FIDIS

Future of Identity in the Information Society

Title:	"From Regulating Access Control on Personal Data to Transparency by Secure Logging"
Author:	WP14
Editors:	Günter Müller, Sven Wohlgemuth (ALU-FR)
Reviewers:	Vashek Matyas (MU), Jozef Vyskoc (VAF)
Identifier:	D14.6
Type:	[Deliverable]
Version:	1.0
Date:	Monday, 05 October 2009
Status:	[Final]
Class:	[Public]
File:	fidis_wp14_d14.6_From Regulating Access Control on Personal Data to Transparency by Secure Logging_v1.0

Summary

Identity management controls the disclosure of personal data of data providers to data consumers. However, data providers do not obtain an indication as to whether data consumers use personal data according to the agreed privacy policy. Data providers are left with a number or privacy promises or expectation but do not get evidence that data consumers followed the agreed privacy policy. This deliverable proposes a "privacy evidence" by investigating on the data usage of data consumers for given data providers. This proposal is based on log views on accesses to personal data which can be checked by data providers on the compliance with privacy policies. Building blocks of system architecture for "privacy evidences", their requirements and approaches for their realisation are presented.

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

Copyright Notice:

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

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	03.11.2008	Initial release with sketch of table of contents (Sven Wohlgemuth)
0.2	11.11.2008	Chapter 4.3 "International Security Related Standards" added (Martin Meints)
0.3	21.11.2008	Chapter 3.2 "Legal Requirements" added (Brendan Van Alsenoy)
0.4	26.11.2008	Chapter 5.1 "A Policy Language for AmI Systems" added (Günter Karjoth)
0.5	26.11.2008	Chapters 4.1 "Secure Logging by Cryptography" and 4.2 "Enforcement Mechanisms based on Trusted Computing" added (Stefan Berthold)
0.6	27.11.2008	Chapter "Conclusion" added (Sven Wohlgemuth)
0.7	03.12.2008	Version for FIDIS internal review (Sven Wohlgemuth)
1.0	29.12.2008	Submission version, revised according to the comments of the FIDIS internal review (Sven Wohlgemuth)
1.1	05.10.2009	Correction on p.19. after that v1.0 of this deliverable has been accepted by the EU reviewers (Maike Gilliot, Brendan Van Alsenoy)

Foreword

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

Chapter	*Contributor(s)*
1 (Executive Summary)	Rafael Accorsi and Sven Wohlgemuth (ALU-FR)
2 (Personalisation in Ambient Intelligence Systems)	Rafael Accorsi, Stefan Sackmann, Jens Strüker and Sven Wohlgemuth (ALU-FR)
3 (Requirements for Privacy Evidences based on Log Views)	Rafael Accorsi (ALU-FR), Sebastian Höhn (ALU-FR), Brendan Van Alsenoy(ICRI) and Sven Wohlgemuth (ALU-FR)
4 (Related Work on Secure and Privacy-preserving Logging)	Stefan Berthold (TU Dresden) and Martin Meints (ICPP)
5 (Approaches for Privacy Evidences)	Rafael Accorsi (ALU-FR), Matthias Bernauer (ALU-FR), Günter Karjoth (IBM ZRL) and Sven Wohlgemuth (ALU-FR)
6 (Conclusion)	Rafael Accorsi (ALU-FR), Stefan Berthold (TU Dresden), Stefan Sackmann (ALU-FR), Jens Strüker (ALU-FR) and Sven Wohlgemuth (ALU-FR)

Table of Contents

1 Executive Summary

In a technological setting where some even prophesy the death of privacy (Froomkin, 2000), the need for approaches to mediate and legislate for the collection of personal attributes and their usage is increasingly gaining in momentum and relevance. While such an investigation involves interdisciplinary efforts, we focus on the technical aspects. In this context, identity management systems (henceforth IMS) play an essential role in circumventing the privacy threats inherent to the deployment of information technology. They allow data providers to selectively disclose attributes to data consumers, possibly enabling data providers to formulate policies under which collected attributes can or cannot be employed.

The rationale of IMS is to convey a sense of control to data providers, where the "control" stands for the regulation of attribute disclosure. However, data providers today obtain no indication as to whether data consumers actually behave according to the policies agreed upon. Put other way, data providers are left with a number of privacy promises or expectations, but obtain no creditable evidence that their policies have been adhered to. Thus, this setting clearly fails to reproduce the established understanding of control individuals have in mind, in which control comprises not only the regulation of a set of activities, but also the supervision that this set of activities indeed takes place as expected. As a result of lacking supervision, data consumers often fear that their personal attributes could be (unauthorized) shared with third parties or used for purposes other than those stated (Sackmann, Strüker and Accorsi, 2006).

We close this gap by investigating the technical building blocks necessary to realise supervision in Ambient Intelligence systems, i.e. open and adaptive systems based on ubiquitous computing technologies (Kenneally, 2004). Addressing supervision requires a conceptional change, though. Traditional IMS build on observability, unlinkability and unidentifiability and therefore use a number of techniques, such as pseudonyms and partial identities over anonymous communication channels (Wohlgemuth and Müller, 2006). In addition to this, recent IMS allow data providers to formulate policies and stick them to data, a concept called to as "sticky policies" (Casassa-Mont, Pearson and Bramhall, 2003). (We refer to (Bauer, Meints and Hansen, 2005) for a comprehensive survey on techniques for IMS.) Thus, current techniques aim at an a priori, preventive protection of privacy. In contrast, when investigating supervision we found ourselves in an a posteriori setting where techniques to verify the compliance with privacy policies are needed.

To realise this, we employ the concept of privacy evidence (Sackmann, Strüker and Accorsi, 2006). Its rationale is to make the behaviour of the data consumer regarding data collection and enforcement of privacy policies evident to data providers. Intuitively, privacy evidence is one record consisting, on the one hand, of all the information collected from and related to a particular data provider – a so-called log view – and, on the other hand, the result of an automated audit of this log view based on the policies of the data provider. Together, these pieces of information build the basis for supervision and thereby pave the way for a holistic realisation of control.

The thesis we purport is that investigation towards a holistic realisation of control for informational self-determination in IMS is indispensable. Due to the improved transparency inherent to privacy evidence, such realisation of control has the chance to increase the confidence placed on the data consumers and even foster the willingness to disclose personal attributes, which is an essential factor for the acceptance of dynamic system in general and for the deployment of personalised services (Strüker, 2007) in particular. Eventually, both data providers and data consumers could equally profit from such an extended notion of control.

This deliverable is structured as follows:

Chapter 2 presents a scenario for personalised services in Ambient Intelligence and the problem that data providers are not able to control the enforcement of agreed privacy policies by data consumers. It argues that context data of a user, collected among others by RFID reader and video surveillance, becomes also personal data. Since today's privacy technologies focus on the disclosure of personal data but not on the enforcement of their use, privacy policies cannot be enforced by users. An approach for an ex post enforcement is the creation of privacy evidences by checking the logs concerning the usage of personal data.

Chapter 3 introduces the building blocks of an information system to create privacy evidences by its requirements. These requirements stems from legislation and technology. They essentially consider the basic building block for privacy evidences: secure logging of accesses on personal data by data consumers.

Chapter 4 investigates on the suitability of existing work on secure and privacy-preserving logging and shows its advantages and disadvantages.

Chapter 5 presents our approaches for realising the building blocks: privacy policy language, secure logging, logs views and automated audits. Chapter 6 concludes our work.

2 Personalisation in Ambient Intelligence Systems

Fifteen years after Mark Weiser's inspiring paper on ubiquitous computing (Weiser, 1991), his vision has become technically feasible. Objects of everyday use has already became increasingly interconnected and mobile communication of all bandwidth and devices of all sizes are used in various ways. Ambient Intelligence systems (AmIS) are emerging, bringing new challenges for the management of information systems: having to cope with components that enter and leave the system spontaneously and be autonomous in their actions. The changing and possibly conflicting requirements of the single components have to be taken into account leading to a dynamic negotiation of requirements. Moreover, such dynamic systems have to be able to contend with constant growth of communicated data avidly collected in various forms.

Solving the challenges of AmIS is accompanied with a prospect of economic potential. A first realization is the present rollout of AmIS by major retail groups worldwide. Currently, cost savings through process automation is of prime importance but the use of this technology in retailing goes beyond mere productivity improvements. Tagging items with RFID-chips in combination with other wireless technologies, equipping customers with mobile communication devices, and using upcoming sensor-networks allow, for example, personalizing services that have so far been successfully used in client-server e-commerce scenarios (Murthi and Sarkar, 2003).

2.1 From Anonymous to Personalised Shopping Experience

Internet has substantially changed the way of personalisation. As depicted in Figure 1, three ways of tailoring services to customers can be distinguished. Firstly, online retailers use the Internet today on a large scale to recommend products to known customers according to their previous purchases or interests (Srikumar and Bhasker, 2005). These personalised services build upon a one-to-one communication channel and require personal data as input factor. Secondly, retailers also use the Internet to offer individualised services, which do not require personal data. For instance, the recommendation of products according to the sequence of clicks, pages requested or items that have been added to the shopping cart. Since such individualised services can be realised without necessarily identifying the customers, they allow improved shopping experience, at the same time maintaining their anonymity. Thirdly, universal services such as a product search function or having a look at customer reviews need neither personal nor context data. Even so, they are a form of personalisation because a single customer can choose a service that meets his needs at a particular time. All three kinds of services can be part of a personalisation strategy with the objective of building up customer relationships, increasing customer satisfaction, generating a 'lock-in' situation, and in the end realizing higher turnover.

Today, consumers are faced with thousands of products in a physical store and have to walk far to find them. The introduction of Ambient Intelligence Systems (AmI) systems in stationary retailing enables an electronic one-to-one communication channel and allows the collection of context data comparably cheaply and effectively as in current e-commerce environments. In grocery stores such as the 'Extra-Future-Store' in Germany, computers with a touch screen attached to a shopping cart are deployed as personal shopping assistants (PSA) (Litfin and Wolfram, 2006). Today, these devices are equipped with a barcode reader and customers can interact with the retailer's information system over WLAN. Future forms of interaction may include customers using their mobile phones to communicate with RFID-tagged products and the retailer's information system (Litfin and Wolfram, 2006). Furthermore, sensors embedded in customers' clothing or products might also become the subject of interactions. Such a technical infrastructure enables the context of each customer to be taken into account, for example the current position within the store or the products in the cart. Combining all this context data in real time with customers' personal data and profiles already stored in the information system, the retailer can use the electronic interaction channels (PSA, mobile phone) to enrich customers' shopping experience.

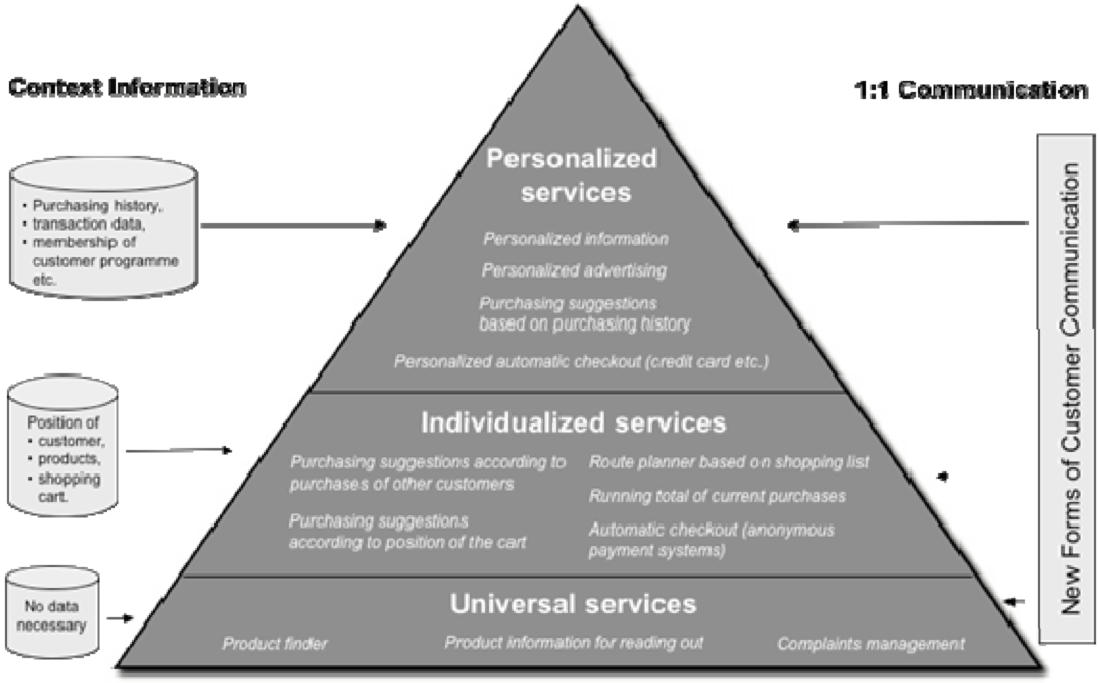

Context Information
1:1 Communication
• Purchasing history,
• transaction data,
• membership of customer programme etc.
Position of
• customer,
• products,
• shopping cart.
No data necessary
Personalized services
Personalized information
Personalized advertising
Purchasing suggestions based on purchasing history
Personalized automatic checkout (credit card etc.)
Individualized services
Purchasing suggestions according to purchases of other customers
Purchasing suggestions according to position of the cart
Route planner based on shopping list
Running total of current purchases
Automatic checkout (anonymous payment systems)
Universal services
Product finder
Product information for reading out
Complaints management
New Forms of Customer Communication

Figure 1 Personalisation pyramid (Sackmann, Strüker and Accorsi, 2006).

Imagine a customer equipped with an appropriate mobile communication device entering a store. To find a certain product, the customer can feed its name into the device and gets its location displayed. To obtain additional information, for example a list of possible recipes using this product or information about its origin, the customer scans the RFID-tagged article. Retailers are able to provide such universal services to all customers without necessarily taking the differences between each of them into account. Individualised services, however, additionally require data of the customer's context as input factor. For instance, a shopping list can be used to optimize the route through the store for time-sensitive or handicapped shoppers. Moreover, special offers or purchasing suggestions can be displayed according to the position of the cart within the store and the products in the cart. The mobile device can also show a running total of current purchases at any time, thereby enabling the customer to control expenditure. Finally, offering personalized services requires personal data such as name, age, purchasing history, or membership in a customer program. By identifying the customer, for example by means of an RFID-tagged customer card, the display can show further items as suggestions based on former purchases. Combining context and personal data is also useful. On the way through the store, special offers can be displayed on the screen according to position and personal needs e.g. fat-free or whole food products. In this manner, allergy sufferers can, for instance, be warned about certain ingredients of products. Finally, thanks to personalized automatic checkouts the customer has no need to rummage for cash, pull out cards or have to queue (Strüker and Sackmann, 2004).

2.2 Context Data Becomes Personal Data

Although the economic potential of personalisation in stationary retailing seems lucrative for retailers and customers, retail groups have slowed down their activities in this area. While Wal-Mart combined RFID-tagged articles with video surveillance, the German Metro Group tried to establish customer loyalty cards with embedded RFID tags (Chicago Sun-Times, 2003). However, after the sharp criticism of privacy activists, Metro decided to drop the use of RFID tags in cards and Wal-Mart also stopped their RFID-based surveillance[1]. If customers were to refuse the processing of context data within the store in general, neither individualised nor personalized services would ever come into being. An analysis of the decisive privacy concerns shows that the loss of control over personal data worries customers. According to a survey of more than 1,000 U.S. consumers, two-thirds identified as a major concern the likelihood that RFID would lead to their data being shared with third parties (RFID, 2008).

Such exploiting sensor networks, RFID identification, automatic video surveillance, localization technologies, and other technologies in AmI undermines the users' desire to control personal data. Extensive and unobservable data collection is an inherent characteristic of AmI:

- Data is increasingly being collected without any indication. There will be no red indicator light on each device signalling the recording of data (Langheinrich, 2005).
- Data collection takes place without any pre-defined purpose, for example, the shopping cart continuously defines and reports its position to the retailers' information system. This information can be used for optimising the store arrangement, for generating purchase suggestions as well as for identifying the customer.
- Data once collected will be persistent and not deleted due to continuously decreasing cost of data storage.
- Different devices record each event simultaneously from different view points, for example, a customer browsing a product is recognized by the smart shelf as well as by the video surveillance or the shopping cart. The combination of these different views allows, in combination with further context data, recognition or even identification of the customer.
- Recording devices register multiple events simultaneously, for example, video surveillance can record customer A browsing a certain product, customer B passing the corridor, and customer C e.g. stealing a chocolate bar. The interpretation of the logged raw data for various purposes and the extraction of single events make the assignment of a valid privacy policy impossible.

[1] Cf. http://www.bigbrotheraward.de

The realization of AmI leads to a paradigm shift of data collection and facilitates the relation of context data to individuals. The borderline between context data and personal data increasingly vanishes.

2.3 Today's Privacy Technologies Support Obscurity

The inherent data collection in AmI obliterates present-day privacy-enhancing technologies (Langheinrich, 2005) because they are all based on concealing data - a privacy approach referred to as 'obscurity' throughout this study. Today's privacy mechanisms are incompatible with the objective of any retailer to provide both: personalisation with useful services and assured privacy as well as security.

In Table 1, a classification of privacy mechanisms is given. In the horizontal columns, the mechanisms are classified according to what they control: access or usage. While access control is usually understood as ex ante defined authentication and authorisation, usage control extends access control and encompasses all those mechanisms that actually deal with the run time detection of privacy violations. In the vertical columns, guidelines, mechanisms and approaches for privacy are distinguished in whether they enable all three forms of personalisation.

	Privacy Guideline	**Privacy Mechanisms**	**Current Examples**	**Enabling Personalisation**	**Privacy Approach**
Access Control	Controlled disclosure of personal data	Anonymity	MIX networks, JAP, Anonymizer (Köpsell, Wendolsky and Federrath, 2006)	No	Obscurity
		Pseudonyms, Identities	Identity Management, e.g. IBM idemix, Liberty Alliance, Shibboleth, iManager (Wohlgemuth and Müller, 2006)	Yes	Obscurity
	Agreement on data collection	Policies, Seals, Certificates	P3P, EPAL, Privacy Aware System (PawS) (Langheinrich, 2005)	Yes	Transparency based upon past
Usage Control	Transparent processing and usage	Monitoring processing of personal data	Obligations and Conditions	Yes	Transparency based upon past *and* present
	Enforcing policy-compliance	**Evidence Creation**	**Secure Logging and Auditing**	**Yes**	**Transparency based upon past *and* present with ex post enforcement**

Table 1 Privacy and transparency (Sackmann, Strüker and Accorsi, 2006).

Anonymity, for example, prevents personalized services that require an identification of the customer. Pseudonyms and identity management, as the most favoured solutions of science and industry, allow personalised services. Both privacy mechanisms follow the obscurity approach and rely on controlled disclosure of data, reducing such a disclosure to the minimal necessary to perform a given transaction. As a result, personalisation is limited to the amount of disclosed data. However, the extensive and unobservable collection of context data for providing individualised services already allows the recognition of customers. This is because transactions are part of a chained process: e.g. filling the shopping cart, walking through the isles, scanning products and payment.

Obscurity, as a privacy approach for personalisation in AmI, is inadequate. Once the access to data is granted, there is no control for customers as to how data is used – irrespective of the retailer's initial intention. Proof of being an "honest" retailer acting according to data protection laws and the declared privacy policy can be produced by making data storage and data usage transparent. Different institutions providing a first step to transparency already exist: certification authorities, trusted third parties, privacy seals, code of conduct, or privacy policies are implemented as a pre-defined agreement regarding the data usage. A promising approach is to supply tools to define individualized privacy and security policies and languages to express it. Currently, the most favoured language for expressing privacy policies is P3P (Platform for Privacy Preferences). P3P uses XML- specifications that state: (a) what kind of data is to be stored; (b) how data is to be used; and (c) its permanence and visibility, that is, how long data is to be stored and the corresponding access rights. Customers, admittedly, can express their desires but are not able to control the usage of their data. On the retailer's side, the rules for access are derived from the specified and possibly individualised privacy policies, for example by translating a valid P3P policy into EPAL (Enterprise Privacy Authorization Language), a formal language to express fine-grained enterprise privacy policies.

An AmI system is only privacy-aware if it enforces formalized and personalised privacy policies. Such enforcement can be based upon past information (access control mechanisms), present and derived information (usage control). Enforcement can be achieved by an information system that has been proven to fulfil the desired properties, in particular self-limitation, and can expect to gain customers' trust by the resultant transparent access to personal data.

However, the characteristics of AmI restrict the effectiveness of formulated policies with regard to their adaptation. On the one hand, the autonomous components mean an increasing complexity for modelling the system and hinder the proof of their behaviour. On the other hand, the changing manner of data collection rules out the assignment of a formulated privacy policy to personal data required for enforcing formulated policies: e.g., data collected outside the scope of a formulated policy, data collected by multiple devices is not integrated and related to a policy in real time, and data collected describing different events inherently interwoven may lead to conflicting policies. Technically, research could pursue the development of an adaptive 'P3P' or the control of the actual usage of data. First efforts try to prevent an unintended usage of data in real time as pursued, for example, by Park and Sandhu (Park and Sandhu, 2004) or Pretschner, Hilty and Basin (Pretschner, Hilty and Basin, 2006).

2.4 Conclusion

Instead of seeking for an ex ante approach to privacy transparency, we introduce in the following the concept of *privacy evidence* for *ex post* enforcement of privacy policies. Transparency in AmI is provided by a cooperative mode between technology for detection and enforceable privacy contracts. The enforcement of privacy contracts requires for all involved parties the possibility to detect privacy violations – e.g. by means of audit – and document in a way that is acceptable as evidence, e.g., in a legal dispute. As depicted in Figure 2, the creation of evidence depends on: policies as reference for a compliant usage of data; and log views that encompass all data about an individual stored in an information system. Secure logging provides log views in such a manner, that access control decisions of a data consumer concerning personal data of a given data provider (customer) are recorded. In doing so, a record will always be in relationship with previous records concerning the same data provider and his personal data. The following section introduces an architecture for creating privacy evidence. Section 4 investigates on related work on the foundation of privacy evidences: secure logging. Section 5 presents our solution for secure logging, whereas section 6 concludes our work.

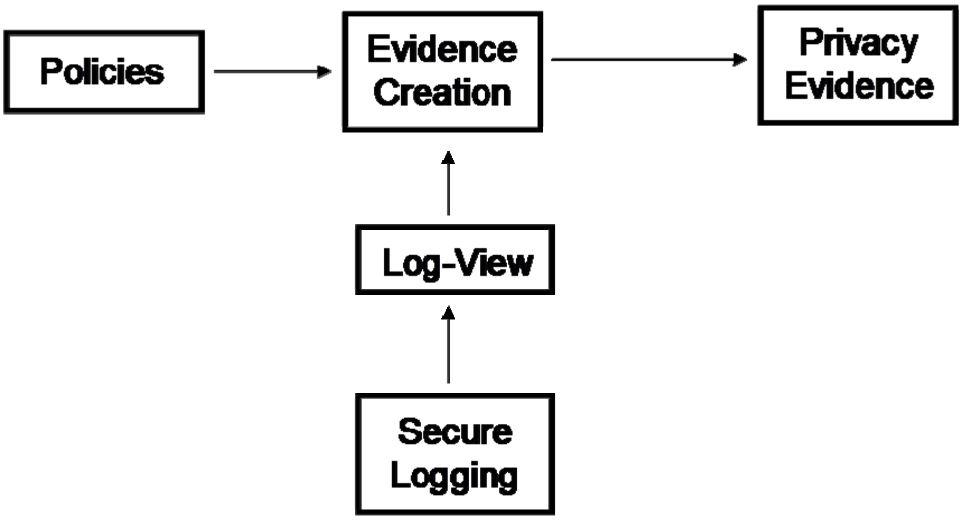


Figure 2 Privacy Evidence Creation (Sackmann, Strüker and Accorsi, 2006).

3 Requirements for Privacy Evidences based on Log Views

Privacy evidences are a proof of data consumers' behaviour concerning the usage of personal data. Usage of personal data means technically access on personal data by services of a data consumer. The behaviour of a data consumer reflects whether he follows the agreed privacy policy. To identify this kind of behaviour, a data provider should know the granted accesses of a data consumer on personal data and be able to check them against the agreed privacy policy. In the following, section 3.1 presents a system architecture for creating privacy evidences by its building blocks. The foundation of privacy evidences which should be created by this system are log views. The legal and technical requirements for a secure logging service concerning accesses on personal data are summarized in the sections 3.2 and 3.3.

3.1 Technical Setting and Building Blocks

The realisation of privacy evidence anticipates the steps depicted in Figure 3. In (1), a data provider A formulates a policy P_A and communicates it to the data consumer. Since we consider Ambient Intelligence systems with implicit interactions, we assume that policies are communicated before joining the system. (Implicit interactions take place without the awareness of the data provider.) When interacting with the system, many events are recorded as entries in log files (2). In fact, we assume that every event is recorded, so that log files offer a complete digital representation of the activity in a dynamic system. At some point in time the data consumer may retrieve the log view S_A containing all the log entries related to A (3). A can then visualise the collected data and start a third-party automated audit process (4) to check whether the policies P_A have been adhered to, thereby generating the corresponding privacy evidence (5).

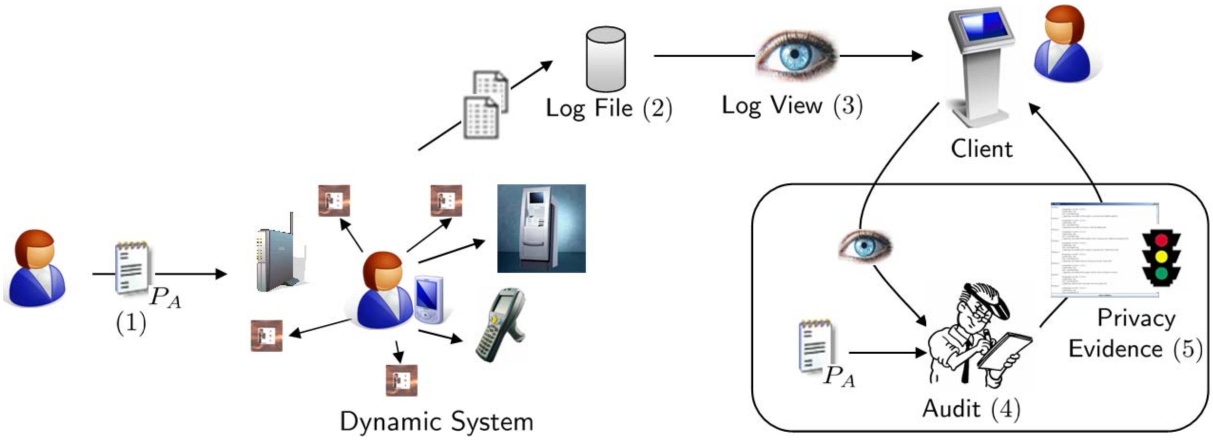


Figure 3 The workflow for privacy evidence (Accorsi, 2008).

To realise privacy evidence, the following central technical building blocks are essential: a *policy language* for the expression of privacy preferences in Ambient Intelligence systems; *log views* to allow the visualisation of recording activity; a secure logging to ensure the authenticity of recorded data, in particular to improve the credibility of log views; and an *automated audit process* for checking the adherence to policies.

In our work, we consider the following *assumptions*. First, every event happening in the system, as well as every access to collected data is recorded as an event in a log file. Second, on interacting with the system, data providers are identified while the events they are involved in are recorded. That is, the entries in the log file are always related to a data provider. Third, while the system is dynamic in that it adapts itself to the data providers' preferences, it is static regarding the data collection possibilities. Technically, this means that the ontology describing the system does not change over time and, hence, the policies of data providers do not become obsolete. Although these assumptions do not hold in general, they hold for some scenarios, as the one we consider.

3.2 Legal Requirements

Every data subject (in the following meant as data provider) has a general right of access with regards to his or her personal data. Upon request, data controllers (in the following meant as data consumers) are obligated to acknowledge whether or not they process data relating to that particular data provider and provide him with information as to the purposes of the processing, the categories of data concerned, and the (categories of) recipients to whom the data are disclosed. Data consumers are also required to communicate in an intelligible form the data that is being processed itself as well as any available information as to their source. The data provider also has a right to learn the logic of the automated processing, certainly in the case of 'automated decisions'[2]. In other situations the scope of this last right is dependant upon the national implementation of the Directive (art. 12 Directive 95/46/EC of (European Parliament and Council, 1995)).

A major complication for the exercise of the right of access is caused by the fact that the data subject will often not know exactly which entities are in fact processing personal his personal data, let alone which entities are acting in the capacity of a controller in doing so.[3] In the proposed architecture data providers have the ability to see which entity has performed actions upon his personal data through so-called "log views" (cf. section 5.3). A portal providing such log views could be of great assistance to data subjects that have fallen victim of unlawful data processing in their search for remedy. It could also, as indicated earlier, be a way to enhance trust in the compliance by data consumers.[4]

[2] Art. 15 (1) of Directive 95/46/EC defines an automated decision as 'a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.'

[3] To reduce the latter complication the Belgian legislator has attempted to introduce some relief in art. 32 of the Royal Decree which accompanies the Data Protection Act: the data subject may also direct its request to any entity processing the information on behalf of the controller (Royal Decree of 13 February 2001, *Belgian State Gazette*, 13 March 2001).

[4] We note that the portal might also be of particular use in those instances where the data subject has not been notified pursuant to art.10-11 of Directive 95/46/EC. Although there is in principle an obligation for the controller to do so, there are nevertheless several exceptions. Furthermore, the nature of the interactions in AmI might make it increasingly difficult to effectively comply with this provision.

3.2.1 Data Protection and Logs

If the aforementioned portal providing log views is meant as a means to satisfy consumers' obligations under art. 12 of the directive, it is necessary that all the elements enumerated in that provision are in fact provided through the portal. This may be particularly difficult to realize in AmI where interactions might be too complex to register all the elements for each data processing. The portal could then still nevertheless be useful to data providers in identifying the entities responsible for the processing of their data, to which they could direct their further requests.

Logging and auditing are considered standard components of information security management (cf. section 4.1). Many national data protection authorities have consequently referred to these measures as being quasi-obligatory pursuant to the controller's security obligation under articles 16-17 of Directive 95/46/EC. For instance, the Belgian Privacy Commission has stated that every data controller should install some type of a 'logging and tracing mechanism'. Such a mechanism should be designed to allow identification of each user that has accessed the personal data at a given time, and which processing operations that user has performed with regards to the data. The final level of detail with which such a mechanism should operate depends on the context, e.g. nature of the data, risks, … (Belgian Privacy Commission, 2008).

By logging every action performed upon personal data, one can create an audit trail ("who did what and when"), which can later be reviewed for compliance (Koom, 2007). If logs are to be used for auditing purposes, it is important that a logged event can not be altered or deleted without this being noticed (Wouters, Simoens, Lathouwers and Preneel, 2008; Broucek and Turner, 2004). Appropriate measures should therefore be in place to ensure the *integrity* of the logs. This requirement can be derived from the data consumer's general security obligation (when the nature of the data being processed and risks are such to reasonably justify the expense), but may also stand as a functional requirement in order to, as will be discussed later, increase the probative value of the logs. Other requirements which map with security objectives in this context include *authenticity* of logged events and ensuring the *completeness* of the logs (see also infra, section 3.3).

Finally, it should also be noted that the data contained in logs generally also qualifies as personal data itself. In first instance, the log files represent actions performed by individual entities which might be natural persons. The personal nature of the data however not only stems from the actions performed by data consumers, but also from the fact that what is being registered in AmI shall often include interactions of a particular data provider with its environment. It is therefore also required that the logs themselves are in compliance with data protection regulations[5], and that all appropriate measures are taken to ensure the *confidentiality* of the data they contain.

3.2.2 Evidentiary Value of Logs

Another goal of the proposed framework is to document processing operations in such a way that it generates evidence in a manner that is 'legally acceptable'. An extensive overview of

[5] In addition to general data protection legislation, consideration should also be given to possible sector-specific legislation, such as those relating to privacy protection of employees and the monitoring of their actions in the workplace.

case law and acceptance of electronic evidence by courts has already been provided in FIDIS deliverable D6.1 (Geradts and Sommer, 2008). We therefore limit ourselves to highlighting those aspects relevant to our further analysis.

There are in fact two distinct legal issues that will determine whether an item or data will be suitable for evidentiary purposes. The first issue relates to the question of *admissibility*. Member States have different rules regarding which types of evidence which may be considered for a particular dispute. The rules relating to the admissibility of evidence may also vary from one legal subject to another (Leroux, 2004). For instance, in France and Belgium there is far greater flexibility in trade matters (commercial proceedings) than in civil proceedings, in which written proof is often a requirement. For legal facts however (such as negligence or the violation of a statute), the necessity of written evidence does not apply, because such events cannot be foreseen.[6] This implies that under those legal systems, there is freedom of evidence when seeking remedy for data protection violations. The rules of admissibility in common law systems are more complex. There are several exclusionary rules which may stand in the way of submitting logs (or the information contained therein) during proceedings, such as the hearsay rule and the 'best evidence' rule (Leroux, 2004). These rules are in turn subject to their own exceptions, which makes it difficult make a general statement as to the admissibility of logs under these systems (Kenneally, 2004).

Many legal systems require that evidence was obtained by 'lawful means', i.e. that no illegality was committed when it was gathered. The sanction for unlawfully obtained evidence does vary significantly. Under Belgian law such evidence must typically be excluded, whereas English courts often have great flexibility in accepting or refusing evidence that was obtained improperly (Leroux, 2004). Evidence obtained in violation of data protection regulations therefore runs a risk of being declared inadmissible, depending on the legal system and the relevant facts.[7]

The second aspect determining whether or not the 'privacy evidences' registered in the log files will be of use to aggrieved data subjects in the vindication of their rights concerns the *probative value* of this type of evidence. Even if an item is considered admissible as evidence, it may be of relatively little value if it is not at all persuasive. The probative value of evidence refers to its usefulness in proving or disproving a particular fact (Black's Law Dictionary, 2004).

There are no harmonized European norms concerning either the admissibility or probative value of digital evidence. There is of course one very significant exception, namely Directive 1999/93/EC on a Community Framework for electronic signatures (European Parliament and Council, 1999). This Directive obligates Member States recognize and provide legal effectiveness for electronic signatures (art. 5). National legislation must ensure that 'advanced & qualified' electronic signatures, created by a secure-signature-creation device (SSCD), are given the same evidentiary value as handwritten signatures do in relation to paper-based data

[6] O. Leroux, *l.c.*, 199-200. It could also be argued that in either event the data contained in logs can at least serve as prima facie evidence ('*commencement de preuve par écrit*'; '*begin van bewijs*'), which acts as an exception to the requirement of written proof under both the Belgian and French system. See also *infra*; concerning art. 16, § 2 the Belgian Law implementing the e-Commerce Directive.

[7] See also M. Asinari, 'Legal constraints for the protection of privacy and personal data in electronic evidence handling', *International Review of Law, Computers & Technology*, 2004 , vol. 18, n° 2, 231-250.

(art. 5.1). Electronic signatures that do not meet all the requirements to be put on par with hand-written signatures may not to be denied legal effectiveness or admissibility as evidence for that reason alone (art. 5.2).

There has been quite some discussion as to the exact scope and implications of the eSignature Directive for identity management systems (Graux, 2007). The controversy focuses primarily on whether or not the eSignature Directive also covers entity authentication. There appears to be no dispute however that the Directive covers other forms of data authentication than those that are implemented to signify agreement with a particular document.[8] Although the Directive only holds that electronic signatures mentioned in art. 5.2 should not be denied legal effectiveness merely based on the fact that they are not advanced, qualified, or generated by a SSCD within the meaning of the Directive, this is still an important qualification as it reflects the principal admissibility of other forms of data authentication as proof (without however making any judgment as to their value or prohibiting other possible grounds of exclusion).

The e-Commerce Directive (European Parliament and Council, 2000) does not explicitly deal with admissibility or value of digital evidence. Several Member States have however updated their national provisions concerning written evidence at the occasion of its implementation. For instance, art. 16, § 2 of the Belgian law9 implementing the e-Commerce Directive provides that 'the requirement of an evidence in writing shall be satisfied by a succession of intelligible characters which can later be accessed, regardless of its carrier or the modalities of transmission.' Needless to say, such digital data will only be automatically put on par with a signed document if it is accompanied by an advanced and qualified electronic signature within the meaning of art. 5.1 of the eSignature Directive (and meets all the conditions stipulated in the annexes of this Directive).

Once determined to be admissible, courts are generally free in their appreciation of the probative value of the evidence which has been submitted. In other words, judges have a great deal of discretion in deciding what weight to accord a particular item of evidence. In some instances national legislation does prescribe a specific probative weight for certain types of evidence, such as documents produced by government officials or notaries. But generally speaking, computer-derived evidence will need to have the same attributes as conventional evidence in order to be as persuasive: it should be authentic (in the sense that it is possible to positively tie the evidentiary material to the incident), reliable (in the sense that the evidence must have been collected and handled in a way that does not create doubts as to its authenticity and veracity), as complete as possible, and believable (Leroux, 2004). In complicated cases, the court is likely to appoint an expert to assist it in establishing its relevance and credibility.

[8] Based on the definition of electronic signatures in art. 2, 1 of the eSignature Directive ("electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication'). See also CEN/ISSS, 'Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects', CWA 14365-1, March 2004, p. 15, available at ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14365-01-2004-Mar.pdf (last accessed 18 November 2008).

[9] Law of 11 March 2003 concerning several legal aspects of information society services, *Belgian State Gazette*, 17 March 2003.

There are many factors which can influence the value of digital evidence, not all of which can be easily controlled: from whom or where the evidence emanates (e.g. does it come from a party with a clear personal interest or rather from an independent entity?), when the evidence was created (had there been earlier indications of problems or was it generated 'in tempore non suspecto'?), whether or not the system generating the evidence may be said to have been functioning properly, etc.

As to its reliability, digital evidence is renowned for its manipulability and possibilities of tampering (Geradts and Sommer, 2006). There are however additional measures that can be taken to combat this issue, particularly by implementing the appropriate protocols for data origin authentication and preventing unauthorized modification. The probative value of digital evidence such as logs is likely to increase if one can demonstrate that all appropriate measures have been taken to ensure integrity, authenticity, and completeness of logged events and that relevant standards have been adhered to. Of course, security measures are only as strong as their weakest link and therefore the evidence might still be challenged accordingly.

A final aspect which requires consideration is that the data subject must have the ability to extract information from the log views in a way that he can subsequently present that information as evidence. A print-out or simple transmission to another digital carrier runs a risk of being disqualified or becoming useless as it no longer offers any particular guarantees as to its authenticity. A possible solution to this problem would be to enable the data subject to have a given transcript *time-stamped* by a Trusted Third Party (TTP).

Electronic time-stamping is a process whereby an expression of time is attached as an attribute to a digital record or token (ITU, 2007). Time-stamping comes in many forms. Here we refer to a time-stamp as a digital 'certificate' that contains the hash value of a particular file together with a trusted time indication, and which has been digitally signed by a Time Stamping Authority (TSA) (Dumortier, Dekeyer and Loncke, 2004). A time-stamp by itself does not provide any guarantees as to the accuracy of the underlying record or document. It merely proves that the file existed in a given state and at a given time and date (Dinant, 2004). But seeing as asymmetric cryptography is used, it does establish that the underlying file has not subsequently been tampered with (Dumortier, Dekeyer and Loncke, 2004).

The probative value of the time-stamped file depends on two aspects: the trustworthiness of the TSA and the trustworthiness of the underlying data. The latter is evidenced, as indicated earlier, by showing that all appropriate measures have been taken to ensure accuracy, integrity, authenticity, and completeness of that data. As to the trustworthiness of the TSA, it is interesting to note that the Belgian government undertook to regulate such service providers.[10] By imposing certain qualitative criteria and specific obligations, certain types of documents and data produced by such service providers were to be given a legal status (Dumortier and Somers, 2007). At European level, the eSignature Directive only imposes such criteria upon the providers of qualified certificates for purposes of electronic signatures.[11] Perhaps the existing framework should be supplemented to increase legal certainty towards the evidentiary value of other certification services. At the moment, the

[10] Law of 15 May 2007 concerning a legal framework for certain providers of trust services, *Belgian State Gazette*, 17 July 2007. The effectiveness of this law has been compromised however due to the fact that the implementing Royal Decree it required wasn't adopted within the prescribed time frame.

[11] See Annex II of Directive 1999/93/EC, despite the mention of time-stamping services in recital (9).

evidentiary value of other forms of digital evidence remains to be determined on a case-by-case basis.

3.3 Conclusion

Log data can only provide a sound basis for further services when it is authentic. We define authenticity as the simultaneous fulfilment of data integrity and uniqueness, as illustrated in Figure 4. Confidentiality of log entries is necessary for privacy and is considered as an extra protection goal. A log service is labelled secure when integrity, uniqueness and confidentiality properties are fulfilled.

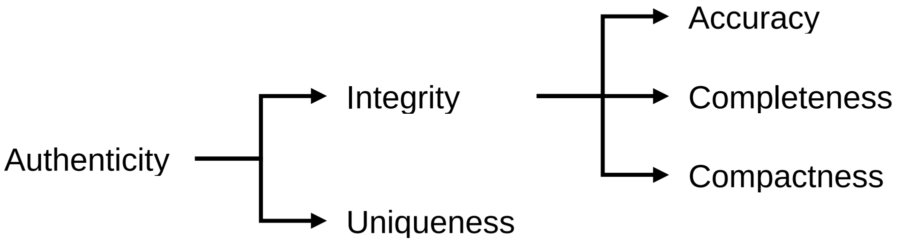


Figure 4 Authenticity property for secure logging (Höhn, Accorsi and Maier, 2007).

- Integrity states that log data faithfully reflects the state of the devices, i.e., the log data is accurate (entries have not been modified), complete (entries have not been deleted), and compact (entries have not been illegally added to the log file). Thus, log data is not modified, deleted, or appended during the transmission to, and storage at, the collector.
- Uniqueness states that log data shall not allow for parallel realities. Concretely, it is impossible to intercept log data sent from d_1 to c_1 and to resend it (possibly in modified form and claiming a different device identity) to c_2. Log data must be uniquely tagged.
- Confidentiality states that log entries cannot be read by unauthorised individuals, for this would harm inner privacy. Note that confidentiality is also related to uniqueness, for log data transmitted in clear-text can be easily duplicated.

These properties are implemented with cryptographic techniques, which need to ensure tamper evidence, i.e., attempts to illicitly manipulate log data must be detectable to a verifier (Itkis, 2003), and forward integrity, i.e., log data contains sufficient information to confirm or rebuke allegations of log data modification before the moment of the compromise (Bellare and Yee, 1997). The goal of the attacker is to gain access to private log data and, thus, to violate its integrity, uniqueness, and confidentiality. The threats posed by an attacker are described using an attacker model. While we are aware of recent ongoing research on formally characterizing attacker models for dynamic environments (Creese, Goldsmith, Harrison, Roscoe, Whittaker and Zakiuddin, 2005), we refrain from sticking to a particular model.

4 Related Work on Secure and Privacy-preserving Logging

Secure logging of system's events is the foundation for privacy evidences. This chapter investigates on the deployment of related work to secure logging on privacy and so the enforcement of obligations in the AmI scenario. Section 4.1 focuses on the use of cryptography for secure logging whereas section 4.2 focuses on the use of Trusted Computing in order to ensure the authenticity of log data. Section 4.3 introduces the standards so far for secure logging.

4.1 Secure Logging by Cryptography

The step from simple logging to secure logging was firstly motivated by the insufficient security properties of *syslogd*, a logging service which is widely used on Unix systems. *Syslogd* basically writes logs about system events in ordinary text files without having any protection in place. As long as we can assume that the log files remain unspoiled, the simple *syslogd* service is useful for detecting, for instance, system malfunctions. This does in fact not include scenarios where an attack is mounted against a system, and in consequence the attacker seeks to cover his track by removing the corresponding log entries after the fact.

(Bellare and Yee, 1997) introduce the application of message authentication codes (MACs) in order to achieve forward integrity. Forward integrity for log entries assures that previous entries cannot be altered, even if the system is compromised. To achieve that property, Bellare and Yee divide the timeline into several epochs and use different keys for the message authentication in each epoch. Thus, if an attacker compromises the system and obtains the key, he will be able to alter log entries of the current epoch, but still not be able to change log entries of previous epochs, since the authentication keys are destroyed at the end of each epoch. An auditor is able to check the authenticity of all log entries by reproducing the MAC keys. Bellare and Yee propose to derive the authentication key for each epoch from the key of the previous epoch. In cryptography, we refer to such a scheme as *key evolution*. The derivation of new keys has to be done by a non-reversible mapping such that the attacker is not able to reverse this step and obtain a key of a previous epoch. For the auditor, however, it is sufficient to be in possession of the first authentication key, since she can derive all other keys from that one. This protocol makes changes in the log entries apparent to the auditor, but does yet not help out when the attacker deletes log entries within an epoch. Bellare and Yee propose to include sequence numbers in the log entries. Then, an attacker would be able to delete a log entry, but would lack the capability to reproduce a log entry with the then missing sequence number. By that, even deletion becomes apparent to auditors.

(Schneier and Kelsey, 1999) designed a protocol with similar features as the one by (Bellare and Yee, 1997). Forward integrity in Schneier's protocol is also assured by MACs with a non-reversible key evolution scheme. In addition to the previous protocol, the deletion of log entries instantly corrupts all subsequent log entries. This is ensured in a cryptographic manner by means of a hash chain. In a hash chain for log entries, the hash[12] of the current log entry

[12] A hash is a number or a string of limited length which almost uniquely represents larger amounts of data, for instance log entries. Two important properties are (a) if the data changes marginally, the hash changes significantly, and (b) it is hard to generate for a given hash value data which is represented by the same hash value.

does not only depend on the content of the log entry, but also on the hash of the previous log. Thus, the hash of a log entry would only be reproducible as long as the hash value of the previous log entry exists (and is valid). In fact, a hash error in a single log entry transitively propagates to all subsequent log entries, due to the dependency of the hash. In addition to forward integrity, Schneier and Kelsey include an encryption scheme in their protocol. For their encryption, they use a hash of the current MAC key together with a permission mask. This reuse of the MAC key does not reduce the security, but is rather an elegant way to avoid further complexity in the protocol. The permission mask works like an access control on cryptographic level. Only those auditors that are in possession of the correct permission mask are able to generate the key for decryption. However, any auditor who is in possession of the first MAC key is able to verify all log entries, that is regardless of whether she is able to decrypt the log entry or not, since the MACs are established over encrypted log entries. Thus, this scheme allows non-selective verifiability of log entries and at the same time selective accessibility. Figure 1 in (Schneier and Kelsey, 1999) gives a clear and concise overview of their protocol.

While privacy evidences and ex post supervision is generally a good idea to deal with personal data, privacy policies, and the behaviour of data consumers (service providers in the previous example), it is yet not said how to obtain accurate and complete logs. This marks a serious conflict of interests. The data consumer is in fact interested in affirming his policy compliant behaviour while he would certainly be distracted from behaving according to the privacy policy of a user, if there is a benefit for him in not doing so. Thus, the data consumer is interested in logging all actions which support the impression that he behaves according to the privacy policies, but he is definitely not interested in logging any action which could be taken as evidence for abusing the personal data of the data subject (the service user in the previous example). The data subject is indeed interested in accurate and complete logs, but particularly in those entries which could be an evidence for the abuse of her personal data. However, in the basic scenario of the previous paragraph is the data subject not able to control whether all actions are logged or not. Thus, the data consumer has a clear advantage over the data subject by means of deciding on which actions to log. (Accorsi and Bernauer, 2007) suggest to use trusted computing[13] in order to assure that continuous and non-selective logging of all events is performed by the data processor.

4.2 Enforcement Mechanisms Based on Trusted Computing

(Greenstadt and Raymond, 2004) outline a scenario where trusted computing is applied for protecting personal data in medical records. The scenario depends on the current specification of the Trusted Software Stack (TSS) which is TSS 1.2. The authors argue that secure logging would be achievable by means of a TSS which implements the TSS 1.2 specification, since such an implementation would already include integrity protection, encryption, and secure time stamping. While such an approach seems straightforward, if trusted computing exists, it would not provide the forward integrity by means of key evolution as the secure logging protocol of (Bellare and Yee, 1997). This seems not necessary at the same time, since a central assumption in trusted computing is that the secret keys are either safe or will be

[13] Trusted computing in general has been discussed in FIDIS Deliverable 3.9 and in FIDIS Deliverable 14.3, in the latter with a focus on business processes.

destroyed before an attacker can get hold of them. In contrast to (Schneier and Kelsey, 1999), this approach does not include any access control to the logged data.

(Hengartner, 2008) discusses a scenario where we have three parties, a network provider of a cell phone network, the cell phone user and a service provider who offers a location-based service (LBS). The authors describe their approach for secure logging in more detail than (Greenstadt and Raymond, 2004), but base it on the same technical assumptions. In the scenario of Hengartner et al, the user is interested in the logging and the service provider is forced to log by means of trusted computing mechanisms. The cell phone network, however, needs to be ultimately trusted and is as such auditing the trusted computing at the site of the LBS service provider as well as establishing access control on the log entries for different users. A serious drawback of this approach is that the logging (or evidence creation) might help the user to discover privacy breaches of the LBS service provider, but only with the collaboration of the network provider. Without such collaboration, the data subject would probably not even be able to notice a privacy breach.

(Korba and Kenny, 2003) as well as (Böhme and Pfitzmann, 2008) investigate on the use of Digital Rights Management (DRM) for the purpose of managing personal data. Korba and Kenny focus on the requirements arising from Directive 95/46/EC of the European Parliament, whereas Böhme and Pfitzmann discuss general aspects of Privacy Rights Management (PRM) based on DRM. Korba and Kenny suppose that DRM as such is achievable and discuss which aspects of the Data Protection Directive can be implemented by means of DRM. Böhme and Pfitzmann call the dependability of DRM into question and reason about the basics of known DRM implementations. The assumption that DRM could work properly leads Korba and Kenny to the conclusion that some required principles, such as encryption, are enforceable by DRM technology. Böhme and Pfitzmann come to the conclusion that the requirements raised by PRM are much stricter than those in DRM while methods for achieving DRM are quite error-prone or even not deployable under these conditions. Thus, PRM is even less realistic than DRM.

Trusted computing might in some cases be a promising path to go for secure logging. However, supposed that it is possible to force a data consumer to keep logs against his interests, it would also be possible to force the data consumer to act according to the privacy policies. Sufficient behaviour controlling needs to be in place for the data consumer anyway, since even if only logging is enforced, the data consumer certainly has a strong interest in not violating the privacy policies. Thus, from a technical perspective, there is hardly a reason, to use trusted computing just for the enforcement of logging. It would be rather appropriate to enforce a combination of policy compliance in the general case and logging, if data is going to leave the trusted environment. This would in consequence relax the requirement to keep logs in many cases, since a data subject could take for granted that the data processor is unable to violate privacy policies, provided all processing mechanisms are trusted and personal data does not need to leave the trusted environment for rendering the service. However, once personal data have to leave the trusted environment, secure logging can only provide privacy evidences for the leakage, but not for any further processing. If the leakage is intended and not as such violating a privacy policy, data subjects would thus have a strong interest in further measures for controlling or tracking the processing of their personal data.

In general, logs of data processing can be understood as metadata of the processed data. Thus, the less logs exists the less mechanisms are necessary to protect the (meta) data against unauthorized access (or leakage) and the easier is it to reason for privacy properties of a protocol or system. Logging and the need for audits is in fact, whenever involving personal data, causing new privacy issues that need to be addressed in a careful manner in order to let the protocol or system benefit and not suffer from the logging.

4.3 International Security Related Standards[14]

Audit logging is equally well established in the context of Information Security Management Systems (ISMS) and in the context of information security related products. Naturally the respective standards show significant overlap – combined they represent the state-of-the-art in audit logging. In this section based on his experience as information security auditor the author provides a summary of significant logging requirements documented in the ISO/IEC 27000 series, Common Criteria (ISO/IEC 15804) and CobiT (version 4.1)[15].

4.3.1 ISO/IEC 27000 Series

The ISO/IEC 27000 series currently[16] contains 4 international standards dealing with various aspects of ISMS (abbreviation of the titles in brackets):

1. ISO/IEC 270001 (ISMS – Requirements)
2. ISO/IEC 27002 (Code of Practice)
3. ISO/IEC 27005 (Information Security Risk Management)
4. ISO/IEC 27006 (Accreditation Requirements)

In the context of audit logging the first two standards are of relevance. ISO/IEC contains requirements for the certification of ISMS. Control objectives and control relevant in the certification process are summarised in Annex A of ISO/IEC 27001. The description of these controls is only in brief – typically in addition to a title they contain one short descriptive sentence. Especially the control objective A.10.10 and its six related controls are referring to audit logging:

- A.10.10 (Monitoring)
    - i. A.10.10.1 (Audit logging)
    - ii. A.10.10.2 (Monitoring System Use)
    - iii. A.10.10.3 (Protection of Log Information)
    - iv. A.10.10.4 (Administration and Operator Logs)
    - v. A.10.10.5 (Fault Logging)
    - vi. A.10.10.6 (Clock Synchronization)

The number of the control objectives and controls in Annex A in ISO/IEC 27001 is referring to corresponding chapters in ISO/IEC 27002. In these chapters non-mandatory recommendations are made on how these controls could be implemented. These

[14] This contribution is based on (Meints, Thomsen 2007)

[15] CobiT in the current version is available free of costs via http://www.isaca.org.

[16] November 2008

recommendations, however, are typically not relating to specific technical implementations such as certain operating systems. In the context of audit logging they are nevertheless quite concrete as the following example shows. For audit logs (A.10.10.1) ISO/IEC 27002, chapter 10.10.1 contains the following implementation guidance:

- "Audit logs should include, when relevant:
    - User IDs;
    - Dates, times, and details of key events […];
    - Terminal identification or location […];
    - Records of successful and rejected system access attempts;
    - […]"

The implementation guidance referring to the other five controls mentioned is detailed on a similar level. An example for this is the guidance given in ISO/IEC 27002 concerning protection of log information (chapter 10.10.3: Protection of Log Information):

"Controls should aim to protect against unauthorized changes and operational problems with the logging facility including:

a) alterations to the message types that are recorded;

b) log files being edited or deleted;

c) storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

[…]"

To the author this implementation guidance seems to be important. The reason for this being, that many products e.g. operating systems widely used in a default installation provide insufficient internal protection mechanisms against manipulation of audit data by (local or domain) administrators.[17] In addition in some cases the events or incidents logged are insufficiently adjustable.[18] In these cases specific configuration[19] or additional so called syslog systems and reporting tool are needed[18] to comply with the aforementioned implementation guidance.

4.3.2 CobiT

CobiT (Control Objectives for Information and Related Technology) is a criteria system for IT governance containing control objectives and controls similar to ISO/IEC 27001, though CobiT does not provide a certification scheme for management systems. Nevertheless CobiT provides a relevant framework in the context of compliance with the U.S. American Sarbanes-Oxley-Act (SOX), which alongside other drivers also supported its relevance (Meints, Thomsen 2007). In addition to information security also aspects of compliance to relevant legislation and IT operations are addressed.

[17] This refers as well to Microsoft Windows operating systems (e.g. Windows Server 2000 and 2003) as Unix operating systems such as Solaris 10 or Suse Linux Enterprise 10.

[18] This refers to Windows Server 2000 and 2003 including the corresponding LDAP-service ActiveDirectory.

[19] Unix operating systems typically allow for an appropriate division of roles to ensure secure logging.

CobiT does not contain specific and detailed technical or organisational requirements or guidance for audit logging – generally audit logging is referred to only in the context of various controls. In most cases this reference is containing one or two short sentences only. Mainly CobiT is describing *where* audit logging is needed, but does *not* refer to *how* it should be implemented. Examples for references to audit logging are:

- Control Objective DS5 (Ensure Systems Security)
    - Control DS5.5 (Security Testing, Surveillance and Monitoring); this is referring to the relevance of audit logs when monitoring unusual or unwanted events or activities
- Control Objective DS12 (Manage The Physical Environment)
    - Access to buildings and rooms should be logged
- Control Objective DS13 (Manage Operations)
    - Quality and quantity of audit logs should be planned carefully, audit logs should be evaluated regularly as this provides important input for Control Objective DS 10 (Manage Problems)
- Control Objective DS9 (Manage The Configuration)
    - Logging of changes in system's configuration

4.3.3 Common Criteria (ISO/IEC 15804)

The Common Criteria for Information Technology Security Evaluation (CC) are used for certifying security related products. This certification covers product properties, especially security targets and functions, but also aspects of product related maintenance and services by manufacturers and vendors. The CC is developed by national standardisation organisations and information security agencies such as the U.S. American National Institute for Standards and Technology (NIST) and the German Federal Office for Information Security (BSI). They are also internationally standardised by the International Organization for Standardization (ISO) as ISO/IEC 15804. The current version of the CC V. 3.1 Release 2, which is described in this sub chapter, still is in the international standardisation process at ISO.[20]

In part 2 the CC lists a number of so called "security functions" in classes, families and related functions. In the context of audit logging the class "FAU: Security Audit" is relevant. In this class possible product functions for the detection, storage and evaluation of security relevant events are covered. The security functions are typically described by at least one sentence, pointing out in a formalised way potentially relevant events and actions (e.g. selection, deletion, modification, addition) that should be supported by the product.

The following figure gives and overview on the content of the class "FAU: Security Audit":

[20] Currently (November 2008) part 3 is internationally standardised, while parts 1 and 2 are still in the standardisation process at ISO.
The Common Criteria are available free of costs at http://www.commoncriteriaportal.org/thecc.html. An overview on products and protection profiles currently certified can be found at http://www.bsi.de/zertifiz/zert/report.htm

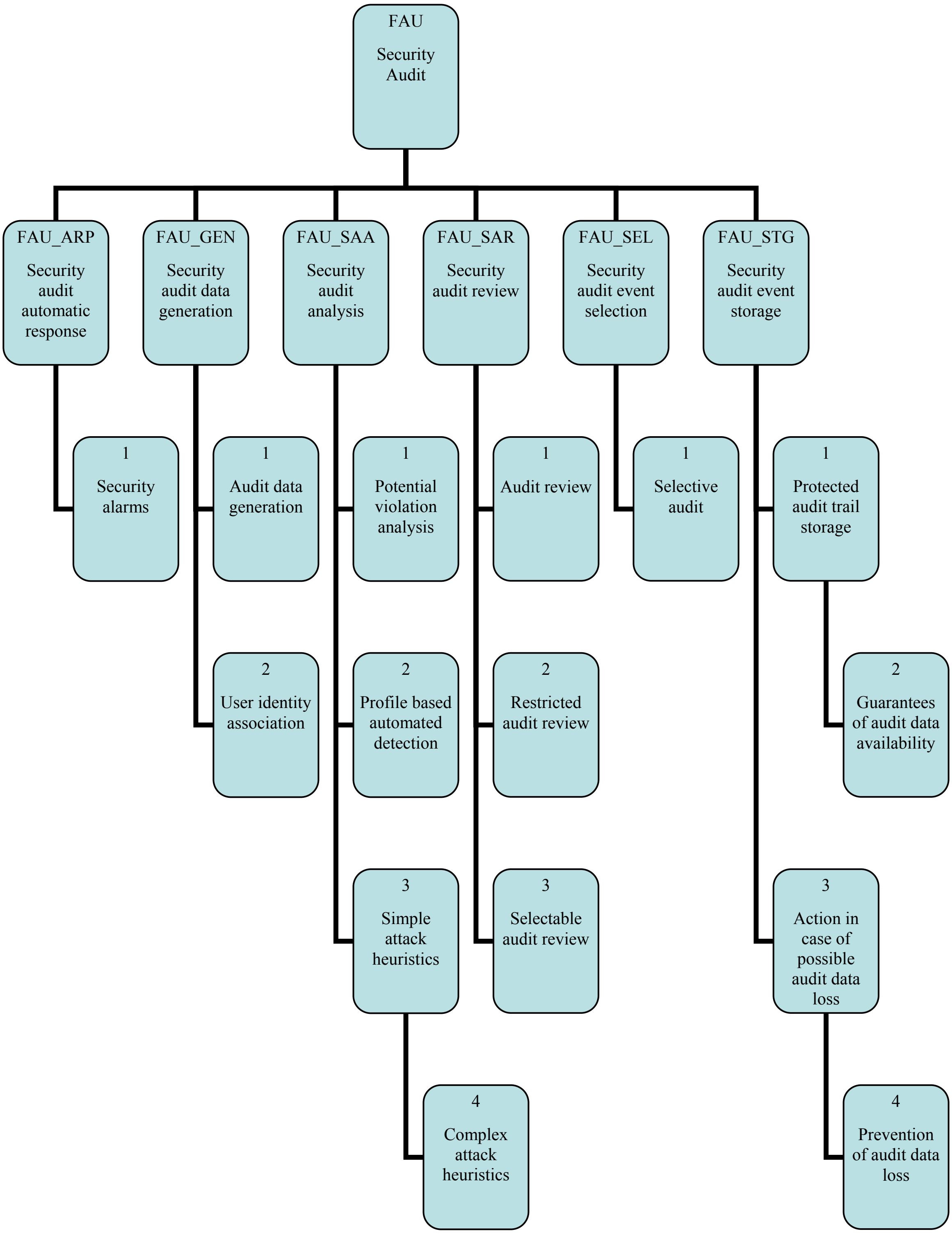

FAU
Security Audit
FAU_ARP
Security audit automatic response
1
Security alarms
FAU_GEN
Security audit data generation
1
Audit data generation
2
User identity association
FAU_SAA
Security audit analysis
1
Potential violation analysis
2
Profile based automated detection
3
Simple attack heuristics
4
Complex attack heuristics
FAU_SAR
Security audit review
1
Audit review
2
Restricted audit review
3
Selectable audit review
FAU_SEL
Security audit event selection
1
Selective audit
FAU_STG
Security audit event storage
1
Protected audit trail storage
2
Guarantees of audit data availability
3
Action in case of possible audit data loss
4
Prevention of audit data loss

Figure 5 Overview on families and functions in the class FAU

4.3.4 Summary and Conclusions

While CobiT only provides a quite generic overview where to use audit logs other international standards, especially ISO/IEC 15804 and ISO/IEC 27001 and 27002 provide relevant guidance how audit logging should be designed, implemented and used. Though not referring explicitly to the requirements listed in section 3, these standards well take them into account.

For stakeholders in information security management the control objectives in ISO/IEC 27001 Annex A.10.10 and the related implementation guidance in chapter 10.10 in ISO/IEC 27002 provide relevant information on the implementation and usage of audit logs. ISO/IEC 15804 especially is relevant in the context of product procurement, especially for products that are security relevant such as security gateways and firewalls. The security families and functions in the class FAU can be well referred to in calls for tenders or technical specifications in early phases of product development to describe security functions needed.

5 Approaches for Privacy Evidences

The realisation of the system for privacy evidences does not only take a secure logging service into account. For an audit, the resulting log views have to be compared against the agreed privacy policy. Since the usage of personal data is beyond access control of the data provider, such a policy language has to consider obligations. Section 5.1 presents policy languages for AmI systems supporting obligations. Section 5.2 shows our approach for the secure logging service by using cryptographic primitives. Section 5.3 investigates on the generation of log views, which are individualised for the corresponding data provider. Section 5.4 shows an approach for checking automatically the resulting log views against a privacy policy, e.g. specified in one of the policy languages of section 5.1. Section 5.5 shows additional mechanisms.

5.1 A Policy Language for AmI Systems

With the advent of privacy policy languages, the concept of obligations (Jajodia, Kudo, and Subrahmanian, 2001; Kudo and Hada, 2000) has become an important feature of access control languages (Karjoth and Schunter, 2001; Park and Sandhu, 2002). Obligations are mandatory requirements that a subject has to perform after obtaining or exercising rights on an object. In real world implementation, however, this may have to be done by agreeing on the fulfillment of obligations before obtaining the rights and at the time obligation-related authorization rules are checked. In the following, we introduce the *eXtensible Access Control Markup Language* (XACML) as a prominent example for a policy language with obligations.

5.1.1 Access Control Policies

XACML, developed by the *Organization for the Advancement of Structured Information Standards (OASIS),* is a framework that standardises various aspects of access control. Most prominently, XACML comes with an XML language for specifying access control policies. In addition, it proposes a second XML language for formulating access requests and it defines an architecture for the evaluation of those access requests against access control policies. There are a number of XACML profiles that propose ways to model typical access control situations; the privacy policy profile introduces two additional attributes, resource:purpose and action:purpose (Oasis, 2005).

XACML policies are based on four entities: *subjects*, *resources*, *actions* and *environments*. Besides the common entities subject, resource, and action, environments may be used to specify additional properties such as time constraints or relations among subjects. A quadruple containing a set of subjects, a set of resources, a set of actions and a set of environments forms a *target*. Targets are used in several places of XACML access control policies. Together with a set of *conditions* and an *effect*, targets form a triple called *rule*. An effect can either state Permit or Deny. Conditions help to formulate additional predicates on requests' attributes. They have three possible return values: True, False or Intermediate. An access request matches a rule if its attributes match with the rule's target and the rule's condition hold. Then the rule's effect serves as return value. If the condition's return value is Intermediate, so is the return value of the entire rule. Alternatively, if the condition evaluates to False, the rule is considered NotApplicable.

A set of rules forms a *policy*. Conflicting rule evaluations are resolved using *rule combining algorithms* which are associated with each policy. Five different algorithms are available: deny-overrides (ordered or unordered) implies that a single rule evaluating to Deny lets the entire policy evaluate to Deny. Similarly, permit-overrides (ordered or unordered) implies that the entire policy evaluates to Permit if a single rule evaluates to Permit. Furthermore, first-applicable returns Permit if the first (according to their order in the XML file) rule evaluates to Permit and Deny likewise.

A set of policies can be grouped in a *policy set*. A PolicySet may recursively be contained in other policy sets. Similar to conflicting rules in one policy, conflicting policies within one policy set are resolved using a *policy combining algorithm*. In addition to the five algorithms mentioned above, there is a sixth algorithm available for policies: only-one-applicable returns the outcome of the one and only policy in a policy set which evaluates either to Permit or Deny. If no policy in the set is relevant, the algorithm returns NotApplicable. If there is more than one relevant policy in the set, Intermediate is returned.

A policy or a policy set may also have a target element on its own that filters access request. Only those requests that match this target are evaluated on the rules (policies) contained in the policy (set). Furthermore, a policy or policy set may define obligations. When such a policy is evaluated, its obligations are passed up to the next level of evaluation only if the effect of the policy matches the value of the FulFillOn attribute of the obligation. An effect of this evaluation is that only policies and policy sets contribute to the final set of obligations if they are evaluated and their result also matches the final FulFillOn attribute.

5.1.2 Access Requests

XACML access requests are based on the same four entities as XACML targets – a subject, a resource, an action and an environment. Each of theses entities consists of a set of attributes such the name of a subject or the path associated with a resource. A PDP will try to match these entities and their attributes with the corresponding attributes values and conditions stated in the XACML access control policies.

Figure 6 illustrates the reference monitor architecture. This drawing is slightly simplified compared to the original data-flow diagram given in the standard.

1. In a first step, a policy administrator creates an XACML access control policy and stores it in the *policy administration point (PAP)*. Policies are described using XACML's access control policy language.

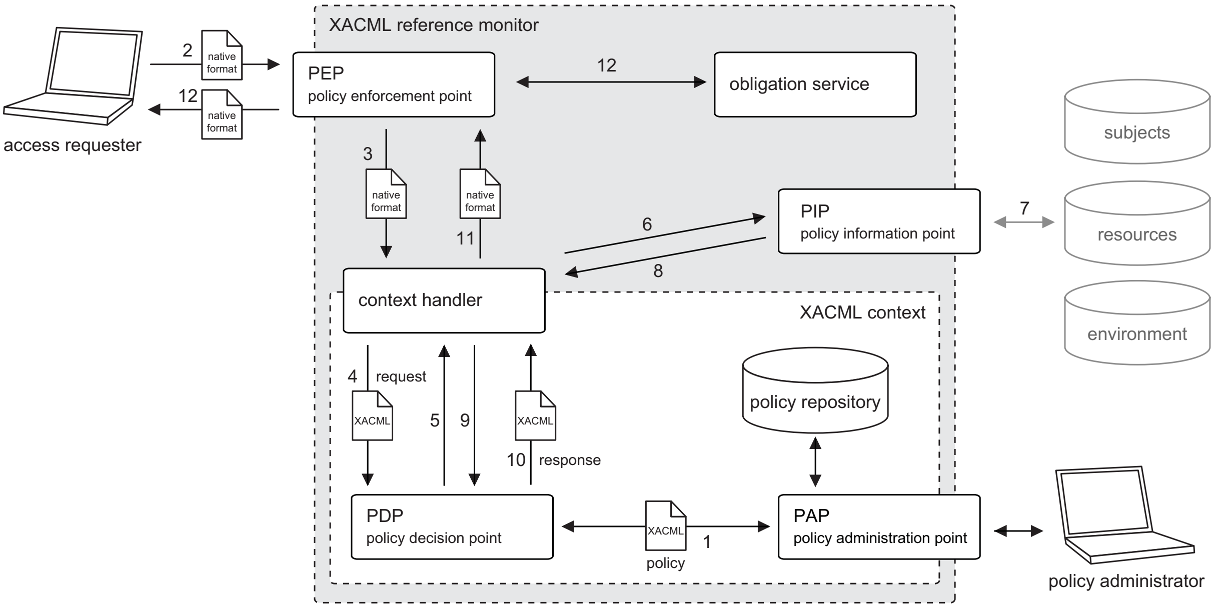


Figure 6: XACML Reference Monitor Architecture

Steps 2 to 12 describe the flow of information when deriving an access request decision.

2. An access requester issues an access request in its native format.
3. The *policy enforcement point (PEP)* forwards the access request to the context handler. Optionally, the PEP may add some additional subject, resource or environment attributes to the request.
4. A context handler acts as interface between native access request formats and the XACML XML-language. It translates native requests to XACML requests and forwards them to the *policy decision point (PDP)*.
5. Based on the XACML policies retrieved from the PAP, the PDP may query additional attributes in order to evaluate the policies for a given access request.
6. The context handler forwards attribute queries to the *policy information point (PIP)*.
7. The PIP gathers all subject, resource and environment attributes needed – possibly from external sources.
8. Attributes are returned to the context handler.
9. The context handler forwards them to the PDP.
10. Now that the PDP has collected all necessary information, it can compute an access request decision, including a set of obligations, wrapped in a XACML response and returned to the context handler.
11. The context handler translates decisions back to the native request format and returns them to the PEP.
12. Finally, the access request decision, either Permit or Deny, is returned to the access requester. In case obligations are returned with the access decision, the PEP forwards these obligations to the obligation service.

5.1.3 Obligations

In XACML, obligations are a set of operations that must be performed by the PEP in conjunction with an authorization decision. An obligation consists of an obligation identifier and a sequence of attribute assignments. No further requirements on obligations are expressed by the XACML standard.

In the recent literature, a few obligation models have been proposed. They either focus on the monitoring of obligations (Bettini, Jajodia, Wand and Wijesekere, 2002) or refine obligations into pre-obligations, post-obligations, conditional obligations, and repeating obligations (Ni, Bertino and Lobo, 2008).

5.2 Secure Logging

Based on (Accorsi, 2008), we present in the following the basis of a secure logging service. There are two kinds of actors in a logging setting: the devices sense the environment and communicate changes therein in the form of events to a collector, whose responsibility is to sequentially record these events. Assuming that the communication between devices and collectors cannot be manipulated, here we focus on the collector and the corresponding mechanisms to ensure the authenticity of recorded data.

In our approach, log data is secured when recording the entry associated to an event and not as a separate process. Each log entry E_j is (symmetrically) encrypted with an evolving cryptographic key K_j obtained from a secret master key A_j and an index field W_j . (The latter is used to describe the data provider to which the entry refers.) A hash chain Y associates the previous entry E_{j-1} and the current. This procedure is depicted in Figure 7, where the numbers correspond to:

1. $A_j = Hash(A_{j-1})$ denotes the authentication key of the *j*th log entry. The confidentiality of this information is essential as it is used to encrypt log entries. Thus, we assume that the computation of the new value irretrievably overwrites the previous value.
2. $K_j = Hash(W_j ,A_j)$ is the cryptographic key with which the *j*th log entry is encrypted. This key is based on the index W*j*, so that only corresponding data providers gain access to the entry.
3. $\{D_j\}_{Kj}$ is the encrypted log entry D_j.
4. $Y_j = Hash(Y_{j-1}, \{D_j\}_{Kj} ,W_j)$ is the $_j$th value of the hash chain. Each link of the hash chain is based on the corresponding encrypted value of the log data.

The generated log entry, denoted $E_j = W_j, \{D_j\}_{Kj}, Y_j$, consists of the index W_j, the encrypted log entry $\{D_j\}_{Kj}$, and the hash chain value Y_j.

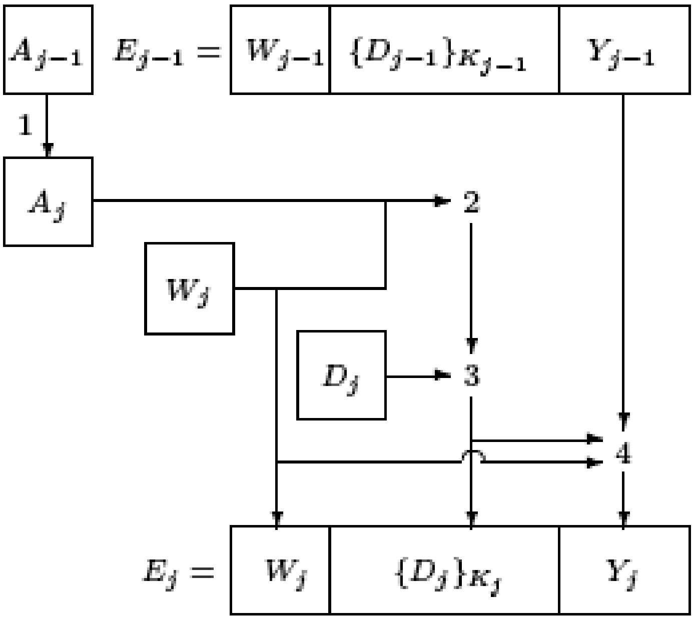
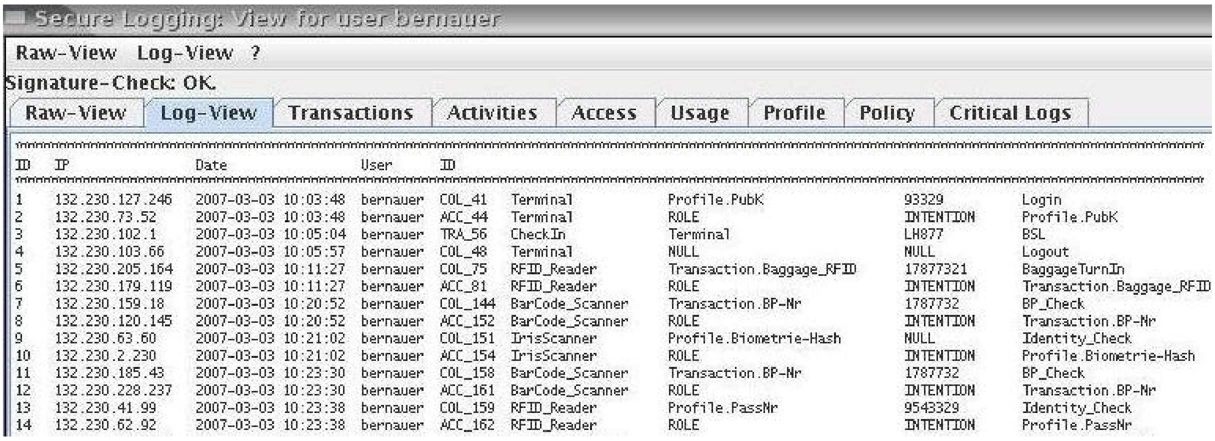


Figure 7 Adding and entry to the log file (Accorsi, 2008).

5.3 Log Views and their Generation

A central concept to allow supervision is to furnish data providers with timestamped information regarding which attributes have been collected, who has had access to them and how collected attributes have been used. In our approach, these pieces of information are compiled into a *log view* (Sackmann, Strüker and Accorsi, 2006), a concept bearing similarity with its homonymous counterpart in the field of databases.

Log views are individualised audit trails consisting of factual data (performed transactions, collected attributes, etc.) and monitored data (access and usage information) about a particular data provider, as well as meta data – in the form of a digital signature – about the generating data consumer and the integrity of a view. Figure 8 illustrates a part of log view of a data provider referred to as "bernauer".



Signature-Check: OK.

```
ID  IP               Date                 User      ID
1   132.230.127.246  2007-03-03 10:03:48  bernauer  COL_41   Terminal         Profile.PubK               93329       Login
2   132.230.73.52    2007-03-03 10:03:48  bernauer  ACC_44   Terminal         ROLE                       INTENTION   Profile.PubK
3   132.230.102.1    2007-03-03 10:05:04  bernauer  TRA_56   CheckIn          Terminal                   LH877       BSL
4   132.230.103.66   2007-03-03 10:05:57  bernauer  COL_48   Terminal         NULL                       NULL        Logout
5   132.230.205.164  2007-03-03 10:11:27  bernauer  COL_75   RFID_Reader      Transaction.Baggage_RFID   17877321    BaggageTurnIn
6   132.230.179.119  2007-03-03 10:11:27  bernauer  ACC_81   RFID_Reader      ROLE                       INTENTION   Transaction.Baggage_RFID
7   132.230.159.18   2007-03-03 10:20:52  bernauer  COL_144  BarCode_Scanner  Transaction.BP-Nr          1787732     BP_Check
8   132.230.120.145  2007-03-03 10:20:52  bernauer  ACC_152  BarCode_Scanner  ROLE                       INTENTION   Transaction.BP-Nr
9   132.230.63.60    2007-03-03 10:21:02  bernauer  COL_151  IrisScanner      Profile.Biometrie-Hash     NULL        Identity_Check
10  132.230.2.230    2007-03-03 10:21:02  bernauer  ACC_154  IrisScanner      ROLE                       INTENTION   Profile.Biometrie-Hash
11  132.230.185.43   2007-03-03 10:23:30  bernauer  COL_158  BarCode_Scanner  Transaction.BP-Nr          1787732     BP_Check
12  132.230.228.237  2007-03-03 10:23:30  bernauer  ACC_161  BarCode_Scanner  ROLE                       INTENTION   Transaction.BP-Nr
13  132.230.41.99    2007-03-03 10:23:38  bernauer  COL_159  RFID_Reader      Profile.PassNr             9543329     Identity_Check
14  132.230.62.92    2007-03-03 10:23:38  bernauer  ACC_162  RFID_Reader      ROLE                       INTENTION   Profile.PassNr
```

Figure 8 Part of a log view for data provider "bernauer".

As for the generation of log views, to retrieve a log view S_A the data provider A employs a trusted device (e.g. a home computer or a terminal dedicated to this purpose) to authenticate himself to the data consumer, who then starts a query over (possibly distributed) log files. Intuitively, the index of each entry is checked against the authenticated data provider. If they match and the entry passes an integrity check (based on the hash chain), then the content of the entry is decrypted and added to the log view of A. When all the entries are queried, the resultant view is signed and sent back to the inquiring data provider.

5.4 Automated Audits and Digital Privacy Evidence

Log views would, at least in theory, suffice to realise the holistic sense of control we argue for in this manuscript: data providers could browse through their log views and check whether their privacy policies have been adhered to or not. However, this is more intricate than it seems. Log views can easily include thousands of entries and their interrelationships are often hard to comprehend and reconstruct, regardless of how much effort we put into improving their readability.

We develop an approach to audit log views parameterised by the policies of data providers. Intuitively, given a policy $P := \{r_1, . . . , r_n\}$ and a log view S, we define a transformation v that takes P and returns the set of rules $V_P = \{v_1, . . . , v_n\}$ such that each v_i in V denotes the violation of the corresponding rule r_i. To illustrate this, consider the rule r_2 in Figure 9. By applying the transformation v, the following violation is generated:

$$v_2 := (\text{ allow, RFID-Reader, *, * }).$$

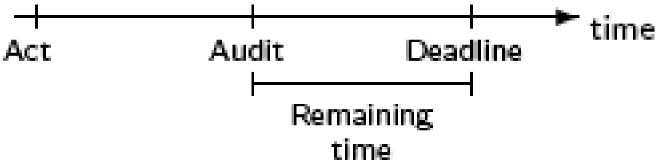


Figure 9 Condition leading to an amber semaphore (Accorsi, 2007).

This denotes that the collection of attributes through RFID readers is allowed, thereby contradicting the original desire of the data provider. With V_P at hand, we then search for violations in the log view of the corresponding data provider. To this end, we define the pinpoint relation Δ between views and the set of violations V_P such that $S \Delta v_i$ if v_i can be pinpointed, i.e. detected, in S. If there is a v_i *in* V_P such that $S \Delta v_i$, then there is an execution of the system that violates r_i and, in consequence, the policy P. In contrast, if there is no such v_i, such that $S \Delta v_i$, then a violation of P can be ruled out. Technical details are found in (Accorsi and Bernauer, 2007).

We employ a semaphore notation to make the result of audit evident to the pertinent data provider. In this case, red obviously stands for a violation of some rule, while green denotes the compliance with a policy. An amber semaphore indicates that some obligation-based rule could not be pinpointed and therefore stands for a warning. Such a warning is triggered whenever a log view S is audited before the deadline of a pending obligation, as illustrated in Figure 8.

A log view, together with the corresponding audit analysis, constitutes a privacy evidence. In the case of a violation, an individual may click over the semaphore and obtain details on which rules have been violated as well as the entries that led to this result. A similar procedure can be carried out when the semaphore shows amber.

6 Conclusion

Ambient Intelligence Systems enable several novel ways to personalize the relationship with the customer in stationary retailing. For this, the extensive collection and use of personal and context data are essential, but inherently raise privacy concerns: customers increasingly lose control over and awareness about which data is captured or how it is used. Surely enough, concerns of this kind considerably undermine the success of future personalisation strategies.

In AmI systems, transparency with regard to the utilization of data is the only way to maintain privacy. The concept of privacy evidence we introduce in this paper is an initial step in this direction, as it permits an objective view into the data collected about a customer. Evidence could be used as a “sword” for the customer to incriminate in the case of a misuse, or as a “shield” for the retailer to absolve in the case of a privacy-compliant usage. *Privacy evidence* paves not only the way to transparency, but also to an acceptable deployment of AmI systems.

While privacy evidences and ex post supervision is generally a good idea to deal with personal data, privacy policies, and the behaviour of data processors (service providers in the previous example), it is yet not said how to obtain accurate and complete logs. This marks a serious conflict of interests. The data consumer is in fact interested in affirming his policy compliant behaviour while he would certainly be distracted from behaving according to the privacy policy of a user, if there is a benefit for him in not doing so. Thus, the data consumer is interested in logging all actions which support the impression that he behaves according to the privacy policies, but he is definitely not interested in logging any action which could be taken as evidence for abusing the personal data of the data provider (the service user in the example of this work). The data provider is indeed interested in accurate and complete logs, but particularly in those entries which could be an evidence for the abuse of her personal data. However, the data provider is not able to control whether all actions are logged or not. Thus, the data consumer has a clear advantage over the data provider by means of deciding on which actions to log. (Accorsi and Bernauer, 2007) suggest to employ trusted computing in order to assure that continuous and non-selective logging of all events is performed by the data processor.

Finally, the approach we propose does not exclude traditional Identity Management techniques. On the contrary, it complements them. It would thus be interesting to see more case studies using our techniques, as well as other developments, for supervision. This will substantiate the importance of supervision as a distinguishing factor for future Identity Management and privacy-aware (dynamic) systems.

7 References

Rafael Accorsi. Towards a Secure Logging Mechanism for Dynamic Systems. In: Proceedings of the 7th IT Security Symposium. 2005.

Rafael Accorsi. On the relationship of privacy and secure remote logging in dynamic systems. In S. Fischer-Hübner, K. Rannenberg, L. Yngström and S. Lindskog (eds.): Proceedings of the 21st IFIP TC-11 International Security Conference: Security and Privacy in Dynamic Environments. International Federation for Information Processing vol. 201. p. 329—339. Springer. 2006.

Rafael Accorsi. Automated Privacy Audits to Complement the Notion of Control for Identity Management. In Elisabeth de Leeuw and Simone Fischer-Hübner and Jimmy Tseng and John Borking (eds.): Policies and Research in Identity Management. Proceedings of IFIP International Federation for Information Processing vol. 261. Springer. 2008.

Rafael Accorsi and Matthhias Bernauer. On privacy evidence for UbiComp environments – Broadening the notion of control to improve user acceptance. In A. Bajart, H- Müller and T. Strang (eds.): Proceedings of the 5th Workshop on Privacy in UbiComp. p. 443-438. 2007.

Matthias Bauer, Martin Meints and Marit Hansen (eds.): Structured Overview on Prototypes and Concepts of Identity Management Systems (D3.1). European Commission Framework Programme Future of Identity in the Information Society (FIDIS). 2005.

Belgian Privacy Commission, 'Reference measures for the protection of every processing of personal data', reference measure 7, available at http://www.privacycommission.be/nl/static/pdf/ referenciemaatregelen-vs-01.pdf (last accessed 17 November 2008).

M. Bellare and B. Yee. Forward integrity for secure audit logs. Technical report, University of California at San Diego, Dept. of Computer Science & Engineering. 1997.

Black's Law Dictionary. Thomson & West, 8th edition, 2004.

C. Bettini, S. Jajodia, X. Wang, and D. Wijesekera. Obligation monitoring in policy management. In 3rd International Workshop on Policies for Distributed Systems and Networks (POLICY 2002). IEEE Computer Society, 2002.

Rainer Böhme and Andreas Pfitzmann. Digital Rights Management zum Schutz personenbezogener Daten? Datenschutz und Datensicherheit (DuD). Volume 32, Number 5. Vieweg Verlag. May 2008.

V. Broucek and P. Turner. 'Intrusion Detection: Issues and Challenges in Evidence Acquisition', *International Review of Law, Computers & Technology*, vol. 18, n° 2, p. 149—164. 2004.

M. Casassa-Mont, S. Pearson and P. Bramhall. Towards accountable management of privacy and identity. In E. Snekkenes and D. Gollmann (eds.): Proceedings of the European Symposium on Research in Computer Security. LNCS 2808. p. 146—161. Springer. 2003.

Chicago Sun-Times. Chipping away at your privacy. November 9th, 2003.

S. Creese, M. Goldsmith, R. Harrison, B. Roscoe, P. Whittaker and I. Zakiuddin. Exploiting empirical engagement in authentication protocol design. In: D. Hutter and M. Ullmann (eds.):

Proceedings of the 2nd International Conference Security in Pervasive Computing. LNCS 3450. p. 119—113. Springer. 2005.

J.-M. Dinant. 'The Long Way from Electronic Traces to Electronic Evidence', *International Review of Law, Computers and Technology*, vol. 18, n° 2., 2004.

J. Dumortier, H. Dekeyser and M. Loncke. 'Legal Aspects of Trusted Time Services in Europe', Research paper commissioned by Amano, 24 May 2004, p. 12, available at http://www.e-timing.net/legal%20report%20E-timing%20ICRI%20TS.pdf (last accessed 20 November 2008).

J. Dumortier and G. Somers. 'De wet van 15 mei 2007 tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten: een eerste verkenning', *Tijdschrift voor Belgisch Handelsrecht*, p. 649—659, 2007.

European Parliament and Council. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, p. 31—50. 23 November, 1995.

European Parliament and Council. Directive 1999/93/EC on a Community Framework for electronic signatures, O.J. L 13, p. 12—20, January 1999.

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

M. Froomkin. The death of privacy? Stanford Law Review, 52(5). p. 1461—1543. May, 2000.

Z. Geradts and P. Sommer (eds.). "D6.1: Forensic Implications of Identity Management Systems", January 2006, p. 70-108 available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf (last accessed 17 November 2008).

H. Graux e.a.. 'eID Interoperability for PEGS - Analysis and Assessment of similarities and differences – Impact on eID interoperability', report prepared for the IDABC program, November 2007, p. 93, available at http://ec.europa.eu/idabc/en/document/6484/5644 (last accessed 17 November 2008).

R. Greenstadt and J. F. Raymond. Trusted Computing for Medical Privacy. Presented at the PORTIA Workshop on Sensitive Data. Stanford. 2004.

U. Hengartner. Location Privacy based on Trusted Computing and Secure Logging. In Proceedings of the 4th International Conference on Security and Privacy in Communication Networks (SecureComm 2008). September 2008.

ITU-T SG17 Focus Group for Identity Management. "Report on Identity Management Use Cases and Gap Analysis", September 2007, p. 59, available at www.itu.int/ITU-T/studygroups/com17/fgidm, accessed 4 December 2007.

S. Jajodia, M. Kudo, and V. S. Subrahmanian. Provisional authorization. In A. Ghosh, editor, E-commerce Security and Privacy, p. 133—159. Kluwer Academic Publishers, 2001. Also published in Workshop on Security and Privacy in E-Commerce (WSPEC), 2000.

G. Karjoth and M. Schunter. A Privacy Policy Model for Enterprises. In 15th IEEE Computer Security Foundations Workshop, p. 271—281. IEEE Computer Society, 2002.

E. Kenneally. Digital logs – Proof maters. Digital Investigation, 1(2). p. 94—101, June, 2004.

R. Koorn (ed.). 'Privacy Enhancing Technologies – White Paper for Decision-Makers', written for the Dutch Ministry of Interior and Kingdom relations, December 2004, available at http://www.dutchdpa.nl, p. 35 (last accessed 22 May June 2007).

Larry Korba and Steve Kenny. Towards Meeting the Privacy Challenge: Adapting DRM. In Proceedings of the ACM CCS-9 Workshop, DRM 2002, Revised Papers. Springer Berlin/Heidelberg. 2002.

Stefan Köpsell, Ralf Wendolsky and Hannes Federrath. Revocable Anonymity. In Günter Müller (ed.): ETRICS 2006. LNCS 3995. p. 208—222. Springer. 2006.

M. Kudo and S. Hada. XML document security based on provisional authorizations. In 7th ACM Conference on Computer and Communications Security, p. 87—96. ACM Press, 2000.

Marc Langheinrich. Personal Privacy in Ubiquitous Computing – Tools and System Support. PhD thesis No. 16100, ETH Zürich, Zürich, Switzerland. May, 2005.

O. Leroux. 'Legal Admissibility of Electronic Evidence', *International Review of Law, Computers & Technology*, vol. 18, n° 2, 198. 2004.

T. Litfin and G. Wolfram. New Automated Checkout Systems. In M. Krafft and Murali K. Mantrala (eds.): Retailing in the 21st Century: Current and Future Trends. p. 143—159. 2006

M. Meints and S. Thomsen. „Protokollierung in Sicherheitsstandards" Datenschutz und Datensicherheit, vol. 31, no. 10, pp. 749—751, Wiesbaden 2007.

B. P. S. Murthi and S. Sarkar. The Role of the Management Sciences in Research on Personalization. Management Science, vol. 29, no. 10. p. 1344—1362. October, 2003.

Q. Ni, E. Bertino, and J. Lobo. An obligation model bridging access control policies and privacy policies. In *13th ACM Symposium on Access Control Models and Technologies* (SACMAT '08), p. 133—142. ACM Press, 2008.

G. Itkis. Cryptographic tamper evidence. In: Proceedings of the Conference on Computer and Communication Security. ACM Press. p. 355—364. 2003.

OASIS. Privacy policy profile of XACML v2.0, OASIS Standard, 1 Feb 2005.

John Park and Ravi Sandhu. Towards Usage Control Models: Beyond Traditional Access Control. 2002, In SACMAT '02, p. 57—67. ACM Press, 2002.

Joon Park and Ravi Sandhu. The UCON$_{ABC}$ usage control model. ACM Transactions on Information and System Security 7(1). p. 128—174. 2004.

Alexander Pretschner, Manuel Hilty and David Basin: Distributed usage control. In Communications of the ACM 49(9). Special Issue "Privacy and security in highly dynamic systems". p. 39—44. ACM Press. 2006.

RFID and Consumers. Understanding the Mindset, commissioned by Cap Gemini and the National Retail Federation. Available at http://www.pl.capgemini.com/resources/thought_leadership/rfid_and_consumers_understanding_their_mindset/?d=1, last accessed in October, 2008.

Stefan Sackmann, Jens Strüker and Rafael Accorsi. Personalization in Privacy-Aware Highly Dynamic Systems. Communications of the ACM 49(9). p. 32—38. 2006.

Bruce Schneier and John Kelsey. Secure Audit Logs to Support Computer Forensics. ACM Transactions on Information and System Security (TISSEC). Volume 2, Issue 2, pp. 159—176. 1999.

K. Shrikumar and B. Bhasker. Personalised recommendations in e-commerce. Int. J. Electronic Business, vol. 3, no.1. 2005.

Jens Strüker. Der gläserne Kunde im Supermarkt der Zukunft. Wirtschaftsinformatik, 49(19). p. 39—44. January, 2007.

Jens Strüker and Stefan Sackmann. New Forms of Customer Communication: Concepts and Pilot Projects. In: Proceedings of the America's Conference on Information Systems (AMCIS '04), August 6-8, New York, USA. 2004.

Mark Weiser. The Computer for the Twenty-First Century. In: Scientific American, p. 94—10. September, 1991.

Sven Wohlgemuth and Günter Müller. Privacy with Delegation of Rights. In Günter Müller (ed.): ETRICS 2006. LNCS 3995. p. 177—191. Springer. 2006.

K. Wouters, K. Simoens, D. Lathouwers and B. Preneel, "Secure and Privacy-Friendly Logging for eGovernment services", Ares 2008 - Proceedings the Third International Conference on Availability, Security and Reliability, March 2008, IEEE Computer Society, p. 1091—1092, March 2008.