4 High-Tech ID and Emerging Technologies

Martin Meints and Mark Gasson

Summary. Technological development has undeniably pervaded every aspect of our lives, and the ways in which we now use our identity related information has not escaped the impact of this change. We are increasingly called upon to adopt new technology, usually more through obligation than choice, to function in everyday society, and with this new era of supposed convenience has come new risks and challenges. In this chapter we examine the roots of identity management and the systems we use to support this activity, ways in which we can strive to keep our digital information secure such as Public Key encryption and digital signatures and the evolving yet somewhat controversial role of biometrics in identification and authentication.

With an eye on the ever changing landscape of identity related technologies, we further explore emerging technologies which seem likely to impact on us in the near to mid-term future. These include RFID which has more recently come to the fore of the public consciousness, Ambient Intelligence environments which offer convenience at the potential cost of privacy and human implants which surprisingly have already been developed in a medical context and look set to be the next major step in our ever burgeoning relationship with technology.

The field of high-tech Identity (high-tech ID) is immense and is rapidly expanding because of developments in fundamental technologies. The evolution of technological mechanisms such as electronic ID cards, internet enabled devices and individualised services have arguable served to make our lives easier, and more efficient, and yet they risk leaving us more vulnerable in a variety of contexts. Understanding technologies which potentially have an impact on identity becomes increasingly important for a socially well developed and prosperous information society.

In this chapter, the results of research carried out in the context of new and emerging technologies to support identity and identification are summarised. Because of its fundamental importance, one of the core research focuses was on Identity Management Systems (IMS) where the key research questions were:

- How is identity management carried out now and in the future?
- What are the primary targets of identity management from the perspectives of the stakeholders involved?
- What are relevant technological trends in identity management?
- How should these technologies be put to use in identity management systems from a legal, technical (including privacy and data protection aspects) and a social point of view?

Based on criteria developed, recommendations were elaborated that mainly address the following stakeholders: policy makers (public sector), enterprises (private sector), scientists and the general public (citizens and customers). In an early phase of the work an overview on relevant technologies in the context of IMS was created. Important technologies from the point of view of the FIDIS researchers were:

- Technologies for a centralised identity management such as directory services, Public Key Infrastructure (PKI), biometrics (Section 4.2), technologies for mobile identity management (see Chapter 5), chip or smart card technology (Meints and Hansen, 2006: 15-18) and RFID (Section 4.2.4)
- Data Mining and Knowledge Discovery in Databases (KDD, see Chapter 7)
- Technologies for a user-controlled identity management such as credential systems (see Section 4.2.5), anonymisation services, and various functions for user-controlled identity management including related commercially or freely available solutions
- Supporting technologies such as Trusted Computing (TC), Digital Rights Management (DRM), networking protocols and protocols for privacy policy languages (see Section 4.3)
- Emerging technologies (see Section 4.4).

The criteria developed were also applied to real-life implementations of identity management systems. Focal areas of research were various implementations of data mining and RFID systems, biometric systems and others. In the context of this chapter two selected use cases will be discussed: CardSpace and ID documents (see Section 4.5).

4.1 Identity Management and Identity Management Systems[1]

As shown in Chapter 2, concepts of identity show a wide range. The same applies also to the term ‘identity management’. In a general sense identity management is

[1] Author: Martin Meints, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ICPP).

understood as 'management of partial identities of a person' (Pfitzmann and Hansen, 2008) or 'management of digital identities or digital identity data' (Bauer, Meints, Hansen, 2005: 13). From a legal point of view this may apply as well to natural as legal persons. In the context of FIDIS both aspects have been researched. In this chapter the focus clearly is put on natural persons and related identities. A number of different activities carried out by different entities are summarised under the term identity management, e.g., (Bauer, Meints, Hansen, 2005; Buitelaar, Meints, van Alsenoy, 2008 etc.):

- Assignment or linking of (context specific) identifiers to a physical person
- Identification, authentication, authorisation and access control in the context of applications, IT resources and physical environment (buildings, rooms etc.)
- Management of life cycles of the identity of a physical person (e.g., enrolment and assignment of roles and rights, use or execution of assigned roles and rights, changes in roles and rights, de-enrolment etc.
- Aggregation and linking of attributes of a group of persons (group profiling) or individuals (individual profiling) from one or more sources, the use of profiles, e.g. by categorising or classifying individuals
- The application of pseudonymisation and anonymisation techniques
- The use of partial identities by an individual in various communicational contexts including role specific assignment and use of pseudonyms

In a general sense Identity Management Systems (IMS) are understood as technical systems supporting the process of management of (partial) identities. So far this term is used quite broadly in many different domains (e.g., economy, public administration, science) describing different technologies (how is the identity managed) used in different ways (who manages which identities). Examples range from centralised directory based solutions for organisations, organisations spanning federation frameworks, application of profiling practice and corresponding tools up to user centric and user controlled approaches and frameworks. Until 2004, to the knowledge of the author, no classification or typology was available helping to structure IMS.

To facilitate further analysis of existing IMS in the context of FIDIS research, three basic types of IMS were identified and described (Bauer, Meints, Hansen, 2005). In this model the aspect of control (control by an organisation or the user concerned), and methods used for the identity management (central account management, profiling techniques or user-centric methods) were covered. This resulted in the following typology:

1. Type 1: IMS for account management, implementing authentication, authorisation, and accounting
2. Type 2: IMS for profiling of user data by an organisation, e.g., detailed log files or data warehouses which support e.g., personalised services or the analysis of customer behaviour

3. Type 3: IMS for user-controlled context-dependent role and pseudonym management.

This typology maps nicely with the tiers of identity introduced by Durand (Section 2.3.2), though independent development leads to a missing map of numbers used in both models. Tier 1 identity (according to Durand, the personal or chosen identity) can be understood as a result from type 3 identity management (user-controlled identity management). Tier 2 identity (corporate or assigned identity) is a result of type 1 identity management (organisation centric identity management), and tier 3 identity (marketing or derived identity) results from type 2 identity management (profiling). Fig. 4.1. summarises major properties of these types of IMS.

In addition it was researched which role identity management functionality plays in products investigated. In this context a classification was developed:

1. Class 1: Main functionality of the product is identity management (example: directory services)
2. Class 2: Identity management is an important function; nevertheless the product also offers additional functionality (example: the Hushmail mail system for encrypted communication)
3. Class 3: The core of the product is not focused on identity management; however, identity management functionality is included (example: web browsers)

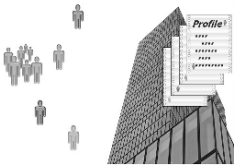
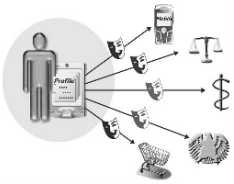
Type 1		Account Management: assigned identity	By organisations
Type 2		Profiling: derived identity	By organisations
Type 3		Management of own identities: chosen identity	By users themselves, supported by service providers

Fig. 4.1. Types of IMS

A number of such identity management systems have been analysed and observed over three years in a publicly accessible identity management database[2]. It should be noted that implementations of IMS can also be of hybrid types combining different organisational structures and methods characterising the introduced types. Examples for hybrid types are credential systems (focus: type 3 identity management) in which trusted third parties are involved (type 1 identity management).

From a market point of view in the context of type 1 identity management systems a concentration was observed. Many of the products investigated based on a study (Hansen et al., 2003) commissioned by the Institute for Prospective Technology Studies (IPTS) were taken over by competitors on the market. Currently the market for class 3 IMS seems to be growing rapidly. One example for this trend is the development on the market for social networks (see also Chapter 2); most of them do not have social networking as an economic core and gain their revenue through other activities, mainly market research and advertising.

4.2 Technologies and Technical Components

In this section established core technologies in the context of identity management are described. The focus concentrates on high technologies, especially those related to computer technologies and computer science. Technologies covered in this chapter are:

- Public Key Infrastructure (PKI)
- Electronic signatures
- Biometrics
- Radio Frequency Identification (RFID)
- Credential Systems

The description includes an introduction into functional principles of the technologies, properties, strengths and weaknesses with respect to identity management, and recommendations for the application in the context of identity management systems.

4.2.1 Public Key Infrastructure[3]

Cryptography can be used to provide secrecy of message contents or to provide integrity and accountability of messages. One of the most fundamental principles of modern cryptography was defined by Auguste Kerckhoffs (1883) and is now known as Kerckhoffs' principle: 'The security provided by a given cryptographic

[2] See http://imsdb.fidis.net/.

[3] Authors: Stefan Köpsell and Stefan Berthold, TU Dresden.

algorithm should not depend on the secrecy of the algorithm itself, but on the secrecy of cryptographic keys.'

Talking about secrecy of cryptographic keys in relation to communicating parties and their knowledge, one can distinguish between cryptographic algorithms which use symmetric keys and algorithms which use asymmetric ones. The terms 'symmetric' and 'asymmetric' refer respectively to the knowledge related to the keys: In the first case it is symmetric, i.e., both communicating parties know exactly the same key. This key is used for encryption as well as decryption. In the case of an asymmetric algorithm, each party has its own secret decryption key and a publicly known encryption key. Therefore the knowledge with respect to the keys is asymmetric between the parties.

One of the biggest obstructions from an organisational and usability point of view of modern cryptographic algorithms and protocols is the burden of key distribution. If one wants to use symmetric algorithms, this is more obvious as a trustworthy (i.e., secure) channel is needed for the transportation of the secret keys. But even in the case of asymmetric cryptography where public keys are used and therefore no concealed channel is necessary, one still faces the problem of integrity and accountability when distributing keys.

Public key infrastructures (PKIs) are a basic approach to solving these problems. Using PKIs, public keys are reliably assigned to persons by means of digital signatures and a certification authority (CA). A certification authority is an organisation or institution which accredits that a given public key belongs to a given entity. The entity is usually a human being but could also be a machine, e.g., a web-server. The assignments are also known as (digital) key certificates. These certificates are digitally signed by the certification authority. Figure 4.2 exemplifies the basic functionality of a PKI.

A typical use case for digital key certificates is to link a certain public key to an entity named within the certificate with its real identity, i.e., using the real name and not a pseudonym. But it is also possible to issue digital key certificates for pseudonyms. In this case the certification authority in fact knows the real name of the entity for which it issued a pseudonymous key certificate. This way the CA can reveal the true identity if necessary, e.g., if required by law.

Another type of certificates is the so-called attribute certificate, which binds a set of arbitrary attributes to an entity. Thus it can be seen as a generalised form of a digital key certificate as the public key can be seen simply as an attribute of the related entity.

In order to verify a digital certificate, one needs to know the public key of the certification authority. One possibility is to get this public key from another certification authority B which accredits the public key of certification authority A. Thus the relations between certification authorities form a hierarchical tree. The topmost element is called a root certification authority (Root CA). The tree could be used for implicit trust management, i.e., an application could define that it accepts all certificates which are directly signed by a certain certification authority B (e.g., the root certification authority) or subsequently signed by a certification authority A which has a certificate signed by B. Note that the very root of this tree

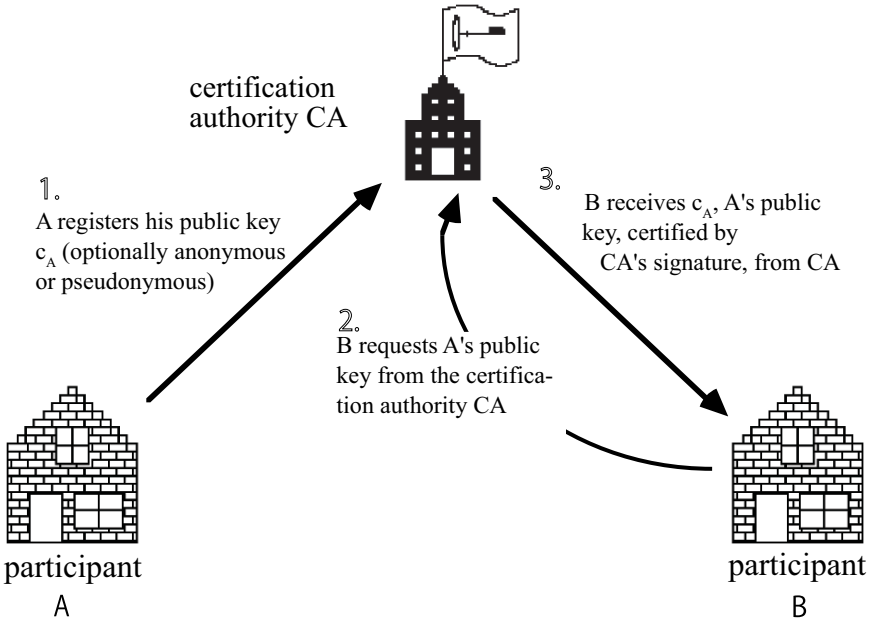


Fig. 4.2. Basic functionality of a certification authority[4]

is not authenticated by means of cryptography. Instead the integrity and validity of the root certificate has to be checked manually, e.g., by comparing the hash value of that certificate with a publicly known value which could be published in news papers or governmental communications, i.e., via a different channel.

One weakness in this hierarchical concept is the large tree of implicit trust it spans. This becomes more obvious if one considers that different certification authorities might have slightly different policies with respect to the steps required before the CA will sign a certificate. One CA might demand an official document proving the identity of the key owner before it signs the certificate while other CAs might not. To give just one example, in January 2001 the company VeriSign Inc.—one of the world's leading CAs—issued two digital certificates to a person who fraudulently claimed to be a representative of Microsoft Corporation. The issued certificates allowed the person to sign software in the name of Microsoft[5].

Another weak point of current PKIs is the way they deal with revocation. Certificates may get lost due to accidents or burglary, for instance. The common way is to provide a certificate revocation list (CRL) in order to keep every user informed about the validity of certificates. The distribution of such CRLs, however, requires users of PKIs to be online and up-to-date whenever they intend to use a certificate since they would need to check it before usage. This is quite inconven-

[4] Figure taken from Pfitzmann (2008).

[5] http://www.verisign.com/support/advisories/authenticodefraud.html.

ient since PKIs without revocation would not require the user to be online. In fact, there are several approaches to improve the distribution of certificates and trust chains. However, there is yet no improvement for the distribution of CRLs which is significantly better than broadcast.

One measure to bind the size of a revocation list is to limit the validity of a given certificate to a certain period of time (typically one or two years). This validity period is encoded in each digital certificate. But as now digital certificates can become outdated, one has to renew them from time to time. This implies additional effort for the users of digital certificates.

All these processes—the registration process, to take care of the revocation list and to renew certificates—cause costs which needs to be covered by the users of a certification authority if this authority is operated by a private company. Therefore the users typically have to pay an annual fee. Naturally this is a disadvantage of PKIs—especially if the benefits of using them will not overcompensate the costs.

From a practical point of view there are even more problems which are related to interoperability, although there exists a whole series of standards related to public key infrastructures. In 1988 the International Telecommunication Union (ITU-T) published the X.509 standard titled 'The Directory: Public-key and attribute certificate frameworks' within their X.500 information technology-related standards which focus on open systems interconnection. Most digital certificates today conform to the current version 3 of the X.509 standard. This version introduces extensibility by means of profiles. One of the (if not the) most important profile is developed by the Public-Key Infrastructure (X.509) working group of the Internet Engineering Task Force (IETF), called PKIX. The goal of this working group, which was established in 1995, is to develop standards for a public key infrastructure to be used on the Internet. The group produces more than 40 so-called 'Requests For Comments (RFCs)'—they are effectively Internet standards.

Not only is the 'correct' implementation of all these standards a hard task—as there is always room for interpretation—but also the inherent flexibility and extensibility of X.509 supports application- or domain-specific extensions which hinder global interoperability.

4.2.2 Electronic Signatures[6]

For high-tech IDs, there are roughly two relevant standard applications of electronic signatures defined in Article 2 of the EU directive 1999/93/EC, the advanced signature and the qualified electronic signature. An exhaustive discussion of these signature types with respect to requirements, legal effects, and their probative value can be found in (Gasson, Meints, Warwick, 2005: 26). In this section, we focus on the main differences between advanced and qualified electronic signatures and their relation to PKIs.

An advanced electronic signature is, according to the EU directive 1999/93/EC[7], an electronic signature with four requirements:

---

[6] Authors: Stefan Köpsell and Stefan Berthold, TU Dresden.

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control; and
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Even though the legal effectiveness of advanced electronic signatures is limited for business, it still creates a unique link between the signed data and the signatory.

Of more interest for business cases are qualified electronic signatures. The validity of qualified electronic signatures is based on a qualified certificate, which is basically a digital certificate issued by a certification authority. A certification authority can be conceived as the root of a PKI or as a subsequent authority within a PKI certification tree. In the latter case, the PKI certification tree is used to delegate the permission to issue certificates from the root CA to a subsequent certification authority, see 'Public Key Infrastructure' in Section 4.2.1. Such permission can be limited in order to achieve a separation of duties between several subsequent certification authorities. In addition to the necessary qualified certificate, qualified electronic signatures are required to be created by a 'secure-signature-creation device'. This type of signature has legal effects comparable to a hand-written signature, as defined in Article 5 of 1999/93/EC.

Technically, electronic signatures can be seen as the counterpart of asymmetric encryption schemes. That is, there is a secret key for signing a message and a public key for verifying. In contrast to message authentication codes, electronic signatures can be used to convince third parties of the authenticity of a message, since the signing key is secret and must not to be shared by the sender with anyone else. The basic principles of generating and verifying an electronic signature are depicted in Figure 4.3.

An electronic signature is generated by first applying a hash function to the message and afterwards using the core signature algorithm to sign just the resulting hash value. Note that for electronic signatures to be secure, both parts—the hash function and the core signature algorithm—need to be uncompromised and work properly.

From a technical point of view the requirements of advanced and qualified electronic signatures induce some (controversially discussed) challenges and problems. Of special importance are two requirements on a secure-signature-creation device, 'the signature-creation-data used for signature generation can be protected in a reliable way by the legitimate signatory against the use of others' and 'secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.' Both requirements are hard to assure with current technology. Today's standard PCs with

[7] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:EN:PDF.

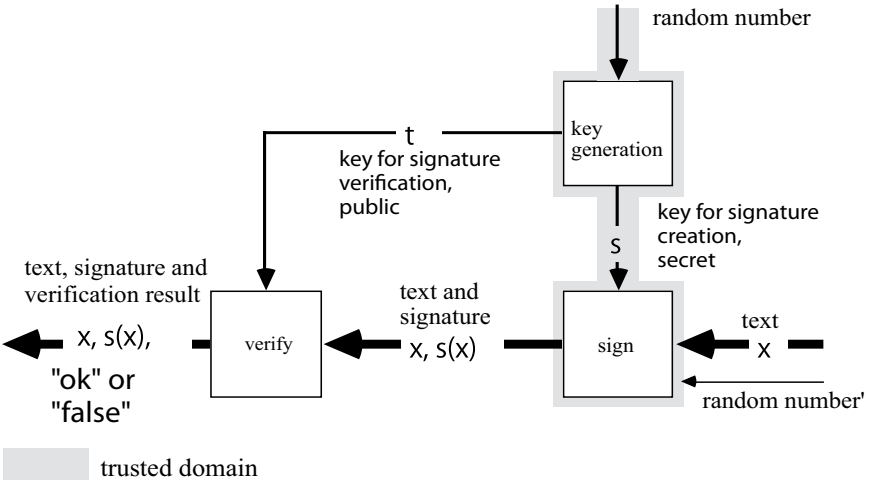


Fig. 4.3. Digital signature system[8]

standard operating system cannot be used as secure signature-creation devices. Given all the security weaknesses of PCs they can neither ensure that 'the signature-creation-data used for signature generation can be reliably protected' nor 'what I sign is what I see'. Therefore specialised hardware and software is needed, e.g. external card readers. Such devices need at least a means for input to authorise the signing process and a display (or other means of output) to inform the user about what he will sign. So from an organisational and usability point of view electronic signatures are slightly impractical and costly.

In addition to the problem of achieving the previous two requirements, an advanced electronic signature is required to be 'created using means that the signatory can maintain under his sole control'. Then, the problem is that the secret keys used for signing are typically created by certification authorities, not by the users themselves. Thus, a user can never be sure of having the process of signing 'under his sole control'.

4.2.3 Biometrics[9]

Biometrics is defined as the automated recognition of individuals based on their biological and/or behavioural characteristics. Typical examples for suitable biological characteristics used in biometric systems are fingerprints, iris filament structures or face forms. Recognition of hand written signatures or gesture dynamics are examples for behavioural characteristics. Any biometric system in-

[8] Figure taken from Pfitzmann (2008).

[9] Authors: Els Kindt, KU Leuven, Lorenz Müller, Axionics and Martin Meints, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

cludes a measurement process that allows defining a query template with formalised features of the measured characteristics. These results are then compared with a reference template that has been acquired when the individual enrols into the biometrically secured system.

All suitable characteristics for biometrics have some mandatory qualities like universality (all persons have the characteristics), distinctiveness (every person has a different specificity of the characteristics), permanence (the characteristic is sufficiently invariant over a long time period) and collect ability (the characteristics can be physically measured on all individuals). There are some additional desired qualities like separability (the difference between individuals is much larger than typical measurement errors), performance (the measurement of the biometric characteristic is robust, fast, accurate and efficient), acceptance (individuals accept the measurement process) and reliability (the characteristics and the usual measurement are difficult to counterfeit).

Biometrics as Authentication Factor

Biometric recognition of individuals is a suitable method to establish a strong link between a person and an identity. It has the advantage that it is difficult for the concerned individual but also for potential impostors to manipulate this binding. This broad protection even against insider attacks differentiates biometrics from other authentication factors like token or knowledge based methods such as PINs or passwords. On the other hand, a biometric link between an individual and some identity-related data is difficult to revoke even if there are good and legal reasons to do so. Most of the biometric characteristics are stable for a long time in the lifespan of an individual, much longer than typical business relationships. Therefore a widespread use of biometrics for identity management in civil or business applications may expose a person to extensive profiling and thus seriously harm her right to privacy.

Biometric Recognition Process

All biometric systems have some common main functional components in a typical processing chain. These components are (see Figure 4.4):

- a storage entity with the biometric data samples (reference templates) of the enrolled individual that is linked to or integrated in a database with the identity information of the corresponding individual
- a sensor device and some pre-processing to capture the biometric data sample from an individual as input data
- a comparison process that evaluates the similarity between the reference templates and the captured data sample and that results in a similarity score
- a decision function that decides if a data sample matches a certain reference template.

The result is the approval or refusal of a mapping of the captured template to the identity information that belongs to the selected reference template.

Biometric Recognition Quality

Another important point is the fact that any biometric technique includes a physical measurement, which is intrinsically error-prone. Therefore the comparison between the query sample data and the reference template will normally not lead to an exact match but to a similarity score. Using this score value the system then has to decide if the query and the reference template are both coming from the same individual or not. This decision is based on probability estimates. Therefore a biometric recognition process can lead to false results in the sense that the authorised individual is rejected (False Rejection Rate—FRR) or that an impostor is accepted (False Acceptance Rate—FAR). The relative and absolute rates of such intrinsic errors in function of the threshold setting on the similarity score are the quality characteristics of a biometric system. These error rates depend on the

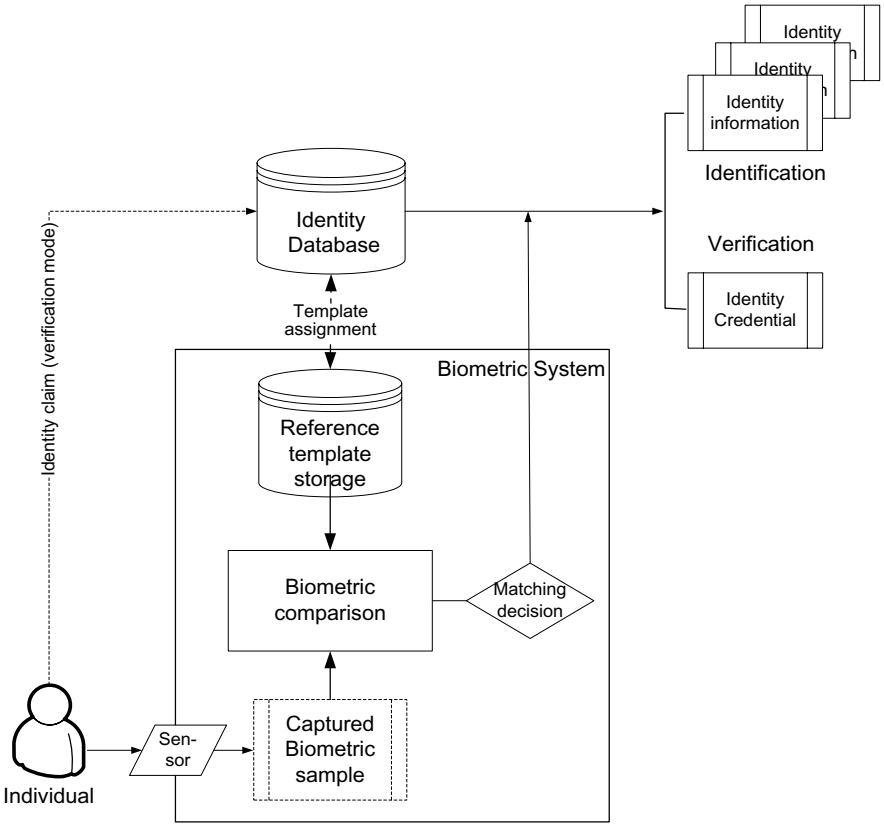


Fig. 4.4. The main processing components of a biometric system

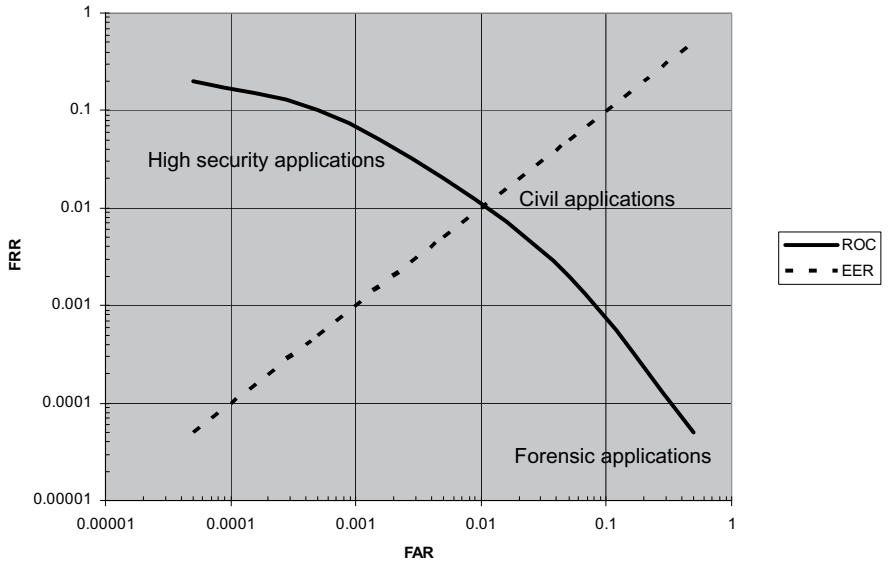


Fig. 4.5. Receiver operating characteristics curve of a typical biometric system that shows the correlation between the False Acceptance Rate (FAR) and the False Rejection Rate (FRR)

chosen characteristic, on the technical realisation of the biometric system and on the decision threshold setting. The two error rates are strongly negatively correlated and the overall quality of a biometric system is represented by the correlation plot called ROC (Receiver Operation Characteristics) curve that emerges when the threshold setting is changed over the full range of possible similarity scores (see Figure 4.5). A simplified form of this quality representation is the Equal Error Rate (EER). This single value represents the error rate of the FRR and the FAR when both values are equal.

Operation Phases and Modes

All biometric systems run in two separate processing phases. For each individual that shall be recognised by a biometric system first an initialisation procedure, called enrolment, takes place. In this processing phase the individual subject provides samples of a biometric characteristic to establish a new so called reference template. After the enrolment, the subject is known by the biometric system. In the subsequent query phase, the subject provides when requested a new biometric data sample called a query template. This query template is processed and compared with the saved reference templates of all enrolled subjects (identification mode) or with the saved template of a specified subject that claims a certain identity (verification mode). The output of the system may be a simple yes / no, or an identity credential with identity information about the subject for a system that operates in the verification mode, or a list of identity data that correspond to the best matches (comparison scores) for a system running in identification mode.

Legal Aspects

The privacy aspects of biometric systems and technologies have been widely discussed and, at least on the European level, have over all been well agreed.[10] FIDIS research has pointed out various privacy risks of the implementation of the technology as well.[11] These risks include the massive data collection in and outside Europe, hereby creating a global surveillance infrastructure, the risk of 'repurposing' of the collected data as past experience has already learned, the increasing chances for identity theft, unobserved authentication, direct identify ability and linkability, and unrestrained monitoring and profiling[12] of individuals. Increasing the security in identification or authentication systems with the use of biometrics however does not necessarily mean that the privacy and data protection rights of the individuals concerned should decrease. The processing of biometric characteristics of individuals is in principle subject to Article 8 of the Convention for the Protection on Human Rights and Fundamental Freedoms (the right to respect for one's private life) and Directive 95/46/EC which provides the general legal framework for the processing of personal data. The Directive, however, does not mention biometric data as such. The Article 29 Data Protection Working Party has therefore issued specific guidelines for the processing of biometric data in a working document of August 2003 (Art29DPWP, 2003), also see (Gasson, Meints, Warwick, 2005: 98-101) and (Kindt and Müller, 2007: 77-82). These guidelines include that (i) 'raw' biometric data shall not be stored because such data may reveal information about a person's health or race, (ii) templates should preclude the processing of data that is not necessary, (iii) central storage of biometric data is to be avoided, (iv) the use of unique identifiers should be avoided by the manipulation of the templates, (v) other personal information should be segregated from the biometric information, and (vi) the controller shall take all appropriate technical and organisational security measures to protect the biometric data.[13] National Data Protection Authorities, including those of Belgium, France, Greece and the Netherlands, have also issued opinions on the use of biometric systems, in general or in specific situations.

However, not all privacy concerns have been resolved. There is for example the uncertainty whether or not privacy-critical information for example concerning health can be extracted from templates, as this has not been thoroughly investigated (Kindt and Müller, 2007: 83-87). There is also the risk of biometric data becoming a primary key for the interoperability of systems. The inappropriate

[10] The specific privacy concerns for biometrics have been outlined in various documents and opinions, including Council of Europe, *Progress report on the application of the principles of convention 108 to the collection and processing of biometric data*, Strasbourg, February 2005, 26 p.

[11] In this first reference the use of biometrics for the enhancement of PKI also was extensively researched.

[12] See also Hildebrandt and Gutwirth (2008).

[13] On each of these principles, further explanation can be found in Gasson, Meints, Warwick (2005: 101-105).

security architecture for the storage of biometric data in the Machine Readable Travel Document (MRTD) has also been argued and demonstrated in a dedicated FIDIS deliverable (Meints and Hansen, 2006: 160) and was subject of the Budapest Declaration of the FIDIS research community.[14]

Control Models for the Operation of a Biometric System

Biometric systems can be understood as information and communication technology (ICT) systems (or parts thereof). From a security point of view control in ICT systems is an important prerequisite for effective security. In this context a classification has already been developed (Rannenberg, Pfitzmann, Müller, 1999):

- Centralised control in one organisation
- Distributed control in a group of trusted organisations following homogeneous and mutually accepted security targets (mainly developed in one joint and shared security concept)
- Distributed control with differing security targets, also called multilateral security. This model is especially of interest as research approaches for its implementation and no real-life implementations exist yet.

Based on these categories, taking relevant stakeholders in the operation and use of today's biometric systems (public and private sector, citizens and consumer) and relevant purposes together with the analysis of legal ground for the operation into consideration a typology of biometric systems was developed (Kindt and Müller, 2007: 55-67):

1. Type 1: Government controlled ID model;
   based on legal grounds, a group of organisations is running the biometric system either based on commonly agreed security targets or multilaterally; examples are the epass or biometrics enabled national ID cards
2. Type 2: Access control model;
   based on the consent of the user, the system is run by private or public sector organisations centralised or distributed; examples are pay per touch and access control systems for public and private buildings, one particular setting in this category is the shared control between the organisation and the biometric subject (see below 'encapsulated biometrics')
3. Type 3: Mixed model;
   mainly based on consent, biometric data is shared between private and public organisations (distributed control), but mainly common security targets exist; example: PRIVIUM (biometrics enabled border control)

[14] FIDIS, Budapest Declaration on Machine Readable Travel Documents (MRTD), September 2006, available at http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.en.20061106.pdf.

4. Type 4: Convenience model;
   based on consent, biometric data is either controlled by the user directly or shared with a service provider. Control can be centralised (at the user or the service provider) or distributed (from the service provider to the users); examples are biometric access control for private notebooks or the administration of school meals or books in libraries
5. Type 5: Surveillance model;
   based on legal grounds (public sector) or consent (private sector), biometric data is used centralised or distributed for surveillance purposes, mostly in the context of public security or fraud and theft prevention (private sector); examples are CCTV-based biometric systems at public places or private property.

Specific Risks for and Through Biometric Systems

These concerns point towards the need for an appropriate legal framework, in additional to privacy-enhancing biometric solutions.

In the context of biometric systems a number of risks have been discussed for operators and users. They are mainly (e.g., Meints and Hansen, 2006:105-115):

- Identity takeover or usurpations (generally called 'identity theft'; see also Chapter 8).
- Violation of purpose binding by use of additional information in biometric data or use of the biometric data for purposes other than the original purposes for which the data were collected (also called function creep).
- Violation of purpose binding is especially eased through the fact that biometric data can not be anonymised; the linkability of biometric characteristics to a person is a central functional principle of biometrics. Linkability of biometric data to other sources of data increases the risk of profiling to the disadvantage of the user of biometric systems.
- Violation of informational self determination by forcing users into the use of biometric systems where no legal ground for their use is in place.
- As biometric systems can be run hidden they may be used, and without proper legal grounds abused, for non-recognised and non-interactive authentication, tracking and surveillance purposes. On the other hand this feature of biometric systems includes them into the enablers of Ambient Intelligence (AmI).
- Improperly used biometric systems may lead to devaluation of established forensic methods.

Technical and Organisational Security Measures

Technical and organisational security measures need to meet criteria defined as 'state-of-the-art'. This can be achieved based on relevant standards for information security management systems such as the ISO/IEC 27000 series and CobiT[15]. On a product level, Common Criteria (CC, ISO/IEC 15408) can be used to counter general risks for identity management systems. The Biometric Evaluation Methodology for Common Criteria[16] covers especially threats in the context of deliberate attacks on biometric systems. In this context the following aspects seem to be especially relevant:

- Protective measures against theft of reference data in biometric systems. It has already been demonstrated that reference data in template formats can be used to reconstruct reference data to spoof sensors applying a so-called hill climbing attack (e.g., Hill, 2001; Adler, 2003). In a hill-climbing attack reference data is recalculated from templates in iterative cycles using, e.g., the match score of the system to evaluate the quality of the calculated data after each calculation cycle. To hamper hill-climbing attacks the biometric system should not return any match scores.
- Protective measures against infiltration of biometric systems with unauthorised reference data need to be taken.
- Detection measures for the use of copies of biometric characteristics (anti-spoofing measures for sensors are especially important as the successful use of copies of characteristics has been demonstrated with many sensor types[17]); additional data collected in this context must not be used for purposes other than security.
- Physical (environmental) protection of as many parts of biometric systems as possible and effective access control measures on all levels of the system (physical access control, effective login and data access procedures); this also should include the deactivation of interfaces of the system not needed to prevent sensor override attacks[18].
- Assurance of the authenticity of biometric reference data via appropriate organisational and / or technical measures in the enrolment phase.
- Logging of transactions and appropriate auditing of logs in biometric systems, especially of configuration parameters such as changes of thresholds.

---

[15] The Control Objective for Information and Related Technology (CobiT) are available at http://www.isaca.org.

[16] See http://www.cesg.gov.uk/site/ast/biometrics/media/BEM_10.pdf.

[17] See, e.g., Geradts and Sommer (2006).

[18] Sensor override attacks are described by, e.g., Heinz, Krißler, Rütten (2007).

- Inclusion of relevant stakeholders when biometric systems are introduced or modified (release management). Relevant stakeholders may be for example representatives of the works counsels, the information security officer and the data protection officer.
- When buying or outsourcing parts or the whole biometric system, corresponding service level agreements and security service levels need to be included in the contracts. An important part of these service levels is a control or auditing and enforcement strategy (e.g., via fines or disciplinary actions).

Technical and Organisational Data Protection Measures

From a data protection point of view the control model used for sensor and reference data is of interest. In some cases Data Protection Commissions in European member countries decided that for convenience driven applications the use of central reference data repositories under control of the service provider was not proportionate (e.g., Kindt, 2007). Alternatively reference data can be stored under the control of the data subject (e.g., using a token) or it can be encrypted with a key under control of the data subject. From a data protection point of view the control model implemented in encapsulated biometrics is currently the best. Encapsulated biometric systems integrate sensors, matching systems and reference data storage in one device under control of the user of the biometric system. This device reports only a match or non-match (Kindt and Müller, 2007). Characteristics or reference data in this case are not transferred to systems outside this device. This concept will be further described and evaluated in the next section. In any case it should be evaluated with care whether identification and thus a centralised reference data repository is really needed.

Another important aspect is hindrance of linkability of biometric reference data. This can be achieved, e.g., by storing biometric reference data separately from other personal data, keeping it fragmented and encrypting these fragments with different keys. The application of template protection measures (see, e.g., Jain, Nandakumar, Nagar, 2008) or the use of biometric encryption (Cavoukian and Stoianov, 2007) also can hinder linkability as well as decentralised storage of reference data under control of the user.

Biometric characteristics are, in difference to other factors of authentication, non-revocable. To hinder identity theft based on reference data schemes for revocable reference data (see, e.g., Cavoukian and Stoianov, 2007; Zhou et al., 2007) should be used.

Biometric raw data (mainly images of faces, finger tips, voice recordings etc.), data used for liveness detection and supposedly in some cases also templates contain information in addition to the characteristics needed for the biometric matching. In some cases this data is health or racial origin related and thus belongs to the special categories of personal data as defined in the European Data Protection Directive 95/46/EC (Kindt and Müller, 2007: 83-87). For this reason reference data should be especially protected against unauthorised access and use. In some

European countries (e.g., Luxemburg, Belgium etc.) prior checking of planned biometric systems by Data Protection Officers or Commissioners is recommended or required. To reduce additional information in biometric reference data, templates should be used instead of raw biometric data.

In many cases the implementation of biometric systems in Europe requires consent by the users (data subjects). In this context transparency among others about the data used and the procedures used in processing need to be described understandably to the user. In this context the three layer approach for privacy policies suggested by the Art. 29 Data Protection Working Party (Art29DPWP, 2004) may be useful. Important instruments to support trust in biometric systems' security and privacy are information system management (ISO/IEC 27001) and Common Criteria (ISO/IEC 15408 including Biometrics Evaluation Methodology) certificates as well as privacy seals[19]. When biometric systems are introduced based on consent as a general rule a non-biometric back up procedure is required as users may opt out at any time.

Encapsulated Biometrics—a Privacy-Enhanced Operation Mode

A biometric comparison is far more complex than a password or PIN code check. It always includes a physical measurement process to capture a query template. Biometric authentication systems therefore all need some locally installed infrastructure to which the subject needs physical access. This fact constrains the possible architectures of biometric systems. It is not possible to concentrate all processes in a physical completely secured environment; there are always points with immediate interaction with the outside world.

Today's biometric systems often work within architectures with entirely or partially centrally controlled components. The server or the server controlled peripherals collect biometric data from the individuals through the local capture devices. The further processing is done under the sole control of a centralised biometric application infrastructure which keeps the biometric information of all enrolees in an operator controlled database. Even if the centralised equipment is well protected, at least the capture devices are weak points in the system exposed to all kind of attacks and manipulations. In addition, the specific biometric characteristic may be expressed in very different forms from human to human. General purpose measurement equipment may fail to make an optimal raw data capture over the full population. As a consequence the requested features may not be reconstructed by the feature evaluation algorithm for a substantial fraction of the population or the resulting query templates may be too far away for a unique and reliable result in the comparison step. In addition centralised control systems bear all the dangers to the security and the privacy of the enrolled individuals that have been discussed in the above paragraphs.

[19] E.g., the Data Protection Seal of the federal state of Schleswig-Holstein in Germany, see https://www.datenschutzzentrum.de/guetesiegel/, or the European Privacy Seal EuroPriSe, http://www.european-privacy-seal.eu/.

All the above problems are directly or indirectly related to the system architecture with centralised components and data. Especially for type 2 models (access control) new approaches with a decentralisation of the biometric data have been developed to ease the above outlined drawbacks of biometric authentication. Systems with templates or even templates and the matching process on personal smart cards are examples of such improved architectures with reduced exposure of biometric data. An even more radical improvement can be achieved with the architecture model of encapsulated biometrics. In this scheme the whole biometric system is enclosed in a personal device that performs the full biometric recognition process customised for the user. The system has to recognise only one person and thus it stores only one set of reference templates. The encapsulated biometric system is securely enclosed in a tamper resistant device that performs the biometric recognition process in a predefined and secure way. The result of the biometric recognition of the user is communicated to the requesting organisation through cryptographic credentials which cannot be manipulated by the legitimate user nor a third party. The authenticating organisation does not hold any biometric data and thus it cannot jeopardise the biometric privacy of the authenticated subjects.

The encapsulated biometric model represents a shared control model where the authenticating organisation defines and controls the biometric evaluation process and its results and the biometric subject controls the biometric data and the usage of the biometric device (see Figure 4.6). This model fulfils the security needs of the authenticating organisation and the privacy need of the authenticated biometric subject in the best possible way. A necessary precondition for a biometric system to work in an encapsulated model is the ability to enclose the whole process in a secured personal device that works reliable even in a hostile environment. Fingerprint, iris, handwriting or voice biometric characteristics are suitable for such architecture. First realisations of such a user-centric model have appeared now on the market of authentication devices[20].

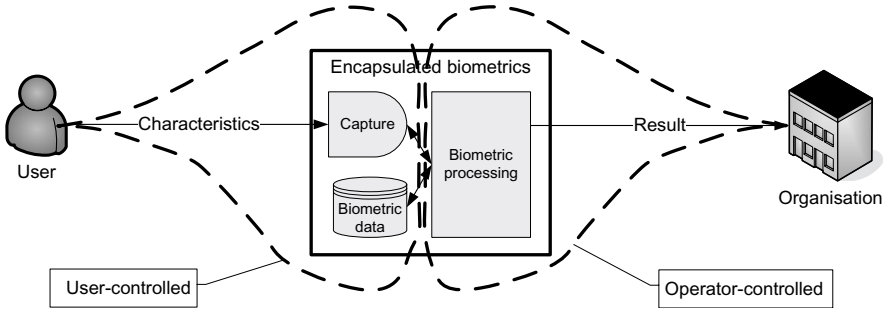


Fig. 4.6. Encapsulated biometrics enclosed in a device that allows a sharing of control: The data and the usage is controlled by the using subject; the processing and the evaluation result is controlled by the authenticating organisation

[20] Bodily functions, Finance & Economics, The Economist, 2008-07-10.

4.2.4 RFID[21]

Radio Frequency Identification (RFID) technology is increasingly used for various applications, including retail applications, transportation, aviation, healthcare, automatic toll collection, security and access control. RFID tags are tiny electronic radio tags that can be embedded in or affixed to objects for the purpose of identifying the object via a radio link. RFID readers can read the unique ID code and any other information stored in RFID tags remotely by sending and receiving a radio frequency signal. In an RFID system, RFID readers are connected to a backend system which processes the data read from tags and can link them to other data stored in backend databases (see Figure 4.7)

RFID tags in general come in many different types and have different characteristics regarding e.g., power source, operating frequency and functionality. Thus they can be classified in a number of different ways. A common way to classify RFID tags in a general way is to divide them into active or passive tags. Active RFID tags have a permanent power supply. Hence these tags can perform 'computations' continuously and independently from the environment.

Active tags also have in general much more computation power compared to passive ones. Hence they can do much better cryptographic operations. Both properties make active tags much more appropriate for applying security and privacy protecting mechanisms. But active tags are orders of magnitude larger than passive ones.

Passive tags can from a privacy and security standpoint be further divided into: **basic, very low-cost tags; symmetric-key, low-cost tags; and public-key, more expensive tags.**

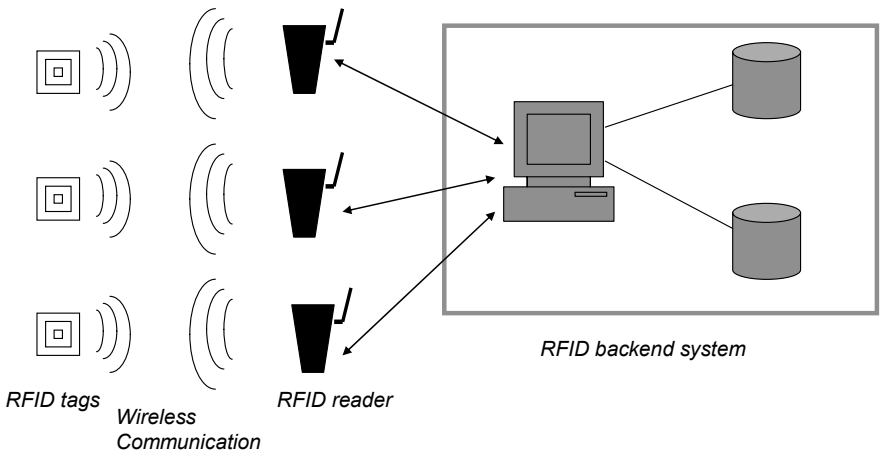


Fig. 4.7. An RFID system

[21] Authors: Simone Fischer-Hübner, Hans Hedbom, Karlstad University.

According to NIST[22], 'the most prominent industry standard for RFID are the EPCglobal specifications and standards for supply chain and patient safety applications'. EPCglobal divides the tags into different classes. The different classes have different security and cryptographic capabilities. Tags belonging to the EPCglobal Class-0 or Class-1 of the first generation have no security functionality.

The operating distance, data transfer speed and tag reading speed of an RFID-system is dependent on the radio frequency of the tag. In general one could say that the higher the frequency the higher the data transfer speed and the tag reading speed. High frequency tags are also usually designed to operate over longer distances.

The use of RFID systems can enhance the efficiency and functionality of such applications, create new services and can provide further benefits and added value for the owner of RFID tagged items (e.g., smart fridges operating in combination with RFID tagged items, or the possibility to include warranty information on tags).

Privacy Issues

Besides such benefits and opportunities, RFID technology however also poses severe privacy problems. Privacy as an expression of the right of self-determination and human dignity is considered a core value in democratic societies and is recognised either explicitly or implicitly as a fundamental human right by most constitutions of democratic societies. In the era of modern information technology, an early definition of informational privacy was given by Alan Westin: 'Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others'. The German Constitutional Court had also defined privacy in its Census decision as the right to informational self-determination, i.e., individuals must be able to determine for themselves when, how, to what extent and for what purposes information about them is communicated to others.

The question whether information on RFID tags qualify as personal data is not always straightforward to answer. Moreover this question also usually depends on the tag's lifecycle, as in some parts (usually in the beginning) of the lifecycle the information on the tag may not classify as personal data whereas in other parts it may. RFID tags can either directly contain personal data, e.g., biometrics that are stored on RFID tags in European passports, or can include data that could be linked to an identified or identifiable person and thereby classify as personal data. Examples for the latter case are for instance situations where individuals carry or wear tagged items, which can be associated with them, where data on the tag can be linked to identifiable data stored in the backend databases or where individuals have RFID tags implanted (see also the next section). The problem whether profiling on the basis of a unique product code on a tag (e.g., on the watch of a customer

[22] (U.S.) National Institute of Standards and Technology, Guidelines for Securing Radio Frequency Identification (RFID) Systems Special Publication 800-98, April 2007.

visiting a supermarket) is enough to justify personal data processing, even if the identity of the person (name, address, etc.) cannot be determined with reasonable efforts, has been controversially discussed. Whereas according to the traditional view, the data on the tag are not personal data, the opposite opinion was recently voiced by the Article 29 Working Party (Art29DPWP, 2005) as well as in (Hildebrandt and Meints, 2006) who have interpreted the term 'identifiable' more broadly encompassing also re-recognition of a person.

RFID-related privacy threats can basically be divided into privacy threats within the reader-tag system and privacy threats at the backend. Privacy threats within the reader-tag system comprise unauthorised reading and manipulation of information, cloning of tags and real-time tracking of individuals. RFID readers can potentially secretly scan and track RFID tags that individuals passing by are wearing or carrying, without the concerned individual's knowledge or consent. Consequently, privacy principles implemented by the European Legal privacy Framework, such as transparency, informed consent, or more generally the right of informational self-determination, are at stake. Privacy threats at the backend include profiling and monitoring specific behaviour. Besides, there are security-related threats for the confidentiality, integrity (including malware threats), availability and authenticity of personal data stored on the tag or in the backend system.

The Article 29 Working Party and privacy and consumer organisations, such as CASPIAN and EPIC have voiced privacy concerns and discussed high-level privacy guidelines / requirements for RFIDs. Several trials and plans for using RFID in supply chain applications were confronted with protests by consumers, who felt that their privacy was at risk.

Towards a Holistic Framework

RFID-related privacy problems can however not be addressed solely by legal and / or technical measures but require a holistic approach. For instance, RFID applications, such as RFID implants, even though they are legally compliant, might raise ethical questions that need to be addressed as well. Besides, social aspects of user acceptance and trust also need to be taken into account. The FIDIS Deliverable D12.3 presents a first attempt of 'A Holistic Privacy Framework for RFID Applications'. After discussing the problem space from the technological, legal, ethical and social science perspectives and illustrating those problems with the help of scenarios, a holistic approach to privacy-enhancements is presented, which follows a development approach starting with social, ethical and legal requirements and measures, and then continuing with classifying technical and organisational measures and guidelines to some of those requirements. Important requirements and measures for an holistic approach to privacy-enhancements, which are discussed in more detail in D12.3, can be summarised as follows:

- User control as a prerequisite to technology acceptances needs to become a general guideline for manufacturers and vendors (see also Bizer and Spiekermann, 2006).

- The basic principles of the current European regulatory framework on privacy and data protection apply and need to be interpreted for RFID applications. Important legal principles include the principle that data are processed fairly and lawfully and only under the grounds of Art. 7 EU Directive 95/46/EC (e.g., if the data subject has given his / her informed consent), the principles of data minimisation, transparency and right of the data subjects in RFID applications. The principle of transparency, which is especially at stake in AmI environments, requires that each RFID reader and RFID tag must be clearly labeled if analogical laws existent in other privacy-related areas (like in the case of surveillance cameras) are adopted.
- Available technical privacy-enhancing measures, which can also be applied in combination, can be classified as follows:
  - Measures for preventing unauthorised read-outs, e.g., with the help of the kill- or sleep-commands.
  - Measures for blocking access to the tags, e.g., with the help of blocker tags, proxy-devices (watchdogs).
  - Authentication measures, e.g., based on symmetric or asymmetric cryptographic protocols.
  - Cryptographic measures for enhancing privacy, including 'minimalistic cryptography' for rotating pseudonyms that are replacing the tag's code, or universal re-encryption of the tag's identifier.
  - Measures for preventing tracking at application layer (i.e., via its unique global identifier), communication, and / or at network layer.
  - Privacy-enhancements by pseudonym usage.
  - Privacy measures for enforcing user self-control or voluntary commitments by organisations for processing data properly. Such measures include 'soft-blocking' based on a user-defined privacy policy or measures based on the trusted computing concept for controlling the adherence to a commitment.

Overall Conclusions

Summarising, the overall conclusions are the following (Fischer-Hübner and Hedbom, 2008):

- The use of RFID technology in several contexts and its role as a prime Ambient Intelligence enabler raises important data protection and privacy threats.
- The current legal privacy framework partly gives too much room for interpretation and does not always give clear answers with regards to RFID technology. For example, the essential question how to determine the data

controller in an RFID application who is responsible for the lawful data processing, is not always straightforwardly answered. Also, specific provisions of the e-Privacy Directive 2002/58/EC are not always applicable, as they presuppose processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks. RFID technology however neither needs a publicly available electronic communications network nor does it involve respective providers. Such issues are currently being addressed by the EU.

- We believe that in order to get a privacy-friendly RFID system both the RF-subsystem and the backend system needs to provide privacy protection. Since the backend system presumably is under the control of the data controller while some parts of the RF-subsystem is not (notably the RFID tag), it is of utmost importance that the RF-subsystem provides for its own privacy protection.
- Many proposals for Privacy-Enhancing Technologies (PETs) for RFID exist—but only a few of them really seem to be feasible and all of them have some shortcomings, i.e., none provides the 'ultimate' solution addressing all RFID-related privacy problems. One of the main problems is that low-cost RFID tags by themselves currently cannot offer any solution for strong privacy. Nevertheless, in the short term the mechanisms suitable for a given area of application should be implemented in order to increase the level of privacy the RFID system offers.
- The state-of-the-art at the moment is to have a privacy patchwork for RFID rather than a holistic and integrative approach. A lot more effort in terms of research and development seems to be necessary to finally get a true holistic privacy framework for RFID applications. Among other things, low cost RFID tags with better and stronger cryptographic mechanisms need to be developed, transparency and awareness needs to be raised and the incentives for manufacturers and users of RFID technology to develop more privacy-friendly and secure solutions need to be increased.
- The combination of RFID and profiling, eventually coupled with many other privacy-sensitive means and techniques such as biometrics, may be a major privacy concern, as RFIDs, profiling and biometrics themselves already bear many risks, which are multiplied in combination.
- And finally, more research into life cycle analysis methods for RFID systems is needed to gain a clearer view of the data flows throughout the application's lifecycle and for subsequently developing a more fine-grained set of recommendations.

4.2.5 Credential Systems[23]

Access control typically is carried out based on a claim of the user (e.g., I'm authorised to use this application), the verification of this claim (these steps are also called authentication) and the assignment of a set of rights to the user (this step also is called authorisation). In distributed identity management environments the claim of the user also may include the rights he requests in the context of the application. In this case we also speak of claim-based access control.

Claim-based access control relies on credentials to tackle cross-domain authorisation. A credential is used by a party (holder) to prove its attributes. A credential is issued by a trusted third party (issuer) that asserts some attributes or claims regarding the holder. The integrity and origin of the claims are guaranteed by a signature of this issuer. Credentials are strongly associated with a secret of the holder, e.g., private key, to make sure that they cannot be used by another party. Knowledge of this secret is proven when using the credential, e.g., when signing a message. As a result, a third party can check the attributes of the message author (see also Bauer, Meints, Hansen, 2005).

This section focuses on two advanced types of credentials. First, 'minimal disclosure tokens' rely on cryptographic primitives that make it possible to reveal a subset of the claims and to ensure unlinkability, i.e., the issuer cannot trace the holder. Second, the logic-based 'Security Policy Assertion Language' enables taking access control decisions based on large sets of claims extracted from policies and credentials.

Minimal Disclosure Tokens

In today's online world, individuals are registered in hundreds if not thousands of organisational databases. Organisations are under increasing pressure to share this identity-related information with others to improve service, cut costs, and combat fraud. Both organisations and individuals stand to benefit.

In response to the demand for cross-organisational data sharing solutions, the computer industry has been working since the late nineties on an emerging identity infrastructure that will enable online data sharing across disparate computer systems. The emergence of an Internet-scale online identity infrastructure is not without challenges, however.

Firstly, care must be taken that individuals do not lose all control over the extent to which others can monitor their actions and learn (let alone misuse) private information about them. Making individuals a choke point for the flow of information about them is far from sufficient: this 'user-centric' approach may do nothing but greatly expand the ability of organisations to share personal information. This is particularly troublesome if each data sharing results in a common identifier for previously unlinked accounts: once all of an individual's accounts are 'feder-

[23] Authors: Stefan Brands, Microsoft; Laurent Bussard, EMIC; Joris Claessens, EMIC; Christian Geuer-Pollmann, EMIC; Ulrich Pinsdorf, EMIC.

ated', nothing stops organisations from directly exchanging information about the individual between themselves. The resulting online infrastructure would have unprecedented privacy consequences and be a huge boon to identity thieves.

Second, there are major security challenges for organisations. For example, when an online service provider relies on an identity 'claim' that has been issued by another organisation, how can it be sure that the information is authentic and pertains to the individual that is requesting a service? How can the issuing organisation be prevented from learning competitive information about the service provider's clients, let alone from surreptitiously accessing their accounts? How to prevent denial-of-service attacks and ensure availability of third-party identity claims? Compounding the challenge is that the threats in a distributed data sharing environment do not come only from outsiders: attacks may originate from the organisations that issue identity claims, as well as from hackers of these organisations.

Following the invention of public-key cryptography in the mid seventies, cryptographers have worked for several decades on a holistic solution to these challenges. This research has resulted in sophisticated techniques for so-called 'minimal disclosure tokens' (sometimes also referred to as anonymous credentials, a term that does not do justice to the power of the technology). Minimal disclosure tokens are basic cryptographic constructs for protecting digital information. They are issued by 'issuers' to 'users' by means of an issuing protocol, presented by their users to 'verifiers' by means of a presentation protocol, and optionally forwarded by verifiers to third parties (such as auditors). Since minimal disclosure tokens are just sequences of zeros and ones, they can be transferred electronically and can be verified by computers.

Minimal disclosure tokens are ideal for sharing identity-related information across organisations:

- **User-centric:** Using minimal disclosure tokens, organisations can securely share information via the individuals to whom it pertains or via other intermediating parties (such as brokers and outsourcing suppliers). The multi-party security features of minimal disclosure tokens prevent any unauthorised manipulations of protected information, not only by outsiders but also by intermediating parties. For instance, issuers can protect identity claims against unauthorised lending, pooling, cloning, discarding, and reuse by encoding them into minimal disclosure tokens. At the same time, intermediating parties can see the information that is shared, enabling them to boycott inappropriate exchanges. They can also be actively involved in the flow of protected information, helping to determine how organisations conduct data exchanges. Furthermore, they can store protected information upon issuance so that it can be ported and used off-line.
- **Selective disclosure:** Identity information encoded into minimal disclosure tokens can be selectively disclosed in a fine-grained manner. By way of example, the user of a minimal disclosure token stating that its holder is a Dutch citizen born on August 12, 1966 can present the token in a manner

that reveals only that the holder is over 18 and European.[24] As another example, a token that specifies its holder's real name can be presented in a manner that proves that the name is not contained on a blacklist of suspected terrorists, without revealing anything else.

- **Unlinkability:** Minimal disclosure tokens can be issued and presented without creating unwanted linkages. This enables organisations to issue authentication tokens to identified individuals that can subsequently be used to access protected resources anonymously or pseudonymously. It also enables account holders to retrieve and present protected identity claims without thereby enabling organisations to link the source and destination accounts. This protects against unwanted profiling across spheres of activity and minimises the risk of identity theft by insiders and hackers. At the same time, individuals who abuse services can be excluded from further participation via several revocation methods that do not contravene the privacy features of minimal disclosure tokens.
- **Non-transferability:** Issuers can prevent users from transferring (copies of) minimal disclosure tokens that convey privileges, entitlements, and other personal credential information. One solution is to encode private information of the designated token holder into the tokens; the token holder can hide this data at presentation time (owing to the selective disclosure feature), but would need to reveal it in order to enable others to present the tokens. For stronger protection, issuers can electronically bind minimal disclosure tokens to a previously issued trusted module (such as a tamper-resistant smart card or a Trusted Computing chip) that can enforce security policies (such as non-transferability) throughout the life cycle of the tokens; in contrast to PKI certificates, a single low-cost module can protect arbitrarily many minimal disclosure tokens.
- **Private audit trails:** Relying organisations can capture signed transcripts that prove their interactions with individuals. Prior to storing or forwarding signed transcripts, some or all of their disclosed contents can be censored without destroying their verifiability. This enables organisations to protect their own privacy and autonomy interests vis-à-vis auditors.

A detailed description of how these features are achieved is outside the scope of this section.[25]

---

[24] Technically, the 'over-18' property is proved by providing a zero-knowledge proof that the value (e.g., total number of days or minutes) representing today's date minus the token value representing the birth date is greater than the value that represents 18 years. The 'is-European' property is proved by demonstrating in zero-knowledge that the country code encoded in the token is in the set of country codes representing all European countries.

[25] A starting point to learn more is Stefan Brands: 'Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy,' MIT Press, ISBN 0-262-02491-8, available at http://www.credentica.com/technology/book.html.

The privacy features of minimal disclosure tokens hold unconditionally, in the strongest possible sense: issuing and relying organisations cannot learn anything beyond what users choose to disclose when presenting their tokens, even if they collude and have unlimited resources to analyse protocol data.

Minimal disclosure tokens are not merely an academic construct: leading industry players are working to productise minimal disclosure token technologies. For example, Microsoft has announced plans to implement its U-Prove technology (see http://www.credentica.com) into Windows Communication Foundation and Windows CardSpace, and IBM has developed a similar technology (see http://www.zurich.ibm.com/security/idemix) that it plans to contribute to open source.

Advanced Claims: Security Policy Assertion Language

SecPAL (Becker et al., 2006; Humphrey et al., 2007) is a security policy language developed to meet the access control requirements of large-scale Grid Computing Environments. SecPAL is declarative, logic-based, and builds on a large body of work showing the value of such languages for flexibly expressing security policies. It was designed to be comprehensive and provides a uniform mechanism for expressing trust relationships, authorisation policies, delegation policies, identity and attribute assertions, capability assertions, revocations, and audit requirements. This provides tangible benefits by making the system understandable and analysable. It also improves security assurance by avoiding, or at least severely curtailing, the need for semantic translation and reconciliation between disparate security technologies.

A very simple example could look as follows (see also Becker et al., 2006). Researcher Fanny wants to access a file on a file server. The company's security token service (STS) issued a token to Fanny: 'STS says Fanny is a researcher'. The assertions are encoded in XML and signed by the issuer of the assertion, typically the STS. Let's assume that the file server has a security policy: a) 'STS says FileServer can say x can read y' and b) 'FileServer says x can read file://project if x is a researcher'. Finally, Fanny wants to read a file on the file server. She sends her read request together with her assertion to the file server. The file server is protected with a policy enforcement point that triggers the following SecPAL query at the policy decision point: 'Fanny can read file://project'. In this case we assume that the STS acts both as token issuer and as policy decision point. The SecPAL engine has Fanny's assertion, the policy and the query and uses an inference mechanism to determine if the query can be deduced from the policy and the assertions.

It is remarkable that the assertions, the policy and the query are expressed in the same language. The verbs 'says' and 'can' acts as a special keyword in the SecPAL even allows limited and unlimited delegation chains with a combination of both keywords 'can say'. In the example we see this when the STS allows the file server to define who may access the files. SecPAL defines a set of verbs such as 'read', 'write', 'execute' but is open for new verbs. However, the

current research license allows only a fixed set of verbs in the context of Grid Computing.[26]

Becker et al. (2006) mention a list of design principle for the language: expressiveness, readable syntax, unambiguous semantics, effective decision procedure and extensibility. Humphrey et al. (2007) provide details from an implementation using SecPAL as fine-grained access control for GridFTP where SecPAL outperforms the other tested access control mechanism.

4.3 Supporting Technologies

In this section technologies supporting identity management intentionally or indirectly are introduced and discussed. In the context of FIDIS research the following technologies are investigated:

- Trusted Computing
- Protocols with respect to identity and identification
- Service Oriented Architectures
- Digital Rights Management

Most of these technologies carry the potential to be (ab)used for profiling and surveillance like identity management. However, for some of them application scenarios were developed that need to be considered as enhancing. In this section the problem domains and privacy enhancing application scenarios are presented.

4.3.1 Trusted Computing[27]

An important point when implementing cryptographic schemes and protocols is the fact that security needs some kind of 'trusted anchor', i.e., one cannot achieve protection within a completely untrusted environment. Trusted Computing (TC) is about establishing this trusted anchor.

The first seminal publications in the field of Trusted Computing can be dated back to the early 1970s (e.g., Baran, 1973). It became an 'emerging' technology in the past few years due to the fact that an industry consortium — the Trusted Computing Group (TCG)[28] — started to develop industry standard specifications that support trusted computing for PCs, clients and servers, mobile devices and a trusted infrastructure. The TCG has more than 120 members including nearly every important IT company (e.g., AMD, HP, IBM, Intel, Microsoft and SUN). The powerful market position of these companies drives the spreading of Trusted Computing as defined by the Trusted Computing Group.

[26] See http://research.microsoft.com/projects/SecPAL/ for details.
[27] Author: Stefan Köpsell, TU Dresden.
[28] http://www.trustedcomputinggroup.org/.

Nevertheless it is still (emotionally) discussed what exactly TC is[29] and whether it has more benefits for users or for commercial organisations, e.g., in scenarios like Digital Rights Management (DRM).

In general TC comprises at least the following technologies and mechanisms:

- **Trusted computing base** which is the minimal set of hardware (e.g., the TPM-chip specified by the TCG), firmware and software (e.g., a secure operating system) which is necessary for enforcing a security policy.
- **Secure I/O** which offers protected paths for all data from the input through the processing until the output. That means for instance that the user can be sure that the inputs he made can not be intercepted by malicious software like keyboard loggers.
- **Sealed memory** which refers to a protected memory which prevents other processes (and even unprivileged parts of the operating system) from reading / writing to it.
- **Sealed storage** a technology which ensures that persistent data can only be read and modified by exactly the same combination of hardware / software which has written the data.
- **Authentic booting and (remote) attestation** which allows a user to be sure with which well defined hard- / software he interacts and to prove this even to third parties.
- **Unique digital identities for computers** which means that each Trusted Computing base has a unique digital identity enabling the owner of a computer to prove that a certain message originated from a computer he owns or that two messages come from the same computer; that two messages do not come from the same computer.

An important fact and fundamental principle about Trusted Computing is, that Trusted Computing does not mean that the computing environment (hard- and software) can be trusted—but instead one has to trust it. According to Ross Anderson, 'In the US Department of Defense, a 'trusted system or component' is defined as 'one which can break the security policy'.'[30] This simply means, if the trustworthiness assumptions one has about a certain Trusted Computing based ICT system are wrong, then the whole protection offered by this system (in terms of security and privacy) can be broken.

Immediately the question arises to what extent should one trust the Trusted Computing. If one is willing to absolutely trust the Trusted Computing, many (if not all) security- and privacy-related problems can be solved easily. The reason is that most of the complex and complicated cryptographic mechanisms and proto-

[29] This is not surprising as the term 'trust' itself is heavily discussed within different communities.

[30] Ross Anderson: 'Trusted Computing' Frequently Asked Question. Version 1.1 (August 2003), http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.

cols just exist or were designed with the goal to circumvent the untrustworthiness of the computing environment (soft- and hardware) used by the communication partners and third parties.

As example in (Müller and Wohlgemuth, 2007) the delegation of rights and secrets to proxies which act on behalf of the customer was identified as one of the fundamental problems (with respect to security and privacy) in multi-stage business processes. Clearly if these proxies are not trustworthy, then they can use the data provided by the user to contravene the interests of the user and violate his privacy.

Using Trusted Computing on the proxy side could easily solve this problem (under the assumption that one is willing to absolutely trust the Trusted Computing as mentioned above). In this case the proxy would be trustworthy (and can be trusted) 'by definition'.

On the other hand the history of security and privacy technologies as well as ICT in general has shown that such absolute error-less and correctly designed and working systems do not exist and will (with high probability) never exist. Therefore Trusted Computing should only be seen as a 'helping tool' which could be used to enhance the overall security a system provides.

In (Iliev and Smith, 2005) the fundamental property of Trusted Computing is described as follows: 'We call the physically protected and trusted components of a server K, [...]. In any given client-server application, we can view K as an extension of the client: from a trust perspective, K acts on the client's behalf, but physically, K is co-located with the server.'

Derived from this fundamental property, using Trusted Computing comprises at least the following two overall goals / approaches:

- To *prevent* security threats by implementing (traditional) security mechanisms in a more trustworthy way or (more general) use Trusted Computing to secure the basic operations of the devices (e.g., client PCs, servers or mobile phones). This comprises all the well known technologies offered by Trusted Computing.

  In order to exemplify this one can look at a typical e-business scenario where the communication between the involved parties (users and services) has to be confidential and integral. The (cryptographic) protocols and measures used can benefit from TC and the TPM, e.g., the cryptographic keys could be stored under the control of the TPM (using the Sealed Memory and Sealed Storage functionality) making attacks on the communication confidentiality much harder.

  In general it seems that this 'classical' approach for enhancing the security is the one which is in the focus of the industry and corresponding business consultancies[31].

[31] See for instance: Jon Oltsik: 'Trusted Enterprise Security. How the Trusted Computing Group (TCG) Will Advance Enterprise Security.' White Paper, Enterprise Strategy Group, January 2006, https://www.trustedcomputinggroup.org/news/Industry Data/ ESG_ White_Paper.pdf.

- Enabling the communicating parties to *check, monitor* and *audit* the trustworthiness of each other using remote attestation. Even third parties could be permitted to do so (e.g., on behalf of a communicating entity).

  Online banking can serve as an example scenario to illustrate this. If trusted computing is used on the service side (i.e., the bank) then the user can check if the bank server is secure. Moreover if trusted computing is used on the user side then the bank can check if the computer of the user is secure, e.g., not tampered with malicious software. Depending on the detected security status both parties can for example limit the maximum amount of money allowed for online banking transactions. Finally these checks could be outsourced to third parties, e.g., the bank side could be audited by data protection authorities.

The FIDIS consortium analysed the potential of Trusted Computing for supporting security and privacy within various areas and scenarios. The different possibilities of applying Trusted Computing in e-Business scenarios are elaborated in Müller and Wohlgemuth (2008). Finally Alkassar and Husseiki (2008) give a broader overview on the applicability and implications of Trusted Computing in the area of identity management.

Note that so far the standards and technologies developed by the Trusted Computing Group focus primarily on software based attacks and not hardware based (i.e., physical) ones. Therefore TC does not offer protection if a device itself could be manipulated by the attacker. This has to be taken into account when considering the overall security of a given system, especially in scenarios where mobile devices are involved which could easily get lost or stolen. But even in the online banking scenario as illustrated above this has to be evaluated. On the one side one can assume that the bank is well experienced in offering excellent physical protection for valuable goods including their servers. On the other side one has to consider that many banks outsource their IT resulting in much less physical protection to the servers.

But focusing on software-only attacks is not the only controversial issue of Trusted Computing as defined by the Trusted Computing Group. Trusted Computing might have a negative impact on the privacy of its users as for instance remote attestation reveals the whole configuration of users' devices (e.g., all running software, installed hardware etc.). Each TPM device has a unique cryptographic key which could be misused to uniquely identify the device and consequently its users (e.g., if Trusted Computing is applied to mobile phones). Trusted Computing could also be misused to prevent the execution of certain 'unwanted' software or operating systems (e.g., Open Source ones). Alkassar and Husseiki (2008) as well as Müller and Wohlgemuth (2008) discuss the shortcomings of Trusted Computing and related legal and social aspects in more detail.

Summarising one can say that Trusted Computing is a necessity for privacy and security in the information society but needs to be carefully designed so that it does not do completely the contrary.

4.3.2 Protocols with Respect to Identity and Identification[32]

In computing, protocols are standards that control or facilitate the connection, communication, and data transfer between two endpoints. As communication is the basis of our Information Society, protocols are highly relevant for all activities in information and communication technologies. What is more, usually users are not aware of running protocols at least as long they function seamlessly and facilitate the desired services. This also means that people lack knowledge on privacy risks or other identity-related aspects when using protocols. One example is the repeated usage of some identifiers, e.g., MAC (Media Access Control) addresses or Cookies, which enable linkage and profiling by any observer. In some cases the network infrastructure relies on the transfer of these identifiers—real data minimisation would require a major redesign of the protocols.

When discussing protocols, there is a need to distinguish between their specification and implementation. Although these should be one and the same, in practice implementations do not always properly adhere to what is laid down in the specifications—this may be done accidentally, but in some cases deviations from the specifications are intended, e.g., when implementing light-weight versions of the full specification or when contradictions are discovered in the documents which cannot be overcome.

When describing networking protocols, typically the ISO/OSI layer model is used. This model describes seven layers with the following functions (Tanenbaum, 2003):

Table 4.1. Layers and corresponding functions in the ISO/OSI reference model

Data Unit	ISO/OSI layer	Function
Data	7: Application	Network process to application (http)
	6: Presentation	Data representation and encryption
	5: Session	Interhost communication
Segments	4: Transport	End-to-end connections and reliability (TCP)
Packets	3: Network	Path determination and logical addressing (IP)
Frames	2: Data link	Physical addressing (MAC & LLC)
Bits	1: Physical	Media, signal and binary transmission

In (Hansen and Alkassar, 2008) an overview is given of the identity-related aspects of network protocols on different technical layers: host-to-network layer (e.g., Local Area Network (LAN) and Wireless LAN (WLAN) communication), Internet layer (e.g., Internet Protocol (IP) and Internet Protocol Security (IPSec)),

[32] Author: Marit Hansen, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

Table 4.2. ISO/OSI layers of selected protocols from the TCP/IP suite

TCP/IP layer	ISO/OSI layer	Protocols	
Application	5-7	HTTP	SMTP Telnet DNS SNMP SSH RTP
Transport	4	TCP	UDP SCTP
Internet	3	IP (IPv4, IPv6)	ICMP IPSec
Link / Physical / Host-to-Network	1-2	Ethernet (CSMA/CD), WLAN, Token Ring, PPP, ISDN, Modem	

transport layer (e.g., Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)) and application layer protocols (e.g., HyperText Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP) and Domain Name System (DNS)). The following figure shows how the analysed protocols belonging to the TCP/IP protocol suite map to the ISO/OSI seven layer reference model.

In addition, protocols for privacy policies (ISO/OSI layer 7) are being analysed concerning their potential for improving the user's privacy. For both categories of protocols, the main results of the survey done in (Hansen and Alkassar, 2008) are summarised in the following paragraphs.

Network Protocols

When analysing identity and identification aspects of network protocols, the following criteria were put in the focus:

- Which identifiers are used in the protocols? How unique are they? Are all identifiers visible, or may there be hidden identifiers?
- Is linkage of different protocol runs possible? Could users be profiled or even identified by this linkage?
- Which additional user data—i.e., which data directly linked to the user involved (or his machine)—are disclosed?
- Is it possible to avoid or circumvent the information disclosure, and if yes: with which effort?

The analysis of network protocols shows that virtually any commonly used protocol reveals linkable information which could be used for profiling. For instance, transmitted identifiers such as IP addresses (in all Internet communication), Cookies (in HTTP) or MAC addresses (in Ethernet or WLAN communication) enable for each observer linkage of different protocol usages and thereby profiling of the user's

(or computer's) behaviour. Dynamically assigned IP addresses are not uniquely bound to the user's computer—unlike the MAC address which typically is static to the network interface. However, IP addresses of one and the same Internet provider change only within a certain range, and in addition they can be mapped to geographical data to find out the region where that IP address was registered. This is also relevant for location privacy when mobile users use various WLANs.

The profiling possibility with linkable data may yield so extensive profiles that the link to the user can be easily established and thus they become personal data. Further, there are protocols which explicitly disclose user data, e.g., the header fields 'Referer', 'User-Agent', 'Accept' or 'Accept-Language' in HTTP or the information on sender and receiver of e-mails in SMTP. Again, these data alone or in combination may identify the users and are privacy-relevant. For instance, sender and receiver of e-mails give observers such as eavesdroppers or other parties the information that there is a relationship between the e-mailing parties. It can be used to figure out a user's social network. This is also true when the e-mails are encrypted: The header information stays the same even if the payload, i.e., the e-mail's body, is encrypted. Concerning HTTP, the content of the header field 'User-Agent' may be used to categorise the user as 'early adopter' (if very new browsers are employed) or it can be used as first analysis of possible security vulnerabilities on the user's computer (if old versions have not been updated). 'Accept-Language' informs about the cultural background of the user. The 'Referer' field contains the URL where the user came from—if this had been a search engine, the Referer usually also comprises the search terms.

Looking into protocols is not done by many users. Several people are aware of those options which can be configured in their application software, in particular in the browser. However, the choices that can be made on that level are very limited. For HTTP, browsers usually offer to configure the behaviour when setting or deleting Cookies. Since of the middle of 2008, so-called 'privacy modes' are being established from various browser manufacturers which among others may prevent the transmission of Referer information.

For most cases avoiding or circumventing the shown protocol-related threats for privacy and data protection cannot be done easily, though. One partial solution could be anonymisation services or other data minimisation techniques on the lower protocol layers that can be used to blur some of the traces one leaves while using the Internet. For browsing this can be done by substituting IP addresses or suppressing Cookies and interesting information in HTTP header fields. However, these services neither offer a convincing level of protection nor have they achieved a level of stability and quality of service necessary for every day use by the masses. Nevertheless they are suitable tools at least for some use cases. An easy to implement measure (from a technological point of view) would be to use link encryption of every single data link. This would greatly enhance privacy against outsiders—e.g., eavesdroppers on the lines—who would neither learn the communications' content nor (most of) their circumstances.

What are the odds that upcoming Next Generation Internet protocols will take into account the sketched privacy issues and handle them in an appropriate way?

FIDIS work (Hansen and Alkassar, 2008) took a look into important consortia dealing with new protocols to straighten out flaws created decades ago or to meet requirements stemming from actual usage patterns that were not foreseeable when the old protocols were designed. Important proposals comprise:

- the Internet2 Network[33] which provides a high-performance backbone network to U.S. research and education institutions, offering community control of the fundamental networking infrastructure.
- the GÉANT[34] and GÉANT2[35] network infrastructure, i.e., a multi-gigabit pan-European data communications network, reserved specifically for research and education use across Europe.
- the 'TRIAD – Translating Relaying Internet architecture integrating Active Directories'[36] architecture meant as overlay to the current Internet by defining an explicit content layer.
- the U.S. initiative 'FIND – Future Internet Network Design'[37] and the European 'Future Internet Research and Experimentation'[38] initiative, both long-term approaches to provide networks for new Internet-enabled applications and services.

All these proposals aim at improving security and robustness. Identity management and accountability are less prominently dealt with; privacy issues are rarely addressed as yet.

The next section describes privacy policy languages and protocols which are situated on higher levels in the network—they indeed try to take care of data protection issues.

Privacy Policy Languages and Protocols

In the World Wide Web, privacy policies are an important mechanism to inform users on the planned data processing. However, privacy policies often are hard to understand as they may be written in foreign languages or contain too much legalese. They are hard to compare with each other because they differ in scope, tackled issues and granularity. And why bother to read them if they usually offer no choices anyway (except for 'take it or leave it')?

This could be different with machine-readable privacy policies, expressed in specific languages: Privacy policy languages are designed to support organisations and users in managing their privacy policies and preferences. The development of privacy policy languages, the specification of their syntax and semantics, and the

[33] http://www.internet2.edu/network/.
[34] http://www.geant.net/.
[35] http://www.geant2.net/.
[36] http://gregorio.stanford.edu/triad/.
[37] http://find.isi.edu/.
[38] http://cordis.europa.eu/fp7/ict/fire/.

interaction with ICT systems, e.g., protocols for negotiating and matching policies, belong to a highly dynamic field. Since 1997 when W3C started the development of the Platform for Privacy Preferences (P3P), a variety of languages and protocols have been proposed which are specifically designed to manage privacy policies or—even if their main objective was less privacy-specific—can be applied for data protection purposes as well.

The vast area of privacy policy languages is not limited to the World Wide Web. Four categories of privacy policy languages are distinguished (Kumaraguru et al., 2007):

1. sophisticated access control languages (e.g., SAML, WSPL or XACML).
2. enterprise privacy policy languages (e.g., Enterprise Privacy Authorisation Language (EPAL)).
3. web privacy policy languages (e.g., P3P on the organisational side, APPEL or XPref on the user's side).
4. context-sensitive languages (e.g., Geopriv as an authorisation policy language for controlling access to location information or Protune (Provisional trust negotiation) as a rule-based trust negotiation framework).

In all of these areas, several proposals are being developed and evaluated. After involvement in P3P and EPAL, the World Wide Web Consortium continues its work on privacy policy language in the Policy Languages Interest Group (PLING). It is unlikely that the outcome of that work will be the one and only policy language. Instead other ways for interoperability of privacy policy languages are envisaged, e.g., by specifying common interfaces or establishing gateway services between different policy language domains.

Without doubt, protocols for negotiating policies and enforcing them will play a prominent role in the next years. As full data avoidance is not an option in many practical cases, policies and policy enforcement have to step in. From today's perspective it is not clear which languages and protocols will prevail in which areas.

Importance of Designing Protocols with Privacy Experts

According to Lessig, protocols belong to the major regulators which have a profound impact on society and whose implications must be considered (Lessig, 1999). This applies for all implementations of protocols, forming the architecture of ICT and providing today's possibilities for usage. In addition, the specifications of protocols already play a role as they are the blueprint not only for implementations thereof, but define interfaces to other specifications and implementations. If protocols, i.e., their specifications and / or their implementations, are faulty, the applications on top usually cannot eliminate the mistakes, but often even intensify the consequences.

Considering the complexity of the area and the massive influence of protocols on the Information Society, a privacy and linkability analysis should be performed

during the design phase of each protocol, taking into account also linkage possibilities from and with the environment where the protocols will be run. Article 20 of the Directive 95/46/EC deals with 'prior checking' which should be carried out when the processing operations are 'likely to present specific risks to the rights and freedoms of data subjects'. In particular outside the European Union, e.g., in Canada, the United States, Australia and New Zealand, a similar procedure is also known as 'Privacy Impact Assessment'. Taking this seriously, privacy experts would have to be involved right from the beginning in each design process of communication protocol specifications.

The general participation of Data Protection Authorities (DPAs) and other trusted parties in the technology design process for better trust and trustworthiness might help. But this is no silver bullet since DPAs lack resources for skilled personnel travelling and participating in meetings where protocols are being specified. Indeed during the last decades very few DPAs were involved when protocols were specified, and those involved usually participated only in the design of specific protocols and languages focusing on privacy and data protection (such as P3P or EPAL). However, all kinds of protocols have been discussed and criticised in the privacy community, e.g., because of shortcomings concerning important privacy concepts such as data minimisation, transparency or the user's self-determination. Mostly the criticism came only after or in a late phase of the specification process, having a limited effect.

Summarising, a major challenge is not only the understanding of today's protocol world, but also the design and specification of new protocols. In particular in those areas where right now standardisation work is being performed, it is highly recommended to integrate experts from the fields of identity and privacy in the processes. Naïve specifications and implementations of global standards will usually cement not so privacy-friendly information and communication technologies. Even if privacy-invasive requirements such as demanded data retention are an obstacle to pure privacy-enhancing design of protocols, data protection functionality could be massively improved. In addition, the impact of these protocols, their interdependencies and the whole specification process have to be made more transparent to decision makers and citizens because protocols are the backbone of our Information Society.

4.3.3 Identity Management in Service Oriented Architectures[39]

Service Oriented Architecture (SOA) is a collection of cooperating services, which jointly fulfil a higher-level operation through communication. They fall in the class of distributed systems (Coulouris et al., 2005). A special attribute of SOA is the loose binding between the services. Typically the binding happens only at run-time, which means that a service learns only at this point in time with which actual service

[39] Authors: Stefan Brands, Microsoft; Laurent Bussard, EMIC; Joris Claessens, EMIC; Christian Geuer-Pollmann, EMIC; Ulrich Pinsdorf, EMIC.

instance it is communicating. This feature is called loose binding and is in fact said to be one of the core characteristics of SOA (Cabrera and Kurt, 2005).

This leads us back to identity management, since each service typically runs on behalf of a user's or organisation's identity. Considering that SOA allows, in addition to direct user interaction, an automated, intermediated and even delegated access to resources, leads to challenging identity management issues. Services which are bound only at run-time have to establish a verifiable trust relationship based on the identities of service owners. These issues are even amplified if we consider large, distributed service landscapes involving multiple business roles. Although SOA is commonly used inside organisations[40], service calls may even span across company boundaries, which leads to so called service federations between the hosting organisations (Goodner et al., 2007).

The need for standardisation of protocols to establish trust among services was already identified back in 2002, for instance the W3C created a number of working groups on various aspects of web services (Jacobs, 2002). The first version of the WS-Trust protocol was published in December 2002.

In the remainder of this section we want to introduce the most important protocols in the Web services world. Web services represent the most widely used type of SOA. The communication is XML-based and typically transported via HTTP. Web services fulfil a number of basic standards such as the Simple Objects Access Protocol (SOAP) for method invocation or Web Service Description Language (WSDL) for interface description. We describe the protocols WS-Security, WS-Trust and WS-Federation. WS-Trust is actually an identity protocol for trust establishment. It is based on WS-Security which supports the primitives for identity, key exchange, cryptography and signatures (see also Bauer, Meints, Hansen, 2005). WS-Federation goes a step further than WS-Trust and allows establishing of virtual collaborations across trust boundaries; it is thus comparable to a cross-certification in the PKI world. Having described the protocols, we want to introduce CardSpace in Section 4.5.2 as a use case that uses WS-Trust and WS-Security for identity management.[41]

Trust in Service Oriented Architectures

The WS-Trust specification (Nadalin et al., 2008) introduces the concept of 'security token services' (STS). A security token service is a Web service that can issue and validate security tokens. For instance, a Kerberos ticket granting server would be an STS in the non-XML world. A security token service offers functionality to issue new security tokens, to re-new existing tokens that are expiring and to check the validity of existing tokens. Additionally, a security token service can convert one security token into a different security token, thus brokering trust between two trust domains.

[40] The Open Group maintains an extensive list of SOA reference projects at http://www.opengroup.org/projects/soa-case-studies/page.tpl?CALLER=index.tpl&ggid= 996.

[41] CardSpace focuses mainly on user-centric identity management interaction, but it is applicable in SOA scenarios as well.

For example, a Web service describes required security tokens for Web service calls using WS-SecurityPolicy (Lawrence et al., 2008). A requestor may want to call that specific Web service but may not have the right security tokens indicated by the policy. The Web service may require Security Assertion Markup Language (SAML) credentials from a particular trust domain whereas the requestor only has an X.509 certificate from its own domain. By requesting the 'right' matching token (credential) from the security token service, the requestor may get back a token from the STS that can be included when calling the Web service in question. The decision what exactly the 'right' token is can be made either by the requestor or by the STS. After inspection of the Web service's policy, the requestor may specifically ask the STS: 'I have the attached X.509 certificate and need a SAML token.' The other option is that the requestor includes its possessed tokens and states what Web service it intends to call: 'I possess the following tokens and I would like to call the Web service http://foo/bar. Please give me whatever token may be appropriate.'

WS-Trust provides a rich interface that permits the implementation of various use cases. For instance, the requestor may include time variant parameters as entropy for a token generation process. The token service may return secret key material to the requestor (so-called proof-of-possession tokens) along with the requested security token, so that the requestor can prove that it possessed the security token. For instance, the requested security token may be a certificate whereas the proof-of-possession token is the associated private key. The security token service may also return multiple keys like a certificate along with its validation chain or it may create key exchange tokens with which the requestor can encrypt key material for the intended Web service. A requestor can also express requirements on algorithms and key strengths for required tokens.

WS-Trust defines protocols including challenge-and-response protocols to obtain the requested security tokens, thus enabling the mitigation of man-in-the-middle and message replay attacks. The WS-Trust specification also permits that a requestor may need a security token to implement some delegation of rights to a third party. For instance, a requestor could request an authorisation token for a colleague that may be valid for a given time interval. WS-Trust utilises WS-Security for signing and encrypting parts of SOAP messages as well as WS-Policy / SecurityPolicy to express and determine what particular security tokens may be consumed by a given Web service. WS-Trust is a basic building block that can be used to rebuild many of the already existing security protocols for trust establishing and make them fit directly in the Web services world by using Web service protocols and data structures.

The WS-Security (Lawrence et al., 2006) specification defines mechanisms for integrity and confidentiality protection, and data origin authentication for SOAP messages and selected parts thereof. Hence, it offers the basic primitives to establish mutual trust using WS-Trust. The cryptographic mechanisms are utilised by describing how XML Signature and XML Encryption are applied to parts of a SOAP message. That includes processing rules so that a SOAP node (intermediaries and ultimate receivers) can determine the order in which parts of the message

have to be validated or decrypted. These cryptographic properties are described using a specific header field, the <wsse:Security> header. This header provides a mechanism for attaching security-related information to a SOAP message, whereas multiple <wsse:Security> headers may exist inside a single SOAP message. Each of these headers is intended for consumption by a different SOAP intermediary. This property enables intermediaries to encrypt or decrypt specific parts of a message before forwarding it or enforces that certain parts of the message must be validated before the message is processed further.

Besides the cryptographic processing rules for handling a message, WS-Security defines a generic mechanism for associating security tokens with the message. 'Associating a security token' means that one or more tokens are included in <wsse:Security> headers in the message and that a referencing mechanism is introduced to refer to these tokens. Tokens generally are either identification or cryptographic material or they may be expressions of capabilities (e.g., signed authorisation statements).

For instance, the certificate for signature validation may be added into the header. That may be done by either placing it into the signature itself (which makes reusage a bit complicated and fragile) or by directly making it a child of the <wsse:Security> header and referencing it from the signature. The latter use has the advantage that other signatures or security operations may also directly refer to that token. WS-Security, available in version 1.1 since February 2007, defines a simple username token, a container for arbitrary binary tokens (base64 encoded), a container for XML-formatted tokens, and an encrypted data token.

WS-Federation introduces mechanisms to manage and broker trust relationships in a heterogeneous and federated environment. This includes support for federated identities, attributes and pseudonyms. 'Federation' refers to the concept that two or more security domains agree to interact with each other, specifically letting users of each security domain access services in the other security domain. For instance, two companies that have a collaboration agreement may decide that employees from the other company may invoke specific Web services. These scenarios with access across security boundaries are called 'federated environments' or 'federations'. Each security domain has its own security token service(s), and each service inside these domains may have individual security policies. WS-Federation uses the WS-Security, WS-SecurityPolicy and WS-Trust specifications to specify scenarios to allow requesters from the one domain to obtain security tokens in the other domain, thus subsequently getting access to the services in the other domain.

To illustrate this concept with an example, imagine that a user Fanny from company A intends to access Frank's Web service in company B. Fanny and Frank do not have any prior relationship, but both companies have agreed to federate certain services, and the decision is that particular users from company A may access dedicated services inside company B. By some means, Fanny knows the endpoint reference of Frank's service. Using the basic mechanisms defined in WS-PolicyAttachment, WS-MetadataExchange (Ballinger et al., 2006), and WS-SecurityPolicy, Fanny retrieves the security policy of Frank's service and detects that the security token service STS_B of company B issues tokens to access this

service. Fanny issues a security token request to the security token service STS_A of company A and claims to need a token to access STS_B. Company A and company B are federated together, therefore STS_A is able to issue a security token for Fanny. Of course, that may depend on whether Fanny belongs to the group of A's employees that are permitted to access Frank's services. In the next step, Fanny requests a token for accessing Frank's service from STS_B and proves her authorisation by utilising the token issued by STS_A. After validating that the STS_A security token is valid, STS_B issues a security token for access to Frank's service (assuming that Frank's Web service belongs to the group that company B offers to company A). In the last step, Frank's Web service is invoked by Fanny. During that final request, Fanny presents the token issued by STS_B.

Besides this introductory example, WS-Federation shows how such a federation could work across multiple security domains or how delegation could be used. Delegation means that a user may delegate certain access rights on one federated resource to a different federated resource. Additionally, WS-Federation defines mechanisms to handle pseudonyms (aliases used at different services and federations) and management mechanisms for the pseudonyms, including single sign-in and sign-out (sign-out refers to the removal of pseudonym-related information at different services).

The whole suite of Web service-related specifications is much broader, even just the part dealing with security and privacy. Geuer-Pollmann and Claessens (2005) as well as Cabrera and Kurt (2005) provide a solid overview on the most relevant standards and their relations to each other.

4.3.4 Digital Rights Management[42]

Digital rights management (DRM) refers to several concepts to restrict arbitrary use of data and to limit it in accordance with a certain defined policy (e.g. Hansen and Möller, 2005). The core-functionality of DRM also can be summarised as policy enforcement. Policies in this context contain access control policies. As a result DRM also can be understood as an implementation of identity management core-functionalities (namely authentication and authorisation). The concepts for DRM differ in the technological approaches used and the targets DRM is used for. The targets are mainly (Alkassar and Husseiki, 2008: 42):

- DRM in companies or governmental administrations to protect customers' / citizens' data
- DRM for personalised files
- DRM for media files and
- DRM for software products.

[42] Author: Martin Meints, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

In addition the use of DRM has been discussed in the context of fraud prevention, especially the prevention of manipulation of bank notes[43]. Many recent DRM concepts rely on Trusted Computing. Many existing and planned technical implementations of DRM were investigated with respect to their potential impact on the privacy of customers and users. In most cases the impact on privacy was considered to be negative or at least discussed controversially (for an overview see Hansen, Möller, 2005, Alkassar, Husseiki, 2008 pp. 42-45 and references cited therein).

In the context of FIDIS research it was mainly investigated whether and how far DRM could be used to protect privacy of customers and citizen. While the direct application of DRM by customers in their relationship to organisations for technical and economic reasons does not seem to be promising, the application of DRM in organisations supported by trusted third parties (from the customers' viewpoint) seems to be more realistic. Together with policy management languages such as the Enterprise Privacy Authorization Language (EPAL)[44] DRM may become an important tool for the organisation internal and inter-organisation-client enforcement of security and privacy policies. Potential applications are the protection of the confidentiality of highly sensitive data, and the enforcement of the processing of this data for a defined purpose. These approaches also may be of interest for the processing of sensitive data along a chain of organisations, where service oriented architectures (SOA) are used and in the context of application service providing (ASP, also called saas, software as a service).

However, these concepts are more or less in an early conception phase and further research is necessary (also see Grimm et al., 2005).

4.4 Emerging Technologies[45]

In some contrast to the FIDIS research on IMS discussed thus far, the research in the area of emerging technologies has focused on less well developed technology, services or applications which may prove to have a weighty impact in the field of identity. 'Emerging technologies' is a topic which pervades all of the areas into which the work of FIDIS is separated and clustered, and so it is important to understand the potential impact which emerging technologies may have. While a relatively formalised description of emerging technologies has emerged over the last few years, i.e., the result of the convergence of nanotechnology, biotechnology, information technology, cognitive science, robotics, and artificial intelligence, within FIDIS the term is considered to be broader. We have defined this as (identity-related) technologies or applications whose practical usage is still far behind their potential.

---

[43] E.g., Schulzki-Haddouti, C., *EU-Kommission für Banknoten-Kopierschutz*, Heise-News, http://www.heise.de/newsticker/meldung/47083.

[44] See, e.g., EPAL 1.2, W3C Member Submission, http://www.w3.org/Submission/EPAL/.

[45] Author: Mark Gasson, Reading University.

The use of techniques to profile people from varying sized sets of data have become increasingly utilised in light of the evolving underlying technologies which both enable the processing through powerful infrastructures, and the development of the profiling techniques themselves. It is obvious that this type of technology will continue to develop inline with the technologies which support it, and many have prophesised a shift in the way in which we interact with machines based on the extrapolated potential of this technology. The focus of the work investigated within FIDIS based on emerging technologies is broadly related to this developing area, the emergence of Ambient Intelligence.

4.4.1 Ambient Intelligence

Ambient Intelligence (AmI) has been presented for many years as the panacea for the human / technology interaction bottleneck. The very essence of AmI is to enrich the user experience by capitalising on the potential that additional computing processing can bring. Part of this enrichment is achieved by augmenting the user in their daily lives through additional services and access to additional information. However, this is achieved whilst actually reducing the focus on the traditional explicit data input / output paradigm—a true shift in our concept of what a computer is, and how we should interact and use it. The aim of the AmI environment is to provide a context aware system, using unobtrusive computing devices that will improve the quality of people's lives by acknowledging their needs, requirements and preferences and thus acting in some way on their behalf. To achieve this, the 'intelligent' environment, or rather, an intelligent agent within the environment needs to build up a profile of each individual, and be able to subsequently link the profile with the correct individual. In essence, the environment itself has become the interface to the distributed, seamless and invisible AmI. AmI itself will not be the outcome of any single technology or application—rather it is an 'emergent' property. Essentially, AmI is more than just the sum of its parts. Ubiquitous Computing is the next wave of technology, whereby many thousands of wireless computing devices are distributed in the environment in everyday objects around us. Clearly this technology integration into the environment is a key aspect of AmI. Ubiquitous Communication will allow robust, ad-hoc networks to be formed by this broad range of mobile and static devices, forming a ubiquitous system of large-scale distributed networks of interconnected computing devices. By adding intelligent user interfaces and integrating sensing devices, it should be possible to identify and model user activities, preferences and behaviours, and create individualised profiles. These key aspects are all required to achieve the ideal AmI environment.

The concept of AmI is largely based on the idea that by augmenting an environment with sensor technologies and by providing near unlimited storage and processing capabilities, the intentions, needs and desires of people can be predicted and catered for. The result is that people will not need to know how to operate complex technologies—instead the technology will interact with them in

intelligent and intuitive ways. Clearly collating information is the key. However, if an environment is to know what a person wants or needs without being explicitly told, then this information needs to come from indirect means—i.e., the technology, or rather the environment as a whole becomes less interactive, and more proactive. Through varying levels of sensor data gleaned from pervasively embedded sensors, dynamic autonomic profiles can be drawn to enable this proactive ability. Intuitively these profiles can only be as good as the data that feeds them, and the processing available to create them, and hence the focus of development is to extract as much data as possible from all aspects of the users and their interactions within an AmI space, as well as developing the underlying infrastructure through which this data can be 'mined' for new information. This is further discussed in Chapter 7. From an implementation point of view, there are a range of technologies which are considered applicable in the fabric of an AmI environment. These stem from fundamental sensor technology for AmI spaces which will enable the data capture from which new information can be inferred, to enabling technology, i.e., technology which will serve in the underpinning infrastructure to provide the networking and processing capabilities necessary in the envisaged future scenarios of augmented living. Notably, and in contrast to other texts on AmI-related technology, we have investigated the concepts of 'sensors which detect sensors' and 'mobile user-controlled sensors' which may prove to be ways in which our privacy can be conserved to a greater extent in environments where data capture becomes ubiquitous.

In any case, it is likely that the user and the controller of the data will not be one and the same. Indeed in some cases it may be unclear who is collecting data from sensors and what it is being used for. One route to counteract such issues is the idea that new technologies should incorporate 'privacy by design', that is the mechanisms necessary for user control of their data should be an inherent aspect of the technology. To this end, many privacy advocates have suggested that emerging technologies and applications such as AmI should undergo mandatory privacy impact assessments before they are released into the mass market. To a large extent the technologies for AmI are speculative in that, in the main, they have not reached a mature level of development or deployment. Thus, it is exactly at this point where such technology needs to be discussed beyond the domain of those creating it to ensure that we are able to stay in control. 'Staying in control' is a broad turn of phrase, and indeed its exact meaning and context here is open to interpretation. However, what is for sure is that there are fundamental rights and freedoms which must be ensured.

The area of AmI has been extensively explored by the FIDIS NoE from the perspective of various disciplines. The fundamental enabling technologies which may form key parts of the AmI infrastructure have been discussed in Gasson and Warwick (2007), and Schreurs et al. (2005). Further to this, the very pertinent legal issues which need addressing, and the possible routes through which they may be addressed have been highlighted by Hildebrandt and Koops (2007), while solutions to the inherent security and privacy issues have been further developed by Hildebrandt and Meints (2006) and Fischer-Hübner and Hedbom (2008).

4.4.2 Human ICT Implants

The relatively new trend for low-tech human implants has recently risen in the public consciousness, although less publicised developments of high-tech implants in the medical domain have been progressing for several decades. Indeed, a significant drive behind the development of so called Information Communicating Technology (ICT) implant devices is medical—i.e., restoring deficient human abilities. It is clear that this application area is one which can be greatly enhanced through the new emerging technology phenomenon, and it is not clear where this may ultimately take us. The ability to form direct, bi-directional links with the human brain will open up the potential for many new application areas. Scientists predict that within the next thirty years neural interfaces will be designed that will not only increase the dynamic range of senses, but will also enhance memory and enable 'cyberthink' — invisible communication with others and with technology (McGee and Maguire, 2007). But are these claims realistic, and should they be taken seriously? As discussed by Kosta and Gasson (2008), current applications alone introduce challenging questions. Indeed the increasing commercialisation of human ICT implants has generated debate over the ethical, legal and social aspects of the technology and its products.

The basic foundations of advanced ICT implant devices are being developed for clear medical purposes, and it is reasonable to assume that few would argue against this progress for such noble, therapeutic causes. Equally, as has been demonstrated by cosmetic surgery, we cannot assume that because a procedure is highly invasive, people will not undergo it. So, while we may be some way away, there is clear evidence that devices capable of significant enhancement will become reality, and most probably will be deployed in applications beyond their original purpose. Thus, clear consideration needs to be given now to the fundamental moral, ethical, social, psychological and legal ramifications of such enhancement technologies. From a legal perspective, the implantation of ICT devices may challenge the right of bodily integrity for every human being, as a further expression of the right to self-determination. Moreover the use of human ICT implants allows the development of vast numbers of applications that will enable the tracking, tracing and profiling of the individual, as the unique number of the implant and / or the information stored on it can be linked with great certainty to an identified or identifiable natural person. However, the processing of such information should follow the principles on the processing of personal data, as they are described in the European data protection directive.

The use of ICT implants, especially in the medical sector, has been most welcome as it has introduced devices such as cardiovascular pacemakers, cochlear implants, deep brain stimulators for Parkinson's disease, and insulin pumps. Notwithstanding the positive impact of such devices to the health condition of the patients, the restoration of human capabilities and especially the enhancement of existing ones are not free of ethical issues. The ethical debate reveals a number of counter arguments against the use of ICT implants on human beings.

Given the current situation, it is not too soon to start real debate. To this end, the European Group on Ethics in Science and New Technologies have published their opinion on the use of ICT implants and notes that implants, if not used properly, may prove to be a threat to human dignity, by at the very least not respecting an individual's autonomy and rights. Such dangers are already present with current medical ICT implant devices, whereby even simple security such as basic access control is not implemented.

4.5 Use Cases

In this chapter user cases of identity management systems relying on the technologies described are presented and analysed. This includes:

- ID documents and the electronic passports (referring especially to PKI, electronic signatures, biometrics and RFID)
- CardSpace (referring especially to credential systems, WS-Security and WS-Trust)

4.5.1 ID Documents[46]

As a use case for IMS in e-government ID documents were investigated. ID documents are mainly used to authenticate or identify citizens in the context of general governmental procedures or procedures in specific sectors such as health or social insurance. Another important functionality is facilitating electronic signing together with PKI. Apart from a general overview covering these functionalities, national ID cards, citizen cards and European implementations of the epassport were investigated in depth (Meints and Hansen, 2006). The selected implementations are especially of interest as a number of technologies are already implemented in this context, e.g., electronic signatures, PKI and biometrics. In addition these ID documents are increasingly understood as an important enabler for e-government. With the transition from paper based government to e-government electronic IDs (eIDs) are needed to authenticate or identify participants such as governmental officials or citizens. In this context (semi-) automated border controls procedures using Machine Readable Travel Documents (MRTDs) are also understood as authentication and authorisation procedures.

Traditionally the binding between an ID document and its (authorised) user was ensured by a seal, a hand written signature of a governmental official or a traditional photo of the user. In the electronic world this does not work anymore as these attributes can be verified electronically only with difficulty and spoofing becomes

[46] Author: Martin Meints, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

easy. In the electronically enabled ID documents investigated in the FIDIS project mainly two ways were used to ensure the binding between an ID document and its user: (1) knowledge, typically a PIN, and (2) biometric reference data (typically biometric raw data such as standardised images of the face or finger tips).

A special focus was put on the Austrian and Belgium citizen card as they are both conceptualised as key-enablers for the national e-government strategies. Both concepts were investigated from a security and privacy point of view.

The Austrian citizen card is no traditional smart card based solution, but can be implemented in various formats, e.g., USB sticks and on mobile phones. The Austrian citizen card concept is remarkable due to the authentication mechanism used (see Meints and Hansen, 2006: 90-94). Based on a decree, the so called 'Bereichsabgrenzungsverordnung', governmental sectors are defined. The citizen card provides specific identifiers for each citizen in each of these defined sectors. The authentication of citizen is carried out based on SAML certificates and requires a specific local software component. In addition the Austrian citizen card can be equipped with an electronic signature. Linkability between sector-specific identifiers (called sector-specific PINs) is possible only in exceptional cases and needs to be carried out by the data protection authority acting as a trusted third party. In the context of the public sector this is the strongest mechanism to enforce purpose binding and to hamper function creep implemented today. In December 2005 the first prize for data protection in the category of European public authorities was awarded to Austria for the concept of the 'Bürgerkarte' by the Data Protection Agency of the Community of Madrid.[47]

The Belgian citizen card is based on a traditional smart card. The authentication of the user is based on X.509v3 certificates and is ensured and secured via PKI run by order of the Belgian state and a PIN (Meints and Hansen, 2006: 90-99). The citizen card itself has in the first version no privacy-enhancing functionality (De Cock et al. 2006). Recently as a transparency enhancing measure the online access of citizens to their own files at the National Register was introduced. [48] In this file also the access of citizens' data by Belgian public authorities is stored together with the purpose of the access.

Intensive research was carried out in the context of the electronic passport (epass). With the integration of an RFID chip and biometric reference data the epass became part of a largely distributed border control infrastructure. Vulnerabilities, threats and resulting security and privacy risks for the citizen were analysed and recommendations for future versions made. The technical concept of the first version of the epass, issued since November 2005, showed severe weaknesses, and for some of these exploits were already demonstrated (Meints and Hansen, 2006; Kosta et al., 2007; Meints and Hansen, 2008). Examples are:

---

[47] http://www.austria.gv.at/DesktopDefault.aspx?TabID=4951&Alias=bka&infodate=19.12.2005 and http://www.ptapde.gr/news/PR_e-PRODAT_20051215.pdf.

[48] Access is possible via https://www.mijndossier.rrn.fgov.be/, but requires a client certificate which is provided from the citizen card.

- Cryptographic weaknesses in the central access control mechanism called Basic Access Control (BAC); in addition in many cases BAC is not effective as together with the epass the BAC key has to be handed over to private organisations, especially hotels; in Sweden data needed to calculate the BAC key was publicly accessible for all Swedish citizens.[49]
- The reading range of the passport could be extended from the planned 10 to 15 cm up to 50 cm; communication between reader and epass can be eavesdropped from a distance up to 10 m.
- The issuing process for the epass was not mature, official passports with photos not belonging to the epassport holder could be retrieved in 14 European member countries[50].
- No security concept compliant with international standards such as ISO/IEC 27001 or CobiT is available covering all countries, epass and reader infrastructure and organisational aspects.
- The data minimisation principle is not implemented because biometric raw data (photos of fingerprints and faces) is used instead of templates; biometric raw data contain additional information that might be used for different purposes apart from border control (Kindt and Müller, 2008: 83-84). In addition the finality principle (purpose binding to prevent function creep) is not ensured internationally.

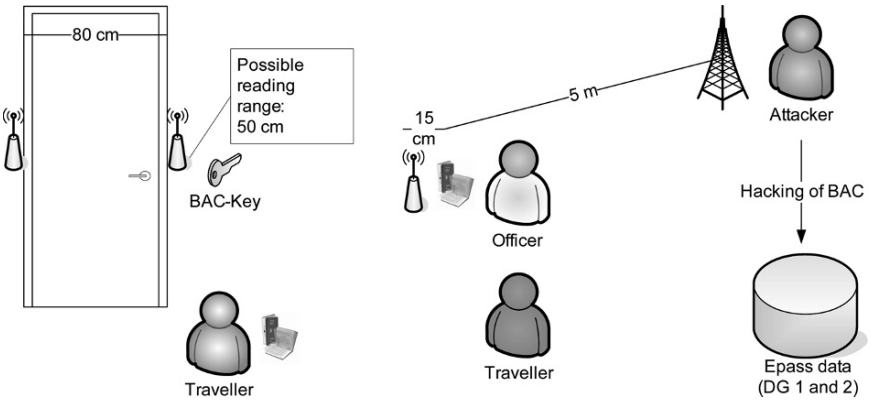


Fig. 4.8. Attack scenarios for the epass: tracking / deployment of events and eavesdropping

[49] This was officially confirmed by the responsible issuing authority for epassports in the county of Värmland on 2nd of February 2007.

[50] See the BBC report: 'My faked passport and me', http://news.bbc.co.uk/2/hi/programmes/panorama/6158927.stm.

In the literature the use of these risks in the context of the following scenarios were discussed: (1) tracking and deployment of person-specific events and (2) eavesdropping and (ab-) use of epass data, especially the content of the so called Data Groups 1 and 2 (DG 1 and 2). The scenarios can be demonstrated as shown in Figure 4.7.

Using the Attack-Tree-Analysis-Methodology developed by Schneier (1999) the applicability of these scenarios by states, private organisations and criminal organisations was qualitatively analysed based on the first version of the epass (Meints and Hansen, 2008). This is still highly relevant, as epasses of the first version remain valid for five to ten years. The following tables summarise and visualise the results of the analysis, whereby the colours illustrate qualitatively the risk for the data subject (dark grey = low, light gray = medium, no background = high):

Table 4.3. Qualitative analysis of the tracking scenario

Tracking	States	Private Organisations	Criminal Organisations
Costs	High, but at insular places only	Very high; area covering infrastructure needed	Very high; area covering infrastructure needed
Benefit	Low apart from exceptional cases where traditional instruments of surveillance cannot be used	Limited, as cheaper, more target oriented and legal methods are available, e.g., in the context of customer loyalty programs	Limited, as cheaper and more target oriented methods are available, e.g., in the context of established surveillance techniques
Risks for the attacker	Low / none	High compliance risks (e.g., Data Protection in the EU), damage of reputation	Moderate / managed

Since November 2007 in most European countries the issuing of the second version of the epass started. This version was in most European countries improved by: (1) with respect to the entropy of BAC key; (2) information needed to prepare fall-back procedures in case biometrics for technical reasons (Failure To Enrol (FTE) or False Rejection Rate (FRR)) do not work; (3) maturity of the issuing process, as fingerprints are collected directly at the holder of the epass; and (4) additional security features in the chip to prevent cloning. These improvements make the eavesdropping scenario even more unlikely. But data protection risks grew, as with the photos of the finger prints additional biometric raw data are stored on the epass.

For immediate implementation FIDIS researchers recommend (Meints and Hansen, 2006; Kosta et al., 2007; Meints and Hansen, 2008):

Table 4.4. Qualitative analysis of the deployment-of-events scenario

Deployment of events	States	Private Organisations	Criminal Organisations
Costs	High, but at insular places only	High; but at insular places only	High; but at insular places only
Benefit	Low apart from exceptional cases where international laws are ignored and traditional instruments cannot be used	Limited, as cheaper, more target oriented and legal methods are available, e.g., in the context of customer loyalty programs	Effective for person-selective threatening, blackmailing and assassination
Risks for the attacker	Low / none	High compliance risks (e.g., Data Protection in the EU), damage of reputation	Manageable. The event can be prepared far in advance, criminals do not need to be in place. Violation of legislation seem 'acceptable and managed'

Table 4.5. Qualitative analysis of the eavesdropping scenario

Eavesdropping and (ab-)use	States	Private Organisations	Criminal Organisations
Costs	Very high; area covering infrastructure needed	High; at insular places or as area covering infrastructure	High; at insular places or as area covering infrastructure
Benefit	Very low as more easy and already legal alternatives are in place	Limited, biometric raw data, especially the highly standardised photo of the face, may be of interest; in many cases more simple and legal alternate solutions are available	Very low by using epass data for identity theft
Risks for the attacker	Low / none	High compliance risks (e.g., Data Protection in the EU), damage of reputation	Moderate / managed

- The epass should be protected using a Faraday cage
- Technical and organisational measures to hamper eavesdropping such as shielding of readers should be implemented
- The epass should be carried around only when needed
- With the second version of the epass the electronic time stamp should be updated before leaving the home country
- Passport holders need to be informed about organisational security measures concerning themselves
- The epass concept should not be transferred to national eIDs without modifications especially concerning the improvement of access control mechanisms

In the long run the following recommendations should be taken into consideration:

- The technical and security concept should be revised taking data and privacy protection aspects into consideration; in this context it should be checked especially whether protected templates or encapsulated biometrics could be used
- As the epass is deployed for international use, the security concept needs to take the control over the passport by many states and private organisations into consideration
- It should be considered whether a wireless technique is really needed; in any case the wireless data transfer needs to be secured more effectively
- As the epass is a component of a large information system, life cycle management is needed. In this context it should be checked carefully how long biometric reference data can be used without raising false rejection too much e.g., caused by aging of the epass holder.

4.5.2 CardSpace[51]

The software product CardSpace (Alrodhan and Mitchell, 2007) is an example for advanced identity management based on WS-Trust, WS-Security, WS-SecurityPolicy and some related protocols. CardSpace is the identity selector provided by Microsoft, which is shipped with Windows Vista and the .NET Framework 3.0 and later. It provides four major features:

- support for any digital identity system
- consistent user control of digital identity

[51] Authors: Stefan Brands, Microsoft; Laurent Bussard, EMIC; Joris Claessens, EMIC; Christian Geuer-Pollmann, EMIC; Ulrich Pinsdorf, EMIC.

- replacement of password-based Web login
- improved user confidence in the identity of remote applications.

Those principles follow the seven laws of identity (Cameron, 2005). CardSpace is built on top of the Web Services Protocol Stack. It uses WS-Security, WS-Trust, WS-MetadataExchange and WS-SecurityPolicy. This means that it can be integrated with other WS-* applications (Maler and Reed, 2008). In CardSpace a so called Information Card contains all claims which are associated with an identity of a user. If a web site shall accept Information Cards for authentication, the developer needs to add an <object> tag to the HTML code of the Web site. This tag declares what claims the Web site needs for authentication. The developer has then to decrypt and evaluate the token that CardSpace sends to the Web site. In an application based on Web services, CardSpace talks directly to the services using the aforementioned protocols to learn the service's policy requirements and to deliver the appropriate security token.

We typically rely on a number of different digital identity systems, each of which may use a different underlying technology. To think about this diversity in a general way, it is useful to define three distinct roles:

1. User is the entity that is associated with a digital identity.
2. Identity provider is an entity that provides a digital identity for a user.
3. Relying party is an application that in some way relies on a digital identity to authenticate a user, and then makes an authorisation decision.

Given these three roles, it is not difficult to understand how CardSpace can support any digital identity. A user might rely on an application that supports CardSpace, such as a Web browser, to access any of several relying parties. The user might also be able to choose from a group of identity providers as the source of the digital identity it presents to those relying parties. Whatever choice the user makes, the basic exchange among these parties comprises three steps:

First, the application gets the security token requirements of the relying party that the user wishes to access. This information is contained in the relying party's policy, and it includes things such as what security token formats the relying party will accept, and exactly what claims those tokens must contain. Once it received the details of the security token this relying party requires, the application passes this information to CardSpace, asking it to request a token from an appropriate identity provider. After this security token has been received, CardSpace gives it to the application, which passes it on to the relying party. The relying party can then use this token to authenticate the user or for some other purpose. Working with CardSpace does not require relying parties or identity providers to implement any proprietary protocols.

CardSpace implements an intuitive user interface for working with digital identities (see also Pettersson and Meints (2008) for usability aspects of selected func-

tions of CardSpace). Each digital identity is displayed as an Information Card. Each card represents a digital identity that the user can potentially present to a relying party. Along with the visual representation, each card also contains information about a particular digital identity. This information includes which identity provider to contact to acquire a security token for this identity, what kind of tokens this identity provider can issue, and exactly what claims these tokens can contain. By selecting a particular card, the user is actually choosing to request a specific security token with a specific (sub-)set of claims created by a specific identity provider. In fact, the user does not need to disclose the full information that is associated with an Information Card, but can verify what will be revealed to the relying party.

4.6 Summary and Conclusions

It is clear that it is essential to understand the impact which High-tech IDs can and may have on those that use them. The technologies analysed in this chapter provide tools (a) to form and shape partial identities under the control of the identity bearer or (b) to describe and model them under the control of external parties which are in many cases organisations. Both functions are of high importance in the Information Society which is characterised through intensive use of information in society and economy, facilitated by highly automated and digitised means of communication. In this way the technologies described already and will further fuel the information society in the near future. Also important in this context are economic aspects – the technologies analysed provide the platform for new products and services and thus economic welfare. But how are the functions described put to use?

The first function allows a user to present itself and to make claims in a new communicational context based on information that supports the level of trust needed. Important in this context is that the user gets some means to control the balancing between opacity and transparency regarding the disclosure of identity related information or attributes. The second function provides mechanisms needed to verify trust related information provided by the user through user independent sources of information and to verify claims made. In this context the access to more and more user independent sources for identity related information plays an important role. Both functions are not new as such; the difference with the described technologies is that they are (a) from a knowledge point of view demanding and (b) depending on the way they are used may change the balance between opacity and transparency between parties involved in communication. In this context organisations typically have more financial and personal resources for setting up more sophisticated IMS, potentially resulting in information, and thus power, asymmetry. Extreme application scenarios range from opaque and not trustworthy clients dealing somehow with organisations on one hand and completely transparent clients dealing with overly powerful and opaque organisations on the other hand. The technologies analysed clearly support both extreme scenar-

ios. An overly opaque client for example could be generated by the use of credential systems not relying on a trusted third party, and surveillance like application scenarios of DRM, biometrics and RFID or abuse of data collected in AmI environments clearly could enable overly powerful organisations.

In many cases a shift in this balance of transparency and opacity does not happen on purpose. Weaknesses in the technological design and security holes are common reasons providing the platform for a potential shift in the balance of power as control by operators and users gets lost. Real life abuse scenarios today in many cases seem to be criminally motivated (see Chapter 8).

Society cannot function with both of the described extreme communication models and thus will balance them mainly by developing moral, social and legal norms. FIDIS research results support this balancing process by recommendations for stakeholders in research, industry and policy making and the general public concerning:

- Application scenarios concerning available and emerging technologies with respect to compliance with the existing legal framework
- Organisational advice for citizens and clients of organisations on how to use established identity management systems or components thereof (e.g., the epassport)
- Further research topics e.g., in technology design to support balanced technical implementations with a reliable control situation
- Further development of legal frameworks to ban unwanted application scenarios and to provide the ground for improved and balanced technical solutions

It should be noted that most emerging technologies, such as AmI and ICT implants, are different as technological concepts and are not well developed and described. As such, their impact on humans and society cannot be assessed based on hard facts. In this context existing visions and partial technological concepts can be consolidated in scenarios which can be used for formal or non-formal analytical methods such as a Technology Impact Assessment (TIA) or Strength, Weakness, Opportunity and Threat (SWOT) analysis. Especially in case of ICT implants, the potential impact by far exceeds aspects of the management of identities – potentially the personality of the persons concerned may be affected or altered. On the other hand for policy makers there is no immediate need to act, other than on the issues surrounding their research and development, as these technologies are relatively far from being implemented and importantly, there is still time for a socio-ethical debate.

To summarise the FIDIS recommendations, the adoption of the legal framework to the advancement of new technologies should be accompanied by addressing the ethical and social issues that the development of new devices may bring. It is not only privacy and data protection that are at stake and the discussion on secu-

rity issues forms only a (temporary) part of the wider debate on how to live in tomorrow's information society. Respect for human dignity and equality and the freedom of thought, conscience and religion as well as the freedom to express, move, associate and assemble are only some of the rights and freedoms that are essentially at stake, where such activities suppose the increasing intervention of ICT and converging technologies provided and controlled by third parties.

References

Adler, A. (2003), 'Can images be regenerated from biometric templates?', Biometrics Conference, Washington.

Alkassar, A. and Husseiki, R. (eds.) (2008), *FIDIS Deliverable D3.9: Study on the Impact of Trusted Computing on Identity and Identity Management,* Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.9_Study_on_the_Impact_of_Trusted_Computing_on_Identity_and_Identity_Management.pdf.

Alrodhan, W. A. and Mitchell, C. J. (2007), 'Addressing privacy issues in CardSpace', Third International Symposium on Information Assurance and Security (IAS 2007), IEEE Computer Society, pp. 285-291.

Article 29 Data Protection Working Party (Art29DPWP) (2003), *Working Document on Biometrics,* WP 80, Brussels. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf.

Article 29 Data Protection Working Party (Art29DPWP) (2004), *Opinion on More Harmonised Information Provisions,* WP 100, Brussels. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.

Article 29 Data Protection Working Party (Art29DPWP) (2005), Working document on data protection issues related to RFID technology, WP 105, Brussels. http://www.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

Ballinger, K., Bissett, B., Box, D., Curbera, F., Ferguson, D., Graham, S., Liu, C. K., Leymann, F., Lovering, B., McCollum, R., Nadalin, A., Orchard, D., Parastatidis, S., von Riegen, C., Schlimmer, J., Shewchuk, J., Smith, B., Truty, G., Vedamuthu, A., Weerawarana, S., Wilson, K., Yendluri, P. (2006), Web Services Metadata Exchange (WS-MetadataExchange), BEA Systems Inc., Computer Associates International, Inc., International Business Machines Corporation, Microsoft Corporation, Inc., SAP AG, Sun Microsystems, and webMethods. Specification Version 1.1.

Baran, P. (1964), 'On Distributed Communications: IX. Security, Secrecy, and Tamper-Free Considerations,' Memorandum RM-3765-PR, The Rand Corporation, 1700 Main St, Santa Monica, California, 90406. Reprinted in Hoffman L. J. (ed.): Security and Privacy in Computer Systems; Melville Publishing Company, Los Angeles, California, 1973, pp. 99-123. http://www.rand.org/pubs/research_memoranda/RM3765/.

Bauer, M., Meints, M., Hansen, M. (eds.) (2005), *FIDIS Deliverable D3.1 Structured Overview on Prototypes and Concepts of Identity Management Systems,* Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf.

Becker, M. Y., Gordon, A. D., Fournet, C. (2006), SecPAL: Design and Semantics of a Decentralized Authorization Language, Technical Report MSR-TR-2006-120, Microsoft Research, Redmond.

Bizer, J. and Spiekermann, S. (2006), TAUCIS – Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, study commissioned by the German Federal Ministry of Education and Research, Berlin. https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf

Buitelaar, J.C., Meints, M., van Alsenoy, B. (eds.) (2008), *FIDIS Deliverable D16.1: Conceptual Framework for Identity Management in eGovernment,* Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp16-del16.1-conceptual_framework_for_identity_management_in_egovernment.pdf.

Cabrera, L. F. and Kurt, C. (2005), Web Services Architecture and Its Specifications: Essentials for Understanding WS-*, Microsoft Press, Redmond.

Cameron, K. (2005), The Laws of Identity, published as weblog. http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

Cavoukian, A. and Stoianov, A. (2007), Biometric Encryption, Ontario, Canada. http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf.

Coulouris, G., Dollimore, J., Kindberg, T. (2005), Distributed Systems. Concepts and Design, Addison Wesley.

De Cock, D., Wolf, C., Preneel, B. (2006), 'The Belgian Electronic Identity Card (Overview)', in *Sicherheit 2005: Sicherheit—Schutz und Zuverlässigkeit, Beiträge der 3. Jahrestagung des Fachbereiches Sicherheit der Gesellschaft für Informatik e.V. (GI),* Lecture Notes in Informatics (LNI), Bonner Köllen Verlag, Bonn, pp. 298-301. http://www. cosic.esat.kuleuven.be/publications/article-769.pdf.

Fischer-Hübner, S. and Hedbom, H. (eds.) (2008), *FIDIS Deliverable D12.3: A Holistic Privacy Framework for RFID Applications,* Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp12-del12.3.A_Holistic_Privacy_Framework_for_RFID_Applications_v2.pdf.

Gasson, M. and Warwick, K. (eds.) (2007), *FIDIS Deliverable D12.2: Study on Emerging AmI Technologies,* Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp12-d12.2_Study_on_Emerging_AmI_Technologies.pdf.

Gasson, M., Meints, M., Warwick, K. (eds.) (2005), *FIDIS Deliverable D3.2 A Study on PKI and Biometrics,* Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.2.study_on_PKI_and_biometrics.pdf.

Geradts, Z. and Sommer, P. (eds.) (2006), FIDIS Deliverable D6.1: Forensic Implications of Identity Management Systems, Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf.

Grimm, R., Puchta, S., Müller, M., Bizer, J., Möller, J., Will, A., Müller, A., Jazdejewski, S., (2005), *Privacy4DRM,* Study commissioned by the German Federal Ministry of Education and Research, Berlin. https://www.datenschutzzentrum.de/drm/privacy4drm.pdf.

Goodner, M., Hondo, M., Nadalin, A., McIntosh, M. Schmidt, D. (2007), Understanding WS-Federation, Technical Report, IBM and Microsoft Corporation.

Geuer-Pollmann, C. and Claessens, J. (2005), 'Web services and web service security standards', Information Security Technical Report, Vol. 10, pp. 15-24.

Hansen, M. and Alkassar, A. (eds.) (2008), *FIDIS Deliverable D3.8 Study on protocols with respect to identity and identification – an insight on network protocols and privacy-aware communication,* Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.8_Study_on_protocols_with_respect_to_identity_and_identification.pdf.

Hansen, M., Krasemann, H., Krause, C., Rost, M., Genghini, R. (2003), *Identity Management Systems (IMS): Identification and Comparison Study,* Kiel. https://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf.

Hansen, M. and Möller, J. (2005), 'Digital Rights Management zwischen Sicherheit und informationeller Selbstbestimmung', in: Bundesamt für Sicherheit in der Informationstechnik (BSI, ed.): IT-Sicherheit geht alle an!, proc. of the 9. German IT-Security congress of the BSI, pp. 159-171. http://www.datenschutzzentrum.de/vortraege/050510_hansen-moeller_bsi.htm

Heinz, B., Krißler, J., Rütten, C. (2007), 'Fingerspitzengefühl', *c't Magazin für Computertechnik* 12, pp. 98-101.

Hildebrandt, M. and Gutwirth, S. (eds.) (2008), Profiling the European Citizen. Springer.

Hildebrandt, M. and Koop, B. (eds.) (2007), *FIDIS Deliverable D7.9: A Vision of Ambient Law,* Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-d7.9_A_Vision_of_Ambient_Law.pdf.

Hildebrandt, M. and Meints, M. (eds.) (2006), *FIDIS Deliverable D7.7: RFID, Profiling, and AmI,* Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.7.RFID_Profiling_AMI.pdf.

Hill, C. J. (2001), Risk of Masquerade Arising from the Storage of Biometrics, Department of Computer Science, Australian National University, Canberra / Australia.

Humphrey, M., Park, S., Feng, J., Beekwilder, N., Wasson, G., Hogg, J., LaMacchia, B., Dillaway, B. (2007), 'Fine-grained access control for GridFTP using SecPAL', 8th IEEE/ACM International Conference on Grid Computing, IEEE Computer Society, pp. 217-225.

Iliev, A. and Smith, S. W. (2005), 'Protecting Client Privacy with Trusted Computing at the Server', IEEE Security and Privacy 3 (2), pp. 20-28.

Jacobs, I. (2002), Architectural Principles of the World Wide Web, W3C Working Draft, 30 August 2002 (outdated). http://www.w3.org/TR/2002/WD-webarch-20020830/.

Jain, A. K., Nandakumar, K., Nagar, A. (2008), 'Biometric Template Security', to appear in EURASIP Journal on Advances in Signal Processing. http://biometrics.cse.msu.edu/Publications/SecureBiometrics/JainNandakumarNagar_TemplateSecuritySurvey_EURASIP08.pdf.

Kerckhoffs, A. (1883), 'La cryptographie militaire', Journal des sciences militaires IX, pp. 5-38 and pp. 161-191.

Kindt, E. (2007), 'Biometric applications and the data protection legislation,' Datenschutz und Datensicherheit 31 (3), pp. 166-170.

Kindt, E. and Müller, L. (eds.) (2007), FIDIS Deliverable D3.10: Biometrics in identity management, Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.10.biometrics_in_identity_management.pdf.

Kosta, E.and Gasson, M. (eds.) (2008), *FIDIS Deliverable D12.6: A Study on ICT Implants,* Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp12-del12.6.A_Study_on_ICT_Implants.pdf.

Kosta, E., Gasson, M., Hansen, M., Meints, M. (2007), 'An analysis of security and privacy issues relating to RFID enabled ePassports', in *New Approaches for Security, Privacy and Trust in Complex Environments, proc. of the IFIP SEC2007,* Springer, New York pp. 467-472.

Kumaraguru, P., Cranor, L., Lobo, J., Calo, S. (2007), 'A Survey of Privacy Policy Languages', SOUPS 2007, Pittsburgh, PA, USA. http://cups.cs.cmu.edu/soups/2007/workshop/Privacy_Policy_Languages.pdf.

Lawrence, K., Kaler, C., Nadalin, A., Goodner, M., Gudgin, M., Barbir, A., Granqvist, H. (2008), WS-SecurityPolicy 1.3, OASIS Editor Draft 1.

Lawrence, K., Kaler, C., Nadalin, A., Kaler, C., Monzillo, R., Hallam-Baker, P. (2006), Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS Specification.

Lessig, L. (1999), Code and other laws of cyberspace, Basic Books, New York.

Maler, E. and Reed, D. (2008), 'The Venn of Identity: Options and Issues in Federated Identity Management', IEEE Security & Privacy 6, pp. 16-23.

McGee, E. M., Maguire, G. Q. (2007), 'Becoming borg to become immortal: regulating brain implant technologies,' Camb Q Healthc Ethics 16 (3), pp. 291-302.

Meints, M. and Hansen, M. (eds.) (2006), FIDIS Deliverable D3.6: Study on ID Documents, Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.6.study_on_id_documents.pdf.

Meints, M. and Hansen, M. (2008), 'Der ePass—eine Sicherheits- und Datenschutzanalyse', in: *Proceedings of the Sicherheit 2008, 2-4 of April 2008 in Saarbrücken*, Gesellschaft für Informatik, Bonn, pp. 31-43.

Müller, G. and Wohlgemuth, S. (eds.) (2007), FIDIS Deliverable D14.2: Study on Privacy in Business Processes by Identity Management, Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp14-del14.2-study_on_privacy_in_business_processes_by_identity_management.pdf.

Müller, G and Wohlgemuth, S. (eds.) (2008), FIDIS Deliverable D14.3: Study on the Suitability of Trusted Computing to support Privacy in Business Processes, Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp14-del14.3_Study_on_the_Suitability_of_Trusted_Computing_to_support_Privacy_in_Business_Processes.pdf.

Nadalin, A., Goodner, M., Gudgin, M., Barbir, A., Granqvist, H. (2008), OASIS WS-Trust 1.4, OASIS.

Pettersson, J. S. and Meints, M. (eds.) (2009), *FIDIS Deliverable D3.12: Study on Usability of Identity Management Systems*, to appear March 2009.

Pfitzmann, A. and Hansen, M., *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management,* TU Dresden, Dresden, February 2008. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf.

Pfitzmann, A. (2008), *Security in IT Networks: Multilateral Security in Distributed and by Distributed Systems,* TU Dresden, Dresden. http://dud.inf.tu-dresden.de/%7Epfitza/SecCryptI_II.pdf

Rannenberg, K., Pfitzmann, A., Müller, G. (1999), 'IT Security and Multilateral Security', in: Müller, G. and Rannenberg, K. (eds.): *Multilateral Security in Communications, vol. 3: Technology, Infrastructure, Economy*, Addison-Wesley, München, pp. 21-29.

Schneier, B. (1999), 'Attack Trees', *Dr. Dobbs Journal*. http://www.schneier.com/paper-attacktrees-ddj-ft.html#rf7.

Schreurs, W., Hildebrandt, M., Gasson, M., Warwick, K. (eds.) (2005), *FIDIS Deliverable D7.3: Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence,* Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.3.ami_profiling.pdf.

Tanenbaum, A. S. (2003), Computer Networks, forth edition, Prentice Hall, Upper Saddle River, NJ.

Zhou, X., Kevenaar, T., Kelkboom, E., Busch, C., van der Veen, M., Nouak, A., (2007), 'Privacy Enhancing Technology for a 3D-Face Recognition System', BIOSIG 2007: Biometrics and Electronic Signatures, pp. 3-14. http://www.3dface.org/files/papers/zhou-CAST2007-TemplateProtection.pdf