with it (e.g. is it still accurate, being used properly etc)	Replace by “an identity is suspended when the appropriate level assurance with regards to the identity is compromised”	
FIDIS 20	9.1 Components overview p31		Ge	“Aside of technical components, a framework for identity management must again consider including: -[…]” → two services which definitely merit consideration are not mentioned: - a revocation service: a service which allows entities	Add: - a revocation service - a transparency service	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
				to revoke their own credentials + consult the validity status of the credentials of other entities (e.g. CRL) - a transparency service: a service which allows natural persons to exercise their right of access		
FIDIS 21	9.1.1 Identity manageme nt system p32		Ge/ed Ed	Last sentence 1st par "It provides tools for managing the identity registry and eases the delivery of identity information to systems of the context that may need it" → should be conditional upon authorization + Replace 'eases' by 'facilitates' Last sentence 2nd par: "These sources are called authoritative sources since they control the identity information origins and updates" → they verify / validate, they don't actually "control" these sources + readability rewrite	Replace by: It provides tools for managing the identity registry and facilitates the delivery of identity information to systems that are authorized to receive it" Replace by: "These sources are called authoritative sources since they verify the origin and trustworthiness of identity information and keep it up-to-date"	
FIDIS 22	9.1.4 Identity Registry p33		Ge/ed	"An identity registry (or IdMS registry) collects on behalf […] and makes this information available *to any system that may need it* through identity providers" → see comment 19: conditional upon authorization	Replace by: […] and makes this information available *to authorized entities* through identity providers"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 23	10.2 Identity and Access Management p35		Ed	1st sentence under fig: "Identity management is an essential part of many security services without *what* the control being provided are some*where* useless because of not being capable of ensuring the genuine of the player's identity" → rewrite	Replace by: "Identity management is an essential part of many security services without *which* the control<u>s</u> being provided are some*what* useless as they *will be unable to ensure the genuineness of an actor's identity*"	
FIDIS 24	10.3 Entity's identity References and Object identifiers p35		Ge/ed	Last sentence 1st par: "When the resources is an element to give access to other resources (e.g. a passport), then the identifier becomes a means to authenticate" → is the identifier itself then really a means to authenticate? Isn't there merely an ID associated with the object used to authenticate? E.g.: just because you know my passport number does not mean you will be able to cross the border in my name. Otherwise every credential could be reduced to 'something you know'	Delete sentence	
FIDIS 25	10.3.4 Pseudonyms p36		Ge/ed	1st sentence 2nd par: "Pseudonymization can be defined as the process of distinguishing identity references of a same entity" → rewrite: 'distinguishing is inaccurate here"	Pseudonymization can be defined as the process of replacing direct identity references with substitute references. These references are generally intended to be meaningful only to authorized entities.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 1 to SC 27 N7543

[FIDIS[1]] comments on ISO/IEC 6th WD 24760

Date: 2009-04-03	Document: **SC 27 N7237**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by FIDIS**	**Proposed change by FIDIS**	**Resolution on each comment**
FIDIS 26	10.4 Privilege Management p36		Ed	1st sentence: "The processes of managing privilege usually *take assumption* that the identification of entities is guaranteed" → rewrite	Replace by: "Privilege management usually *operates under the assumption* that the proper identification of entities is guaranteed"	
FIDIS 27	10.4.2 Authorization process p37		Ed/Ge	Description/definition Authorization process: "The Authorization process ensures privileges are securely granted tot entities with a number of approvals from different actors" → rewrite (as it reads now It might as well refer to the actual granting of privileges itself; whereas this is treated in the following section (10.4.3.1). What is meant here is that prior to actual provisioning there is an evaluation of applicable policies to ensure that only the intended entities receive those privileges they need to receive.	Rewrite	
FIDIS 28	10.4.3 Provisioning Management p43		Ge	What about credential provisioning? Why is it not discussed here? Out of scope?	Credential provisioning should be added to the list	
FIDIS 29	10.5.1 Entity's authentication p41		Ge	Definition of entity authentication also refers to authorization	Replace first sentence with definition 3.2	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 2 to SC 27 N7543

[FIDIS[1]] comments on ISO/IEC 1st CD 29100

Date: 2008-04-03	Document: **SC 27 N7239**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the FIDIS**	**Proposed change by the FIDIS**	**Resolution on each comment**
FIDIS 1	Introduction			"The framework can serve as a basis for desirable additional privacy standardization initiatives, for example for a technical reference architecture, for the implementation and use of specific privacy technologies, for overall privacy management, for the assurance of privacy compliance for outsourced data processes, for privacy impact assessments or for specific engineering specifications." This text is present in two places both as bullet point (c) as well as at the end of the introduction.	Consider deleting one of the occurrences.	
FIDIS 2	3.1 Anonymity p1		Ge	What is meant by "unique characterization"? Assignment of ID or IR? Even without an ID or IR an entity can very often remain identifiable and will therefore not be anonymous	Add clarifying note	
FIDIS 3	3.15 Privacy breach p3		Ge/ed	"situation when PII on an individual … without having the permission to do so …" → replace by: "without being authorized to do so"	Replace without having the permission to do so …" by: "without being authorized to do so"	
FIDIS 4	5.2 Actors p7		Ge/ed	1st par under table 1: "The PII principle is the individual … PII processor (Role (b) in Table 1), in which case *he would not control* the data being processed" → even when designating a processor, the PII controller still is considered to be responsible and to be "controlling" the processing. It is just that he no longer performs all the actual operations himself => verb "control" is poorly chosen here	Replace "in which case he would not control the data being processed or both" By "in which case he would not necessarily perform all data processing operations himself"	
FIDIS 5	5.3		Ge/ed	2nd par under table 3:	Insert "or identifiability"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the FIDIS**	**Proposed change by the FIDIS**	**Resolution on each comment**
	Identifying and providing PII P8			"Information in an anonymous form (i.e. without identification of an individual) …" → should read: without identification or identifiability		
FIDIS 6	6.4 Use, retention and disclosure limitation p13		Ge	This text should also be explicit in terms of secondary use (as on p22): when new use is anticipated which was not foreseen at moment of collection, additional consent (or at least notification) may be required	Add text	
FIDIS 7	7.3.1 Pseudonymization p18		Ge	Description of pseudonimization appears inconsistent with definitions. (what is described here seems to reflect what is otherwise referred to as encoding). Wrt 3rd, 4th and 5th paragraph: secondary processing for statistical or research processes generally requires anonymization, not pseudonymization	Rewrite	
FIDIS 8	7.5.2 Transfer 7.5.3 Use p20-21		Ge	This text should also be explicit in terms of secondary use (as on p22): when new use is anticipated which was not foreseen at moment of collection, additional consent (or at least notification) may be required (this is discussed under 7.5.3) Additionally, it seems that some aspects are covered both by the "transfer" (7.5.2) and the "use" (7.5.3) section	Add text + consider revising to avoid overlap	
FIDIS 9	7.7.1.6 Minimize data p23		Ge	Minimizing the creation of personal data not mentioned (compare p. 13 section 6.5)	Insert "creation"	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 2 to SC 27 N7543

[FIDIS[1]] comments on ISO/IEC 1st CD 29100

Date: 2008-04-03	Document: **SC 27 N7239**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the FIDIS**	**Proposed change by the FIDIS**	**Resolution on each comment**
FIDIS 10	7.7.1.7 Ensure accuracy p23		Ge	Accuracy must be ensured, regardless of use	Insert “particularly”	
FIDIS 11	A.2 Security controls p28		Ge	12.3 (cryptographic controls) should be added	Insert “12.3”	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 3 to SC 27 N7543

[FIDIS] comments on ISO/IEC 3rd WD 29101

Date: 2009-04-03	Document: **SC 27 N7241**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the FIDIS**	**Proposed change by the FIDIS**	**Resolution on each comment**
FIDIS 1	The whole document		Te	personal or personally? In the Introduction the word 'personally' is used. Also in Section 4. However personal is used in other places.	Harmonize the use throughout the document.	
FIDIS 2	The whole document		Te	Is there a difference between 'privacy enhanced' and 'privacy enhancing' technology? If not than one should go for one term for the whole document. [Otherwise it might be necessary to explain the differences.]	Harmonize the use throughout the document.	
FIDIS 3	5.2.1.5	5 bullet point	Te	This seems not to be a 'requirement'. It is more like a 'remark'. Maybe one can rephrase this in a way like: 'The same safeguards which are use to secure collected PII must be applied to secure any derived PII, e.g. by means of profiling.	Change to: 'The same safeguards which are use to secure collected PII must be applied to secure any derived PII, e.g. by means of profiling.	
FIDIS 4	6.2.1		Te	The whole paragraph only seems to talk about database like anonymization - so probably one should rename the chapter. It seems that network (communication) anonymization is not addressed here. So maybe one should include a chapter on that as well.	Suggest including a chapter on network (communication) anonymization.	
FIDIS 5	6.2.1	Second bullet point		“assessment of the risk of identification through inference” This is in contradiction to the general statement above which says that 'de-identification cannot be reversed'. So i suggest changing the statement above in something like 'cannot be easily reversed'.	Suggest changing: “on the data as will ensure the de-identification process cannot be reversed.” To: “on the data as will ensure that it is computationally hard to reverse the de-	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the FIDIS**	**Proposed change by the FIDIS**	**Resolution on each comment**
					identification process."	
FIDIS 6						

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N7543

[FIDIS[1]] comments on ITU-T X.eaa | ISO/IEC 4th WD 29115

Date: 2009-04-03	Document: **SC 27 N7235**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
FIDIS 1	Whole document		Te	There is number of spelling errors, erroneous words and grammatical errors within the document.	Please revise the language of the document	
FIDIS 2	3.9		Te	**man-in-the-middle attack** an attack in which an attacker is able to read, insert and modify messages between two parties without either party knowing that the link between them has been compromised. It is still a man-in-the-middle attack if one or more of the parties knows about it however it might not be a successful one.	Change: an attack in which an attacker is able to read, insert and modify messages between two parties without either party knowing that the link between them has been compromised. To: an attack in which an attacker is able to read, insert and modify messages between two parties.	
FIDIS 3	6		Te	The language in this whole section has somewhat of a “sales pitch” or “whitepaper” style and contains wording like “this component can” and “and for the first time” and so on. Since it is a framework and not en implementation we do not know what the components can do since they are not implemented yet.	Revise the text and make it more “standard” style e.g. by changing “the component can” to “a component for”	
FIDIS 4	6.1		Te	Is enrolment really a necessary part consider e.g. In general it would be nice to see for the whole framework how it fits to the case of the 'Japanese tobacco machine'. This machine grants access to tobacco via biometric means by comparing a picture of the individual requesting tobacco with a set of known pictures to decide if the requesting individual is of certain age or not. So there was no enrollment with the respect to the individual--but with respect to the group of people of a certain age. So the 'entity' in this scenario is a group of people.	Discussion on if this should be reflected in the framework or if it should if it currently is.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Attachment 4 to SC 27 N7543

[FIDIS[1]] comments on ITU-T X.eaa | ISO/IEC 4th WD 29115

Date: 2009-04-03	Document: **SC 27 N7235**

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
FIDIS 5	6.1		Te	"This component includes validation services that help weed out invalid or duplicate applicants, and provides for the capture and analysis of new or additional identity data such as biometrics and breeder documents." Does this mean that every entity can have only one identity within a given context? If this is the case then it stands in conflict with 24760. Otherwise it should be clarified what is meant by duplicate and give the circumstances where "individualization" is needed.	Please Clarify.	
FIDIS 6	8.3.2	"Something you are"	Te	"Although admittedly difficult, an attacker may obtain a copy of the token owner's identification and construct a replica." This is a wish not a truth - otherwise give a references, especially if 'admittedly' is stated.	Change: Although admittedly difficult, an attacker may obtain a copy of the token owner's identification and construct a replica. To: An attacker may obtain a copy of the token owner's identification and construct a replica.	
FIDIS 7	9.5		Te	"For a false negative to occur, the legitimate user's value is rejected as not matching the stored value and the most sensitive information and resources will be withheld." In most systems all resources and information related to that authentication will be withheld.	Change: "For a false negative to occur, the legitimate user's value is rejected as not matching the stored value and the most sensitive information and resources will be withheld." To: "For a false negative to occur, the legitimate user's value is rejected as not matching the stored value and information and resources will be	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
					withheld."	
FIDIS 8	9.6		Te	Missing aspect of the 'usage costs' e.g. the costs of an entity performing the authentication procedure as well as the costs for the verification. Note that 'cost' is a general construct and does not only reflect monetary costs but also cost in term of time , learning investments etc.	Add usage cost aspect	
FIDIS 9	9.8		Te	Iris scan might be simple to use - but many people might not like it. So the general acceptance has to be considered - not only if a method is simple or not.	Consider adding general acceptance as an aspect	
FIDIS 10	9.11		Te	"Additionally, the strength of an authentication system can adversely affect the privacy of an individual" Probably one should highlight this 'can' - because there exists many cryptographic strong authentication methods which have no negative impact on privacy, e.g. anonymous credentials, group signatures etc. And in general it is a very well established misconception that authentication and anonymity (privacy) are opposites. So one should state that it is possible to have strong authentication and strong privacy.	Consider adding these aspects of authentication v.s. privacy.	
FIDIS 11	9.12			This section introduces biometrics as the overall solution to repudiation (and implicitly to authentication assurance). We believe that the description here is highly biased and do not discuss the drawbacks concerning privacy and safety risks as well as the legal considerations of using the technology as well as the current impreciseness and other drawbacks of the technology.	Consider revising the paragraph	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
FIDIS 12	3.1 Access control		Ge	Current definition: "A procedure used to determine if an entity should be granted …" → this definition may just as well be referring to "authorization" (compare def 3.4 ISO 24760) → access control includes a wider variety of measures than just the authorization process → rephrase as to refer to the set of procedures and mechanisms *used to restrict* access to resources …	Replace by: "the set of procedures and mechanisms used to restrict access by entities to resources, facilities, services or information based on pre-established rules and specific rights or authority associated with the requesting party"	
FIDIS 13	3.2 Identity vetting assurance		Ge	How is "identity vetting" different from identity proofing? If synonymous, the term 'proofing' may be preferable to enhance consistency of terminology with other documents. Furthermore, why only refer to credentials? Why not include creation of the identity?	Consider revising	
FIDIS 14	3.6 Credential		Ge	Credentials are only verified when presented by a requesting/asserting entity	Replace by: an object that is presented by an entity to serve as corroboration of a claim, and which is verified by the relying party in an authentication transaction Or Replace by definition 24760 (3.8): "credential set of data presented and that can be verified and authenticated to provide evidence of a claimed identity	
FIDIS 15	3.10 Non-		Ge	Definition should not include the term being defined + "prove" is ambiguous here (legal rules of evidence may	Replace by:	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
	repudiation			differ) + suggested definition is more consistent with 3.11 (repudiation)	Non-repudiation refers to the concept of ensuring that a commitment or action cannot later be denied by one of the entities involved (based on Modinis IDM glossary)	
FIDIS 16	6.1 Framework components		Ge	Logical access control mentions authentication and non-repudiation, but omits the obvious “authorization”	Insert “authorization”	
FIDIS 17	7 Criteria for authentication effectiveness		Ge	Last sentence introductory paragraph: “Each assurance level represents the organization’s degree of certainty that the user has presented an identifier …” → an assurance level refers to more than just whether or not an identifier was presented, it also refers to the degree of certainty that the identity and credentials being used is the entity to whom it was issued or assigned (compare definitions)	Revise	
FIDIS 18	7.1 Authentication Principle		Ge	The text as it stands now refers (“examples of authentication principles are …”) mainly to what is commonly know as authentication “factors” (something you know, have, are, etc) (see also 7.2: “Multifactor authentication involves two or more of the above authentication principles”) A “principle” is typically something normative. What is described now as “authentication principles” are merely	Revise	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				factors → when normative statements are made about these factors (e.g. wrt to their strength) it may be legitimate to refer *to those statements* as 'principles'.		
FIDIS 19	7.2 Authenticati on		Ge	Text as it stands is rather vague and ambiguous; e.g. authentication is not just process of establishing whether identifiers or attributes are authentic, it involves the verification of a claim according to a pre-established level of confidence	Revise	
FIDIS 20	8.3.1 Authenticati on protocol threats		Ge	Attacks may be mitigated by … - requiring additional or re-authentication; - including references to prior authentications or protocols; - ensuring that the 'chain' of authentications remains intact (e.g. in SSO)		
FIDIS 21	8.3.2 Authenticati on Token threats		Ge	The term "token" is used here to refer to the "manifestations" of factors of authentication. Note that the term "token" is also often understood as a "security token", which covers digital vouchers (e.g. SAML assertions) (see also e.g. Cardspace). Different types of measures may needed to protect against these threats (see comment concerning authentication protocol threats)	Revise	
FIDIS 22	8.5 Certificate substitution		Ge	Approaches only describe registration process, not what happens once certificate is in use.	Add: storing certificate and key-pair on secure signature creation device (SSCD)	
FIDIS 23	9.11 Privacy		Ge	This section requires further elaboration. As it stands now, it only refers to risks associated with extended or systematic recourse to the same identifier (which is in	Consider revising and expanding scope	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				fact an important risk to discuss further), but additional risks should also be discussed. FYI, the following risks have been associated with extended or systematic recourse to the same identifier for either authentication purposes or account management: (i) Unauthorized data exchange: data is communicated from one entity to another in violation of data protection principles (i.e. proportionality, finality etc.) or in violation of otherwise agreed policies; (ii) Loss of confidentiality: an attacker, i.e. an unauthorized entity, is able to learn attributes (here: personal data other than identifiers) corresponding to a particular entity while it is not authorized to do so (either through unauthorized access or interception); (iii) Loss of “transactional” privacy: an attacker may be able to monitor and link the (trans)actions per-formed by a particular entity and may be able to continue this activ-ity when the observed entity en-gages in (trans)actions at a later time; (iv) Unauthorized data aggregation: an attacker, who may be authorized to learn certain attributes of an entity for a particular purpose, is able to bring these and other attributes together for an unlawful purpose (be it an entirely different unlawful purpose or an excessive amount of attributes with regards to a particular legitimate purpose); (v) Unauthorized profiling and Knowledge Discovery in Databases (KDD): refers to the situation		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
FIDIS[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				where, once data has been aggregated or otherwise collected, the attacker proceeds to manipulate these data (e.g. through data mining), to assess, predict or otherwise gain knowledge with regards to the subject; (vi) Identity theft: an attacker is able to fraudulently impersonate another entity. (Source: B. VAN ALSENOY and D. DE COCK, 'Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card', Datenschutz und Datensicherheit, March 2008, p. 180)		

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.