



Project no. ICT-2007-216339

TURBINE

TrUsted Revocable Biometric IdeNtitiEs

Grant agreement for: Large-scale integrating project (IP)

Theme 3: ICT - Information and Communication Technologies Secure, dependable and trusted infrastructures

D1.4.1

Legal Issues of Identity Management Schemes

Due date of deliverable: M12

Actual submission date: M12

Start date of project: 1 February 2008

Duration: 36 months

Organisation name of lead contractor for this deliverable: KUL-ICRI

Project co-funded by the European Commission within the Seventh Framework Programme (FP7/2007-2013)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of Contents

Glossary	4
Executive Summary	5
1. Introduction	6
2. The Concept of Identity Management and Identity Management Systems	7
2.1 Research, concepts and key terminology	7
2.2 Some examples of identity management systems	10
3. Functional Requirements, Architecture and Organizational structure of Identity Management Systems	13
3.1 Functional requirements	13
3.1.1 <i>Identification, use of pseudonyms and anonymity</i>	13
3.1.2 <i>Authentication</i>	15
3.1.3 <i>Authorisation (permission/delegation/mandate)</i>	16
3.2 Additional requirements	16
3.3 Architecture and organizational structure	18
4. Legal Aspects of Identity Management Systems	22
4.1 Identity, identifiers and identification	22
4.1.1 <i>Identity</i>	22
4.1.2 <i>Identifiers</i>	25
4.1.3 <i>Identification</i>	28
4.2 Pseudonyms and anonymity	28
4.3 Authentication and authorisation (permission/delegation/mandate)	33
4.4 Legal aspects of additional requirements and architecture	35
4.5 Legal risk management	36
4.6 Responsibility of system designers ?	36
5. Legal Compliance	37
5.1 Article 8 of the European Convention on Human Rights and Article 7 and 8 of the EU Charter	37
5.2 The Data Protection Directive 95/46/EC	39
5.2.1 <i>Purpose specification and finality of the IdM system</i>	40
5.2.2 <i>Need for a legal ground for IdM processing</i>	41
5.2.3 <i>Determination of the (co) controller(s)</i>	42
5.2.4 <i>Notification of IdM system and/or prior checking requirement</i>	43
5.2.5 <i>Minimization of the data collection and processing</i>	43
5.2.6 <i>Proportionality requirement</i>	44
5.2.7 <i>Prohibition to process data revealing racial or ethnic origin and data concerning health (unless exemption applies)</i>	45
5.2.8 <i>Avoidance of unique identifier requirement</i>	46
5.2.9 <i>Central and local storage requirements</i>	46
5.2.10 <i>Identification of data subject for no longer than is necessary requirement</i>	47
5.2.11 <i>Data quality requirement</i>	48
5.2.12 <i>Information and transparency to the data subject - Access and correction – right to revoke - right to control ?</i>	48
5.2.13 <i>Retention and/or destruction of the data</i>	50
5.2.14 <i>Security of the IdM processing</i>	51
5.2.15 <i>Confidentiality of the processing requirement</i>	52
5.2.16 <i>Outsourcing to a processor requires a written contract</i>	53

5.2.17	<i>Transfer of personal data outside EU countries requires ‘adequate level of protection’</i>	53
5.2.18	<i>Prohibition of automated decisions and right to know</i>	54
5.2.19	<i>Practical applications</i>	54
5.3	The E-Privacy Directive 2002/58/EC	55
5.3.1	<i>IdM systems in ‘public’ communications networks</i>	55
5.3.2	<i>IdM systems in mobile environments</i>	56
5.4	The Data Retention Directive 2006/24/EC.....	57
5.5	The E-Signature Directive 1999/93/EC.....	57
5.6	The E-Commerce Directive 2000/31/EC	58
5.7	Specific requirements for e-government.....	59
5.8	Specific requirements for IdM systems for e-health applications	61
6.	Legal Challenges and Recommendations for Identity Management Systems	62
6.1	Defining the roles	62
6.2	Other difficulties in complying with Directive 95/46/EC and Directive 2002/58/EC	63
6.3	Criteria for enrolment for critical IdM systems	64
6.4	The Use of Unique identifiers.....	65
6.5	Criteria for a Privacy Impact Assessment of IdM systems.....	65
6.6	Confidentiality of electronic communications and IdM systems	66
6.7	Defining the degrees and the needs of anonymity and pseudonymity	67
6.8	IdM systems and liability of service and identity providers	68
6.9	Evidence	69
6.10	PETs : Embedding privacy protection into technology	69
7.	Conclusion	71
8.	Bibliography	73

Glossary

The meaning of terms, abbreviations and acronyms often used in this report are described or defined hereunder.

<u>Term/Abbreviation / acronym</u>	<u>Description</u>
Civil Identity (Civil ID)	Identity attributed to an individual by a state (e.g. name, date of birth, social security number) (see D14.1.b of PRIME EU project)
Controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (definition Art. 2(d) of Directive 95/46/EC)
Data subject	An identified or identifiable natural person. An identifiable person is an individual who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (definition Art. 2(a) of Directive 95/46/EC)
DPA	Data Protection Authority
EDPS	European Data Protection Supervisor
FIDIS project	Future of Identity in the Information Society project
FP6	Sixth Framework programme
FP7	Seventh Framework programme
Identity Management	Systems and processes that manage and control who has access to resources, and what each user is entitled to do with those resources, in compliance with the organization's policies (PRIME White paper v.3.0)
IdM	Identity Management
IdM system(s)	Identity Management system(s)
P3P	Platform for Privacy Preferences
Personal data	Any information relating to an identified or identifiable person (definition Art. 2(a) of Directive 95/46/EC)
PETs	Privacy Enhancing Technologies
PIA	Privacy Impact Assessment
PRIME project	Privacy and Identity Management for Europe project
Processor	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (definition Art. 2(e) of Directive 95/46/EC)
Pseudonym	A pseudonym is an identifier of a data subject other than the data subject's civil identity (see PRIME White paper v.3.0)
PUID	Microsoft's .NET Passport Unique Identifier
SSO	Single Sign-On

Executive Summary

Identity management systems (IdM systems) have been mainly researched from a technical point of view. While there are a large variety of IdM systems, some recurring elements permit to discern the building blocks of such system and to provide a legal analysis. Based on the requirements, the present report explores legal aspects of IdM systems and provides a view on some specific issues that need to be addressed.

The legislation which explicitly addresses IdM systems is scarce. This does not prevent that current legislation, mainly with regard to privacy and data protection, applies to the processing of personal data contained in such systems. The report discusses the applicable data protection provisions of the Directive 95/46/EC. Other provisions of other directives, such as with regard to electronic commerce, electronic privacy, data retention and electronic signatures, are also relevant for IdM systems, as will be described.

The principles of respect for privacy and data protection currently guide the development of IdM systems. The data minimisation requirement is such principle which shall be at the core of IdM systems. The use of pseudonyms as identifiers wherever this is possible follows from data minimisation. Unlinkability of the information contained in an IdM system, unobservability and revocability are other requirements and have to some extent been expressed as such by Data Protection Authorities in their opinions. User control over personal data becomes another important aspect of IdM. These principles, however, have not been clearly pronounced in legislation as legal requirements for IdM systems. The law may need to lend its support to confirm these principles in a more explicit way.

These principles and other unsolved legal aspects of IdM systems, such as relating to the complex role of participating identity and service providers, the field of application of the e-privacy directive, the criteria for and organisation of the enrolment which is key for a reliable system and the use of (unique) identifiers deserve attention from a legal point of view as well.

Other recommendations which are described in this report include the use of privacy impact assessment tools, such as for measuring the level of control of a data subject, a definition of relevant degrees of anonymity and pseudonymity and a further description of the liability of identity and service providers of an IdM system.

The report could be used as a start for spotting the legally relevant topics which need to be tackled in a subsequent deployment of an IdM system, but also for identifying issues for further regulations or legislation.

The views expressed in this report are those of the author and do not necessarily reflect the views of the European Commission

1. Introduction

Identity management is becoming of crucial importance in the digital environments of our information society. Individual persons, organizations, companies, but also governments experience an increasing need to organise and administer identities in networks in a reliable way, while technology is emerging and is proposing various solutions to cover such needs.

Identity management and identity management systems (IdM systems) are for this reason at the centre of attention of many national and international research projects. Most research however covers mainly the technical aspects of the development of IdM systems.

This report for the TURBINE project explores the legal aspects of IdM systems and aims at providing an overview of various legal issues relating to IdM systems, which need to be taken into account, not only during the implementation of an application, but preferably also when developing an IdM system.

IdM systems as such are almost not referred to in legislation. On one hand, there is an increasing awareness that some crucial principles of our networked (democratic) society, such as the right to remain anonymous where appropriate, derived from existing fundamental rights, risk to disappear with the ever increasing requests or needs to identify. The use of identifiers allows for linking information from different contexts to one individual. Therefore some rights such as the right to remain anonymous or the right to use pseudonyms have been proclaimed in a more general way in some legal texts. On the other hand, the way how these principles need to be implemented, or the precise conditions of such use, however, are not clarified.

First, the report will review the concepts and the terminology used to describe IdM systems as they vary from source to source. It will analyse to what extent the notion of '*electronic identity*' exists in legislation. Other relevant questions will be tackled: to what extent is one *entitled to use pseudonyms or to remain anonymous*, and what are the restrictions thereto? Is there a (sufficient) legal basis for the requirement that personal information shall not be linked? These and other questions which are relevant for IdM systems will be briefly discussed, aiming at providing a general understanding of the purposes and functionalities of an IdM system, including the legal aspects thereof.

In addition, the processing of the data of persons in such systems will in almost all cases be subject to the legislation relating to data protection, since the purpose of the IdM system itself is the identification of a natural person. The *application* of such legislation, however pose distinct *difficulties*. For example, the information obligation aimed at providing transparency to the data subject seems to require for an IdM system to provide more details about the functioning and the relevant data flows of the system than legally specified. Also, the distinct roles of providers in an IdM system seem to be not adequately covered by the general framework directives which apply to IdM systems. Furthermore, the notion of public communication networks and services, in which context IdM systems will be deployed, is changing quickly and requiring new legislation to rule out legal uncertainties.

These, and several other aspects, such as to the liability of the actors in an IdM system, therefore deserve attention from a legal point of view and may require further legislation. It seems, however, that most countries are now paying full attention at the requirements for further enabling E-government. For this sector, stakes are high and discussions (for example, about the use of national versus sector-based identifiers) therefore long.

Turbine is developing new technology aimed at serving as a privacy preserving solution for IdM systems. The report will indicate how the Turbine solution complies with the existing requirements for privacy enhanced IdM systems and at the same time meets far reaching expectations from privacy and data protection point of view, such as a user-controlled IdM device, with strong authentication means, enabling the user a choice to use various identities, which are revocable.

The report could hence not only be used as a start for spotting the legally relevant topics which need to be tackled in a subsequent deployment of IdM systems, but also for identifying issues for further regulations or legislation or at least as an overview of matters to be taken care of in the development and the use of IdM systems.

2. The Concept of Identity Management and Identity Management Systems

2.1 Research, concepts and key terminology

Various research projects have examined different aspects of identity management. While it is impossible to give a complete overview of research in identity management, some are by way of example mentioned below. Brief reference to the results of these projects are taken into account for this report where appropriate and relevant.

The research in Privacy Enhancing Technologies ('PETs') often relates to identity management. PETs include technologies for increasing or guaranteeing anonymity in infrastructures and over networks, technologies to effectuate data minimisation, as well as technologies for the negotiation of privacy preferences (for example, P3P¹). The research priorities for PETs have been studied and outlined in the Roadmap for Advanced Research in Privacy and Identity Management (RAPID) in 2003.² The study concluded *inter alia* that the solutions offered by PETs, however, remained rather fragmented and that the adoption of PETs remained in general quite low and therefore not yet satisfactory.

Other international programs and projects which have researched identity management include the Network of Excellence (NoE) Future of Identity in the Information Society (FIDIS) and the project Privacy and Identity Management for Europe (PRIME), both under the Sixth framework programme of the EU Commission. In FIDIS, the requirements for the future management of identity were researched by a multidisciplinary network of research groups from various countries. These requirements are described in various deliverables outlining the technologies, infrastructures and framework needed for the trustworthy and secure management of digital identities.³ PRIME aimed to demonstrate the viability of privacy-enhancing identity management and set out the principles and requirements for an architecture and the development of a demonstrator for a user-centric IdM system based on roles and credentials.⁴ PRIME work is continued in the Seventh framework programme in PrimeLife.⁵ The GUIDE project researched the creation of an architecture for e-government electronic identity services and transactions across Europe.⁶ Research on privacy and data protection aspects of identity management was also done in a LEGAL-IST study of 2005.⁷

Furthermore, a study of the ENISA Ad Hoc Working Group on Privacy and Technology studied the gaps between data protection regulation and realities presented by state-of-the-art technologies, including technologies used in IdM systems.⁸

TURBINE focuses on the deployment of multiple pseudo-identities, authenticated with the use of biometrics.

¹ See below at section 6.10. The World Wide Web consortium ('W3C') developed a Platform for Privacy Preferences ('P3P') which is a format for specifying the privacy policies of web servers. P3P enabled web browsers enable users to specify their privacy preferences, which are then matched against the web server's privacy preferences. See for P3P in general also <http://www.w3.org/P3P/>

² *Roadmap for Advanced Research in Privacy and Identity Management (RAPID)*, EU project nr. IST-2001-38310 under the Sixth Framework Programme.

³ *Future of Identity in the Information Society project (FIDIS)*, EU project nr. 507512 (2004-2009), www.fidis.net

⁴ R. Leenes, J. Schallabök, M. Hansen, PRIME white paper, Third and final version, 15 May 2008 (hereafter PRIME White paper v.3.0), p. 7.

⁵ See <http://www.primelife.eu/>

⁶ See GUIDE, EU project nr. IST-2003-507498, of which project information was previously on <http://www.guide-project.org/>

⁷ Legal-IST, Doc. No 11, *Report on Privacy-Identity Management*, 4 November 2005.

⁸ ENISA Ad Hoc Working Group on Privacy & Technology, *Technology-Induced challenges in Privacy & Data Protection in Europe*, M. Langheinrich and M. Roussopoulos (eds.), October 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_wg_report.pdf

Identity management has also been subject of national research. Examples include the IDEM project and the ADAPID project⁹ in Belgium and 'the Identity Management Systems (IMS) : Identification and Comparison Study'¹⁰ in Schleswig-Holstein in Germany.

In the present research report, various legal aspects of IdM systems are analysed and described.

For this purpose, a recapitulation of some basic concepts and terms as they appear in previous research reports and publications is necessary.

This report will not discuss in depth the use of biometrics in IdM systems. The legal aspects of biometrics is subject of another TURBINE deliverable.

Identity management

'*Identity management*' can be generally described as systems and processes utilized *to administer and control* user access rights and restrictions to resources, to authenticate the users and, if needed, to confer authorization rights.

Identity management may seem a recent topic, but it is in fact is not so new. Many governments and private entities issue since long documents such as passports, identity (ID) cards, drivers licenses, bank or employee cards, etc to 'manage' individuals. These documents are used for identity authentication (in particular user/person authentication) or as proof of particular privileges, e.g. the right to drive a car, the right to manage a bank account or the right to enter the factory premises. Paper documents usually contain one or several authenticating factors that make it possible to authenticate the card holder (e.g. a picture or a signature) and a reference, for example a document number. Paper documents shall also be tamper proof so that one can have a sufficient degree of confidence that the document is authentic and duly issued. If these basic requirements are fulfilled, the paper documents can be used as an ID document.¹¹

While there are similarities between paper-based and IT-based identity management systems, the term 'identity management' is mainly used to refer to an IT-based system.

Persons in both the physical and the digital world are often represented by only some of their characteristics, also called *attributes*, for example, being an employee and having an employee number or being a customer and having a loyalty card. These attributes reflect a *partial identity* of a person.

In a digital world, however, these partial identities are represented by data sets and can be managed by technical means. Identity management provides *tools for managing these partial identities*.

Another way to define 'identity management' is hence as 'the managing of partial identities of entities, i.e. definition, designation and administration of identity attributes as well as choice of the partial identity to be (re)-used in a specific context'.¹²

⁹ For the IBBT project 'Identity Management for eGovernment' (IDEM) of the Belgian and Flemish government, see <https://projects.ibbt.be/idem/index.php?id=126> ; For the ADvanced APplications for electronic IDentity Cards (ADAPID) project of the Flemish government, see <http://www.cosic.esat.kuleuven.be/adapid/>

¹⁰ Independent Centre for Privacy Protection (ICPP) & Studio Notarile Genghini (SNG), *the Identity Management Systems (IMS) : Identification and Comparison Study*, September 2003, available at http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMSStudy.pdf

¹¹ See Legal-IST, o.c. at footnote 7, p. 52 ; T. Olsen and T. Mahler, 'Identity management and data protection law : Risk, responsibility and compliance in 'Circles of Trust' – Part I', *Computer Law & Security report*, 23 2007, (342), p. 343 *et seq.*

¹² Modinis, Study on Identity Management in eGovernment. Common Terminological Framework for Interoperable Electronic Identity Management, v.2.01, November 2005, p. 11, available on <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf>.

Identity Management system (IdM system)

An '*Identity management system*' (IdM system) is a system which 'is the organizational and technical infrastructure used for the definition, designation and administration of identity attributes'¹³, 'including the development and choice of the partial identity and pseudonym to be (re)-used in a specific context or role'.¹⁴ Others have describe IdM systems simply as a 'way to transfer, store, and process personal data in electronic form'.¹⁵

There are many descriptions and definitions of IdM systems possible since the concept of IdM system refers to a broad category of systems that can be used to support a controlled access to resources which for some reason are being restricted to certain users. Such systems are many and varied.¹⁶ Even information systems with the aim of profiling user's behaviour and preferences as part of for example personalized services or Customer Relation Management (CRM) systems have sometimes been seen as identity management systems.¹⁷

IdM systems can also be seen as an integral part of information security. Information security is designed to protect information of value against unauthorized access and changes.¹⁸

An IdM system can be divided into three phases¹⁹:

- (1) *registration* or *enrolment*, i.e. registration of a person by deciding upon one or more identifier(s) that will be used for that person in the system and by issuing to the same person authenticators for later access to the system ;
- (2) *authentication*, i.e. the presentation by the enrolled person of the identifier(s) and the use of the authenticator(s) to verify the legitimate use of the identifier(s) ; and
- (3) *authorization*, i.e. after successful authentication, establishing the rights and privileges that person has with regard to the services.

A clear distinction needs to be drawn between authentication (the process whereby confidence is established in an assertion of identity) and authorization (what rights does the user have).²⁰ Authentication and authorization will be further described in section 3.1 below.

IdM systems aim to rationalize the three processes set out above.

Identity providers and service providers of an IdM system

Authentication of the user could in principle be carried out by the service provider or, in case the service provider does not provide the authentication, an identity provider who is in that case a third party. The *authorization* to resources and applications is most often managed by the service provider based on a so-called credential and/or certificate (see also *below*) provided by the identity provider.

¹³ *Ibid.*, p. 12.

¹⁴ See A. Pfitzmann and M. Hansen, Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (Version v0.31 Febr. 15, 2008), p. 31. available at http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf

¹⁵ M. Rundle, *The New Identity Management Infrastructure – Helping Governments Serve Citizens*, presentation of 9 March 2007, Barcelona, slide 5, available on http://www.egovbarriers.org/downloads/Mar09Workshop/The_New_Identity_Management_Infrastructure.pdf

¹⁶ See M. Bauer, M. Meints and M. Hansen, *D3.1 Structured Overview on Prototypes and Concepts of Identity Management System*, FIDIS, September 2005, available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf.

¹⁷ A characteristic of these is that the user's profile or 'identity' is derived or abstracted from observing the user's behavior and use of the system.

¹⁸ F. Tewari, *Identity management defined. How to position enterprises into the identity management framework*, 19 December 2005, p. 5, available on <http://www.tudelft.nl/live/binaries/70163a1a-37c1-4f78-8cb0-50653874a96b/doc/frank-t.pdf>

¹⁹ See also Legal-IST, *o.c.* at footnote 7, p. 53-54; About authentication, see also R. Clarke, *Authentication: A Sufficiently Rich Model to Enable e-Business*, 26 December 2001.

²⁰ R. Clarke, *o.c.* at footnote 19, p. 19.

Service providers and identity providers can be public authorities or their agents or independent private entities.

When the service provider is at the same time identity provider, e.g., an employer for the IdM system of his employees, such organization is also referred to as a '*closed, enterprise or organizational managed IdM system*'.

In a *multi-organization identity management system*, the authentication of users is in principle delegated to an identity provider. In case the service provider involves a third party identity provider, this is also referred to as an '*open or third party managed setting*'.²¹ This setting implies that the service providers need to *trust* the identity provider with respect to the authentication of users.

In addition, the enrolment by the service or the identity provider whereby the person has been identified shall also be trusted.

This enrolment or registration will be *one of the most important and crucial aspects* of an IdM system, while being at the same time one of the most weak elements. As it has been rightly pointed out by Roger Clarke, this is about the process whereby a real-world entity is recognised, and its 'identity' established.²² Even in case strong identifiers are used in an IdM system (e.g., a biometric in a passport), which could improve the authentication process considerably, such identifiers will only prove to be useful and effective in so far as a reliable enrolment (connecting the right identifier to the right identity) has taken place. More checks may be needed than just 'standard procedures'.²³

The enrolment or registration is an aspect that is often poorly understood and underestimated in IdM systems. It is often not addressed or sufficiently specified.

Single Sign-On (SSO)

'*Single sign-on*' (SSO) is the solution which allows that a data subject can use his user account(s) at different services based on the login to one user account at one service. SSO offers the facility to provide identification and authentication data *just once*, after which the data subject is able to make use of different services, for example on the Internet, without repeatedly having to provide same data. SSO is intended to provide data subjects with a so-called 'more seamless user experience'.²⁴

SSO may be provided by *one* organization (for example, by an university or an employer) or by several organizations (*multi-organizational SSO*) (for example in the Microsoft .NET Passport system for managing data subjects' access to multiple websites and resources after a single authentication procedure, as discussed *below*).

2.2 Some examples of identity management systems

Because of the legal analysis later in this report, including various comments of the Article 29 Data Protection Working Party, two examples of identity managements will hereinafter be discussed : .NET Passport and Liberty Alliance.

²¹ See Th. Nabeth (ed.), *FIDIS deliverable D2.3. Models (v2.0)*, 6 October 2005, available at <http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.3.models.pdf> ; See also Turbine document 1.2.1 'Services and scheme for multiple trusted identities',

²² See also Legal-IST, *o.c.* at footnote 7, p. 54.

²³ See also J. Grijpink, 'Een beoordelingsmodel voor de inzet van biometrie', *P&I*, 2006, p.14 *et seq.*

²⁴ Legal-IST, *o.c.* at footnote 7, p. 57.

.NET Passport

.NET Passport was an Internet-scale identity management systems that was set up in 1999 by Microsoft. While the system was initially mainly aimed for registering and accessing a Hotmail account at Microsoft and for registering and accessing MSN, it soon provided SSO across multiple organizations to help users to save time and avoid repetitive data entries when surfing on the Internet.²⁵

In 2002, there were over 250 million registered accounts worldwide and 69 external websites participated in .NET Passport, of which 22 were in the EEA.²⁶

Due to privacy and data protection concerns, the Article 29 Working Party started an investigation into the functioning of the .NET Passport service in 2002.²⁷

These enquiries resulted in a number of requirements that had to be met by Microsoft in order to be compliant with the EU Data Protection Directive. The requirements addressed the lack of information given to data subjects, the value and the quality of the consent given by the data subjects, the proportionality and quality of data collected and stored by .NET Passport and further transmitted to affiliated sites, the data protection rules applied by the websites affiliated to .NET Passport, the necessity and the conditions of the use of a unique identifier, the exercise of the rights of the data subjects and the security risks associated with the operations.²⁸

Microsoft later on discontinued its use of .NET Passport for sites outside the Microsoft domain in 2003. .NET Passport became a single-organization single sign-on identity management system.

.NET Passport has been subsequently renamed into 'Windows Live ID' which may be integrated into Windows CardSpace, part of Windows Vista and which allows the management of various digital identities by the user.

Liberty Alliance

The Liberty Alliance Project is very different from .NET Passport. It was in fact formed in 2001 - as a reaction to Microsoft's' success - as a *contract-based group*, establishing open standards for federated network identity. It is an ad hoc industry consortium of more than 100 organizations worldwide as of early 2003, in which different companies participate, pursuant to the terms of agreements.²⁹

Liberty's *federated identity management* provides a framework for a multi-organization identity management system whereby service providers and identity providers operate in federations that have business relationships with each other based on the Liberty Alliance architecture and operational agreements.

A network of thus collaborating organizations is referred to by the Liberty Alliance as a 'circle of trust'.³⁰ Because compliance with existing data protection legislation was deemed important, the Liberty Alliance has provided an overview of their 'best practices' in complying with these laws

²⁵ About .NET Passport, see also J. Dumortier, 'Combining Personalised Communications Services with Privacy-Friendly Identity Management', Proceedings of the 44th FITCE Congress Vienna, 1-3 September 2005, p. 142-146, available at http://law.kuleuven.be/icri/all_pubs.php?action=pubs_staff&staffid=1&where= ; T. Olsen and T. Mahler, *l.c.* at footnote 11, p. 346 *et seq.* ; R. Oppliger, 'Microsoft .NET Passport and identity management', in *Information Security Technical Report*, Vol. 9 No. 1, 2004, p. 26-34.

²⁶ See Article 29 Working Party, *Working Document on on-line authentication services*, WP 68, 29 January 2003, p. 5, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_en.pdf

²⁷ See Article 29 Working Party, *First orientations of the Article 29 Working Party concerning on-line authentication services*, WP 60, 2 July 2002, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp60_en.pdf

²⁸ Article 29 Working Party, *o.c.* at footnote 26, p. 6-11.

²⁹ See the website of Liberty alliance at <http://www.projectliberty.org/liberty/about> and for its members, see http://www.projectliberty.org/liberty/membership/current_members

³⁰ See Liberty Alliance Project, *Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation*, February 23, 2005. See also T. Olsen and T. Mahler, *l.c.* at footnote 11, p. 346 *et seq.*

when developing the Liberty specifications³¹ as well as guidelines for participating organizations on possible contractual frameworks and operational rules.³²

Other initiatives and the future

Many other examples and initiatives on IdM exist.³³ One is OpenID, which provides for a single sign-on system for the Internet. OpenID is an open, decentralized, free framework for user-centric digital identity and seems to spread fast.³⁴ Shibboleth, which is focusing on SSO, is another important example and often used at universities.

The protocol Idemix provides for an anonymous credential system (pseudonym system with private credentials) for data minimization and is used in PRIME.³⁵

Industry consortia and standardization bodies have been further involved in the development of technical standards for federated identity management.

Other initiatives are inspired by 'The Seven Laws of Identity' (hereinafter the 'Seven Laws'), developed through an open consensus process on the Internet.³⁶ The principles of the 'Seven Laws' are (1) user control and consent, (2) minimal disclosure for a constrained use, (3) justifiable parties (4) directed identity, (5) pluralism of operators and technologies, (6) human integration and (7) consistent experience across contexts (see also *below* in section 3.2).

What is clear at this point is that besides centralized or federated identity management systems, *user-centric identity management* comes its way.

New models 'involve (...) the users in the management of their personal information and how that information is used, rather than to presume that an enterprise or commercial entity holds *all* the data'.³⁷

TURBINE also proposes a user-centric IdM system model, which allows the data subject to manage its partial identities and the personal information released through the use of pseudo-identities or pseudonyms.

³¹ See Liberty Alliance Project, Privacy and Security Best Practice, v. 3.0, November 12, 2003.

³² See Liberty Alliance Project, o.c. at footnote 30.

³³ For some overview, see also Identity management framework examples, available at http://wiki.enisa.europa.eu/index.php?title=Identity_management_framework_Examples&printable=yes

³⁴ For more information, see <http://openid.net/>

³⁵ More information on Idemix can be found at <http://www.zurich.ibm.com/security/idemix/>

³⁶ See K. Cameron, 'Laws of identity in brief', *Kim Cameron's Identity Weblog*, 2006, <http://www.identityblog.com/?p=353>

³⁷ Prime White paper v.3.0, p. 2 where the text was cited from the *Liberty Alliance Project Whitepaper : Personal Identity*, 23 March 2006, available at [http://www.projectliberty.org/liberty/content/view/full/340/\(offset\)/30](http://www.projectliberty.org/liberty/content/view/full/340/(offset)/30)

3. Functional Requirements, Architecture and Organizational structure of Identity Management Systems

3.1 Functional requirements

3.1.1 Identification, use of pseudonyms and anonymity

IdM systems may be used to identify a person. In a computer network infrastructure, however, not only persons, but also items, such as hardware, network or application components, sometimes also called 'entities' or 'subjects', can be identified. For the purpose of this deliverable, we only study the identification of natural persons, herein also called data subjects.

Identification

The concept of *identification* is not clear at all. The term is not found in national, EU or international legal instruments which relate to IdM systems. Conceptually, one distinguishes between two processes in IdM systems, both of which could be called identification.

Firstly, identification could refer to the process of *obtaining an identifier for a user*. This identifier will generally represent only a characteristic of the user ('partial identity', see *below*) and is used to distinguish this user from other users. In practice, many Internet services and also IdM system services do not need to know the (full) identity of the person behind a user name. It suffices to verify that the user is the same as the user who earlier enrolled in the service.

Secondly, the term could be used to describe the process of identifying the individual *behind* an identifier. This process may require additional checks, for example during the registration and enrolment phase of an IdM system.

It is important to understand that these two processes of 'identification' are to be distinguished from one another as they have a very different meaning.

In addition, identification can be done from *various perspectives* : identification can be done from the perspective of an *attacker* of a network or system, but it can also be seen from the perspective of the *owner* of an application (data controller), being it a service supplier, an employer or the government. For each of the fore mentioned interested parties, identification will have a different meaning. The service supplier may want to know whether the person is a customer, the employer wants to know whether the person is an employee and is permitted to enter a high security installation and the government wants to be sure that it is the named citizen that claims the tax refunds. Also *users* of a network or system have an interest in how they are identified. Users have in addition also an interest in identifying and authenticating elements of an IT-system, such an application, system or website, for example for submitting online banking orders. This will however not be further discussed in this report.

From a general technological point of view, the identity in an online environment and in a system architecture in particular is generally not seen as one single entity or identity of a data subject, but rather as a *group of partial identities*³⁸ that need to be managed. Identification will refer to such partial identity. A partial identity may be represented by for example a nick name or an e-mail address in a chat room. These partial identities refer to a characteristic (also called attribute) of a

³⁸ The term 'partial identity' also refers to the fact that a person is in an online environment only represented in part, by some characteristics, underlining the inherent incompleteness of 'digital persons' in an online environment as compared to the real world person. See R. Clarke, *Terminology Relevant to 'Identity in the Information Society*, Revised Version of 9 august 2008, p.3, available at <http://www.anu.edu.au/people/Roger.Clarke/DV/IdTerm.html>

person (for example, being 18 years old), a role (for example, being a customer or being chief editor of a magazine) or a specific context relevant for that person and representing that person.³⁹

For this deliverable, we only investigate how a natural person can be identified for purposes of an IdM application. We hereby approach identity from a legal point of view, making abstraction of identity as a philosophical, sociological or psychological term. In section 4, we investigate whether there are any legal rules relating to the identification of natural persons, in particular the process of providing an identifier for a person, but also relating to the process of checking and revealing the identity behind the identifier, and whether there are rules relating to the authentication and authorization functionalities in an IdM system.

Pseudonyms and pseudonymity

One way to increase one's privacy in accessing services, is using a pseudonym. A pseudonym is in fact an identifier⁴⁰ (instead of the real name) for a (partial) identity.

For international cooperation and technical developments, standards, including for information security, are being developed and sometimes include definitions on terms. Pseudonymity is presently being widely discussed in an attempt to provide clear technical definitions. Pseudonymity is for example defined as '*that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use*'.⁴¹

The use of the pseudonyms is in fact closely related to anonymity (see below) in the sense that the use of a pseudonym prevents the user to reveal his/her identity.

The difference with anonymity is that while for a pseudonym, the association between the user (or his identifier, such as name, username, alphanumeric code or pseudonym) and the underlying entity (the person, in the real world often represented by this civil identity) is not known, *but in principle could be known*, for anonymity the user (or his identifier) cannot be linked to the underlying entity at all.

A pseudonym permits in addition that the (partial) information about one's partial identity that a user provides to a communication partner is not linkable (as compared to a global name or identifier).⁴²

In the context of user-controlled IdM systems, the pseudonym would be understood as be chosen, used in specific contexts and controlled by the data subject.⁴³

Anonymity

Anonymity is *the possibility to use a resource or service without disclosure of the user's identity*.

From a technical point of view, anonymity is defined by some as 'the state of being not identifiable within a set of subjects, the anonymity set'.⁴⁴ The use of a pseudonym, however, will often allow to reverse the situation and to identify the data subject in a controlled way and subject to a list of conditions for accountability purposes if needed.⁴⁵ The use of the term anonymity will often refer to

³⁹ See A. Pfitzmann and M. Hansen, *o.c.* at footnote 14, p. 29.

⁴⁰ About identifiers, see *below* section 4.1.2 .

⁴¹ See the proposals in the framework of the review of the ISO 15 408 – 2 standards on Information Technology – Security techniques – Evaluation criteria for IT Security – Part 2 : Security Functional Components, term 13.2.1. For the text, see the document circulated for information early 2008 and available on <http://www.gammasl.co.uk/ist33/27N6294.pdf>

⁴² See K. Borcea-Pfitzmann, E. Franz and A. Pfitzmann, 'Usable Presentation of Secure Pseudonyms', in *DIM 2005*, p. 70 et seq.

⁴³ About the different types and representations of pseudonyms, see K. Borcea-Pfitzmann, E. Franz and A. Pfitzmann, *l.c.* at footnote 42, p. 71.

⁴⁴ See A. Pfitzmann and M. Hansen, *o.c.* at footnote 14, p. 8.

⁴⁵ See the definition of the term 'reversible pseudonymity' in the framework of the review of the ISO 15 408 – 2, see *above* at footnote 41, term 13.2.6, p. 72.

a more irreversible way of connecting a data subject with his (civil) identity. For the term pseudonym and the term anonym, the term nym, encompassing both, is sometimes suggested.⁴⁶ Because of the varying degrees of anonymity, some scientists have already proposed to measure the degree of anonymity.⁴⁷

3.1.2 Authentication

In an *authentication* process, the authenticity of a claim of a person (for example, of a person who seeks access to a place or a system) is *verified* against previous information. This previous information may be given to that person, obtained about or obtained from that person. The verification of a claim can be done by various means. In general, there are three different methods for authentication.⁴⁸ The verification can be done by something that someone *has* (e.g., a key or a smart card), by control of something that a person *knows* (e.g., knowledge of an access code (user identifier and password), or control of something that someone *is*, or a combination of all these three methods. The latter method refers to the use of biometrics, which allow to check (mostly) unique biological characteristics submitted by an individual with previous biometric reference data of the same person. Because biometrics can in principle not be handed out or forgotten, it is believed that biometric recognition will play an increasing role in the authentication processes.⁴⁹

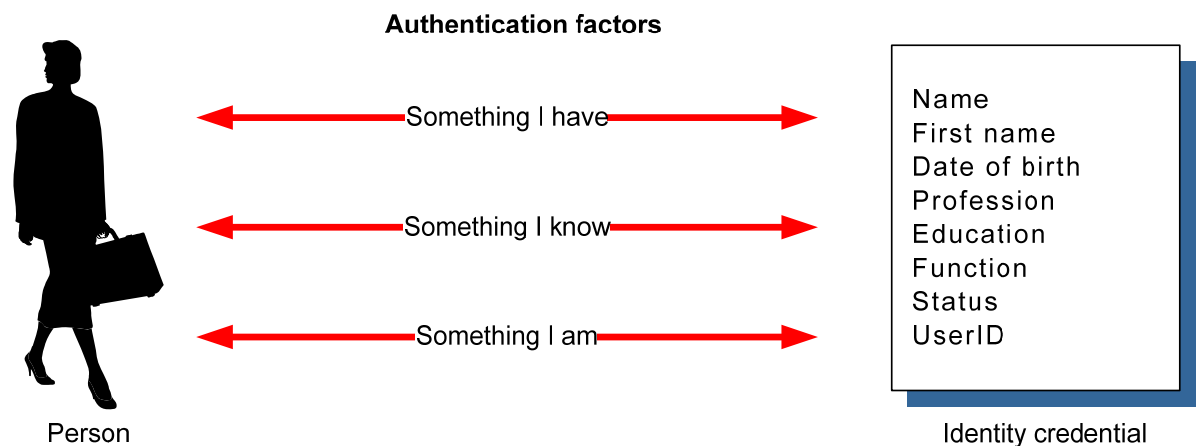


Figure 1: Authentication

There are in general three possible ways to authenticate a person: (1) possession of a credential object, (2) knowledge of a secret and/or personal information and/or (3) an individual biometric feature such as a physiological or anatomical attribute or a distinctive behaviour (biometric comparison).

⁴⁶ See R. Clarke, o.c. at footnote 38.

⁴⁷ See also C. Diaz, S. Seys, J. Claessens and B. Preneel, 'Towards measuring anonymity', in *Designing Privacy Enhancing Technologies*, H. Federath (ed.), vol. 2482, LNCS, 2002, available at <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.10.986>, and the references therein to related research for measuring anonymity.

⁴⁸ Another method for authentication is by the location. The location can often also offer identity information for verification purposes.

⁴⁹ E. Kindt & L. Müller (eds.), *D.3.10 Biometrics in identity management*, Fidis, 28 December 2007, p. 12.

At the same time, the use of biometrics raises concerns. The use of a PIN does not necessarily identify a person. Biometrics, however, mostly involve characteristics which are *unique* for a specific human being and therefore allow identifying a person.⁵⁰

3.1.3 Authorisation (permission/delegation/mandate)

IdM systems may typically also contain authorization functionalities. Such functionality could be described in general as the possibility for a person or a system to authorize or permit a data subject to perform certain actions under specific conditions. Authorization functionalities may range from merely *granting access* to specific information ('permission' or 'privileges') up to *authorization* to perform a legal act on behalf of the grantor. In case the data subject acts on behalf of the grantor, the authorization is often referred to as a 'delegation' or a 'mandate'.

The authorisation functionality of an IdM system could merely establish what permission/privileges or delegation/mandate a data subject (user) has with regard to specific services and allow such person to act accordingly or could provide the possibility to grant such authorizations.

3.2 Additional requirements

In addition to the above three requirements, additional requirements apply for IdM systems. Several additional requirements have been analyzed and described in relevant studies and literature on IdM systems.⁵¹ Some important user-oriented requirements for IdM were also pronounced in the so-called 'Seven Laws of Identity' (see also *above*) (hereinafter 'Seven Laws') which are intended to codify a set of fundamental design principles to which a universally adopted, sustainable identity architecture must conform. The 'Seven Laws' have parallels with general principles of data protection legislation, including the EU Data Protection Directive, but do not fully map with these principles.⁵²

Hereunder are some of the additional requirements which are in our view relevant for our report.

Accountability

IdM systems will in principle require that data subjects and other users can be held accountable when using an IdM system.

Accountability could be described as identifying the interacting parties, verifying *who* did *what* and *when* in an electronic interaction on a network.

Secure logging possibilities for an IdM system and *digital evidence* requirements are relevant to meet this requirement of accountability.

An IdM system shall hence provide means to trace the access to the system and the use of the information therein. This requirement of accountability will hence also be important for liability purposes.

⁵⁰ See also Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 8, in which the Article 29 Working Party has made the same observation about the special nature of biometric data as an example of personal data. Biometric data is particular as they do not only contain information *about* an individual, but also permit to establish a link to a person: '(...) *As such, they can work as 'identifiers'. Indeed, because of their unique link to a specific individual, biometric data may be used to identify the individual. (...)*'.

⁵¹ See e.g. Independent Centre for Privacy Protection (ICPP) & Studio Notarile Genghini (SNG), *o.c.* at footnote 10, p. 73 *et seq.* In this study the requirements were deduced from various scenarios for IdM systems.

⁵² See, e.g., A. Cavoukian, *7 laws of identity – the case for privacy-embedded laws of identity in the digital age*, Information and Privacy Commissioner of Ontario, 2006.

Privacy and Security

Various other requirements are often imposed upon IdM systems because of security and general privacy reasons.

From a security point of view, the IdM system shall for example provide *confidentiality* as to the data contained therein and shall guarantee their *integrity*. Other security requirements include *availability*, *reliability*, *authenticity (prevention of plagiarism)*, *non-repudiation* (the sender cannot deny that a message originates from him), *prevention of unauthorized access* and *prevention of misuse (theft)*.⁵³

From a general privacy point of view, the processed personal data *shall not be linked* (see also below) and *shall be reduced* as much as possible.⁵⁴ Other general privacy requirements include *prevention of profiling* and possibility to use *pseudonyms or anonymity*. *Logging* could also be mentioned in order to be able to trace access by others to one's personal data.⁵⁵

There are various other tools to enhance security and privacy by minimizing the risk of personal data misuses. For example, verifying the communicating entity's digital signature and public key certificate through some form of public key infrastructure (PKI) ensures that private data are only given to communicating parties considered as trustworthy. Such techniques help prescribing which data has to be revealed and for what purpose.

The problem is, however, that many precaution security measures can only serve to protect accidental or unclear private data transmission and *that they cannot protect from a malicious but trusted communicating party*, since the believed trustworthy communicating party can pass on the private data to others intentionally or unintentionally, warehouse it, link it and/or use it maliciously. For this reason, additional requirements shall be formulated.

Such additional requirements are unlinkability, unobservability⁵⁶ and revocability.

(Un)linkability

Unlinkability is the possibility to use multiple resources or services without others being able to discover that the same user is making use of these resources.

For some specific IdM systems, the efficiency and benefit of the IdM system will depend on the possibility to link information or transactions originating from the same identifiers (linkability).⁵⁷

For other IdM systems, especially if an IdM system is used across different contexts (multi-purpose application or multi-organizational identity management), linkability of the information and the transactions will in most cases *not* be desirable (unlinkability).

These link abilities and other types of linking information relating to the individuals involved in IdM systems could be prevented, for example by using a *pseudonymous credential* protocol which only reveals pseudonymous identities.

Credentials, unlike digital signatures for enabling accountability of communication partners and their transactions, can be reliably used in many contexts, as its use does not lead to data trails or unwanted disclosure of personal data.

⁵³ Independent Centre for Privacy Protection (ICPP) & Studio Notarile Genghini (SNG), *o.c.* at footnote 10, p. 73 -74.

⁵⁴ An IdM system which pays much attention to minimize the data processed is for example Idemix which provides for far reaching data minimization.

⁵⁵ Independent Centre for Privacy Protection (ICPP) & Studio Notarile Genghini (SNG), *o.c.* at footnote 10, p. 74.

⁵⁶ See also G. Müller and S. Wohlgemuth (eds.), *D3.3 Study on Mobile Identity Management*, FIDIS, May 2005, p. 24, available at www.fidis.net, where it is stated that the requirements of unlinkability, unobservability (and untraceability) of a subscriber's identity in a mobile service originate from the electronic payment systems world and are also aligned with the general anonymity requirements defined by Pfizmann and Hansen.

⁵⁷ For example, the use of the ITU's X.509 standard for certificates permits that information from different contexts can be linked.

So-called '*private credentials*' are derived from a certificate issued on a *pseudonym* of a same person.⁵⁸ This means more specifically that a data subject may obtain a credential from one organization using pseudonym a, while using the same credential vis-à-vis another organization while use pseudonym b without revealing pseudonym a. The use of different credentials is in principle unlinkable.⁵⁹

Multiple private credentials can be created from a single certificate that are neither linkable (i) to each other or (ii) to the issuance interaction in which the master certificate was obtained.

(Un)observability

Unobservability is the possibility to use a resource or service without others being able to observe that the resource is being used.

Revocation

Another important requirement for an IdM system is revocability of the identifier for the user or of the authentication factor in case of termination of the relationship in which the identifier was issued. Revocation is in addition also crucial in case of misuse or theft of the identifier or the authentication factor. Access rights and other authorizations could also be revoked.

For some specific authentication factors which can not be renewed, such as biometrics, this may be a problem. The TURBINE project focuses on the development of a solution on this requirement for biometrics.

3.3 Architecture and organizational structure

Significance of the architecture of a system

The architecture of a computer system determines how the components of the system are organized and integrated, including the ways the flows of data take place.⁶⁰ The architecture will also determine where the data will be stored (and will be accessible).

In general, the architecture of an IT system will *create possibilities* for the system but *also restricts* its abilities. It is therefore of crucial importance, because it will not only determine how the system will function and can be used, but also how the system can be further developed in the future. The architecture of a system is the core of the system and is further characterized by the fact that it is hardly changeable once implemented, unless the whole system would be replaced. Therefore, the consequences of an architecture need to be analyzed before making a decision about adopting a system.

The architecture of IdM systems is of relevance for an evaluation of the legal aspects of a system. Although the *architecture of a system will not specifically be addressed in (legal) regulations*, it will be necessary to analyse such architecture as it will for example reveal aspects not only relating to security but also relating to privacy and data protection.

Data protection issues shall be addressed at the early stage of setting up the architecture of the system.⁶¹ The general rules on data protection can be found in the Directive 95/46/EC and the

⁵⁸ Private credentials (or certificates) allow for releasing partial information contained in a master certificate, for example that one is older than 18 years. They play a crucial role in the PRIME project. See the PRIME White paper v.3.0, o.c. at footnote 37, p. 8, with references to J. Camenisch, A. Lysyanskaya, 'A signature Scheme with Efficient Protocols', SCN, S. Cimato, C. Galdi, G. Persiano, (eds.), vol 2576 *Lecture Notes in Computer Science*, Berlin, Heidelberg, Springer, 2002, 268-289.

⁵⁹ Independent Centre for Privacy Protection (ICPP) & Studio Notarile Genghini (SNG), o.c. at footnote 10, p. 87.

⁶⁰ Principles and models of architecture are under development all the time. Recently, much attention is given to so-called Service Oriented Architectural (SOA) models and Service Oriented Infrastructures (SOI), for enabling complex collaborations among various users and systems of different expertise and differing levels of authorisation.

Directive 2002/58/EC. In some cases, the architecture of a system is even to be adapted because of data protection concerns.⁶²

Privacy in an architecture is also to be taken care of, but is not understood in the same way as privacy in legal texts. Privacy in an architecture will refer to a more technical understanding of privacy, referring to preventing unintended leakage of information. Particular *privacy threats* in systems include *surveillance* (i.e. the monitoring of electronic communications and transactions), *the aggregation of information* (i.e. the linking of information as related to each other or to a particular subject) and *identification* (i.e., connecting information to a person). In order to prevent or limit such privacy threats, research is ongoing on how to technically limit or exclude such threats to the privacy, often seen from the point of view of attackers to the system.

Privacy protecting concepts in an architecture include *unlinkability*, *unobservability*, *anonymity* and *pseudonymity*. The understanding of these concepts is already outlined to some extent in security evaluation criteria for IT products and systems, such as the Common Criteria system standards, the standards developed in the International Standardization Organization (ISO) (e.g., ISO 15408/1999) and in proposals for definitions by the research community, such as the proposed terminology by Pfitzmann and Hansen.⁶³

To the extent an architecture could guarantee the described privacy concepts of unlinkability, unobservability, anonymity and pseudonymity in a system, the privacy of the system will considerably be improved.

Without explicit legal specifications for specific IdM systems or IdM systems in general, however, these privacy concepts remain general and are difficult to enforce.

Importance of the organizational structure (in particular, the enrolment)

The organizational structure of an IdM system will also be of crucial importance. Guidelines and principles that are applicable include international standards, such as ISO/IEC standard 27002 (formerly ISO 17799).

Because the functionality of the IdM system will either be reliable authenticated access to particular resources or effective 'anonymous' use of particular systems, as appropriate, the organization of, for example the enrolment or of the handing over of personal data to authorities, is crucial.

This is, however, not always addressed in general organizational guidelines.

Centralization v. Federation of Identity and Service providers

There are basically two forms of organization of IdM : centralization and federation.

Centralization means that users enrol with a central identity provider, who acts as a single gateway for the users' management of identity.

Although there may be operational (easiness to maintain and to provide user support) and cost advantages to a centralized identity provider, (e.g., a .NET Passport-like arrangement as described above), centralization implies *concentration of personal data* of users, which may result in possible

⁶¹ See also Legal-IST, Doc. No 11, *Privacy-Identity Management*, 4 November 2005.

⁶² See, e.g., the planned re-architecture of the global messaging architecture of SWIFT, the world's leading financial messaging provider, to a more distributed data processing and storage model. The re-architecture would allow for intra-European data to be stored only in Europe. This was announced by the SWIFT Board of Directors in 2007 after the system was scrutinized under data protection laws and is confirmed in the latest decision of the Belgian Data Protection Commission in the SWIFT case (See, Belgian Data Protection Commission, *Decision of 9 December 2008 relating to the control and the recommendations procedure started in connection with SWIFT CVBA*, p.80). The implementation phase is expected to last three to four years. See SWIFT, *Swift announces plans for system re-architecture*, 15 June 2007, available at <http://www.webcitation.org/mainframe>. The data protection objections were pronounced by the Belgian DPA and the EDPS in various opinions.

⁶³ See A. Pfitzmann and M. Hansen, *o.c.* at footnote 39.

security and privacy breaches (e.g., *monitoring* users behaviour or possibility for the identity provider to *merge* user profiles kept by service providers participating in the scheme) and in an attractive target for attackers.⁶⁴

Federated identity management, on the other hand, sometimes foresees the possibility of *choosing* among multiple identity providers. There is not necessarily a single “weakest link” in federated identity management and the Article 29 Data Protection Working Party esteems that the user may have more control over his identities. Data on users can be combined by pairs of sites only and these sites will determine their own mutual agreements.⁶⁵

Information sharing

An other important aspect of any identity management system is the exchange of information between its components and participating providers.

Information *sharing* can be perceived as a *risk from the point of view of personal data protection law*.

The organizations participating in an IdM system will need to manage the risks arising from the set up and operation of the identity management system. This could be done to some extent by contract.

Risk management however requires a more general approach and shall take into consideration the risks for *all* of the different stakeholders. A *risk analysis* would thus need to take into consideration that the risk picture depends on the perspective: for an end user, the risk of utilizing an identity management system may, e.g. involve the possibility of being monitored and profiled by many organizations. For a service provider, the risk of using an identity management system may, e.g. involve the loss of reputation (and customers) in case of perceived data protection breaches. A service provider should also consider potential liability for infringements of personal data protection laws.⁶⁶

Legal risk management is an integral part of the overall risk management process. Legal risk analysis (see further *below* in section 4) implies that both legal and other risks are considered and managed in an integrated process.

Multiple Identities and user-centric or user-controlled management

The essential research issues identified in the RAPID project included the need to focus on privacy-enhancing technologies for providing multiple and dependable identities to be implemented on the user’s side.

In the short term, users should be able to *create* and obtain identities (identifiers), and be able to *revoke* them when compromised or when not needed anymore.

A user-centric IdM system will require that a data subject is able to *choose* from a range of identifiers with varying degrees of observability and linkability.⁶⁷ This means that users should have a choice to operate anonymously, pseudonymously or known.⁶⁸ The goal of user-centric IdM systems is ultimately to enable the creation of identity providers who operate in the user’s interest

⁶⁴ See Article 29 Working Party, *o.c.* at footnote 26, p. 11.

⁶⁵ *Ibid.* at p. 14.

⁶⁶ T. Olsen and T. Mahler, *l.c.* at footnote 25, p. 349; See in this context also the proposed modifications to the E-Privacy Directive 2002/58/EC relating to notification of data breach.

⁶⁷ For a (more technical) description of user-centric IdM systems and protection methods against attacks on linkability and identifiability, see S. Clauss, D. Kesdogan, T. Kölsch, ‘Privacy Enhancing Identity Management: Protection against Re-identification and Profiling’, *DIM 2005*, p. 84 – 93.

⁶⁸ See also the requirements for privacy-enhancing identity management set forth in the PRIME White paper v.3.0, p. 11.

rather than the interest of the service provider.⁶⁹ The difference with a federated identity system is two fold. First of all, a user-centric allows the data subject to select an identity provider, for example, because of its security and privacy policies and practices, while choosing (another) service provider based on its services or goods. Moreover, the data subject will be able to use his credentials with more service providers in a user-centric model than in a federated system.⁷⁰

A user-controlled IdM system includes that the flow of the user's identity attributes are made explicit to the user and that the user has a large degree of control.⁷¹

In addition, users should also be able to use identities provided by public bodies or enterprises, as well as identities that were created by themselves and to mix the use (or cross-use) of these identities in order to increase or promote accountability. This is also identified as a requirement of an IdM system in the PRIME.⁷²

⁶⁹ OECD, Directorate on Science, Technology and Industry, *At a Crossroads : "Personhood" and Digital Identity in the Information Society*, STI Working Paper 2007/7, 29 February 2008, p. 44, available on <http://www.oecd.org/sti/ict/reports>

⁷⁰ Ibid., p.45.

⁷¹ Pfitzmann and Hansen refer to the 'notice and choice' guiding principle of user-controlled IdM systems. See A. Pfitzmann and M. Hansen, *o.c.* at footnote 14, p.32.

⁷² See PRIME White paper v.3.0, p. 11.

4. Legal Aspects of Identity Management Systems

The identity of a natural person and the identification of such person are not fixed legal concepts.

Both terms have various different meanings depending on the context. In *criminal* matters, identity and identification play a major role and specific criminal procedure law and rules will describe how identity can be established (for example, with the use of DNA) and how a person shall be identified (for example, with a line-up of witnesses). In *civil law*, the (civil) identity of a person may be relevant and required, for example, for entering into a land purchase contract or for family law purposes (such as for an adoption or a matrimonial contract). In *administrative law*, the identity of a person is laid down in some specific regulations (e.g., regulation concerning a national registry and registry number) and will be used in his or her relations with the government (e.g., for the filing of tax returns). In *human right* law and cases, the right to identity of a person covers many aspects, such as the development of personality and a right to dignity and even some very personal aspects, such as the right to change gender.

These are only examples which illustrate the different understanding of the concept of identity and identification.

In the sections below, a preliminary exploration of some legal aspects of the terms, concepts and functionalities which are relevant in IdM systems is made for purposes of unravelling the legal aspects of IdM systems. To illustrate this first analysis, examples of relevant legislation in different countries are given, without the aim of being exhaustive.

4.1 Identity, identifiers and identification

4.1.1 Identity

Civil identity

The identity of someone is in most civil law countries based upon the *registration* of one's identity at the time of birth in the birth certificate and the registration of this certificate in the birth register. The information that is registered is designed to uniquely identify someone, and typically includes not only name and family name, but also additional information, including date and place of birth, information about origin and about domicile. We will refer to this information about someone's identity as registered at the time of birth by the civil servant hereafter as to the 'civil identity'.⁷³

In many countries, *identity cards* are issued containing evidence of one's civil identity ('civil ID card'). The cards are based on the information in national or local registers, which in their turn are based on the information contained in the birth registers. The civil identity is hence a concept that follows from various provisions contained in the Civil Code of some countries⁷⁴ and which is further used in other areas of law, such as administrative and commercial law. In many countries, progress is made for the introduction of electronic identity cards (eID cards).⁷⁵

In other countries, where the use of identity cards is not common, or only recently in force⁷⁶, there may be a less uniform approach as to the meaning of (civil) identity. However, in such cases, other concepts referring to name and other identifying data are hence used, such as NAW data (the Netherlands, referring to 'Name, Address and Domicile'). In common law countries, where identity cards are not common, civil identity will also refer to one's name and may be proven by various

⁷³ A civil identity will then typically refer to the name, the date and place of birth, but also address etc.

⁷⁴ For example, France and Belgium.

⁷⁵ For example, in Estonia, Finland, Belgium and Italy.

⁷⁶ For example, the Netherlands and the United Kingdom.

other means, such as credit card, social security number or drivers' license. In all these situations, we could say that use of and reference is made to one's 'civil identity'.

The civil identity plays in general an important role in the relation of the citizens with the State and the State's agents/representatives and in relation to other persons in some regulated areas of law, such as the examples mentioned above. In specific circumstances, *legislation* will require the identification and/or require submission of the civil ID card of the person involved.⁷⁷ A person will in principle also have only one civil identity. In these cases, the IdM system where the civil identity of the person has to be proven, will have to be organised in such way that at the time of the *enrolment* of the individuals in the system, the identification is performed with sufficient guarantees.

Identity and the right (and obligation) to use a name

From the above, it is clear that a part of the (civil) identity is the right and obligation to carry a *name*.

Before the information society, which requires the representation of persons in IT systems, the name was important and in some countries strict rules applied as to how a name (including family name) was given. It was in many countries also mandatory to use this name and officials were instructed by law to use only the official name(s) in their documents.⁷⁸ Such legislation may have to be reviewed in view of IdM systems which intend to install the use of pseudonyms for privacy protection reasons.

Other legal aspects of identity

The concept of identity cannot be restricted to civil identity alone and the use of a name as described above. For the research of other legal aspects, it is required to place the concept of identity in a broader context.

The right to an identity will also emerge as a *right of personal expression of individual personality* and is as such closely related to the individual *right to self-determination and self-expression*.⁷⁹

These rights emerge from texts relating to fundamental rights and freedoms⁸⁰ and their meaning is gradually clarified in legal texts and case law. The aspects of human personality that are protected include one's name and identity, freedom from physical constriction, inviolability of the domicile and the right to privacy, freedom of speech and self expression, including in particular the right to choose one's image and the right to protect one's honour.⁸¹

These *fundamental rights* will play a role in the representation of an individual, e.g., the right to be represented by a pseudonym or in an anonymous way, as will be described *below*.

Furthermore, it is relevant to refer to the notion of '*virtual identity*'. While there are many attempts to describe or to define 'virtual identity', for IdM purposes, we assume that the concept of virtual or digital identity in fact refers to *the identifier* used to represent an identity (or partial identity) in the networked environment. As such, a 'virtual identity' will in principle refer to a real world person, who

⁷⁷ See for example, the Netherlands, where the Law on the obligation to identify oneself introduces since 1 January 2005 a more exhaustive and general identification obligation. For another example of legislation requiring identification, see the Law for the prevention of the use of the financial system for money laundering and the financing of terrorism of 11 January 1993, modified in 2004, which requires *inter alia* financial institutions to request copies of the ID cards of natural persons in Belgium.

⁷⁸ For an example, see Belgium, where a decree 'by which it is forbidden for each citizen to use another name or first name than these mentioned in the birth certificate' enacted during the time of Napoleon (Year 6 Fructidor II (23 August 1794)) is still in force.

⁷⁹ Independent Centre for Privacy Protection (ICPP) & Studio Notarile Genghini (SNG), *o.c.* at footnote 10, p. 21.

⁸⁰ The texts acknowledging individual liberties and freedoms are rather recent (period of Enlightenment). For long, identity was for legislation used as a tool to determine the person to whom rights and obligations were conferred (and to prosecute in case the (criminal) law was not abided). See Independent Centre for Privacy Protection (ICPP) & Studio Notarile Genghini (SNG), *o.c.* at footnote 10, p. 8.

⁸¹ *Ibid.*, p.12.

makes use of an identifier. In the Web 2.0 environment, various questions raise as to what extent the existing legal rules apply (e.g., relating to defamation, etc) and as to whether a virtual and real world identity have to be treated in the same way. This is here not further developed.

Roles and characteristics

In many contexts, however, the (civil) identity of a person is not always relevant, but rather a *characteristic, the capacity or the role* of a person in which he or she acts.

For the purchase of goods (other than real estate for which there is a publicity requirement by registration of the purchase deed or specific goods the purchase of which is regulated by law (e.g., alcohol) or services (other for which mandatory identification is obliged, such as financial services), for example, products in a store, the price and the subject has to be determined but the identity of the contracting parties is in many cases not relevant (except for some information for reliable later payment (e.g., by credit card) or later delivery). In a pharmacy, it is for the pharmacist important to know whether you have a prescription and/or whether you are insured. On the other side, it is important for the user to get the prescribed medicine from an established pharmacist. In these contexts, it is important that this additional information that is needed for the transaction (e.g., about the capacity or insurance) is provided, rather than information about just identity (although this may come with the additional information).

Legislation will in many cases protect the exercise of some specific roles which are relevant for the society, such as the role of pharmacists, but also of doctors, public notaries etc. and such professions will further to such legislation usually be organized in a professional organization which control the access to and the exercise of the profession. The enrolment of persons with such specific role in an IdM system shall in principle take such legislation into account and the professional organization may be best fit to organize the enrolment. A person may in principle also have various roles or capacities.

In again another and different context, identity nor the role of a person will be relevant. In such situations, it is sometimes sufficient to know that someone is a member of a group (without actually knowing who the person is) (e.g., in chat rooms for youngsters, knowing that all participants are under 18 years old). Identification will in that case be the identification of such membership. In case of private membership clubs, legislation will in such case not much regulate how membership could be established. In case of membership of a group of employees, however, labour law may be relevant if the person is an employee and could be identified in the sense of the Directive 95/46/EC.

In an IdM system, privacy principles require that no more information than needed is used to represent a person. This is also known as the data minimisation principle. This requirement is described in the PRIME White paper as follows :

*'Personal data disclosure should be limited to adequate, relevant and non-excessive data. Implied in this requirement is that data needs to be provided on a need-to-know basis and stored on a need-to-retain basis.(...)'.*⁸²

The TURBINE IdM model would provide for use of pseudo-identities in situations where a civil identity is to be used and in situations where a mere role of a person is sufficient for identification purposes.

Where a civil identity will be required, *due enrolment procedures* will be essential. The use of the e-passport, in so far fingerprint would already be registered on the chip of such passport,⁸³ could be a means to correctly identify the person and his civil identity behind the fingerprint and the identifier to the extent this is required for the application (see *below*). This requires equally, though, that the enrolment by the government upon issuing the passport is error free.

⁸² Prime White paper v.3.0, p. 6. About the data minimization principle, see also below, section 5.2.5.

⁸³ The introduction of fingerprint into the e-passports is in many countries not yet fully operational.

Current legislation, such as relating to e-passports, however, is not explicit or clear to what extent the e-passport and the information on the chip could be used by private parties for purposes such as the setting up of an IdM system. The use of an e-passport and of the personal data on the chip for setting up an IdM system is another purpose than the use of the passport in situations where the law provides for an obligation to submit such passport (e.g., submission of the passport to airlines) and the use of the data on the chip for (i) verification of the authenticity of the document and (ii) verification of the identity of the holder of the e-passport.⁸⁴ Specific legislation, allowing for the use of the e-passport for specific IdM purposes, would therefore be necessary.

For roles, due enrolment procedures will be of equal importance. However, the rules for the enrolment of 'roles' are less strict and a private party (e.g., the employer) will in principle have his own procedures for establishing certain roles, which may be transposed to IdM systems.⁸⁵

4.1.2 Identifiers

Significance and importance of identifiers in IdM systems

In IdM systems, the challenge is to represent individuals who exist in the real world in (i) either an (in various degrees) authenticated way or (ii) in a way without revealing the identity of the person. The representation of the person should be further done in a reliable and effective manner by the IT system with its many components (hardware, software and computer applications), paying respect to the functional requirements for an IdM system as set out above and the data minimisation and other privacy and data protection principles (see also *below* section 5).

For this purpose, so-called 'identifiers' are used to represent persons, or better characteristics (also referred to as attributes) of persons in the IdM system. Identifiers *are designed to make the link* between the real world and the computer applications. Identifiers are hence key elements of the IdM system and the identification process, if any.

An identifier refers to data or a set of data that represent a person's attributes which uniquely identifies the person within one or more contexts or sectors.

How identifiers shall be chosen or used, are in general (with exception though with regard to the use of unique identifiers (see *below*)) not regulated. Identifiers can be meaningful (those that can be used to extract meaningful information about the person, such as the name but also a number revealing date of birth) or meaningless (those from which no meaningful information can be obtained, such as an arbitrary number). Identifiers can be assigned by private organizations as well as by governmental agencies.

Identifiers can be divided into many categories. *Global identifiers* usually refer to identifiers which are used as a substitute *for the person's name or other designation of the person's civil identity* and are generally intended to be used in multiple (potentially, all) contexts/sectors. Examples of this type of identifiers include numbers of passport or ID cards and social security numbers. *Role identifiers* are those identifiers whose use is limited to specific roles, such as a customer number or an online chat nickname. They can be assigned or self-imposed. *Relationship identifiers* are identifiers used for communications with the same partner, even if in different roles. An example could be an e-mail address. *Transaction identifiers* are those used for one transaction only, such as randomly-generated transaction numbers. A transaction identifier is unlinkable with any other such identifier or, in fact, any other item of interest.

⁸⁴ See Regulation 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Article 4 (3).

⁸⁵ However, national legislation may require otherwise. See for example, the Netherlands, where the Law on the obligation to identify oneself, which has introduced a more exhaustive identification obligation effective since 1 January 2005, requires that employers shall identify the employees on the basis of a valid original identity document (and keep a copy of such document).

In IdM systems, the identifier for data subject may hence include elements of his or her civil identity, such as a name, or include a relevant characteristic, such as a biometric, or refer to a role or other attribute of that person which is relevant for the system.

In Turbine document 1.2.1 'Services and scheme for multiple trusted identities', the specific term Identity Reference (IR) is used instead of identifier.

Notwithstanding the above kinds of identifiers can be distinguished, , as discussed, it is necessary to review the use of identifiers also as being 'unique v. purpose-specific' and as for multiple identities.

Unique v. Purpose-specific Identifiers

Unique identifiers have been introduced as an efficient means to administer data flows in computer system. Because of increased data exchanges, there grew a need to match data from different sources and sectors. Unique identifiers were put forward as an efficient solution to tackle this problem. Unique identifiers, however, are now also increasingly used as global identifiers to represent persons, especially by governments.⁸⁶

In Belgium, for example, much attention was given to the choice of the identifier by the legislator for the organization of an national e-health platform for the exchange of information concerning health. While the Belgian Privacy Commission was initially not in favour of the use of an unique national identifier (as compared to a specific sectorised identification number), it stated in a second opinion that because a correct identification and authentication is important, the use of a national unique identifier was justified, since several safeguards were in place, including the fact that the e-Health platform would not centrally store data, but only foresee in a reference for the exchange of the data.⁸⁷ France, on the other hand, would use sectorised identification numbers for e-health purposes as tested out during a trial period. In the Netherlands, a similar debate about the use of the identifier for e-health is currently taking place.

The Article 29 Working Party has clearly warned for the privacy and data protection risks of identifiers :*'The use of identifiers, whatever form they take, entails data protection risks. Full consideration should be given to all possible alternatives. If user identifiers are indispensable, the possibility of allowing the user to refresh the identifier should be considered'*.⁸⁸

The use of an unique identifier by Microsoft in the .NET Passport system was also a major concern of the Article 29 Working Party. The Passport unique identifier (PUID) was generated at the registration and remained the same for the whole life of the account. The PUID as such did not reveal information about the account holder (such as access to a user's profile information), but because it was an unique number associated with the account, could enable participating sites to communicate to each other information about .NET Passport users and build user profiles. Although Microsoft and affiliated sites prohibited selling PUID registers to third parties, cross-site linking without user consent and although severe restrictions were imposed by the parties involved themselves, the Article 29 Data Protection Working Party stated that *'notwithstanding this fact, a risk always exists when the technical possibility is available'*.⁸⁹

The Article 29 Data Protection Working Party stressed the *technical possibility* again as a risk factor in its analysis of the Liberty Alliance system back in 2003. Although it was at that time not possible to exactly foresee the use by Liberty Alliance of their system of 'pair-wise identities' in combination

⁸⁶ See also D. De Bot, *Privacybescherming bij e-government in België*, 2005, p.53 et seq.

⁸⁷ Belgian Privacy Commission, *Opinion N°14/2008 of April 2, 2008 upon request of the Minister of Social Affairs and Public Health and the Minister of Public Officers affairs and Public companies relating to a bill for the establishment and the organization of an eHealth platform (A/2008/016)*, available (in Dutch and French) at http://www.privacycommission.be/nl/docs/Commission/2008/advies_14_2008.pdf

⁸⁸ Article 29 Working Party, o.c. at footnote 26, p. 15.

⁸⁹ See Article 29 Working Party, o.c. at footnote 26, January 2003, p. 9-10.

with so called 'opaque handles' or 'name identifiers'⁹⁰ because the system was not yet fully developed and not yet widely used, the Article 29 Data Protection Working Party nevertheless stressed that it was necessary to scrutinize this from a data protection point of view, '*in particular concerning the technical possibility of sites sharing personal data of the user without his consent*'.⁹¹

As regarding the use of a(n unique) identifier from the data protection legislation point of view, the Directive 95/46/EC addresses in one of its provisions identifiers as follows : '*Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed*' (Art. 8 (7)). From this provision, it follows that 'national identifiers' and 'identifiers of general application' should be further regulated, because of its privacy risks.

This is also in accordance with article 8 ECHR, which requires a legal basis for interferences with the fundamental right to privacy (see *below*). Because of the importance of identifiers in IdM systems, in particular in an e-government context, it is necessary that the use of such 'national identifiers' and 'identifiers of general application' (e.g., the use of such identifiers for the organization of an efficient organization of the tax administration) *is provided for by legislation*, whereby sufficient guarantees are determined for the data subjects.

A solution to avoid 'big brother' scenarios that has been put forward, is the compartmentalization of the individual's sphere into many roles, and the accumulation of the (personal) data about those roles in separate data collections. Important factors for this compartmentalization are the use of context-specific identifiers and the corresponding avoidance of multi-purpose identifiers.⁹² However, identity management systems may precisely challenge the compartmentalization of an individual's personal data into separated data sets for the different roles a person has in society and undo such compartmentalization.

The TURBINE IdM system will provide for the unlinkability of the various identifiers. It is clear from the above that it should also be *technically excluded* that use of various identifiers could be linked across contexts.

Multiple identities and identifiers

The legal aspects of the use of *multiple* identities for the representation of identities within one system or application have not been analyzed in depth yet. This could be a topic of further research for IdM systems. To the extent unique identifiers present privacy risks for linking various (trans)actions and should therefore be avoided, and whereby it is recommended to use multiple identifiers, an IdM system should in principle be able to manage multiple identifiers; provided unlinkability is technologically effectuated.

Only in case legislation would impose the use of an unique identifier, e.g. in the relation with the government for whose benefit one unique identifier shall be used, it should as default be possible to use multiple identifiers.

Is it possible to claim an exclusive right on the use of an identifier or a virtual identity (e.g., a specific pseudonym) or to counter 'theft' of a virtual identity?⁹³ While regulation is not explicit on these issues, some case law emerges on the use and theft of virtual identities.⁹⁴ In such emerging

⁹⁰ These 'opaque handles' or 'name identifiers' were unique identifiers used to provide a link between pair of sites.

⁹¹ See Article 29 Working Party, *o.c.* at footnote 26, p. 12.

⁹² See Clarke, R., *Identity Management. The technologies. Their Business Value, Their Problems, Their Prospects*, March 2004.

⁹³ See also M. Bogdanowicz and L. Beslay, *Cyber-security and the future of identity*, IPTS report, 2002.

⁹⁴ According so some sources, a Japanese women would have been arrested after having deleted the avator from the person whom she divorced in the game 'Maple Story'. See Techconsumer, 'Kill an Avatar, Get Punished', 26 October 2008, available at <http://www.techconsumer.com/2008/10/26/kill-an-avatar-get-punished/>; In the so-called 'Runescape' case in the Netherlands, two boys were punished after they stool a virtual armet and mask from a 13-years old.

case law, existing legal rules, e.g., relating to cybercrime, such as the hacking of computer systems, is applied, without presently an indicated urgent need for new rules on this area.

Some legal authors have pointed to issues when using several identifiers, relating to liability, the legal representation (for example, of pseudonyms used by minors) and the accountability. Such issues need to be clarified for the use of (multiple) identities (or pseudonyms) in the online world.⁹⁵

4.1.3 Identification

Identification in IdM systems will in the context of IdM systems in principle refer to revealing the identifier used in the system. Only in a second step, identification would be the revealing of information about the person (or the capacity or role of a person) as identified or the group to which one belongs.

As such, identification in IT systems does not necessarily mean that the identity of the person behind the identifiers is revealed. This is in principle not the aim of an IdM system, except in very specific situations (e.g., request of judicial authorities for information about users of specific identifiers (such as an IP number)).

Identification in the Directive 95/46/EC is understood as referring to this second step, whereby one needs to judge, for the definition of personal data and the application of the Directive 95/46/EC, if the natural person behind any identifier can be identified, directly or indirectly (see Art. 2)⁹⁶. This definition, however, does not indicate how identification for purposes of IdM systems shall be done.

4.2 Pseudonyms and anonymity

Pseudonyms

The research on the use of pseudonyms and its legal implications in IdM systems is limited.

In a digital network, the identity of users will often be represented by pseudonyms. A user in a chatroom, for example, will often not use his real name but rather a pseudonym or a nickname or several of them. The use of such pseudonym is often chosen to increase the privacy of the data subject. A pseudonymous transaction is one that cannot, in the normal course of business, be associated with a particular individual.⁹⁷ We will hereunder analyse what the meaning is of a 'pseudonym', both in the general understanding as in a more legal understanding, for an IdM system, and whether there are any restrictions to the use of pseudonyms.

The term 'pseudonym' comes from the Greek nouns 'το ψευδος', translated 'the lie', and 'το ονομα', translated 'the name'. The term 'pseudonym' is used in IdM research in general as a term to explain that not the real, 'civil identity' name is used, but another name or another identifier.⁹⁸

Pseudonyms provide for a label (more correctly, an identifier) for (an identity of) a person. From a general, but also technical point of view, pseudonyms can not only be used for replacing a person's name or identity (person pseudonym), but also for a role (for example, for a role as customer) (role pseudonym) or relationship (for example, the use of different pseudonyms for different

⁹⁵ See J. Dumortier and C. Goemans, 'Privacy Protection and Identity Management', *Security and Privacy in Advanced Networking Technologies*, B. Jerman-Blazic e.a. (ed.), NATO Science Series, vol. 193, Amsterdam, IOS press, 2004, p. 205.

⁹⁶ 'Identified or identifiable natural person' means anyone who 'can be identified, directly or indirectly, in particular by reference to an identification number or by one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.'

⁹⁷ R. Clarke, *Identified, Anonymous and Pseudonymous Transactions : The Spectrum of Choice*, April 1999, p. 5, in S. Fischer-Hübner, G. Quirchmayr, L. and L. Yngström (eds.) *User Identification & Privacy Protection : Applications in Public Administration & Electronic Commerce*, Kista, Sweden, June 1999, IFIP WG 8.5 and WS 9.6.; in general, see also S. Clauss, A. Pfitzmann, M. Hansen and E. Van Herreweghen, *Privacy-Enhancing Identity Management*, IPTS report, September 2002, available at <http://ipts.jrc.ec.europa.eu/home/report/english/articles/vol67/IPT2E676.htm>

⁹⁸ See A. Pfitzmann and M. Hansen, o.c. at footnote 39 , p. 20.

communication partners) (relationship pseudonym). The use of pseudonyms provides in this way *for the possibility or the impossibility to link the data subject across various contexts*.

From a legal perspective, it would be useful if pseudonymity could be clearly defined in all its aspects which are relevant in online digital networks in general and in an IdM system in particular. Distinctions amongst pseudonyms (a) chosen by the data subject or attributed by a service or identity provider, (b) used for concealing sender's or receiver's identity, (c) which are revocable or not, and (d) enabling accountability or not may be relevant. The presently proposed definition of pseudonymity (in a technical context, see *above*, section 3.1.1) does not say much about anonymity, authentication or accountability. While these qualities or requirements depend on additional functionalities to be implemented by the IdM system which are not implied by the use of a pseudonym alone, one shall acknowledge that the concept of pseudonymity, from a technology point of view, covers much more than just using an alias, but includes various elements, in particular a relation to anonymity, authenticity and accountability.

The question remains whether there are any *legal rules* or restrictions which need to be taken into account upon the use of pseudonyms in an IdM system in general.

Copyright law. About the use of pseudonyms in general, the legal rules are limited. The deployment of pseudonyms is sometimes provided for and accepted in specific legal texts in some national laws. For example, in the context of copyright, the use of a pseudonym by an author for a copyrighted work is taken into account and acknowledged. Legislation attempts in that case to provide for a mechanism to attribute rights and obligations. In case a work is published, the publisher will, in case the author remains unknown, sometimes be regarded as being the author.⁹⁹ The legislator hereby assumes for accountability purposes that the publisher is informed of who is behind the pseudonym and will know the identity of the author. In case the publisher would not be known, the printer will in some legislations be held liable. In other texts, the use of pseudonyms is (implicitly) not allowed. The above mechanism provided for in copyright law, is probably well applicable in an online environment. For example, in case of defamation or other illegal acts of an author of a copyright protected text, who uses a pseudonym or whose identity cannot be discovered, the publisher-internet provider may be held liable.¹⁰⁰ In case of the use of pseudonyms in an IdM system for a specific application, e.g., a blog, this rule could be applied.

Prohibition to use a false name. On the other hand, the use of a pseudonym could fall under a general prohibition to use a false name. For example, in the Belgian Penal Code, article 231 penalizes 'adopting in public a name which does not belong to oneself' (prohibition to use a false name). The article was introduced with the adoption of the Penal Code by Act in 1867 and is part of Title III 'Criminal offences against the Public Trust'. The purpose of the legislator was to abolish uncertainty with regard to someone's identity.¹⁰¹ Some authors state that the first element which requires for the crime to 'adopt a name' only refers to the family name¹⁰², but this is not clear. The

⁹⁹ For example, article 7 of Belgian Copyright law of 30 June 1994. See also article 2 § 3 of the same law.

¹⁰⁰ Compare also with case law in the Netherlands, Supreme Court [Hoge Raad], 25 November 2005, LJN AU4019 (the so-called Lycos/Pessers case). In that case, the service provider hosting a website of an individual with 'at first sight' illicit content and which refused to provide the identification details of the individual, was held liable.

¹⁰¹ The article is of public order. Three elements have to be combined : (1) the adopting a name, (2) in public, and (3) the name should not belong to oneself. In addition, one shall do this 'knowingly' . It is for this criminal offence not relevant whether the name is the name of someone else or not, but rather essential that it is not the name as mentioned in the certificate of birth. There is also some confusion with regard to the second requirement of adopting a name 'in public'. Some hold that it is sufficient that there is a certain degree of publicity whereby the adoption of the name is visible. The third requirement is that the name should not belong to oneself. As stated before, it is not required that the name should belong to someone else. The use of a pure fictive name is sufficient. It is not required that third persons are involved or incur negative consequences of the adopting of the false name. If these three elements are united, it is sufficient for penalization that someone knowingly adopts and uses this false name, even if this occurs only one time. It is not required for this offence that one has the intention to hide his identity; merely using a false name is satisfactory.

¹⁰² D. Reynders, M. Taeymans & W. Cruysberghs, 'Identiteit en diefstal van identiteit. Een verkennende juridische duiding', in J. Denolf (ed.), *Identiteitsfraude. Misdrif van de toekomst ? Fraude d'identité. Le crime du future ?* Politeia, Brussels, 2005, (31), 43.

Supreme Court has stated in scarce case law that it is sufficient that someone uses a nickname which is not on his certificate of birth¹⁰³ or that someone wants somebody else to believe that the false name is his own name.¹⁰⁴

Article 231 of the Belgian Penal code is an article which was adopted a very long time ago, but is still in force and covers in fact a rather broad area of use of a false name. The use by someone of a (family) name other than mentioned in the birth certificate in chat rooms on the Internet, for signing comments in an electronic visitor's register of a website or even in an e-mail address, could in principle be sufficient for penalization. The principle that criminal provisions should not be interpreted in an analogous way does not seem to prevent the application of this article cases in an online environment.¹⁰⁵ The above is an example of how existing (sometimes very long time ago adopted) legal provisions, which restrict the adoption and use of fictitious names or pseudonyms, need to be reviewed in order to allow a more general justified use of pseudonyms, for example, in IdM systems.

Digital signatures. In the E-Signature Directive 1999/93/EC, it is expressly stated that the signatory shall have the right to mention a pseudonym instead of his real name in the certificates as following : 'Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name' (Article 8 (3)). The conditions under which a pseudonym shall be used, and when the link to the person in the real world could be requested, are however not further specified in the E-Signature Directive and reference is made to national laws.

Data protection legislation. In the context of data protection legislation, reference is sometimes made to the use of pseudonyms (in the context of data minimisation).

The German Federal Data Protection Act, for example, explicitly states as a general principle that 'Data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using *no personal data or as little personal data as possible*. In particular, *use is to be made of the possibilities for aliasing* [*Pseudonymisierung*] and *rendering persons anonymous*, insofar as this is possible and the effort involved is reasonable in relation to the desired level of protection' (stress added) (Section 3.a). Such 'aliasing' is in the same Act further described and defined as an act of the data controller of replacing the name and other identifying characteristics of a data subject with a label to make identification substantially difficult or impossible.¹⁰⁶ In that case, it is expected that the data controller is in control of the pseudonym and is able to make the link with the civil identity of the data subject.

The need for the possibility to connect to a network with a pseudonym has also been confirmed in more recent texts relating to data protection by the Article 29 Data Protection Working Party :

'All possible efforts should be made to allow anonymous or pseudonymous use of online authentication systems'.¹⁰⁷

Electronic communications. Some national legislations have also expressly provided for the use of pseudonymity. For example, the German Act establishing the General Conditions for Information and Communications Services recognizes the use of pseudonyms by stating the following :

*'User profiles are permissible under the condition that pseudonyms are used. Profiles retrievable under pseudonyms shall not be combined with data relating to the bearer of the pseudonym.'*¹⁰⁸

¹⁰³ Belgian Supreme Court, 17 April 1905, *Pas.*, 1905, I, 196.

¹⁰⁴ Belgian Supreme Court, 6 February 1967, *Pas.*, 1967, I, 687.

¹⁰⁵ But see D. Reynders, M. Taeymans & W. Cruysberghs, 'Identiteit en diefstal van identiteit. Een verkennende juridische duiding', in J. Denolf (ed.), *o.c.*, (31), 45.

¹⁰⁶ See Section 3 (6a) German Federal Data Protection Act.

¹⁰⁷ Article 29 Working Party, *o.c.* at footnote 26, p. 15.

¹⁰⁸ J. Dumortier, C. Goemans and M. Loncke, *Anonymity and Privacy in Electronic Services (APES). D.4, General report of the legal issues*, 2003, p.30.

Preliminary conclusion. In view of the limited legal rules relating to the deployment of pseudonyms, and more in particular in relation with IdM systems, it will be necessary to look at the functions which pseudonyms aim to perform in an IdM system ((identification of a person, without full disclosure of identity, while preserving accountability) and the requirements of an IdM system (authentication, accountability and in some cases authorization), and to determine which rules apply to pseudonyms in relation to these functionalities.

For the TURBINE demonstrators, the use of pseudonyms as a (revocable) identifier in a (biometric) multi-identity IdM system solution should be legally permitted and possible in view of the provisions in the E-Signature Directive. However, some existing laws of national states may have to be reviewed to provide the possibility to use pseudonyms in IdM systems, insofar some legislation could restrict the use of pseudonyms.

Anonymity

The concept of anonymity is as a term better represented in legal texts and has been subject to more regulation than pseudonyms.

First of all, anonymity has been recognized as a legal interest and principle in legislation for some very specific situations, for example, in some countries, for protecting witnesses in criminal investigations or in family law related matters, such as donating semen or giving birth¹⁰⁹. In these cases, the actions may be '*organized semi-anonymous*'¹¹⁰ as the identity is kept secret for the outside world but may be known to a third party.

In contract matters, it is less explicitly stated to what extent contracting parties can remain anonymous. For some transactions, it is possible that parties remain '*absolutely anonymous*'¹¹¹. In some civil law countries, for example, a sales agreement is in principle concluded and will take effect as soon as parties agree upon the price and the object of the sale.¹¹² This principle is effective if the purchase would concern goods for which no written contract would be entered into, for example the sale of a good in a shop.

If the object is however a real estate, the sales agreement will have to be passed by a notary public and the sales deed registered and parties to the agreement will for these purposes be fully identified (by the notary public, who has often a legal obligation to do so) in the authentic deed which will be made public (by registration) ('*organized, personalized transactions*')¹¹³.

For public auctions of real estate, legislation sometimes allows bidders to remain anonymous during the auction, by using an agent, provided the agent will upon a successful bid reveal for whom he acted. For other contracts, such as lease contracts, contractor agreements etc where parties draw up a written agreement, parties will usually be identified in the agreement. In these cases, these transactions are '*spontaneous, personalized*' where they use (verified or unverified) identifying personal data.¹¹⁴

In the context of data protection legislation, reference is also made to anonymisation, sometimes as a principle for the processing of personal data in the context of research¹¹⁵ or as a general

¹⁰⁹ See e.g., France, Article 326 of the Civil Code, which states that the mother can, during giving birth, request that the confidentiality of her admission and of her identity is kept. See also the Law N° 93-22 of 8 January 1993 modifying the civil code relating to the civil identity, the family and the rights of the child and installing a family judge (JO N° 7, 9 January 1993) which states that an application for disclosure of details identifying the natural mother is inadmissible if confidentiality was agreed at birth (See Article 325 and 326 of the French Civil Code as modified, available at <http://legifrance.gouv.fr>). This right to anonymity or secrecy was upheld in the case Odièvre v. France of the ECHR of 13 February 2003.

¹¹⁰ For varying degrees of anonymity, see J. Grijpink and C. Prins, 'New rules for anonymous electronic transactions ? An exploration of the private law implications of digital anonymity', in C. Nicoll, et al., (Eds.), *Digital Anonymity and the law – Tensions and Dimensions*, 2003, ITeR, The Hague, (249), p. 251.

¹¹¹ *Ibid.*, p. 251.

¹¹² For Belgium, see article 1583 of the Civil Code.

¹¹³ For the term, see J. Grijpink and C. Prins, o.c. at footnote 110, p. 251.

¹¹⁴ *Ibid.*, p. 251.

¹¹⁵ For example, the Royal Decree of 2001 in execution of the Belgian Data Protection Act (Article 3) and the German Federal Data Protection Act, section 40 (2) ('The personal data shall be rendered anonymous as soon as the research purpose permits this'. (...)).

principle of data minimisation.¹¹⁶ In the Belgian Data Protection legislation, anonymous data are defined as 'data which cannot be linked with an identified or identifiable person and which are therefore no personal data'(Article 1(5)).

In legal proceedings, persons will in principle also be identified.

By way of preliminary conclusion, one could say that anonymity is not only in technical matters, but also for legal purposes a question of degree. Recognizing these degrees of anonymity and making a distinction between the various degrees of required anonymity is hence important, also for evaluating the legal aspects.

Online anonymity

General. Notwithstanding the above, the increasing use of digital networks and communication services, and referring to the principle of secrecy and confidentiality of communications (see below), the principle of anonymity has gained attention.

The need for online anonymity has been recognized already for some time on EU level.¹¹⁷ The E-Commerce Directive 2000/31/EC of 8 June 2000 states that it does not intend to prevent the anonymous use of open networks such as the Internet (recital 14). The E-Privacy Directive 2002/58/EC of 12 July 2002 acknowledges expressly the right to anonymous communications.¹¹⁸ Some national legislations have also expressly provided for the use of anonymity.

The use of anonymity (and pseudonyms) is in general also perceived and accepted as privacy enhancing.¹¹⁹ For very specific situations, online anonymity has been recognised as a legitimate interest, e.g., for drug addicts, to seek anonymously online help.

How anonymity shall be effectuated, however, is not always clear. In some cases, for example the use of anonymous remailers, the transaction may only be '*spontaneous, semi-anonymous*'¹²⁰ as one is never sure if the remailer service effectually deletes all the personal data. Moreover, some authors have pointed out correctly that while the need for online anonymity is accepted, in practice, the use of online anonymity is often controversial.¹²¹

Restrictions as to online anonymity. Legal provisions, however, also restrict or sometimes ban anonymity in a digital environment.

On the EU level, there was an agreement to ban anonymous commercial spam by stating such in the E-Commerce Directive 2000/31/EC.

But also national legislation may impose restrictions and may require a controlled use of anonymity.

For example, in the telecommunications sector, the Belgian Electronic Communication Act prohibits the supply and use of telecommunications services or equipment that render caller

¹¹⁶ For example, the German Federal Data Protection Act, which states as a general principle that '(...)use is to be made of the possibilities for (...) rendering persons anonymous, insofar as this is possible and the effort involved is reasonable in relation to the desired level of protection'. (stress added) (Section 3.a).

¹¹⁷ See for example, Article 29 Working Party, Recommendation 3/97 : Anonymity on the Internet, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp6_en.pdf

¹¹⁸ Recital 9 stresses the need for Member States to take particular account of the objectives of minimizing the processing of personal data and of using anonymous or pseudonymous data where possible. Article 6 of the Directive imposes as a principle anonymity of traffic data when it is no longer needed for the purposes of the transmission of the communication. Article 9 imposes anonymity of location data, unless used with the consent for the provision of value added services.

¹¹⁹ See Article 29 Working Party, o.c. at footnote 117, p.5 : '*Clearly one way of addressing privacy concerns would therefore be to seek to ensure that wherever feasible the data traces created by using the Internet do not permit the identification of the user. With anonymity guaranteed, individuals would be able to participate in the Internet revolution without fear that their every move was being recorded and information about them accumulated which might be used at a later date for purposes to which they object.*'

¹²⁰ For the term and the example, see J. Grijpink and C. Prins, o.c. at footnote 110, p. 251

¹²¹ J. Dumortier and C. Goeman, 'Privacy Protection and Identity Management', *Security and Privacy in Advanced Networking Technologies*, B. Jerman-Blazic e.a. (ed.), NATO Science Series, vol. 193, Amsterdam, IOS press, 2004, p.104. The authors state that this is partly due to a lack of refined and transparent rules on a controlled use of anonymity.

identification impossible, or that otherwise make it difficult to track, monitor, wiretap or record communications. Furthermore, technical and administrative measures can be adopted and imposed on operators or end users in order to be able to identify the calling line in cases of emergency calls as well as for the investigation of specific crimes (Article 127).

A legal ban or restriction on anonymity will often be inspired by law enforcement needs for the prosecution of crime, in the fight against (serious) crime and/or terrorism (see also below).

Other examples are in the banking sector, where financial institutions will require information of the identity of the service users further to specific legislation, such as laws combating money laundering.

Because of these legal restrictions, IDMs systems which provide for anonymity, will have to adapt the architecture, technical specifications and organizational structure in order to provide more information on the users if required by law.

By way of preliminary conclusion, one could say that there is however *not a general self standing right*, constitutional or otherwise, to anonymity. Anonymity is rather a subsidiary or a derivative of other constitutional rights, such as in the context of privacy (France), data protection (in the form of the right to informational self-determination, Germany), the secrecy of communications (Germany), free speech (the Netherlands, Canada and the United States) and the right to individual liberty (France), which is subject to many exceptions.¹²²

4.3 Authentication and authorisation (permission/delegation/mandate)

Authentication

There is no general legal framework which stipulates the conditions for the authentication of electronic identities.

An IDABC study on eID interoperability based on reports for 32 countries, came to the conclusion as to whether there was any specific legal framework with regard to (entity) authentication and as to whether there was any legal definition or regulation on how an identity can be established in an electronic environment, that there was in not one country a generic legal framework detailing on what authentication is, and at which point authentication requirements have been met.¹²³

This is surprising, to the extent that the registration in an electronic system, in combination with (some) authentication, is more and more replacing the traditional methods (for example, the holding of a(n entrance) ticket) for claiming rights (the right to enter a place or to obtain a service).

The Belgian DPA has recently issued an advice on access and user control in E-government.¹²⁴

The Commission stated in this advice that identification and authentication should best be done by the eID card. The Commission argues that the eID card is issued by the government and is legally protected.¹²⁵ However, the opinion does not give advice for other IdM systems.

In the absence of legal rules in general on authentication processes in an digital environment¹²⁶, it is not clear to what extent the identity or service provider who provides or performs the authentication of a data subject through an IdM system may be held responsible in case the authentication proves to be deficient or does not live up to the guarantees given.¹²⁷ One could

¹²² P. De Hert, B-J. Koops and R. Leenes, 'Conclusions and recommendations' in *Constitutional Rights and New Technologies*, The Hague, Asser Press 2008, p.281.

¹²³ H. Graux and J. Majava, *Analysis and Assessment of similarities and differences – Impact on eID interoperability*, November 2007, p. 4, available at <http://ec.europa.eu/idabc/en/document/6484/5644>

¹²⁴ Belgian Privacy Commission, *Recommendation nr. 01/2008 of 24 September 2008 relating to access and user control in the governmental sector*, 10 p.

¹²⁵ *Ibid.*, p. 6.

¹²⁶ With exception of the legal provisions for advanced and qualified electronic signatures (see *below*).

¹²⁷ Identity theft is in fact a case of weak or insufficient authentication.

argue, however, that the general data protection legislation provides a basis to hold the identity or service provider liable in case inaccurate data for authentication or authorisation are processed (see also Art. 6.1.c in combination with Art. 22 & 23 Directive 95/46/EC).

The burden of proof, however, to demonstrate that the authentication does not perform or is not appropriate, will be on the user. The user could for this purpose refer to contractual terms or practices generally applied for authentication services, including some (international) standards for organizational and product security.

Authorisation

The conditions of the mandate will in general usually be specified in *an agreement* between the grantor and the grantee of the mandate. Both parties will be named and identified in the agreement.

In general, the mandate can be for a specific term or for indefinite duration until revocation by the grantor. The mandate agreement will usually also determine for which field and purposes the mandate is given. A mandate may relate to specific goods or services or may have a more general nature. The legal conditions for a mandate to be valid are determined by national laws and may vary from country to country.¹²⁸ Sometimes, a mandate does not need to be in writing, depending on local law, but it may then be difficult to prove the mandate agreement. A mandate should preferably be explicit, but may also be implicit. For IdM systems, it is relevant to note that such implicit mandate could follow, for example, from a function or role someone has in an organization or by the mere performance of acts.

A mandate, however, could also be specified *by law*. For example, company law will stipulate that a person appointed by the general assembly of a company can represent the company. Another example is a law which states that attorneys-at-law can represent clients before a court.

The *evidence* of a mandate agreement is usually governed by the local national legal evidence rules on contracts. Because of the implementation of the E-Commerce Directive 2000/31/EC¹²⁹ by the EU member States, many contracts concluded by electronic means, including a mandate contract (with exception of mandate contracts to be passed by a notary public), could obtain legal recognition and therefore, an authorization or mandate agreement can in principle be concluded by electronic means.

In practice, however, very few explicit agreements will be made on authorization rights as these will often follow (implicitly) from a role someone has in an organization. Moreover, the functionality of permissions and mandates for IdM systems, sometimes also called proxies, can be effectuated in an IdM system by the creation of separate mandate databases.¹³⁰ The legal basis of such separate mandate databases is often not clear.¹³¹

A mandate functionality typically involves the processing of personal data and therefore is subject, beside to legal rules governing the mandate contract and evidence thereof, to the regulation relating to the processing of personal data (see also *below*).

In Turbine, the system architecture may include authorization functionalities. However, this is an additional functionality, which is not the focus of Turbine. In the demonstrators, the authorization functionality is not at the core of the set-ups.

¹²⁸ For a study of the legal framework of delegation techniques and requirements in an IdM system for Belgium, see B. Van Alsenoy, *IBBT IDEM Deliverable D3.1 Delegation techniques and requirements*, November 2008, 34 p. ; The legal rules on a mandate are for Belgium contained in the Civil code, in articles 1984 through 2010 Civil Code.

¹²⁹ See article 9.1 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, O.J. L 178, 17 July 2000, p. 1-16, available on <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031> :EN:HTML

¹³⁰ In Belgium, for example, separate mandate databases are used for purposes of managing the mandates granted by data subjects to their accountant or tax advisor for filing their online tax declarations.

¹³¹ Compare, however, for Belgium, with a recent Act of 18 July 2008, *B.S., 29 October 2008*, where a legal basis was provided for the use of 'authentic databases' to be used in the context of E-government.

4.4 Legal aspects of additional requirements and architecture

Accountability and law enforcement requirements

As stated above, accountability is mentioned as an additional important requirement of IdM systems. Accountability could be described as the possibility to determine to which data subject rights and obligations, including respect of the laws, shall be conferred. *Secure logging* of the actions in the IdM system and other *digital evidence* measures will be needed to assure this requirement, for example, for use of actions in court. Further to the E-Commerce Directive, most EU member states will have adapted their national laws in order to provide probative value to electronic documents and agreements, e.g., those signed with an electronic signature.

The requirement of accountability is closely related with law enforcement requirements. Law enforcement requirements impose limits on processing of personal data for well defined purposes, such as the prevention, detection and prosecution of crimes, national security, defence and public order. In this context, the use of encryption may be restricted or regulated by national legislations. IdM systems will have to comply with these national encryption regulations and additional restrictions imposed for law enforcement purposes.

Unobservability and unlinkability

The requirement for unlinkability is based on the increasing digital availability of personal data over networks. Because of the repeated use of all kind of identifiers, in particular unique identifiers which are sometimes produced by the computer systems themselves (compare with the PUID of the .NET Passport system), data which were produced in one context, could be linked with data prepared for another context.¹³²

General data protection legislation principles require purpose specification and binding for the collection and processing of personal data, which prevent that data should be linked for different purposes. For further references to the general principles of data protection legislation relevant for the principle of unlinkability, including data limitation, reference is made to section 5.2.1 and section 5.2.5.

As to unobservability, the Supreme Court in Germany ('Bundesverfassungsgericht) stated in a (recent) judgement that there is a basic right to the protection of confidentiality and integrity in information systems which complements the by the same court in 1983 recognized 'fundamental right to informational self-determination'. The Court declared in its important decision of 27 February 2008 that a broadly formulated state law of the state North Rhine-Westphalia, which allowed police online searches on computers, violated this fundamental right and that the state law was therefore void.¹³³ Although this decision only applies for the particular case, in particular where police searches were involved, it nevertheless could be referred to as a decision which puts important principles such as the right to confidentiality and that secret online searches must be restricted by technical measures in order not to interfere 'with the core area of the conduct of private life', both related to unobservability, forward as fundamental principles.

Revocability

Revocability of the identifiers and of the authorisations, if any, in an IdM system is *as such* a practical requirement.

The existing privacy and data protection legislation, in particular the provisions relating to the rights of the data subjects, which includes a general right to object, only provides a general basis for this requirement. The requirement as such is not clearly pronounced in legislation.

Architecture

The architecture of IdM systems will have important effects on the flows of personal data, including on security risks.

¹³² See ENISA Ad Hoc Working Group on Privacy & Technology, *o.c.* at footnote 8, p. 25.

¹³³ Bundesverfassungsgericht, 1BvR 370/07 of 27 February 2008, available at http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

With regard to the central or decentralized storage of data, the Article 29 Group has advised to adopt a *'software architecture that minimises the centralization of personal data'*, hereby avoiding the creating of high added-value databases owned and managed by a single company or a small group of companies or organizations.¹³⁴

4.5 Legal risk management

In its discussion with Microsoft about NET Passport, the Article 29 Working Party emphasized that *'[i]t is advisable for the different players to have clear contractual agreements between them where the obligations of each party are made explicit.'*¹³⁵

Not only from this discussion, but also in general, shall parties provide for legal risk management as an integral part of the overall risk management process. A key instrument in legal risk management is contract.¹³⁶ Such contract is required under the Data Protection Directive 95/46/EC between the data controller and the data processor.¹³⁷ However, the Directive does not require joint controllers or collaborating single controllers to contractually agree on how the processing is to be carried out.

4.6 Responsibility of system designers ?

In its opinion on on-line authentication systems, the Article 29 Working Party approached the issue of the responsibility of designers of identity management systems.

The Article 29 Data Protection Working Party stated that *'[b]oth those who design and those who actually implement online authentication systems (authentication providers) bear responsibility for data protection aspects, although at different levels.'*¹³⁸

Also the E-Privacy Directive refers to the design of systems in recital 30 as follows : *'Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum.'*

With these provisions, the question about the responsibility of system designers is without doubt fuelled. System designers are urged already for some time to take data protection issues into consideration when developing the solutions.¹³⁹

However, a system designer of an identity management system will in principle neither be a data controller or a data processor. But, an successful implementation requires that all the parties are aware of their roles under personal data protection law.

¹³⁴ Article 29 Working Party, *o.c.* at footnote 26, p. 15.

¹³⁵ See Article 29 Working Party, *o.c.* at footnote 26, p. 14-15.

¹³⁶ See, e.g. Mahler, T. and Bing, J., 'Contractual Risk Management in an ICT Context – Searching for a possible Interface between Legal Methods and Risk Analysis', Yulex 2006, *NRCCCL* 2006, p. 117–138.

¹³⁷ See Art. 17(3).

¹³⁸ Article 29 Working Party, *o.c.* at footnote 26, p. 14-15.

¹³⁹ It is in this context that J. Borking and Ch. Raab also pleaded for the adoption of PETs. See J. Borking and Ch. Raab, 'Laws, PETs and Other Technologies for Privacy Protection', *JILT* 2001, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking. In addition, they saw a basis in the Dutch data protection legislation for the use of PETs implying the responsibility and liability of system designers if these provisions were not taken into account.

5. Legal Compliance

Notwithstanding the fact that IdM and IdM systems are in general not regulated by specific legislation, IdM systems will fall within the scope of existing legislation. IdM systems shall therefore comply with such legal provisions. The applicable legislation will be international legislation, such as treaties and conventions which refer to respect for privacy as a fundamental right, and national legislation, very often legislation that was adopted in furtherance of EU Directives.

Because it is not possible to comment on the national legislations of all 25 EU member states, only the provisions of the Directives relevant for IdM systems will hereunder be mentioned and analysed. To determine which national law, implementing the provisions from the Directives will apply in a specific case in which the IdM system is implemented, will depend on the conflict of law rules of the countries involved.

5.1 Article 8 of the European Convention on Human Rights and Article 7 and 8 of the EU Charter

Article 8 of the European Convention on Human Rights

With the advent of the new information age, in which IT systems process increasingly personal data, public concern about individual privacy rose. Legal systems needed to respond to the new risks created by the flows of personal data. Not only national legal systems, but also the international community adopted relevant legal instruments. The 1948 United Nations Universal Declaration of Human Rights recognized privacy as a fundamental human right.

The right to respect for one's private and family life is also stated in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter 'ECHR' or the 'Convention') concluded in 1950 in the framework of the Council of Europe and is one of the human rights and fundamental freedoms therein listed.

Article 8 of the Convention reads as follows :

- "1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
- 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

The notion of one's private life is a broad term and is not susceptible to an exhaustive definition. The European Court of Human Rights in Strasbourg (hereinafter the 'Court')¹⁴⁰ recognized in several decisions that the concept of private life *extends to aspects relating to personal identity*, such as a person's name or a person's picture.¹⁴¹ In addition, the Court stated that Article 8 of the Convention *protects a right to identity and personal development*, also in interaction with other persons, even in a public context.¹⁴² It furthermore *includes, beyond a person's name, other*

¹⁴⁰ The European Court of Human Rights was set up in 1959 by the Council of Europe to decide upon claims for alleged violations of the European Convention on Human Rights of 1950. The Court has its seat in Strasbourg. The decisions of the Court are also available from the HUDOC Portal of the Court, which provides free online access to its case-law (<http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/>).

¹⁴¹ In a case of 1995, it was stated that the *unforeseen use* of photographs may amount to an invasion of privacy. See European Court of Human Rights, decision *Friedl v. Austria* of 31 January 1995.

¹⁴² See European Court of Human Rights, decision *Peck v. United Kingdom* of 28 January 2003, §57. See also European Court of Human Rights, decision *Odièvre v. France* of 13 February 2003 : matters of relevance to personal development include details of a person's identity as a human being and the vital interest

means of personal identification and of linking to a family and *the right to establish and develop relationships* with other human beings, in professional or business contexts as in others, and with the outside world.¹⁴³

The concept of the right to respect for one's private life hence knows a continuing evolution in the case law of the Court and of the national courts confronted with cases which challenge the application of existing rules, including cases involving new technologies. For understanding the importance of article 8 ECHR for IdM systems, it is therefore necessary to analyse how 'the right to respect for private life' has been interpreted in relation to the processing of personal data relevant for identity in the subsequent cases by the Court.

In *S. and Marper v. United Kingdom*, involving the retention of DNA samples, profiles and fingerprint, the Court stated that '[t]he mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (...)' (italics added) and that '(...) the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained' (italics added) shall be taken into account.¹⁴⁴ This decision refers to the storage, recording and the nature of the records of personal data, as important elements in order to determine whether the right to privacy was respected. This may also be relevant for IdM systems.

Legal provisions and legislation in the EU should take this fundamental right to privacy, as interpreted by the courts, into account. Already in 1969, the European Court of Justice ruled in a case in which an identity issue was raised, that identity is an important aspect of privacy and that 'the Community's measures should be set aside if they fall short to respect a fundamental human right.'¹⁴⁵

From the above, it is clear that IdM systems shall respect the fundamental right to privacy in their design, development and implementation of the system.

Article 7 and 8 of the European Charter

The Charter of Fundamental Rights of the European Union (Charter) contains various human rights provisions, including an explicit right to respect for privacy (Article 7) and an explicit right to protection in case of personal data processing (Article 8). The Charter was proclaimed and published in December 2000.¹⁴⁶ Subject to the ratification of the Treaty of Lisbon, the provisions of the Charter become legally binding in (most of) the EU Member States.

Article 7 of the Charter is stated as follows :

'Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.'

protected by the Convention in obtaining information necessary to discover the truth concerning important aspects of one's personal identity, such as the identity of one's parents.

¹⁴³ See European Court of Human Rights, decision *Burghartz v. Switzerland* of 22 February 1994, §24.

¹⁴⁴ European Court of Human Rights, decision *S. and Marper v. United Kingdom* of 4 December 2008, §67. In this particular case, which involved the retention of DNA samples and profiles, Article 8 was considered not respected.

¹⁴⁵ Case 29/69, *Erich Stauder v. City of Ulm*, (1969) Eur. Comm. Rep. 419. In this case, Mr. Stauder contested the requirement that he had to identify himself in order to obtain coupons allowing him to purchase butter at a reduced fee.

¹⁴⁶ O.J. C 364/1, 18 December 2000.

Article 8 of the Charter is stated as follows :

'Protection of personal data

- 1. Everyone has the right to the protection of personal data concerning him or her.*
- 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
- 3. Compliance with these rules shall be subject to control by an independent authority.'*

The Charter in fact reaffirms these specific fundamental rights and freedoms as already set forth in the constitutions of the Member States and international treaties, in particular in the European Convention for the Protection of Human Rights and Fundamental Freedoms and these provisions shall be applied in conformity with the interpretation of Article 8 ECHR by the European Court of Human Rights.

5.2 The Data Protection Directive 95/46/EC

In 1980, the Organization for Economic Cooperation and Development (OECD) adopted the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The Guidelines' objective was to reconcile the fundamental but competing values such as privacy and the free flow of information. In 1981, the Council of Europe followed by enacting the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

The United States and the European Union, however, developed distinct approaches to protecting the fundamental right to privacy. The U.S. approach to protection of privacy relies on the philosophy that regulation of private data controllers is based on protecting personal information as a valuable asset and, by default, relies on market self-regulation. By contrast, the EU treats data protection as a fundamental, universal human right, which right plays an important role in its decisions and legislative measures.

The EU hence decided to enact a framework directive for regulating the processing of personal data by public and private controllers, i.e., Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Directive 95/46/EC).¹⁴⁷

The human rights approach to the treatment of personal data of the general Data Protection Directive 95/46/EC as a central source for the EU law on information privacy is clearly stated in the Directive itself. Article 1(1) states that *'Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'*

The Directive 95/46/EC requires each Member State to set up its own Supervisory Authority or Data Protection Authority (DPA), which is an agency dedicated to privacy and the administration of domestic data protection law. DPAs also have enforcement powers, in addition to data subjects' private rights of action. Representatives of the authorities designated by each Member State, along with a representative of the authority or authorities established for the Community institutions and bodies and a representative of the Commission comprise the Article 29 Data Protection Working Party, named so after article 29 of the Directive which envisaged its creation.¹⁴⁸

The Directive 95/46/EC requires all EU Member States to enact their own domestic laws adopting (or "transposing") the provisions of the Directive. The Directive is not limited to electronic (computerized) data, and therefore reaches not only files on paper, but also Internet and even oral

¹⁴⁷ O.J. L 281/31, 23 November 1995, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

¹⁴⁸ See http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

communications. Furthermore, the Directive 95/46/EC required each Member State to pass a data protection law that applies to both government and private entities.

The deadline for Member States to pass their local data laws was October 25, 1998, but in fact full implementation took several years more.

It is important to note that the field of application of the Directive 95/46/EC is limited; processing of personal data for activities outside the scope of Community law, such as processing operations concerning public security, defence, State security and for activities of the State in criminal matters do not fall under the Directive 95/46/EC (Article 3.2).

Another important aspect of the Directive 95/46/EC for businesses based outside of Europe, such as in the United States, is the Directive's provisions relating to transmitting regulated data outside of Europe. The Directive specifically prohibits sending personal data to any country without a 'level of [data] protection' considered 'adequate' by EU standards. The bar is amazingly high. To date, the EU Commission has formally designated only a handful 'third countries' offering this 'adequate level of protection' including Canada and Switzerland.¹⁴⁹ For most legal purposes, this club of countries, together with the European Economic Area (EEA – Iceland, Norway, Liechtenstein), forms a sort of 'EU data zone.' The U.S. system is deemed adequate only insofar as a transfer of data is covered by a Safe Harbour Agreement.

The Directive 95/46/EC's rules break down into three categories:

- (a) Complying with data quality principles and rules;
- (b) Reporting to national data protection authorities; and
- (c) Information to data subjects and addressing their concerns.

The rules and principles of the Directive 95/46/EC which are important for IdM systems and with which IdM systems shall comply, including the TURBINE IdM system, are hereunder described.

Where relevant, an assessment of the proposed TURBINE system in view of the applicable data protection legislation, will also be given.

5.2.1 Purpose specification and finality of the IdM system

The Directive requires that personal data must be collected for specified, explicit and legitimate purposes and that the personal data must be processed compatibly with these purposes (Art. 6.1.b Directive). The data shall not be further processed in a way incompatible with those purposes.

For an IdM system, the personal data that will be collected shall serve well determined purposes.

Companies and controllers may refer to ISO/IEC standard 27002 (formerly ISO/IEC standard 17799) as the purpose for implementing an IdM system. This standard identifies the range of controls needed for information systems used in industry and commerce and is gaining recognition as 'state of the art'.¹⁵⁰

The ISO/IEC standard 27002 requires inter alia the existence of a system for *monitoring access to IT systems*, for *establishing sufficient audit trails* to address threats or problems and for reporting important events to management and the board of directors. The purpose specification for IdM systems may hence refer to these standards. However, in that case, it should be sufficiently clear for the data subjects what the purposes (of these standards) are.

The use of personal data stored in the IdM system could in case of use of the IdM system for increasing secured access *not* be used for incompatible purposes, such as e.g., for *monitoring the behaviour* of customers or personnel.

¹⁴⁹ See Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries, at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

¹⁵⁰ For the importance of what is considered 'state of the art', see Art. 17 (1) §2 Directive and e.g., UK Regulations which define 'appropriate technical and organizational measures' as '*if, having regard to (a) the state of technological development, and (b) the cost of implementing it, it is proportionate to the risks against which it would safeguard*' (compare with Art. 17 (1) §2 Directive). See also the references made to ISO 17799 by the U. K. Financial Services Authority.

Other purposes of an IdM system could also be the creation of identity management with different pseudo-identities for securely accessing various services and whereby the pseudo-identities shall remain under the control of the data subject.

The processing of the data for any additional legitimate purposes of the IDM system shall be discussed, specified and decided upon before the design of the system.

However, because of the increasing availability of personal data over networks, together with the increased possibility to link such personal data, for example because of the use of unique identifiers, unique numbers, cookies etc, *it will become more and more difficult to enforce the purpose binding of personal data*. Therefore, it is advocated to interpret these principles of purpose specification and finality, *as an obligation to prepare personal data for context-specific usage*. This would also be in line with the data minimisation principle.¹⁵¹ This is however not yet specified, detailed or an explicit obligation under the existing data protection legislation.

For biometric data, the purpose specification principle could also be interpreted that the controller shall specify in detail how the biometric data shall be used in the system, for example for identification or authentication purposes¹⁵², although this is not explicitly required in the existing legislation.

An IdM system shall therefore

- specify clearly the use of the distinct (personal) data in the system, such as the identifiers used, in the specifications and architectural design of the system ;
- prevent that data could be used for uniquely retrieving one's (civil) identity unless this is clearly specified as a purpose of the IdM system ; and
- prevent that personal data could be used for linking data (across data bases (contexts)) unless clearly specified as a purpose of the IdM system.

The TURBINE IdM system which shall collect and use the biometric sample only for the extraction of a biometric template which shall be used for the authentication of distinct pseudo identities (which shall not contain biometric data) to be used in different contexts and which cannot be linked and which specifies such use of biometric data in the design of its architecture and the development of the IdM systems, which uses the data in conformity of these purposes, and which informs the data subjects of such use (see also below) complies with the above principle.

TURBINE will also provide for context-specific personal data usage by providing for the creation of various pseudo-identities which cannot be linked. In furtherance of this principle, the TURBINE IdM system will hence limit the use of the pseudo identities for specific, predefined purposes (contexts) and/or applications.

5.2.2 Need for a legal ground for IdM processing

The Directive requires that the personal data processing is based on one of the legal grounds which are stipulated expressly in the Directive (Art. 7 Directive). These legal grounds include when the data subject has given his or her '*unambiguous consent*' and the '*necessity to perform a contract to which the data subject is a party*' or 'in order to take steps at the request of the data subject prior to the entering into a contract(Art. 7 a and b).

Other legal grounds are if processing is *necessary* for compliance with a *legal obligation* to which the controller is subject (Ar. 7 c), processing is *necessary* in order to protect the *vital interest* of the dat subject (Art. 7 d), processing is *necessary* for the performance of a task carried out in the *public interest* or in the exercise of official authority vested in the controller or in a third party to whom the data

¹⁵¹ ENISA Ad Hoc Working Group on Privacy & Technology, o.c. at footnote 8, p. 9.

¹⁵² For the distinction about identification and authentication, see also E. Kindt & L. Müller (eds.), *D.3.10. Biometrics in identity management*, Fidis, 2007, 130 p.

are disclosed (Art. 7 e) and processing is *necessary* for the purposes of the *legitimate interests* pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1) (Art. 7 f).

For an IdM system, the legal grounds shall be determined once the purposes have been defined and all the functionalities are known. Reference to the general security guidelines and standards, such as those set forth in ISO/IEC standard 27002 as discussed above¹⁵³ could justify the processing and make the processing lawful, but may not be sufficient to rely on the ground 'necessity for compliance with a legal obligation'. For this ground to apply, the legislative provision should in our view be very clear as to what processing of data should be done.

If an IdM system is going to be implemented by the employer for access to its intranet resources or to high security places, the employer could argue that such system is necessary to protect and to allow access to its valuable resources. The WP 29, however, has repeatedly stated that the consent of employees is particular, as such consent may not be entirely freely given. For other applications, the 'free, informed and specific' consent of the data subject will be more acceptable and may be the most appropriate legal ground for the processing of the data.¹⁵⁴ The consent, however, may require that consent is also asked as to whether the persons want their personal data used for customisation purposes or not.¹⁵⁵ The form and *the way* in which consent is asked, is in many national legislations not made explicit. Only for specific data processing (e.g., health related data processing), it may have to be in writing in some countries, but for most other data processings, it is sufficient if the consent is free, informed and specific, and if there is evidence of such consent.

For IdM systems, the option of interactive consent, requested on screen, for example by using the technique of a pop up window, is often advocated.¹⁵⁶ Such consent could be combined with a multi-layered information notice (see *below* section 5.2.12).

An IdM system shall therefore

- specify clearly on which legal basis it relies for the processing of the personal data in the system and inform the users thereof ;

The legal basis for the Turbine IdM system will depend upon the specific conditions of the implementation of the system. In case the system is implemented by an employer, the employer may in addition to consent, also rely on the necessity to perform a contract or a specific legal (security) regulation depending on the circumstances.

5.2.3 Determination of the (co) controller(s)

The Directive defines the 'controller' as the natural or legal person, public authority, agency or any other body which alone or with others determines the means of processing personal data and the purpose for doing so. More than one entity may be the controller. For IdM systems along the federated model, it will be difficult to decide who is/are the controller(s) (see also *below* section 6.1). To be the controller, a person or entity does not need to actually possess the data. It is sufficient to have the authority to decide on the means and the purposes of the processing.

¹⁵³ Compare with other legislative provisions which require accountability or improved security and access (e.g., in the United States, the Sarbanes-Oxley Act passed in 2002 to protect against accounting errors and fraudulent practices (cfr. Section 404)).

¹⁵⁴ See also EDPS, *Opinion on a notification for prior checking received from the Data Protection Officer of the Commission related to the Identity Management Service*, Case 2007-349, 6 February 2008, p. 8. The opinion relates to the system for the authentication and access control of users to different Commission information services, managed by different Directorates General.

¹⁵⁵ *Ibid.*, p. 8.

¹⁵⁶ *Ibid.*, p. 8.

For an IdM system, the control of the user over the IdM system, including the biometric data, may be significant and relevant, but *not sufficient* to determine that the data subject becomes the 'controller' in the legal sense.

The controller of a data processing is in principle responsible and liable for the obligations imposed by the Directive and the national data protection laws.

An IdM system shall therefore

- determine the controller(s) of the processing.

The (co)controllers for the Turbine IdM system will depend upon the specific conditions of the implementation of the system. In case the system is implemented by an employer or an organization, the employer or such organization would in principle be the controller.

In case a service provider decides to accept a particular pseudo-identity of the data subject stored in the smart card and authenticated by an identity provider, more than one controller of the data related to the IdM system may exist (see also *below*, section 6.1). Not only the identity provider, but also the service provider could become controller of the personal data processed for the IdM system. In that case, both (co)controllers will be liable for application of the relevant data protection legislation. The present legislation, however, does in principle not require that (co)controllers enter into an agreement on the processing of the personal data that they exchange. Such obligation only exists between a controller and a processor.

5.2.4 Notification of IdM system and/or prior checking requirement

The Directive requires in principle that all personal data processing is notified before the start to the national Data Protection Authorities ('DPAs') (Art. 18 Directive). In case of processing operations identified by the Member States as being likely to present risks to the rights and freedoms of the data subjects, the processing must be submitted for examination prior to the start thereof (Art. 20 Directive).

The processing of unique identifiers and of biometric data could be identified by a Member State as being likely to present risks to the rights and freedoms of the data subjects. In such case, notification is not sufficient and the processing must be submitted for prior examination. This would imply that before the start of the processing, details of the functional (and technical) requirements are submitted, discussed and approved by the Data Protection Authorities (see e.g., France).

An IdM system shall therefore

- be notified and/or be subject to prior approval of the Data Protection Authorities.

The notification/prior approval obligation will equally apply to the Turbine IdM system.

5.2.5 Minimization of the data collection and processing

This principle requires that the collection, the processing and the storage (including the retention thereof) of any personal data shall at all times be 'adequate, relevant and not excessive'. In practice, this means that personal data shall be limited to a minimum and shall be processed only insofar as required for the purpose and finality of the application (Art. 6.1.c Directive).

For an IdM system, this implies that the needs for specific personal data related with the IdM system, such as for the enrollment, the profile if applicable, the smart card registration and use if

applicable, and the set up and deployment of the pseudo-identities, shall be reviewed and limited to a strict minimum.¹⁵⁷

Where appropriate, the IdM system shall make use of pseudonyms and anonymity as the use of pseudonyms and of anonymity is generally accepted as privacy enhancing and protective.

Furthermore, the restriction of data to context-specific usage should be endeavoured.¹⁵⁸ Another way to implement this requirement could be the only *partial representation of (unique) numbers or identifiers* in all or particular phases of the IDM process (e.g., the storage or with results seen by third parties).¹⁵⁹

For biometric data, this principle (in combination with the proportionality principle (see *below*)) should be interpreted that it requires that no biometric samples are retained. If technology would permit so, biometric templates should also not be retained if possible.

An IdM system should therefore

- Restrict the processing of personal data to a strict minimum;
- Prevent the use of the (civil) identity of a person for identification purposes if not needed and make use of *pseudonyms and anonymity* as feasible and proportional with the purposes envisaged;
- Delete any link or correlation between persons and identifiers if this is not necessary for the purposes of the processing as soon as possible.

The processing of the personal data for the Turbine IdM system shall at all times remain restricted to a minimum for the purposes of the processing and the personal data shall be deleted as soon as the specified purposes of data collection are met.¹⁶⁰

5.2.6 Proportionality requirement

The Directive requires that the personal data processed must be 'adequate, relevant and not excessive' in relation to the *purposes* for which they are collected and processed (Art. 6.1.c).

For IdM systems, the Directive does not specify which data may be used. Since IdM systems need to secure access to specific resources, it is likely that the collection of personal data which may present a higher risk for the privacy of a person, such as biometric data, is balanced against the interests of the controller. For such specific kind of data special precautions shall be taken.

The advisory bodies repeatedly referred to this principle of proportionality to stress that the use of biometric data, because of the risks of function creep and abuse, shall be proportional with the (high security) purposes sought. They determine from case to case when the use of e.g., fingerprint is in proportion with the purposes.¹⁶¹

¹⁵⁷ See also the German Federal Data Protection Act, section 3.a, which explicitly states that 'Data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using *no* personal data *or as little* personal data as possible. In particular, use is to be made of the possibilities for *aliasing* and *rendering persons anonymous*, insofar as this is possible and the effort involved is reasonable in relation to the desired level of protection'. (stress added)

¹⁵⁸ See also ENISA Ad Hoc Working Group on Privacy & Technology, o.c. at footnote 8, p. 25.

¹⁵⁹ See e.g., the practice in the banking world relating to references to (credit) card numbers : only last digits are sometimes displayed. See also a recent decisions of the Greek DPA which is favourable for an access system for critical applications and which refers to the partial representation of fingerprint (information available at <http://www.naftemporiki.gr/news/static/08/11/15/1591982.htm>)

¹⁶⁰ See also the data minimization legal requirement in the PRIME White paper, p. 6

¹⁶¹ See for example the review by the European Data Protection Supervisor (EDPS) of the Identity and Access Control System of the European Anti-Fraud Office. In its opinion, the EDPS states as follows : 'The type of data collected, mainly the fingerprint templates of three fingers and related identification information, corresponds to the data required to operate an access control system based on biometrics. From this point of

In order to properly assess the adequacy of the use of particular data for access control purposes, it may be sometimes necessary to carry out a *targeted impact assessment*, evaluating the reasons that justified the use of a specific technique and whether other, less privacy intrusive alternatives, were envisaged.¹⁶²

For an IdM system, it shall

- Be reviewed whether under the applicable national data protection legislations, the use of specific data, such as biometric data, and other identifiers and identifying data, is proportional for the IdM system envisaged.
- Conduct a targeted impact assessment if needed.

The proportionality of the use of biometric data for the Turbine IdM system depends upon (i) the system specifications and (ii) the specific applications for which the system will be implemented. In case the system is implemented for high security needs, it is possible that the proportionality of the used data will be accepted. Such decisions, however, will depend upon the appreciation of the local DPA depending on the circumstances.

5.2.7 Prohibition to process data revealing racial or ethnic origin and data concerning health (unless exemption applies)

For an IdM system, no data revealing racial or ethnic origin shall be processed or data concerning health (sometimes also referred to as 'sensitive data').

The Directive prohibits all processing of such sensitive data (Art.8(1)) unless an express exception applies (Art.8(2)), including, notably, an explicit consent, which is freely given.(Art.8(2) (a)).

Some information revealing access to particular databases or sites, including information such as search strings used and contained in browsers or web page visit information, may reveal sensitive information about an identified or identifiable person. In such case, an IdM system should provide for anonymous access to such databases or sites.¹⁶³

Also biometric data often contain more information than that which is necessary for the identification or the authentication/verification functions of the biometric system. For example, biometric samples may include information about race or about health. It is not known yet to what extent templates may also reveal such information. The WP 29 therefore recommends that the templates should technically be constructed in a way to preclude the processing of such data and in addition to preclude that the biometric sample could be retrieved from the template. Unnecessary data should be destroyed as soon as possible.

For an IdM system, it shall therefore

- Carefully review to what extent some data, including some identifiers, may reveal sensitive information ;
- Examine whether the data subject has been informed of (the possibility of) the processing of sensitive information and whether an exception applies for the processing of such sensitive data ; and
- Preclude the reconstruction of the biometric samples from the biometric template

view, the EDPS considers that the data collected are adequate and relevant for the purposes of the processing.' See EDPS, Opinion of 7 April 2008, Case 2007-0635, p. 7.

¹⁶² *Ibid.*, p. 8.

¹⁶³ See also the requirements set forth in the PRIME project.

To the extent the Turbine IdM system aims to preclude the reconstruction of the biometric samples from the biometric template, and no other sensitive data is processed, this requirement is complied with.

5.2.8 Avoidance of unique identifier requirement

The Directive states that the Member States shall determine the conditions under which an 'identifier of general application' may be processed (Art. 8.(7)).

For an IdM system, this requirement is of specific importance. For IdM systems developed and used by private parties, the use of any such identifiers shall be avoided or at least reviewed under the local applicable legislation. The use by private parties of national registry numbers, e.g., is often regulated and subject to restrictions.

For the use of biometric data in IdM system, this principle is of particular relevance. Fingerprints could in principle be considered as an 'identifier of general application'. Other biometric data, such as iris, could also serve as such. For this reason, the WP 29 finds it desirable to avoid as much as possible that biometric data could be used as a unique identifier to link databases containing personal data.

One of the challenges of an IdM system is in our view *to choose an appropriate kind of identifier* in view of the purposes of the IdM system.¹⁶⁴ This is also related to the purpose and finality requirement and the proportionality requirement : the identifier shall as such not reveal more information about the data subject as is necessary for the finality of the IdM system.

For an IdM system, it shall therefore

- Prevent that personal data, in particular the identifiers and biometric data used to establish the pseudo-identities, could be used as unique identifiers or for linking data subjects across databases (see also *below*); and
- Choose appropriate identifiers in view of the purposes of the IdM system.

The Turbine IdM system pays specific attention to this data protection concern. To the extent the Turbine IdM system will delete the captured biometric sample, and in general, shall not transfer biometric templates, the proposed system, while using biometric characteristics for the calculation of a unique code but which cannot be cross-sector used, avoids that the biometric characteristic could be used as a unique identifier. The Turbine IdM system hence takes this requirement into account.

5.2.9 Central and local storage requirements

The Directive as such does not contain any specific requirement as to the place of storage of personal data. However, it is a general security risk to store personal data in centralized data bases.

In addition, with regard to specific personal data, in particular biometric data, it is strongly advised to avoid central storage of biometric data because of risks of identification of persons and the risk of use of the data without the knowledge of the data subject. WP 29 recommends the use of central databases only after careful assessment and limited for e.g., high security installations. National Data Protection authorities take a similar position.¹⁶⁵

¹⁶⁴ For a social network, for example, the identifier shall not reveal more information than necessary and provide sufficient anonymity to its users. In such applications, data subjects will often have the possibility to choose the identifier themselves.

¹⁶⁵ For example, France : see Communication of the CNIL relating to fingerprint recognition systems with central database storage, December 2007, 12 p.

An IdM system should therefore envisage

- Local or distributed storage of personal data..

To the extent the Turbine IdM system will in principle provide for the local storage only of the biometric identifiers, the proposed system takes this requirement into account.

5.2.10 Identification of data subject for no longer than is necessary requirement

The Directive explicitly states that personal data must be kept in a form which permits data subjects to be identified for no longer than is necessary for the purposes for which the data was collected and processed (Art. 6.1.e Directive).

In an IdM system, the finality of the processing is the identification of a person (which does not necessarily mean revealing the (civil) identity of the data subject behind the identifier). This data protection requirement hence seems then also awkward. However, a distinction should be made about the necessity to identify and the period related thereto, and this from the perspective of the identity provider, the IdM service provider and the other service providers.

For all, identification will – depending on the type of IdM system ('anonymous' or fully authenticated) - be necessary at the time of accessing the application for which the IdM system is used.

However, identification may no longer be required for the IdM service provider and other service providers (for example, in the service profile) once the service has been accessed.

This privacy requirement could be translated as a requirement to use various tools, for example by deleting references to the pseudo-identities if no legal obligation to keep such references exist or by respecting a short term for keeping access control information restricted to the time needed for identifying and responding to incidents.¹⁶⁶

For biometric data, this principle could imply that biometric samples and biometric templates are not stored at all in the IdM system if feasible. This excludes abuse of such biometric data, including positive or negative identification without the knowledge of the data subject.

In any case, the retention of personal data shall be limited.¹⁶⁷

The retention of data, however, will also have to comply with specific legislation requiring the retention of specific data for well determined purposes for a specific period in combination with data retention obligations (see also *below* section 5.4).

An IdM system should therefore envisage

- Delete references to the pseudo-identities in the service profile if possible;
- Deleting access control information when no further needed for investigating security incidents.

To the extent the Turbine IdM system will avoid storage of biometric samples and of biometric templates, and limit the duration of keeping additional identifying information, the system concedes to this requirement.

¹⁶⁶ One year may be too long. See EDPS, *o.c.* at footnote 161, p. 10.

¹⁶⁷ The importance of the retention period from privacy and data protection concerns was also stressed in the recent decision of the ECHR in *S. and Marper v. United Kingdom*, cited *above* in footnote 144.

5.2.11 Data quality requirement

The Directive requires that the personal data processed must be accurate and kept up to date, where necessary. Inaccurate or incomplete data must be erased or rectified (Art. 6.1.d Directive). This principle also applies to the data processed in IdM systems, but also to the personal data contained in certificates. Specific legislation (for example, on electronic signatures (see also *below* section 5.5)) may contain additional rules, for example on liability, when data are not accurate.

Built-in procedures for updating information may be very helpful and is seen positively.¹⁶⁸

In case of a distributed control system, this requirement may pose problems. Contractual agreements shall cover this issue.

An IdM system should therefore

- Update data if necessary;
- Remove inaccurate data; and
- Provide for contractual arrangements regarding the maintenance of the data quality.

The Turbine IdM system shall provide for a mechanism to update the data and shall in that case comply with this requirement.

5.2.12 Information and transparency to the data subject - Access and correction – right to revoke - right to control ?

The Directive imposes a detailed information obligation upon the controllers towards the data subject and states explicitly which information shall be given (Art. 10 & 11 Directive).

The Directive prohibits in fact processing personal data in secret¹⁶⁹: data subjects enjoy a legal right to see what information others have on file about them, and to learn what is being done with it. The latter shall be informed *inter alia* about the identity of the *controller* and the *purpose(s) of the processing*, in principle at the time of the collection of the data.

The Directive also requires in addition that data subjects have access to *additional information* 'without constraint and at reasonable intervals', in particular (i) *confirmation* as to whether or not data relating to him are being processed, the purpose of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, (ii) communication to him in an intelligible form of the *data undergoing* processing and of any available information as to the source of the data, and (iii) knowledge of the *logic* involved in any automatic processing of data concerning him at least in the case of the automated decisions (Art.12 (a) Directive). These access rights include the right to access data such as to the *log files* of the IdM system.¹⁷⁰

One of the Article 29 Working Party's *main concerns* in its opinion with regard to the .NET Passport service was specifically the *lack of information* about the privacy implications of the system. Particularly, the Article 29 Working Party required that the users were provided with clear information about which parties were responsible for which data processing operations and that the users were given choice and control over disclosing information to participating service providers.¹⁷¹

¹⁶⁸ See EDPS, *o.c.* at footnote 154, p. 10.

¹⁶⁹ Note, however, that data processing for particular purposes, which fall outside the scope of Community law, such as processing for public security, defense, State security and in areas of criminal law, does not fall within the application field of the Directive (Art. 3 (2)).

¹⁷⁰ See EDPS, *o.c.* cited at footnote 154 , p. 14.

¹⁷¹ The Article 29 Working Party, *o.c.* at footnote , p.6-8.

How the information has to be provided is less clear. The Article 29 Working Party's opinion does not address in full detail the way the information requirements regarding identity management shall be fulfilled, but makes some suggestions, such as the use of a *prompt*-box and the use of different *languages*. Of relevance may be here an Opinion on harmonized information provisions in 2004 in which the Article 29 Working Party referred to *multi-layered information notices*.¹⁷² This would essentially allow controllers to employ a *simplified short notice in their user interface*, as long as the latter is integrated in a multi-layered information structure, where more detailed information is available, and *the total sum of the layers meets national requirements*.

More specifically, the Article 29 Working Party envisages that there could be up to three layers of information:

- (i) the *short notice*, which provides the essential information (and, in view of the circumstances, any additional information necessary to ensure fair processing);
- (ii) the *condensed notice*, which includes all relevant information required under the Data Protection Directive; and
- (iii) the *full notice*, which includes all national legal requirements and specificities.¹⁷³

For IdM systems, this results in fact in an requirement that the data subject *understands* the functioning of the system. Various principles of the Directive imply indeed that personal data shall be processed in a transparent way. For IdM systems, it would in our view be recommended to inform the data subject of all data required to understand the processing, also about the use of the identifier, e.g., in case of the use of a pseudonym, about the varying degree of anonymity that the pseudonym provides for.¹⁷⁴ For biometric data, this principle could imply that the data subject receives at the time of the collection a comprehensive and more detailed information about the use of the fingerprint than presently is required according to the wording of the information obligation as set forth in the data protection legislation. Biometric systems and IdM systems are indeed very complex and such extended information may be required.

The requirement to inform the data subject and to be transparent shall also be seen in combination with the principle of *fair and lawful processing*.¹⁷⁵ The Directive requires that personal data are processed 'fairly and lawfully' (Art. 6.1.a Directive). For an IdM system which uses fingerprints, which leave easily traces (e.g., on doorknobs, glasses, etc) and which can be retrieved for fraudulent purposes, the fore-mentioned principle implies in addition to the general information and transparency obligation for systems in general that the fingerprint template should for privacy and data protection purposes be stored (if necessary) on an object (e.g., a smart card) that is under the control of the data subject (rather than in a database). As a result, the data subject cannot be identified through the biometric without his knowledge and the data subject knows when his biometric is used in the IdM system. This principle, taken one step further, could also imply that the IdM system cannot deploy (stolen) fingerprint without the active cooperation (and hence the knowledge) of the data subject (e.g., by giving a secret or aliveness detection upon presenting the sample).

The Directive further requires that a data subject has access to the data processed about him (see also above) and can rectify, erase or block the processing of data that are incomplete or inaccurate (Art. 12 (b) Directive).

This article 12 (b) of the Directive in combination with a more general right of the data subject under the Directive to object data processing 'at any time on compelling legitimate grounds relating to his particular situation' unless provided otherwise by national legislation (Art. 14 (a) Directive) could imply that a data subject disposes of a general *revocation right* in case of misuse or theft of his personal data in an IdM system. Such revocation right or possibility, in combination with alternative

¹⁷² The Article 29 Working Party, Opinion on More Harmonised Information Provisions, 25 November 2004, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.

¹⁷³ *Ibid.*, p. 7-9.

¹⁷⁴ For the varying degree of anonymity provided by pseudonyms, see *above*, section 4.2 .

¹⁷⁵ See for example, article 33.3 and article 34.3 of the Dutch data protection act of 6 July 2000, which in fact put forward as a general principle that additional information shall be given depending upon the nature of the data and the processing to guarantee a fair and careful ('*behoorlijke en zorgvuldige*') data processing.

procedures for persons who are not able to enroll or are unduly rejected, has been mainly discussed in the context of biometric IdM systems, but seems valuable for IdM systems in general.

The rights of access and correction and of revocation require for the IdM system an appropriate procedure to be defined and put in operation in general and in case the IdM system is compromised.

In case an IdM system would envisage to use personal data also for direct marketing purposes, the Directive 95/46/EC requires that the data subject is informed beforehand and may object free of charge to the processing of his personal data for such purposes (opt-out) (Art. 14 (b) Directive).

From the above, it appears that to the extent that a system is not transparent, the data subject shall have *an increased control* over the processing of his information, also in an IdM system. The Article 29 Data Protection Working Party has formulated it in its .NET Passport opinion with regard to the communication of profile data to participating service providers as follows : 'A new functionality will also be included to enable users to decide on a site-by-site basis whether they want to communicate their profile data or not'.¹⁷⁶

An IdM system should therefore

- Inform the data subject about the controller(s) (see *above*) and the purposes;
- Provide the appropriate information about the functioning of the IdM system if the data subject exercises the right of access (see also *below*); and
- If possible, explain through user friendly *user interfaces messages* what is happening with the (biometric) data during the process of the use of the IdM system and confer control to the user (for example, by storing the personal data *on an object under the control* of the data subject).

The Turbine IdM system will develop an appropriate interface in order to provide the data subject with the information required in compliance with this requirement. In addition, the data subject shall have control over the deployment of each of its pseudo-identities and over the information sent to service providers.

5.2.13 Retention and/or destruction of the data

Personal data should not be kept for any longer than necessary for the purposes for which the data were collected and processed.¹⁷⁷ This is one of the basic principles of the data protection legislation and relates to data quality, but also to the limitation of purpose principle (see also *above*).

In specific case, such as for crime investigation and prosecution, this may not apply in accordance with mandatory legislation.

This general principle laid down in Directive 95/46/EC is as already stated further amended and completed for specific data for which specific retention periods and obligations apply (see *below* at section 5.4).

An IdM system should therefore

- Determine a retention and/or destruction policy for all personal data.

The Turbine IdM system will have to outline the retention policy for the data involved in order to comply with this requirement.

¹⁷⁶ The Article 29 Working Party, *o.c.* at footnote 26, p.8.

¹⁷⁷ See also *above* section 5.2.10.

5.2.14 Security of the IdM processing

The Directive 95/46/EC requires that controllers implement 'appropriate technical and organizational measures' to protect the personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access or other forms of unlawful processing (Art. 17 Directive).

National Data Protection Authorities sometimes issue guidelines on security measures for personal data in general (e.g., Belgium, Spain). Furthermore, general security standards (such as product and technical oriented security criteria set out in e.g., ISO/IEC 15408/1 and procedure and system related criteria set out in e.g., ISO/IEC standard 27002 (formerly ISO/IEC 17799) and ISO/IEC 27001) are applicable.

For IdM systems, the security measures shall be appropriate to the risks associated with the processing of the data to which the IdM system gives access (e.g., an e-health application will require higher security measures for the access control (IdM) application). This also applies to the processing of biometric data as they present special risks (such as e.g., identity theft, unknown identification...), and the processing of such data also contains specific risks (e.g., unauthorized access, spoof attacks, etc).¹⁷⁸

Risk management will take into account the probabilities of mistakes and the possibility of identity fraud.

Opinions of the Article 29 Working Party and National Data Protection Authorities which describe specific security measures for IdM systems are limited. In the Working Document on E-Government, the Article 29 Working Party stated that, where national DPAs were consulted on projects of online administrative procedures, DPAs nevertheless stressed that (i) *transmission* of data needed to be encrypted, as well as (ii) encryption during the data *storage* and (iii) de implementation of data *loggers and of log files*.¹⁷⁹

For e-health systems, the Article 29 Working Party stated that it was deemed necessary by matter of data security to impose (also by legislation) security measures that foresee the necessity of

- the development of a reliable and *effective system of electronic identification* and authentication as well as constantly up-dated registers for checking on the accurate authorization of persons having or requesting access to the EHR system;
- comprehensive *logging and documentation of all processing steps* which have taken place within the system, especially access requests for reading or for writing, combined with regular internal checks and follow up on correct authorization;
- effective *back up* and recovery mechanisms in order to secure the content of the system;
- preventing *unauthorized access to or alteration* of EHR data at the time of transfer or of back up storage, e.g. by using cryptographic algorithms;
- clear and documented *instructions* to all authorized personnel on how to properly use EHR systems and how to avoid security risks and breaches;
- a clear distinction of functions and competences concerning the categories of persons in charge of the system or at least involved in the system with a view to liability for shortcomings; and

¹⁷⁸ See also various deliverables of the Fidis ('Future of identity in the Information Society') project, including M. Gasson, M. Meints, e.a. (eds.), D.3.2. : *A study on PKI and biometrics*, Fidis, 4 July 2005, 138 p.; M. Meints & M. Hansen (eds.), D3.6. *Study on ID Documents*, Fidis, 2006, 160 p. and E. Kindt & L. Müller (eds.), o.c. at footnote 49.

¹⁷⁹ Article 29 Working Party, Working Document on E-Government, WP 73, 8 May 2003, p. 4.

- regular internal and external data protection auditing.¹⁸⁰

Although the guidelines of DPAs are not mandatory rules that are strictly speaking enforceable (unless they are part of legislation), they have an important impact.

Therefore, an IdM system

- Shall require a detailed risk and security analysis for the IdM system;
- Shall require appropriate security mechanism solutions;
- Shall be aware that central databases are focus points for attacks; and
- Shall take errors and the possibility of identity fraud into account in risk management.

In the Turbine project, the security measures are subject of detailed research. The proposed Turbine IdM system envisages implementing various security measures in order to comply with all identified security requirements in order to cover the risks.

The Turbine IdM system will in principle not focus on storage of the biometric reference templates or pseudo-identities in a central database, unless this would be required for a justified and legitimate purposes, such as duplicate enrolment checking.¹⁸¹

5.2.15 Confidentiality of the processing requirement

The Directive requires that any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data, must not process the data except on instructions from the controller, unless he is required to do so by law (Article 16 Directive).

The local applicable data protection laws may contain provisions which will imply that the controller(s) shall give clear instructions to personnel as how and for which purposes the data shall be used. In addition, the controllers should check whether the persons having access to the data are bound by a confidentiality clause in their agreement with the controller. Such kind of clause may in most cases be found in the employment contract.

The national applicable laws may require additional measures, such as keeping lists of authorized persons who have access to the data processing.

IdM systems in principle can enhance the confidentiality of the processing by providing controlled access to applications. Access to IdM systems and administration competence for the system, however, shall also be restricted.

Therefore, an IdM system

- Shall be accompanied with confidentiality instructions and obligations for the employees, processors and other entities; and
- Control access to the system.

The demonstrator implementations of the Turbine IdM system shall provide indications how to comply with this requirement.

¹⁸⁰ Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, 15 February 2007, p.20, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf.

¹⁸¹ See Turbine document D.1.1.1.

5.2.16 Outsourcing to a processor requires a written contract

The controller may delegate the processing of personal data to a natural or legal person by entering a written contract which stipulates that the processor will act solely on the controller's instructions and on his behalf and will comply with the law.

While this requirement is clear, it may be complicated to apply because the definition of the roles in an IdM system may be very complicated (see also *below* section 6.1).

Therefore, an IdM system

- Shall provide for agreements with the processors.

5.2.17 Transfer of personal data outside EU countries requires 'adequate level of protection'

The Directive only allows the transfer of personal data to a third country if such country ensures an 'adequate level of protection' (Art. 25.1 Directive). This level is assessed by the European Commission or the Member States. Derogations from this principle apply, for example with the consent of the data subject or if necessary for the conclusion or performance of a contract (Art. 26 Directive).

In case of multilateral controlled IdM systems, it will be necessary to map the data flows, the controllers involved and the countries where the data flow take place in order to check and comply with this requirement. Especially for this type of IdM system, this may become a complex task.

Nevertheless, it should be clear that transfer of personal data to and/or storage thereof in the United States may be very problematic, as illustrated by the SWIFT case in the recent past.¹⁸² The risk and difficulties of transfer of personal data outside the EU, however, is not a problem for IdM systems alone and adequate solutions should be found overall.¹⁸³

As will be further discussed below, it is likely that the identity provider(s), the IDM service provider as controllers of the processing of the personal data in the IdM system and the other service providers processing related IDM personal data will each have distinct responsibilities and liability for compliance with this requirement.¹⁸⁴

For an IdM system, this requires that due attention is given to the architecture of the system, including the location of its components. The place of (central) storage of the personal data of the IdM system will in this be also important.

This principle could furthermore imply functionality in the design of the interface that the data subject is informed of any transfer outside the EU (e.g., a website and service provider outside the EU) and could authorize such transfer, if appropriate and needed.

Therefore, for an IdM system, the controller shall

- Carefully map the flow and transfers of the personal data in order to check on compliance of this requirement;

¹⁸² The Belgium Data Privacy Commission stated in its Advice N° 37 of 27 September 2006 relating to the transfer of personal data by SWIFT CVBA further to the orders by the UST (OFAC) that it has to be seen as a gross miscalculation by SWIFT that it has, for years, secretly and systematically transferred massive amounts of personal data for surveillance without effective and clear legal basis and independent controls in line with Belgian and European law (p. 20).

¹⁸³ See in this context, C. Shea, 'A need for swift change : the struggle between the European Union's desire for privacy in international financial transactions and the United States' need for security from terrorists as evidenced by the Swift scandal', in 8 *Journal of High Technology Law* 2008, 143.

¹⁸⁴ See *below* in section 6.1.

- Only transfer the data in case an adequate level of protection is available, unless an exemption applies.

The Turbine IdM system shall in principle provide for a decentralized and local storage of the personal data for the IdM system on a token kept by the data subject. The identity provider, if any, and service providers, however, need to comply with this requirement. This also applies in case of justified central storage of the IdM personal data.

5.2.18 Prohibition of automated decisions and right to know

The Directive requires that data subjects shall not be subject to decisions which produces legal effects or significantly affects them and which is based solely on automated processing of data (Art. 15 Directive).

An IdM system, which allows individuals to authenticate themselves in an automated way, could be seen not only as an automated processing but also, insofar a decision is taken whether access is granted or not, as making an automated decision. As such, IdM systems would be forbidden.

There are however exemptions to this prohibition. If the automated decision '*is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view*', such automated decision is acceptable.

IdM systems could probably qualify as an exception to this prohibition, although this should be clarified.

This compliance requirement, however, could also point in the direction of a requirement to develop IdM systems which are user-centric and under the control of the data subject.¹⁸⁵

In any case, the data subject shall have alternative means in case of (temporary) failure of the system. Other measures to safeguard the data subject's legitimate interests should be determined and be enforceable by laws.

5.2.19 Practical applications

In the Working Document of the Article 29 Working Party regarding on-line authentication services, the .NET Passport IdM system was in detail reviewed and one of the first instances where data protection authorities have analysed legal compliance of an identity management. It is therefore a logical starting point for any analysis of the data protection aspects of identity management. This is further supported by the Article 29 Working Party's position, according to which the conclusions reached in that case 'should be considered as being of general application to any on-line authentication system when dealing with similar issues.'¹⁸⁶

At that point, it was however not possible to tell whether the Liberty Alliance is compliant with data protection law, since this essentially depends on the implementation of the specifications.¹⁸⁷ Time will show if these specifications are implemented in a compliant manner.

Examples of review of specific IdM systems more recently include the review by the EDPS of the Identity and Access Control System of the European Anti-Fraud Office¹⁸⁸ and the review of an IdM system for access to different Commission information services¹⁸⁹

¹⁸⁵ See also *above* section 2.2.

¹⁸⁶ Article 29 Working Party, o.c. at footnote 26, p. 14.

¹⁸⁷ '*The Liberty Alliance protocol is neutral regarding data protection. It allows compliance with the Directive but certainly does not require it and no measures are taken concerning enforcement.*' Article 29 Working Party, o.c. at footnote 26, p. 12.

¹⁸⁸ See European Data Protection Supervisor, o.c. at footnote 161.

¹⁸⁹ See European Data Protection Supervisor, o.c. at footnote 154.

IdM has also been a focus in the review of the Article 29 Working Party on e-government in 2003.¹⁹⁰ From a consultation amongst the DPAs relative to e-government issues, DPAs' observations primarily related to measures of identification and authentication of users as well as of agents or professionals allowed to have access to applications of online administrative procedures. These reviews provide useful guidelines in the interpretation of the Directive 95/46/EC.

Furthermore, additional data protection provisions may apply further to Directive 2002/58/EC.

5.3 The E-Privacy Directive 2002/58/EC

5.3.1 IdM systems in 'public' communications networks

In case an IdM system would fall in the application field of the so-called E-Privacy Directive 2002/58/EC¹⁹¹ more provisions relating to the processing of personal data apply in addition to the Directive 95/46/EC. The E-Privacy Directive 2002/58/EC provides for more specific rules for the processing of personal data related to service provision over public electronic communications networks, in particular traffic data and location data.

The term 'data subject' is used in both the Directive 95/46/EC and the E-Privacy Directive, but the latter also introduces terms 'subscriber' and 'user' that refer to the person who is a party to contracts with providers of electronic communications services, respectively the person who uses such services. It should be noted that the 'user' does not necessarily need to be the 'subscriber' (a user is defined as '*any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service*') and that they both have certain rights under the E-Privacy Directive 2002/58/EC.¹⁹²

Traffic data

Traffic data relating to subscribers and users and that are processed and stored *must be erased or made anonymous* when it is no longer needed for the purpose of the transmission of a communication (Art. 6). *Exceptions*, however exist, such as use for *billing and interconnection* payments, processing with *consent* for providing electronic communications services after providing due information and *processing for specific purposes*, such as customer enquiries, fraud detection, marketing services or providing a value added service (Art. 6 (2), (3), (4) and (5)).

Notification of security breaches

Providers of publicly available electronic communications services must also *safeguard security* appropriate to the risk represented (Art. 4 (1)). In case of a particular risk of a breach of security, they shall *inform the subscribers* and advise on appropriate remedies to be taken, including likely costs, if the risks lie outside the responsibility of the service provider.

Difficulties relating to application field

The obligations of the E-Privacy Directive 2002/58/EC, however, only apply to the provision of 'publicly available electronic communication services' in 'public networks'.

While it was initially intended that the E-Privacy Directive 2002/58/EC would only apply to 'public' electronic communications networks and services, such as telecom operators and internet access and service providers, excluding networks and services that are not made available wholly or

¹⁹⁰ Article 29 Working Party, Working Document on E-Government, 8 May 2003, 18 p.

¹⁹¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereafter the E-Privacy Directive 2002/58/EC), OJL 201, 31 July 2002, p. 37.

¹⁹² For example, in a company, the company may be the subscriber, whereas the employees would be the users. If the user or subscriber is a natural person, he/she will also be a 'data subject' under the two Directives.

mainly to the provision of electronic communications services *to the public* (e.g. enterprise networks and other internal systems), services are now increasingly becoming a mixture of private and public elements. As a result, the unclear definitions give rise to several questions, including as to the quality of a cyber café or a multinational company, providing access to thousands of employees, as providers of (public) electronic communications networks or not.¹⁹³

This is also relevant for IdM services. IdM services of for example a mobile operator for access to the network fall within the application field of the E-Privacy Directive 2002/58/EC. IdM services by other providers of 'publicly available electronic communication services' in 'public networks', however, such as of online banking services, could possibly also fall under the application field.

The Article 29 Data Protection Working Party has already advised that, in practice, the notions of 'public communications network' and 'electronic communications services' are very unclear and should be explained in more detail.¹⁹⁴

Therefore, an IdM system

- Shall require to erase or make traffic data anonymous when no longer needed;
- Shall require an appropriate procedure of notification of security breaches.

5.3.2 IdM systems in mobile environments

The above discussed E-Privacy Directive 2002/58/EC contains also specific provisions relating to location data.

Location data is defined in this Directive as '*any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*' (Art. 2 (b)).

Such location data will become increasingly important for the provision of location services, such as for providing content and information based on the place persons are, when accessing the Internet from various locations and by using a diversity of devices, including mobile phones and personal digital assistants.

Such location data may only be processed when they are *made anonymous*, or with the *consent* of the users or subscribers used for the provision of a value added service, to the extent and the duration necessary for the provision thereof (Art. 9 (1)). In case consent has been obtained, the user must have the possibility by using a simple means and free of charge, of *temporarily refusing* the processing of the location data. (Art. 9 (2)).

IdM systems, provided they are offered by a 'public electronic communications network provider' or are offered by such service provider, shall take these requirements into account. The same unclarity with regard to the application field as set out *above* however applies.

Therefore, an IdM system

- Shall require to make location data anonymous unless with consent of the data subject ;
- Shall, in case consent was obtained, require an appropriate procedure for allowing the data subject for temporarily refusing the processing of the location data.

¹⁹³ Article 29 Working Party, *Opinion82/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive*, WP 126, 26 September 2006, p.3.

¹⁹⁴ Article 29 Working Party, *Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)*, WP 150, 15 May 2008, p.4.

5.4 The Data Retention Directive 2006/24/EC

Under the Data Retention Directive,¹⁹⁵ the EU member states are required, as a derogation from Articles 5, 6 and 9 of the E-Privacy Directive, to adopt measures to ensure that (a) data necessary to trace and identify the *source* of a communication, (b) data necessary to identify the *destination* of a communication, (c) data necessary to identify the *date, time and duration* of a communication, (d) the data necessary to identify the *type of communication*, (e) the data necessary to identify *users' communication equipment* and (f) data necessary to identify the location of mobile communication equipment (but not the "data revealing the content of the communication" (Art.5 (2)) is retained by the providers of publicly available electronic communications services or of public communications networks for periods of not less than six months and not more than two years from the date of the communication." (Art. 5 and 6).

Article 5 details with great precision what categories of data are to be retained. Each national legislation will determine the duration of the data retention and shall therefore be checked.

As to the determination of the applicable local law, the general criterion of Directive 95/46/EC may apply, i.e. the laws of the place where the data are processed (e.g., stored) in the context of the activities of an establishment of the controller (Art. 4 (1) (a) of Directive 95/46/EC).

If the controller has no establishment within the EU, but uses equipment on the territory of a Member State, for purposes other than mere transit, the national laws of such territory shall apply.

It is possible that a device kept by the data subject under his control for using one of the multiple identities, qualifies as such equipment. In that case, the place where the devices are used (and where the data subjects are), will determine the applicable national data retention laws.

Therefore, an IdM system

- Shall check the locally applicable national laws on data retention ;
- Shall retain all data as specified in such national legislation for the period imposed.

5.5 The E-Signature Directive 1999/93/EC

The E-Signature Directive 1999/93/EC harmonizes the legal rules on the use of electronic signatures.¹⁹⁶ There are two types of electronic signature under the E-Signature Directive 1999/93/EC. There is an electronic signature, and an 'advanced' electronic signature. An 'advanced' electronic signature is a digital signature which '(a) is *uniquely linked* to the signatory, (b) is capable of *identifying* the signatory, (c) is created using means that the signatory can *maintain under his sole control*, and (d) is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable'¹⁹⁷ (stress added).

The advanced electronic signatures are based on so-called 'qualified certificates' which are digital certificate issued by a certification authority and are created by a 'secure-signature-creation-device'. Such advanced electronic signatures have legal effect in the same manner as hand-written signatures and are admissible as evidence in legal proceedings (see Article 5).

The requirements for such 'secure-signature-creation-device' however give way to discussion and give rise to problems. Standard PCs for example are not accepted as such 'secure-signature-

¹⁹⁵ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54.

¹⁹⁶ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 139, 19.1.2000, p. 12.

¹⁹⁷ See Article 2 of the EU directive 1999/93/EC.

creation-device'. Electronic signatures which do not meet the above set four criteria, may also have legal effectiveness and be admissible as evidence, but the judge will need to appreciate the situation and to take a decision.

The E-Signature Directive also contains common obligations for certification service providers in order to effectuate cross-border recognition of signatures and certificates throughout the EU.

Under the E-Signature Directive, Member States must ensure that certification service providers and national bodies responsible for accreditation or supervision also comply with the Data Protection Directive (Article 8).

The E-Signature Directive 1999/93/EC expressly states that certification service providers, issuing certificates or providing other services related to electronic signatures, cannot be prevented from mentioning a *pseudonym* in the certificate instead of the signatory's name (Article 8 (3)). It does not prevent, however, that *Member States require identification* of persons pursuant to their national legislation (recital 25).

In addition, the E-Signature Directive 1999/93/EC states common rules on liability to help build confidence among service providers and users who rely on the certificates. The specific liability regime created by the Directive comes on top of national rules regarding liability and is of importance in the relation between certification service providers issuing qualified certificates and any legal or natural person who *reasonably relied* on that certificate.

A service provider issuing a (pseudonymous) certificate can be held liable in three different situations, unless he can prove that he has not acted negligently (see Article 6):

- First of all, such service provider will be liable for the damage resulting from the *inaccuracy and incompleteness* of information to be contained in the qualified certificate *at the time of the issuance* of the qualified certificate. After the certificate is issued, and the information would change, the certificate service provider would not be deemed to permanently verify the accuracy of the information. This is responsibility of the recipient of the certificate, who will possibly have to revoke the certificate.
- Secondly, such service provider issuing a (pseudonymous) certificate should also guarantee that the recipient of the certificate holds, at the time of the issuance of the certificate, the signature-creation data corresponding to the signature verification data given in the certificate.
- Thirdly, if the certification service provider would generate both the signature-creation data and the signature verification data, it should assure that they can be used in a complementary manner.

The service provider issuing a (pseudonymous) certificate shall also ensure that the date and time of revocation of the certificate are accurately registered (Article 6 (2)).

The certificate service provider can limit its liability by indicating in a qualified certificate limitations on the use of that certificate or on the value of transactions for which the certificate can be used, provided that the limitations are recognizable to third parties (Article 6 (3)).

The above rules contained in the Directive 1999/93/EC, especially relating to the liability of the certification service providers, would in principle apply in the case of an IdM service.

5.6 The E-Commerce Directive 2000/31/EC

The E-Commerce Directive 2000/31/EC harmonizes various legal aspects of the so-called 'Information Society Services'.¹⁹⁸ 'Information Society Services' are defined as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request

¹⁹⁸ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *O.J. L* 178, 17 July 2000, p. 1-16.

of a recipient of service'.¹⁹⁹ Interesting in this Directive is the principle that for the matters regulated in this Directive (information provision relating to e-contracts, unsolicited commercial communications, liability of access providers, etc), the national laws of the country where the service provider is established, shall apply (even if the service is provided in other countries within the EU) ('*country of origin*' principle) (Art. 3.1).

IdM systems which are offered as a service based on an economic activity could be considered as an Information Society Service regulated by this Directive and the implementing national local laws.

IdM systems shall therefore comply with the information requirements imposed by the E-Commerce Directive and the implementing local national laws, including the '*rendering easily, directly and permanently accessible (...) at least (a) the name of the service provider, (b) the geographic address at which the service provider is established, (c) the details of the service provider, including his electronic mail address (...) (d) where the service provider is registered (...), (e) (...) the relevant supervisory authority (...)*'. (Art. 5).

Member States may also *not* make the activity of an information society service subject to *prior authorization* or any other requirement with equivalent effect (Art. 4). Reference is hereby made in fact to a prohibition to submit activities of an information society service to a kind of a licensing system. It is not meant to refer to any authorization requirements, if any, by data protection authorities. However, if an increasing use is made of unique identifiers in IdM systems, authorization by data protection authorities may be required. This could possibly be in conflict with this Article 4 of the E-Commerce Directive.

5.7 Specific requirements for e-government

IdM in e-government poses specific requirements. E-government could be described as setting up and promoting the online supply of administrative procedures, to make public administrations more efficient and effective.²⁰⁰

In such a context, a *citizen* will need to electronically prove his claims for access to the e-government services and have the means thereto. For many e-government applications, identity-related claims and authorizations will be required (for example, for filing a criminal complaint). In some cases, strong authentication will be required. Such authentication could be based on biometrics.

The requirement for identification and authentication, however, will not be valid for all e-government applications. For some specific applications, an anonymous access to the services would even be necessary, for example in the case of accessing help-websites (e.g., on alcohol abuse) or for e-voting.

But not only citizen need to be identified and authenticated in e-government applications, also the *members of governmental institutions*.

Various projects and studies relate to identity management for e-government purposes, such as Modinis and Work package 16 of Fidis.²⁰¹ In some projects, the interoperability of various national

¹⁹⁹ Article 1 (2) of Directive 98/48/EC of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, *O.J. L.* 204, 21 July 1998 and *O.J. L.* 217, 5 August 1998. Further to recital 18, it is clear that information society services also include free services, as long as the service is provided in an economic context.

²⁰⁰ For France, see for example '[Mon.Service-Public.fr](http://www.mon-service-public.fr)', which is since December 2008 operational throughout the French territory, aiming to provide citizens with unified, personalised and secure access to online Government services ; on e-government in general, see also the Information Society portal of the Commission at http://ec.europa.eu/information_society/tl/soccul/egov/index_en.htm

²⁰¹ See J. Buitelaar, M. Meints and B van Alsenoy (eds.) *D16.1 Conceptual Framework for Identity Management in eGovernment*, 18 November 2008, 143 p. and J. Buitelaar, M. Meints and E. Kindt (eds.) *D16.3 Requirements for Identity Management in eGovernment*, (in preparation), deliverables available at www.fidis.net ; Modinis IDM, *Modinis Study on Identity Management in eGovernment*, available at <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf> ; for examples of studies by industries, e.g., on federated IdM management, see

e-government services on EU level was even studied.²⁰² It is not the aim of this report to analyse or discuss the needs for e-government in depth.

In general, however, it should be noted that the *degree of authentication* of the electronic identities will vary depending on the 'sensitivity' of the e-government application. Username and password may sometimes be sufficient, sometimes the use of a token is required, all in combination with the use of reference data repositories, but for many applications, a more secure authentication will be desired.

The *identifiers* will also play an important role in e-government. From previous studies, it is clear that there is a lot of divergence in the approach towards the application of such identifiers. Some Member States will use national identifiers, while other Member States use sectoral or contextual identifiers. For the Netherlands, for example, a central number (CSN) will be used for all sectors, while other Member States, such as Germany, oppose to the model of a central identifier.²⁰³ The discussion about the use of such identifiers is in many countries still going on. Therefore, it is at this time not possible to draw general conclusions yet on the type of identifier that Member States will require or use in e-government applications.²⁰⁴ Nevertheless, one should know that in the recent report of IDABC, assessing similarities and differences of practices in 32 countries on eID and interoperability, it was indicated that sector or application specific tokens are in general *not* considered to be a key factor in an e-government strategy.²⁰⁵

The same IDABC study also reported that *mandate management functionality* for e-government in the examined IDM system was still rare.²⁰⁶

One shall also realize that many countries will impose specific IdM requirements for the further development of IdM in e-government in accordance with a conceptual framework that they are developing or have developed.²⁰⁷

Finally, many Member States have in the meantime also introduced electronic identity cards (eID cards). Such eID cards permit citizens to securely authenticate themselves by the means of the digital certificate contained in such eID.²⁰⁸ Whether IdM systems shall take the functionalities and specifications of such national eIDs into account, is not yet clear. First of all, the eID card specifications are different from country to country. Moreover, in some countries, they are mandatory (e.g., Belgium), and in others (e.g., Finland) not. Finally, one could question whether eID systems should rely on the eID card.

The Council of Europe reminded that while the European Commission considers electronic identification management to be among the 'critical key enablers' of e-government, *'[b]iometric national ID cards and eIDM for public services are markedly different : national ID cards serve*

the *Sun Whitepaper : Positioning Federated Identity for the UK Government*, 21 February 2005, available on the Liberty Alliance website, at [http://www.projectliberty.org/liberty/content/view/full/340/\(offset\)/15](http://www.projectliberty.org/liberty/content/view/full/340/(offset)/15)

²⁰² See for example, the GUIDE project, and its report *D1.2.1.B – Identity Interoperability Services Report : Core Service Description*, 30 September 2005, available at <http://istrq.som.surrey.ac.uk/projects/guide/files/documents/D1.2.1.B.pdf>.

²⁰³ See J. Buitelaar, M. Meints and B van Alsenoy (eds.) o.c. at footnote 201, p. 44.

²⁰⁴ For a discussion of the type of identifiers used by governments, see also Article 29 Data Protection Working Party, o.c. at footnote 179, p. 8-9.

²⁰⁵ See the IDABC reports, including 32 Country Profiles on national eIDM schemes, and further in particular H. Graux and J. Majava, o.c. at footnote 123, reports all available at <http://ec.europa.eu/idabc/en/document/6484/5644>

²⁰⁶ *Ibid.*, p.4. 27 countries out of 32 (84%) had no form of mandate management. Four countries out of 32 (12.5%) have implemented an ad hoc form of mandate management covering specific applications or service types, most typically by allowing the designation of an authorised representative in an administration specific database. Only Austria has created a generic system of mandate management, relying on the central sourcePIN Register Authority.

²⁰⁷ See for countries such as the U.K., Belgium, the Netherlands, Germany, Switzerland and Austria, J. Buitelaar, M. Meints and B van Alsenoy (eds.) o.c. at footnote 201.

²⁰⁸ E.g., For Belgium, it is expected that by the end of 2008, all 8,3 million citizens of 12 and older should be in possession of their eID. See *eID without boundaries*, LSEC Information Security Industry Report, February 2008, p. 12, available at http://www.lsec.be/upload_directories/documents/LSEC%20Information%20Security%20Industry%20Report%20Nr.%201.pdf. In the UK, a national ID was only introduced by law in 2006.

public security (...), whereas electronic identification for public services is intended to ease access and offer personalised and smarter services.²⁰⁹

Nevertheless, many expect that electronic identity cards will become more and more important, not only in the context of e-government, but also for all other IdM systems and services in general. In that case, the protection of the fundamental right to privacy and data protection will be crucial in order to enhance trust in these applications.

To conclude, one shall not forget that in general, for IdM systems in e-government, the same rules as with regard to data protection, as discussed *above* in sections 5.2 and 5.3, will apply as well.

5.8 Specific requirements for IdM systems for e-health applications

E-health is an emerging field of application of IdM systems. As for e-government, various projects and studies have referred to or analysed the requirements for IdM systems to be used in relation with e-health applications.

The Article 29 Working Party has stated in its opinion of 2007 that reliable identification and authentication of the persons *having access* to the system, such as the patients, but also the health care professionals, is of crucial importance.²¹⁰ The Article 29 Working Party stressed that for health care professionals *'it will be necessary to develop an identification and authentication system, which proves not only identities but additionally also the role in which a health care professional acts electronically(..)'*.

The Article 29 Working Party also referred to and explained the possible enhancement of data protection by *different data modules* within an EHR system with different access requirements (*modular access rights*), *'that is by forming categories of medical data in an EHR system with the consequence that access is limited to specific categories of health care professionals/institutions'*.²¹¹

²⁰⁹ Commissioner for Human Rights and Council of Europe, *Protecting the Right to Privacy in the Fight Against Terrorism*, 17 November 2008.

²¹⁰ Article 29 Working Party, o.c. at footnote 180, p.14 *et seq.*

²¹¹ *Ibid.*, p. 15 and 18. Examples of such data modules given include a 'vaccination data module', a 'medication data module' and an 'emergency data module', with varying access requirements. For particularly sensitive data, the suggestion is made to build in additional access restrictions, such as explicit consent of the patient and special technical barriers, such as 'sealed envelopes'. See for studies and proposals on federated IdM management in this field of e-health, in particular e-prescription, *Liberty e-Prescription Scenario*, 21 February 2005, available on the Liberty Alliance website, at [http://www.projectliberty.org/liberty/content/view/full/340/\(offset\)/15](http://www.projectliberty.org/liberty/content/view/full/340/(offset)/15)

6. Legal Challenges and Recommendations for Identity Management Systems

6.1 Defining the roles

One of the ways to identifying roles and responsibilities of parties to an identity management system is to verify the roles in the identity management scheme and to check these roles against those available in data protection law.²¹² However, when attempting to do so, one soon realises that *various problems* arise.

First of all, there is the issue of defining *which party is the controller* of the IdM system. A data controller is the entity that determines the purposes and means of the processing. The Article 29 Working Party has suggested that each participant in an identity management scheme is to be considered a controller in respect of their own processing operations.²¹³

Because of the broad definition of 'controller' in the Directive 95/46/EC, participants in an IdM system, whether identity provider of the IdM system or service provider, could indeed be qualified as (co)controller of the data that they process for the IdM system, and be liable for such processing, in the absence of any agreements amongst parties.²¹⁴ This analysis, however, is not shared by all so far because of the complexity of the architecture of some IdM systems.²¹⁵

In case of a centralized system, one could defend that only one controller of the personal data in the IdM system could probably be ascertained. For a centralised IdM system, one controller could in principle decide about the means and the uses (purposes) of the processing of the data of the data subjects registered in the IdM system. For example, the employer who decides to use a particular IdM system for access control for his employees, could be considered the controller of the data in the IdM system. (External) participating companies, that use the IdM system provided by the employer, could be controller as well, for the data processing of the same personal data that relates to their own activities, but not of the IdM system architecture and data processing of the IdM system as such, for which the employer remains the controller. In open multi-organizational IdM systems, the roles of the participating providers will be more complex.

Also because of the varying degrees of collaboration between organizations participating in an IdM system, it will remain extremely complex to determine the roles and responsibilities of parties involved. Particularities of implementing national data protection legislations, such as with regard to the definition of 'controller'²¹⁶, will even further complicate matters.

²¹² See also T. Olsen and T. Mahler, 'Identity management and data protection law : Risk, responsibility and compliance in 'Circles of Trust'', in *Computer law & Security report*, 23 2007, p. 342 (part I) *et seq.* and p. 415 (part II) *et seq.*

²¹³ Article 29 Working Party, *o.c.* at footnote 27, p. 9, 12. In this opinion, the Article 29 Working Party considered Microsoft as controller with regard to the authentication service in .NET Passport, whereas the participating sites were also considered controllers with regard to their own customers.

²¹⁴ See also recital 47 of the Directive 95/46/EC. This recital states that the party offering transmission services may also be considered controller in respect of the processing of the additional personal data necessary for the operation of the service. By analogy, this may also apply to a party offering IdM (identity) services.

²¹⁵ Liberty Alliance, for example, warned that the controller *may change* from one data processing operation to another and that that any participant in Liberty's Circles of trust *may be acting in the capacity of data processor at any given time*. See Liberty Alliance Project, *Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation*, February 23, 2005, p. 15.

²¹⁶ See the example given by T. Olsen and T. Mahler, *l.c.* at footnote 212, p. 419. The UK Data Protection Act 1998, for example, defines a controller as 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed'. The notion of 'in common' is not set forth in the Data Protection Directive. According to the Information Commissioner's Office (the UK's data protection authority) '[t]he determination of the purposes for which, and the manner in which, any personal data are, or are to be, processed does not need to be exclusive to one data controller. Such determination may be shared with others. It may be shared jointly or in common. "Jointly" covers the situation where the determination is exercised by acting together equally. "Determination in

Although the Directive 95/46/EC does not prohibit that agreements are made about the collaboration amongst participants in an IdM system, it is not mentioned in the Directive 95/46/EC how this shall affect the controllers' rights and duties with regard to processing personal data.

→It is therefore advised that parties to an IdM system *carefully map their roles and relations* against those provided for by the Directive 95/46/EC and to enter into appropriate agreements where necessary or appropriate, addressing all aspects of the data processing, including the notification and liability towards the data subject and third parties. The data subject shall also be informed appropriately when the data escape from the control of the IdM participating organizations, for example when data are sent outside the EU.

Another aspect, and as stated above²¹⁷, is that the organizational structure (who has access to an IdM system (e.g., in a hospital) and when) of an IdM system is very important. Guidelines and standards on this facet of IdM, however, will only tackle particular aspects. →Issues such as the *handing over personal data to authorities* in case of request or legal procedure will in most case not be addressed. It is advised that such aspects are be taken care of in the organizational procedure of the IdM system as well.

Furthermore, and as stated above, the determination of the status of an IdM provider in a public communications networks environment, as access provider or service provider in such environment, including the related obligations therewith, is also problematic. →It is recommended that additional *clarification and guidance* is provided as to *when an IdM provider shall comply with the E-Privacy Directive 2002/58/EC*, whether in a modified version of the E-Privacy Directive 2002/58/EC or in authoritative documents of the Article 29 Data Protection Working Party and/or the EDPS.

6.2 Other difficulties in complying with Directive 95/46/EC and Directive 2002/58/EC

The Directive 95/46/EC does not contain specific provisions relating to IDMs. However, as already explained above, the provisions of the Directive will apply to IDMs, notwithstanding some difficulties that may arise from the use of (a specific type of) IDMs (e.g., the difficulty to determine the controller(s) in case of a multi-organizational IdM system, as demonstrated above).

Other provisions of the Directive 95/46/EC may be unfit to cope with the challenges of IDMs. Such provisions which are likely to pose problems are for example the obligation to grant the data subjects access and the right to obtain from the controller additional information about the data undergoing processing and of information as to their source (article 12 (a) Directive 95/46/EC). In the case of federated IDMs, a co(controller) may not be able to give such information as to IDMs information processed by another co(controller). Legal or contractual clauses relating to this right of the data subject, but concluded between parties of a federated IDMs, may prove to be not effective. Also the obligation to rectify, erase or block incomplete or inaccurate data could, for similar reasons, give rise to problems. This will endanger the privacy and data protection rights of the data subject. →It is therefore recommended that, because of the complexity of systems, data subjects have extended rights in order to exercise their right of access and correction. Such rights could guarantee the exercise of the access rights, or provide for increased liability.

Requirements for user-centric and user-controlled system

Notwithstanding the information, access and control rights set forth in the articles 10, 11 and 12 of the Directive, it is not certain whether the Directive would hereby imposes as a principle that the data subject shall have control over the IdM system or should be user-centric.

common" is where data controllers share a pool of personal data, each processing independently of the other'. See the Information Commissioner's Office, Data Protection Act 1998 – Legal Guidance, p.16, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf.

²¹⁷ See above section 3.3.

User-controlled IdM systems, where the flow of the user's identity attributes should be made explicit to the user and where the user has a large degree of control (the notice and control principle), however, are overall deemed to be more privacy friendly. A user-centric IdM system will require that a data subject is able to *choose* from a range of identifiers with varying degrees of observability and linkability.

Nevertheless, the Directive does not provide clear guidelines and principles which shall be followed in case of a user-controlled IdM system. For example, it is not clear if the user would need to receive information, for example with regard to the ability to choose the identifier (such as a pseudonym) and the varying degree of linkability, in real time every time when the personal data is about to be sent or whether it would be sufficient to inform the user at the beginning, in a kind of a framework notice, in order to give the user control. Complementing existing formulation of data protection principles is needed, as they place the individual in a rather passive role and fail to provide him with a proactive right.²¹⁸ → It is therefore recommended that specific criteria are set forth for systems IdM systems which can be labelled user-controlled.

Need for fully international data protection regulation for multi-control/organizational IdM systems

To the extent IdM systems allow to collect, transfer, store and process personal data, and IdM systems are often not limited to controllers established in one (EU) country, but are often organized across national (and EU) boundaries using 'distributed technologies'²¹⁹, it will also be extremely important to provide adequate regulations to protect the personal data in a multi-control led environment and to provide mechanism to ensure compliance. → Such mechanisms could include internal and external audits checking the generally accepted data protection principles (e.g., collection and use limitation, data quality, purpose specification, security safeguards, openness and accountability), but also other mechanism will be required including multilateral security mechanisms (e.g., realisation of strong anonymity and unobservability).²²⁰

6.3 Criteria for enrolment for critical IdM systems

No matter how well an IdM system is designed, including the assignment of identifiers to persons and the authentication, even with strong factors such as biometrics, such IdM system will fail if the identification of the person or the role of a person (e.g., being a doctor) in the enrolment phase before the identifiers are conferred, is not well organized.

Some have commented, such as Clarke and Grijpink, that this important aspect of IdM systems, the identification of the person or role *behind* the identifier during the enrolment, is too often forgotten.

At least in the case of identification for enrolment in systems in the public sector (such as for e-passports or eID), which may later be relied on in the private sector in so far this would be permitted, → legislation should provide for *additional rules* which provide guarantees for a *reliable identification at the time of the enrolment*. Such additional rules could for example be variable background checks based on information available in particular databases, but which are not shown on the documents issued.²²¹

→ In addition, government should *only delegate its powers as identity certification authority to trusted registration authorities according to particular procedures* which can be audited and checked by third parties and according to contracts which provide guarantees for a reliable identification upon enrolment.

²¹⁸ P. De Hert, 'identity management of e-ID, privacy and security in Europe. A human rights view', in *Information Security Technical report*, 2008, (71), 74, referring to M. Rundle, 'The Properties of Identity and Data Protection', in OECD, *o.c.* at footnote 69, p.28.

²¹⁹ 'Distributed technologies' means that many independent parties cooperate, requiring co-ordination and negotiations on a large scale.

²²⁰ See Independent Centre for Privacy Protection (ICPP) & Studio Notarile Genghini (SNG), *o.c.* at footnote 10 p. 93.

²²¹ See J. Grijpink, *l.c.* at footnote 23.

Identification of roles, and the delegation of powers from professional organizations to third parties, is in this context equally important.

6.4 The Use of Unique identifiers

IdM systems could be designed and developed according to the privacy-preserving guidelines and recommendations, as set out above, and hereby comply for example with the principles of anonymity and pseudonymity, for the identification of natural persons. → Hence, the *choice of the identifier* will for privacy-enhancing IdM systems be a central issue and crucial for the system. The regulation of the use of (unique) identifiers and the position taken by national Member States for a particular use, such as in e-health, is however different from country to country. This implies that IdM systems for particular sectors, will be confined to use within one country.

In addition, one shall also take into account that not only persons are identified in a network or system but also various artefacts, such as equipment or network components used by persons. Examples are mobile phones that are identified by a unique number which is the International Mobile Equipment Identity (IMEI) and the International Mobile Subscriber Identity (IMSI) which is unique for each SIM-card.

These numbers amongst other unique numbers in networks may lead to the undesired identification of not only equipment, but also the users of such equipment in an identity management application.²²²

→ The debate which currently exists on the identification capabilities of Internet Addresses (IP numbers)²²³ and which can be compared to the unique identifiers, demonstrates that there is a lot of concern about the use of *such numbers which may identify its users and persons*, and this notwithstanding the implementation of privacy-preserving measures, such as the use of credentials or pseudonyms.

6.5 Criteria for a Privacy Impact Assessment of IdM systems

The need, the opportunity and the practical implementation of a Privacy Impact Assessment (PIA) for technologies which may endanger privacy have been discussed in literature for some years now.²²⁴ Some states even advise or promote the use of such PIA, for example for the use of e-health information or the use of biometrics, or even refer to it in or impose it by legislation.²²⁵

²²² See in this context also the Article 29 Working Party, *Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments : the example of IPv6*, 30 May 2002, 7p.

²²³ See for example, the statements of the European Data Protection Supervisor Peter Hustinx in November 2008 that Internet users' IP addresses and server log records should be treated as personal data and that a decision by a Munich court of October 2008 that IP addresses are only personal data when tied to a person's name was a result of confusion. See also E. Kindt & S. van der Hof, 'Identiteit en identiteitsbeheersystemen in een digitale omgeving' *Computerrecht* 2009 (in preparation).

²²⁴ B. Stewart, *Privacy Impact Assessment On-line resources*, 16 June 2003, available at http://www.foi.gov.uk/sharing/toolkit/pia_online_res.pdf; P. Hope-Tindall, *PIA : Obligation or Opportunity – the choice is ours*, 2002; R. Clarke, *Privacy Impact Assessment : Its Origins and Development*, 9 April 2008, available at <http://www.anu.edu.au/people/Roger.Clarke/DV/PIAHist-08.html>; see also A. Warren e.a., 'Privacy Impact Assessments : International experience as a basis for UK Guidance' in *Computer Law & Security Report*, 2008, pp. 233 – 242.

²²⁵ See, Canada, the Alberta Health Information Act 1999, art; 64 (1) : 'Each custodian must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information', available at <http://www.qp.gov.ab.ca/documents/acts/H05.cfm>; See also in the United States, the US E-Government Act 2002. Reference to and the use of PIAs is also in other countries, such as in Australia, almost common practice. The concept of PIA varies and is sometimes understood as a mere data protection law compliance audit, an instrument of policy or a risk management tool.

The specification of precise criteria for a PIA for IdMs however have not yet been further developed although this would be useful.²²⁶

Because data protection laws do not foresee a specific solution yet for all possible risks for IdM systems on the level of data protection as also indicated and specified in this document, the criteria for the PIA should address the specific risks of IdM (e.g., by providing an evaluation of the kind and the use of the identifiers and credentials) and enable developers, controllers and data subjects alike to assess possible impact of a specific IdM on privacy in general. Furthermore, such PIA should be *integrated into each phase* of the system development life cycle.²²⁷ As stated above, it can be impossible yet very expensive to change the architecture of systems that have already been developed or once they are implemented.

Criteria for a PIA should hence focus on the specific opportunities and functionalities offered by state-of-the-art technologies in IdM systems (e.g., the use of pseudonyms for different usages, the use of private credentials, etc.) and compare these with the functionalities of the IdM system at stake. A *group of experts* could define the criteria for the PIA, which might have to be reviewed from time to time. → The PIA criteria should include *inter alia* the assessment of the level of control by the data subject, the transparency, the functionality for the data subject to choose various identifiers, the risk of the (pseudonymous or anonymous) identifier of re-identification, the risk of observability and linking across various contexts or sectors, and the revocability of the identity.

A PIA could hence provide users with a comprehensive overview as to whether the functionalities of the system are privacy-enhancing or privacy threatening. A PIA would as a consequence in our opinion have to *start* - for those countries which have an extended data protection legislation - once all other general criteria for compliance with the (national) data protection laws (but which may not yet be adapted to the challenges of IdM systems) have already been met.²²⁸ Indeed, if the starting point is compliance with the present data protection legislation as the minimum requirement for IdM systems, a PIA which would only refer to the implementation of the legal requirements seems in our view superfluous.

Legislation could refer to the additional PIA criteria set by the experts, hereby *bridging the gap* between legislation, which often takes much time to adapt to new challenges and technologies, and new existing technologies. This would also give the opportunity to bring concepts which exist for privacy-enhancing IdM under the attention of the broad public while the PIA shall be remaining at the same time technology neutral. Finally, a PIA would also allow to fill in the uncertainties for the time it takes to adopt other appropriate legislative measures.

6.6 Confidentiality of electronic communications and IdM systems

The secrecy and confidentiality of (electronic) communications is a fundamental right and freedom in Western world democracies.²²⁹ This right is protected by international conventions (Art. 8 ECHR (compare with 10 ECHR)), constitutions and national legislations of states, and is repeated in EU directives, in particular the E-Privacy Directive 2002/58/EC on privacy and electronic communications (Art. 5).

Interception of a communication is in general penalized, as well as breaches of the secrecy of private communications and telecommunications, notwithstanding the exceptions provided by law.

²²⁶ Compare also with ENISA Ad Hoc Working Group on Privacy & Technology, *o.c.* at footnote 8, p. 9.

²²⁷ See G. Skinner and E. Chang, *l.c.* at footnote 228.

²²⁸ Some authors, however, include assessment of compliance with data protection regulation into the PIA. See G. Skinner and E. Chang, 'PP-SDLC. The privacy protecting systems development life cycle', in Milutinovic, V., (ed.), *IPSI Conference*, 23 April 2005, p. 7, available at http://espace.library.curtin.edu.au:1802/view/action/_singleViewer.do?dvs=1227513306156~652&locale=nl_BE&search_terms=EPR-603&application=DIGITool-3&frameId=1&usePid1=true&usePid2=true

²²⁹ L. Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam, Otto Cramwinckel Uitgever, 2002.

The identification of the persons involved in a communication is (without consent) also often not permitted.²³⁰

In the case of the use of IDMs in combination with the use of pseudonyms or anonymity, the IDMs identity or service provider *shall in principle respect the principle of secrecy and confidentiality* of the communication. Only in the cases provided by law, lawful interceptions or disclosure about the content and/or the identity of the participants of an electronic correspondence could be made. A lawful recording of the communication and of the related traffic data, including of the participants to the communication, could for example be made when carried out in the course of lawful business practice for the purpose of providing *evidence* of a commercial transaction or of any other business communication. Other exceptions exist for purpose of providing the technical service.

The E-Privacy Directive 2002/58/EC further states that the secrecy and confidentiality *may be restricted by legislative measures* when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of electronic communication system (Article 15 Directive 2002/58/EC).

These exceptions have been proven to be not always very clear. For example, national courts are struggling with the request of representative organizations of the music industry against ISPs to monitor intellectual property infringements and/or to disclose identity data on peer-to-peer networks users.

The European Court of Justice has ruled in this context in the *Promusicae* case in early 2008 that it cannot be derived from European legislation that Member States are obliged to install a duty to provide personal data in the context of a civil procedure to ensure the effective protection of copyright.²³¹

→ It is likely that clarification, either by case law or by additional legislation, for the application of this secrecy principle in relation with IDMs, will be needed in order to clarify under which conditions the identity and service providers are entitled to provide third parties with personal data stored in the IDMs. As some information in the IDMs, however, may be established without a reliable identity provider or by the data subject using pseudonyms, disclosure of the personal data of the IDMs may in some situations also necessitate the disclosure of the IP address and related information. Whether or not IP addresses may be disclosed to third parties in a civil procedure in these cases, is another issue of debate and needs to be tackled.²³²

6.7 Defining the degrees and the needs of anonymity and pseudonymity

As stated above, the term anonymity and pseudonymity and the varying degrees of anonymity and pseudonymity need to be addressed in the relevant instruments which intend to protect anonymity.

→ While anonymity is in general considered an important principle, this should be *more clearly defined* and stated in relevant texts, including in regulations relating to electronic communications and in legislation *de ferenda* relating to IDMs.

These regulations should also provide for the *revocation* of anonymity in particular situations. Users of e-commerce do not wish or need the same degree of anonymity as citizens who participate in for example a voting application.

→ The right of individuals to opt for *the use of a pseudonym in an IdM system in combination with (private) credentials* should for some uses also be confirmed or clarified in legislation. An example of such unclear situation relates to the PKI infrastructure. For example, the E-Signature Directive 1999/93/EC states that use can be made of pseudonyms in the certificates. However, it

²³⁰ See for example, Article 124 of the Belgian Electronic Communication Act.

²³¹ European Court of Justice, *C-275/06, Promusicae v. Telefonica*, 29 January 2008, OJ C 64, 8 March 2008, p. 9.

²³² See for example, F. Coudert and E. Werkers, 'In the aftermath of the Promusicae Case : How to strike the balance?', in *International Journal of Law and Information Technology*, Oxford, Oxford University Press 2008, 23 p (in press).

remains unclear to what extent these pseudonyms need to fulfil other criteria, such as on the level of accountability.

In order to increase the trust of the data subjects in e-commerce, for example, it could be stipulated that the use of pseudonyms in combination with specific credentials or characteristics (for example, which enable accountability and authorization) shall be the default situation.

→ It will also be essential that the distinct situations in which a varying degree of *identification is required* is better defined and that legislation specifies in which cases (contractual) parties may request identification (for example by use of an eID or another unique identifier (e.g., a characteristic, such as a biometric).

6.8 IdM systems and liability of service and identity providers

Referring to the discussion above, it is clear that the role of identity and service providers in IdM systems should be more clearly defined. Some (advisory) opinions of DPAs or the EDPS may shed some light on their role, but this has mainly been limited to the discussion about their role as 'controller' or 'processor'.²³³

→ Also the *issues relating to the liability* of the service and identity providers in general²³⁴ need to be identified. It is, for example, not certain whether IdM systems could be considered as a service of *transmission* of information or a *provision of access* to a communication network (for example, Internet Service Providers (ISPs) are generally considered as such).

The E-Commerce Directive 2000/31/EC²³⁵ requires that Member States shall ensure that a service provider whose service consists of the transmission of information or the provision of access is not liable for the information transmitted if the provider (i) does not initiate the transmission, (ii) does not select the receiver of the transmission, and (iii) does not select or modify the information contained in the transmission (Art. 12.1 ('mere conduit')).

IdM systems are in many circumstances a necessity to transmit information or to have access to a network. In addition, the IdM providers modify in principle not the information contained in the transmission. Recital 43 of the E-Commerce Directive states that 'manipulations of a technical nature' are not considered as ways of involvement of the transmitted information. It is not clear whether IdM systems providing for example for pseudonymity or anonymity could be interpreted as providing a manipulation of a technical nature, without modifying the information in the transmission. If IdM service providers would be considered as intermediary service providers or providers of access, especially in the case of user-centric IdM, one could argue that the IdM service²³⁶ and/or identity provider could under these particular conditions not be held liable for the information transmitted. However, this should not exclude liability of the IdM service and identity provider for the identity and authentication information they provide and on which third parties may rely on. The provisions of the Directive 1999/93/EC could provide some guidance in this respect, but may not solve all relevant questions. For example, the degree of identification (at the time of enrolment) and the liability in case of insufficient checks, remain important and is not addressed.

Awaiting the further widespread adoption of IdM services, it is desirable that this would be further clarified.

²³³ See *above*, at footnote 213. It is important to note that the definitions of controller and processor as such in the data protection legislation have a mandatory character and that the roles cannot be changed, for example by the contracting parties in an agreement. See e.g., Belgian Data Protection Commission, *o.c.* at footnote 62, p.46 (N° 123).

²³⁴ See J. Dumortier and C. Goemans, *l.c.* at footnote 121, p. 205.

²³⁵ See *above* at footnote 198.

²³⁶ For example, providers of the OpenID IdM service (for a list of OpenID providers, see http://wiki.openid.net/OpenIDServers#Identity_Providers)

6.9 Evidence

National legislation determines under what conditions electronic documents and agreements have probative value in general, and in court specifically. Such legislation was adopted in furtherance of the E-Commerce Directive 2000/31/EC.²³⁷ These provisions in the Directive 2000/31/EC (electronic documents shall have the same evidentiary value as paper documents) in combination with the provisions of the E-Signature Directive 1999/93/EC (advanced qualified electronic signatures are given the same legal recognition as handwritten signatures), were to make the information society happen.²³⁸

This legislation, however, will in most cases not be sufficient to confer probative value with regard to the registration of access to particular IT resources, such as logs, and the exchange of IdM information, such as credentials (other than qualified credentials for use for an advanced electronic signature), by the participants in IdM systems.

In general, there are no harmonized European norms concerning either the admissibility or probative value of digital evidence.²³⁹ Judges who have to decide on the evidentiary value of logs will question to what extent the logs are authentic, reliable and intact. Only in the very specific case that digital data is accompanied by an advanced qualified electronic signature, such digital evidence may have a predictable legal effect. In most cases, experts will have to assist the judge in making his or her decision.

→ Additional legislation relating to the probative value of *secure logging* and other *digital evidence* for IdM systems and the conditions (for example, time stamping) for obtaining such value would hence be recommended.²⁴⁰

6.10 PETs : Embedding privacy protection into technology

An example of research in identity management are Privacy Enhancing Technologies (PETs).

PETs cover a wide variety of *technologies* designed to *enhance the privacy* of data subjects. PETs are defined as 'a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system'.²⁴¹

One of the best known examples of PETs is the Platform for Privacy Preferences (P3P) initiative, which is basically a set of software-writing guidelines developed by the World Wide Web Consortium (W3C).²⁴² P3P is Web-browsing software designed to give users more control over their personal information online. The aim is to give users the ability to configure their browsers in order to receive information and notification as to whether web site privacy policies match their preferences. This should allow web user to decide when and under what circumstances to disclose

²³⁷ See *above* at footnote 198. For example, art. 16, § 2 of the Belgian Act of 11 March 2003 concerning several legal aspects of information society services which implemented the e-Commerce Directive states that 'the requirement of an evidence in writing shall be satisfied by a succession of intelligible characters which can later be accessed, regardless of its carrier or the modalities of transmission.'

²³⁸ See Z. Geradts and P. Sommer (eds.), "D6.1: Forensic Implications of Identity Management Systems", Fidis, January 2006, p. 85, available on www.fidis.net.

²³⁹ See B. Van Alsenoy, 'Legal Requirements. Evidentiary value of logs' in S. Wolhgemut (ed.), D14.6, FIDIS, (in preparation).

²⁴⁰ See e.g., for Belgium, the Act of 15 May 2007 concerning a legal framework for certain providers of trust services, *Belgian State Gazette*, 17 July 2007. This law, which needed additional royal decrees for its execution, has not come into force.

²⁴¹ See J. Borking and Ch. Raab, *l.c.* at footnote 139; For an overview of PETs, see the inventory of the OECD, Directorate on Science, Technology and Industry, *Inventory of Privacy-Enhancing Technologies (PETs)*, DSTI/ICCP/REG(2001)1/FINAL, 7 January 2002, and available on [http://www.oalis.oecd.org/oalis/2001doc.nsf/LinkTo/dsti-iccp-reg\(2001\)1-final](http://www.oalis.oecd.org/oalis/2001doc.nsf/LinkTo/dsti-iccp-reg(2001)1-final)

²⁴² The World Wide Web consortium ('W3C') developed a Platform for Privacy Preferences ('P3P') which is a format for specifying the privacy policies of web servers. P3P enabled web browsers enable users to specify their privacy preferences, which are then matched against the web server's privacy preferences. See for P3P in general also <http://www.w3.org/P3P/>

their personal data. While it is generally accepted that P3P does not offer privacy protection, if implemented, it could greatly advance transparency and be used to support efforts to improve privacy protection.

'Privacy friendly' IdM systems could be seen as a part of the broader PET research objectives.

One of the areas of PETs is privacy friendly *access* to services. Such PETs could include the ability for anonymous accessing services on the Internet²⁴³, technologies to manage the data transmitted by cookies or technologies to keep control over various pseudo identities.

The PRIME console is an example of PET in the area of identity management, using P3P and contributing to replacing the 'take it or leave it' approach to privacy policies by a system of policy *negotiation* and the *enforcement* of agreed policies on the server's side when this server is equipped with the PRIME Middleware.²⁴⁴

The Article 29 Working Party repeatedly made reference to the use of *PETs such as IdM systems* and a legal framework concerning security measures foreseeing reliable electronic identification and authentication.²⁴⁵

Difficulties with PETs, however, are the assessment to what extent PETs comply with all privacy requirements in a given implementation and hence offer (full) privacy protection. The adoption of PETs is in general also rather low. One of the reasons for this is precisely that the solutions developed and proposed tend to provide only a limited answer to the need to increase privacy protection, including in identity management solutions. Insufficient compliance with all legal requirements has often been invoked by critics in relation with PETs. → Therefore, more detailed guidelines on the development of PETs by the Article 29 Data Protection Working Party would be welcomed, as well as post factum approval or certification, where possible.

²⁴³ The private sector has developed Internet tools that strip out personal information in order to protect user privacy. Anonymizing services allow a user to browse the Internet using an intermediary to prevent unauthorized parties from gathering personal data.

²⁴⁴ PRIME White paper v.3.0, p. 9.

²⁴⁵ Article 29 Working Party, o.c. at footnote 210, p. 19.

7. Conclusion

IdM systems are designed to administer and control access by individuals (data subjects) to restricted resources. There exists a large variety of IdM systems, some of which have been developed and used in the past and others which are further designed for use in the future for various purposes. The building blocks of an IdM system and the requirements, however, are to a large extent similar. IdM systems deploy identifiers which in some applications refer to the (civil) identity of a person, but which in other applications could also be used to represent the relevant characteristics (or attributes) of data subjects in a specific context. Authentication of the data subject is in most cases crucial. In centralized systems, the identity and service provider who control the system, dispose of large amounts of personal data. In decentralized systems, the personal information is dispersed over many providers.

Because of the nature itself of an IdM system, which is designed to recognize and to authenticate data subjects, there are privacy, data protection and security risks.

User-controlled IdM systems are suggested to limit privacy and security threats. The use of pseudonyms for sector-specific applications could limit the risks, whereby the personal data shall not be linked across the various applications and the use of the pseudonyms cannot be traced or observed.

IdM systems are in general not the subject of specific legislation. The legislation which explicitly refers to IdM systems is scarce. Notwithstanding this fact, IdM systems will have to comply with existing legal provisions relating to privacy, data protection, electronic communications, data retention, electronic commerce and electronic signatures.

The principles which are based on the fundamental right to respect for privacy and data protection guide the development of IdM systems. *Data minimisation* is such a core principle in the data protection legislation which is important for IdM systems. From this principle, it follows that *pseudonyms* should be used as identifiers wherever such is possible instead of identifiers which reveal the civil identity. The *avoidance of unique identifiers* has also been identified in the data protection legislation as important and is specifically relevant for IdM systems. The report describes the role and importance of identifiers in an IdM system. While such identifiers are a key element for the overall effectiveness of an IdM system, they represent a major risk from the point of view of respect for privacy and data protection because identifiers may also be used to link information contained in data bases across sectors. Biometric characteristics are a particular kind of identifiers which are increasingly used in IdM systems. The Article 29 Data Protection Working Party and the national DPAs have repeatedly warned for the use of such (unique) identifiers. The special privacy and data protection concerns relating to the use of biometrics however were not covered in this report, but will be the subject of a subsequent TURBINE deliverable;

Transparency and information to the data subject is also key for privacy-enhancing IdM systems. The Article 29 Data Protection Working Party and the DPAs have provided some suggestions as to how to comply with this requirement, such as with the use of multi-layer information notices, but it needs to be further tested whether this is viable in IdM systems.

Unlinkability of the identifiers (for example of pseudonyms) and their use and unlinkability of the information revealed together with *unobservability* are other requirements which have been indicated as essential in privacy-enhancing IdM systems. The Article 29 Data Protection Working Party warned at various occasions for the risks when merely the 'technical possibility' was available to link the personal data. The *revocability* of the identifiers is another key element of an IdM system, as well as the importance of user control over personal data.

The importance but also the technical viability of these principles are being demonstrated in various projects, including in TURBINE. These principles, however, are not clearly pronounced in regulation or legislation and are in fact based upon the fundamental right to respect of privacy and data protection.

Because the fore-mentioned principles which are of crucial importance for (privacy-enhancing) IdM systems are not yet clearly pronounced in legislation as legal requirements for IdM systems, it is desirable that legislation refers more explicitly to these principles in the context of IdM systems and provides guidance on how to implement these requirements. Additional clarification on *the*

requirements for enrolment for specific IdM systems and on *identifiers* would also be useful. Because of the importance of identifiers in IdM systems, in particular in an e-government context, it is necessary that the use of 'national identifiers' and 'identifiers of general application' (e.g., the use of such identifiers for the organization of an efficient organization of the tax administration) *is provided for by legislation*, whereby sufficient guarantees are determined for the data subjects.

The use of pseudonyms and the enforcement of unlinkability, however, will not always be possible, for example for law enforcement purposes or e-government applications. A clear legislative basis should describe the exceptions thereto as well.

8. Bibliography

Article 29 Working Party, *Working Document on on-line authentication services*, WP 68, 29 January 2003

Article 29 Working Party, *Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments : the example of IPv6*, 30 May 2002, 7 p.

Article 29 Working Party, *Working Document on E-Government*, 8 May 2003, 18 p.

Bauer, M., Meints, M. and Hansen, M. (eds.), *D3.1 Structured Overview on Prototypes and Concepts of Identity Management System*, FIDIS, September 2005, available at <http://www.fidis.net>

Belgian Privacy Commission, *Recommendation nr. 01/2008 of 24 September 2008 relating to access and user control in the governmental sector*, 10 p.

Cameron, K., 'Laws of identity in brief', *Kim Cameron's Identity Weblog*, 2006, <http://www.identityblog.com/?p=353>

Cavoukian, A., *7 laws of identity – the case for privacy-embedded laws of identity in the digital age*, Information and Privacy Commissioner of Ontario, 2006.

Clarke, R., *Authentication: A Sufficiently Rich Model to Enable e-Business*, 26 December 2001.

Clarke, R. , *Identified, Anonymous and Pseudonymous Transactions : The Spectrum of Choice*, April 1999, p. 5, in S. Fischer-Hübner, G. Quirchmayr, L. and L. Yngström (eds.) *User Identification & Privacy Protection : Applications n Public Administration & Electronic Commerce*, Kista, Sweden, June 1999, IFIP

De Hert, P., 'identity management of e-ID, privacy and security in Europe. A human rights view', in *Information Security Technical report*, 2008, pp. 71 – 75.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 139, 19.1.2000, p. 12.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17 July 2000, p. 1-16.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereafter the E-Privacy Directive 2002/58/EC), OJ L 201, 31 July 2002, p. 37.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54.

Dumortier, J., Goemans C. and Loncke, M., *Anonymity and Privacy in Electronic Services (APES). D.4, General report of the legal issues*, 2003, p.30.

Dumortier, J. and Goemans, C., 'Privacy Protection and Identity Management', *Security and Privacy in Advanced Networking Technologies*, B. Jerman-Blazic e.a. (ed.), NATO Science Series, vol. 193, Amsterdam, IOS press, 2004

ENISA Ad Hoc Working Group on Privacy & Technology, *Technology-Induced challenges in Privacy & Data Protection in Europe*, M. Langheinrich and M. Roussopoulos (eds.), October 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_wg_report.pdf

Future of Identity in the Information Society project (FIDIS), EU project nr. 507512 (2004-2009), www.fidis.net

Graux, H. and Majava, J., *Analysis and Assessment of similarities and differences – Impact on eID interoperability*, November 2007, p. 4, available at <http://ec.europa.eu/idabc/en/document/6484/5644>

GUIDE, an EU project nr. IST-2003-507498, of which project was previously on <http://www.guide-project.org/>, but which site is no longer available.

Independent Centre for Privacy Protection (ICPP) & Studio Notarile Genghini (SNG), the Identity Management Systems (IMS) : Identification and Comparison Study, September 2003, available at http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMSStudy.pdf

Leenes, R., Schallabök, J., Hansen M., *PRIME white paper*, Third and final version, 15 May 2008

Legal-IST, Doc. No 11, Report on Privacy-Identity Management, 4 November 2005.

Müller, G and Wohlgemuth, S (eds.), *D3.3 Study on Mobile Identity Management*, FIDIS, May 2005, p. 24, available at www.fidis.net,

Olsen, T. and Mahler, T., 'Identity management and data protection law : Risk, responsibility and compliance in 'Circles of Trust'', in *Computer law & Security report*, 23 2007, p. 342 (part I) et seq. and p. 415 (part II) et seq.

Modinis, *Study on Identity Management in eGovernment. Common Terminological Framework for Interoperable Electronic Identity Management*, v.2.01, November 2005, p. 11, available on <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01>. 2005-11-23.pdf.

OECD, Directorate on Science, Technology and Industry, *At a Crossroads : "Personhood" and Digital Identity in the Information Society*, STI Working Paper 2007/7, 29 February 2008, and available on <http://www.oecd.org/sti/ict/reports>

OECD, Directorate on Science, Technology and Industry, *Inventory of Privacy-Enhancing Technologies (PETs)*, DSTI/ICCP/REG(2001)1/FINAL, 7 January 2002, and available on [http://www.ois.oecd.org/ois/2001doc.nsf/LinkTo/dsti-iccp-reg\(2001\)1-final](http://www.ois.oecd.org/ois/2001doc.nsf/LinkTo/dsti-iccp-reg(2001)1-final)

Oppliger, R., 'Microsoft .NET Passport and identity management', in *Information Security Technical Report*, Vol. 9 No. 1, 2004, p. 26–34.

Pfitzmann, A. and Hansen, M., *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology* (Version v0.31 Febr. 15, 2008), available at http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf

Roadmap for Advanced Research in Privacy and Identity Management (RAPID), an EU project nr. IST-2001-38310 under the Sixth Framework Programme.

(the above is a selection only)