F. Moyano, R. Roman, A. Abou El Kalam, M. Lacoste and M. Maachaoui, "Security", *Digital Home Networking*, 2011.
NICS Lab. Publications: https://www.nics.uma.es/publications

Chapter 6

Security

6.1. Importance of Security and Privacy

Security and privacy are two features of paramount importance in today digital life. Although users are often familiar with these terms, they do not usually grasp a comprehensive understanding on how important actually they are, and this is due, to a great extent, to the fact that they are not straightforward concepts at all.

The notion of privacy covers a very broad perimeter, some dimensions of which are still not yet well understood. Privacy can be viewed as "the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others" [WES 67]. This notion can broadly be classified into physical, personal, communication, or information types of privacy. Here, information privacy is the most relevant type to the home network. In this setting, privacy is mainly about protection of the user's personal information, that is, how users can control the collection, dissemination, and use of such information inside and outside the home. We will expand this concept in section 6.1.2.

Chapter written by Anas ABOU EL KALAM, Marc LACOSTE, Mohamed MAACHAOUI, Francisco MOYANO and Rodrigo ROMAN.

On the other hand, security is strongly related to the notion of trust. Risks are always present when an interaction with a system is made, as we can never be sure about the reliability of the system. It is then necessary to reduce risks as much as possible by increasing the users' trust on the system. Trust can be earned by providing relevant protection mechanisms that will make users feel (and be) safe, such as confidentiality, integrity, authentication, reliability and availability. We will introduce these concepts in section 6.1.1. Trust can also become an integral component of the system, where a trust based model will give feedback about the status of the elements of the system to the users or the system itself. We will explain this concept in detail in section 6.4.2.1.

6.1.1 Security considerations in digital home scenarios

There are several considerations of great importance to consider when dealing with security in the context of digital home scenarios. First, it is indispensable providing means to prevent any other user at home and outsiders to read your personal information in the system, hat is, preserving confidentiality. Another important goal is preventing attackers (and other users) to modify the information exchanged among the user and the digital home system, or at least, detecting whether such modification has occurred, what is called integrity of the information. By these two features, confidentiality and integrity, we can ensure some good level of security in the system as an attacker won't be able to sniff (and understand) the information flow in the system nor alter it without being detected. These features are key in a digital home system given the big amount of personal information that must be kept away from intruders (photos, videos, shopping lists, ...).

In order to prevent unauthorized users / attackers from accessing the system, it is required to offer other features as well. Identification and authentication are crucial issues in this context. The former consists of making the user to provide an identification token (maybe a name or a number) before entering the system, whilst the latter requires to prove such identity. So, an authentication process entails an identification process plus checking the validity of the identification token. To make it clearer, an user who says *"I am Moyano"* would be identified in the system, but he would only be authenticated as well if he proves that he really is who claims to be (e.g. by means of his fingerprint). Authentication enables authorization, that is, relating *"users"* to *"rights to do something on objects"*, what it is a key requirement for a digital home system where different users may carry out different actions on different data and devices. That is, thanks to the authentication feature, it is possible to establish rules such that *user A* will be able to *visualize Christmas photos* and *user B* will be granted to *upload a video to the hard drive*, for example.

The security of a system is also closely related to dependability, which can be defined as the property of the system which ensures that "*it never does anything that could not be predicted*" [BCS 07]. Dependability, in turn, entails availability and reliability (amongst others) [ESA 00]. These security features must be fulfilled to prevent, say, Denial of Service (DoS) attacks, that can lead an element of the system (for example, a laptop) to run out of a valuable resource (for instance, memory) and become unable to respond to the users' requests.

6.1.2 Privacy considerations in digital home scenarios

What is personal information? Also called Personal Identifiable Information (PII), it is any piece of data that can be used to identify, contact, or locate a specific person unambiguously (e.g. name, date of birth, medical and criminal records, political opinions). By extension, it also covers any information such as context data from which can be derived precise identification of the person, for instance by linking different databases. Privacy is critical in a many application domains, specially in those where a great amount of PII is managed, such as healthcare (are my medical records correctly protected against unauthorized access?), location-based services (is my location secret?), e-commerce (is my financial data not accessible to anybody?), M2M (is information about my home appliances only available to those who need to know to provision home automation services?) or digital homes (are photographs about my last holidays safe from intruders?).

In today digital life, and above all, in home networks scenarios, a new relevant concept has come up: digital personal life. This idea refers to the fact that person's life is stored in digital formats, such as images, sound or video files. These assets, which can be located in many heterogeneous devices inside the digital home, are critically important since unauthorized users must not be granted access to them. So, the big question that arises is how to control effectively and efficiently all this collection, dissemination, use, storage, and disposal of personal data.

These privacy requirements can be partially formalized using the Fair Information Principles (or Practices) [FTC 98], introduced by the OECD in 1980 [OEC 80]. The two main principles are: i) The user should remain in control of his personal data (sovereignty principle), and ii) The amount of personal data disclosed should be kept to the strict necessity (data minimization principle), only transmitted to those who "need to know". Although these principles are theoretically easy to understand, there are important challenges raised by digital home networking at the time of its application. First, the amount of collected data is huge, pervasive throughout the home, for instance through multiple sensors, RFIDs, or localization technologies,

making it difficult to reconcile with the data minimization principle. Secondly, in such a pervasive, complex environment, unobtrusiveness is necessary for the end-user satisfaction. Thus, the user is totally unaware that data about him is collected, or exchanged. As a consequence a satisfactory tradeoff amongst transparency (i.e. users do not need to know how their systems work) and privacy awareness (users interact with the system in order to manage their privacy) has to be found.

There are other issues with privacy that must be taken into account. For example, in order to provide the user with personalized services (e.g. when the user comes into the living room, the Hi-Fi plays his favourite radio station), the digital home must gather contextual or personal information. However, this information is highly sensitive, revealing identity, presence (I am at home vs. the house is empty), activities and habits. So, how to preserve location privacy and provide these services? Besides, we must take into account the resource limitations in a digital home network, since several devices may present severe restrictions on CPU, memory footprint, bandwidth or power, making it unfeasible the use of complex cryptographic computations, traditionally needed for privacy-enhancing technologies. Finally, it is required to consider where the real frontier between public and private is. The home limit is not the real border between inside and outside as contents are widely shared and may be accessed from inside or outside the home. Users move also between homes and management of home appliances may be performed remotely. As a result, the privacy boundaries become blurred and access control very difficult to enforce.

6.1.3 Trust considerations in digital home scenarios

Trust is an essential point in the everyday communication between humans. It is often based on experience as it is very difficult to find how trust is established. It is frequently associated to belief, reliability, hope or expectation, which indicates its dependency on several parameters and probability. But trust is not only important in relationships between humans; in technology trust is also important among machines, network nodes, etc in a system. For example, trust is very important in peer-to-peer systems as nodes are working together or in semantic web where it is needed to have credibility on the sources where the information comes from. In a home digital scenario it is of high importance that users trust the system as they are due to share or give access rights to contents to other users so they may want to be sure that there are not unauthorized accesses, or in the case where they want to access a file and to be sure that file is not actually a fake one.

In a digital home the functionality of the system is distributed through the whole home network, thus devices need to collaborate with each other in order to provide

the services. For example, multimedia information can be locally stored at multimedia servers, but these contents are played through media players. However, the members of the network do not know in advance how other devices are going to behave (is the device a known member of the digital home? Is there any fault within a certain device? Is the connection to that device slow in comparison with other devices?), thus it is not possible to make a flawless decision on the collaboration processes. As a result, there is a degree of uncertainty in the collaboration between the different devices that must be taken into account.

Uncertainty originates basically from two sources [SRI 07]: information asymmetry (a partner does not have all the information it needs about others), and opportunism (transacting partners have different goals). Opportunism is not a problem in a digital home system, because all the elements of the network work towards the same goal (provide services to the users), and have neither reason nor the will to behave egoistically. However, information asymmetry does exist. The performance of certain devices can be lower than expected, they can malfunction, and they can be even attacked and subverted or disabled.

Trust, as explained previously, can help in providing a solution to the problem of uncertainty (information asymmetry in this particular case). All devices belonging to the system will be able to have a basic amount of trust with each other in order to provide certain services. Besides, a device that behaved satisfactorily and provided a good performance in the past is supposed to be more reliable in the future. Therefore, the devices can store how much they trust other devices inside the system in order to automatically choose the most adequate partner for a particular transaction. Furthermore, in certain cases users can choose which devices will collaborate in order to provide a service (e.g. the media renderer that will play a movie), thus the actual state of the devices and their trust values must be provided to the user (in a way that is meaningful and usable) so he can make a more informed decision.

6.2 Security Requirements of the Extended Digital Home

As mentioned in the previous section, security cannot be ignored in the extended digital home. The main objective is to make sure that the digital personal life of the members of the household (e.g., photos, videos, personal data) are protected from misuse by unauthorized parties. For users to safely and securely access home services, it is thus necessary to compile the corresponding security requirements. This means identifying the sensitive assets to protect, the threats to those assets, and the security objectives to guarantee. It is then possible to determine the security mechanisms to use, and how they should be applied. Therefore, the objective of this section is to show

the general security requirements of a digital home, alongside with the process that was followed to obtain such requirements.

6.2.1 Approach

To be thorough, the security analysis should be performed using a standardized methodology which allows to identify both the importance and the risk related to different assets in the digital home. While there are standard documents for defining system requirements (e.g., the IEEE Standard 830-1998 [IEE 98]), there are unfortunately not many concrete techniques for eliciting security requirements [TON 08]. Some examples are the “asset table” methodology [JAA 08], EBIOS [RES 08], etc.

In those methodologies, the main steps to obtain and refine the requirements are the following: (1) define the central concepts (i.e., what is an attack, an asset, a risk, etc.); (2) define the high-level business-centric goals; (3) define the threats; (4) list the sensitive assets; (5) define, categorize, and prioritize the security requirements; (6) compare the requirements with their implementation in the target system; and (7) perform incrementally some updates to the requirements in the system life-cycle.

The requirements might for instance be derived using two separate methodologies. The results may then be combined and consolidated to derive an authoritative list of security requirements for the digital home. To illustrate the process, we chose the academic-oriented “asset table” methodology [JAA 08]. We also looked at a more industry-oriented risk analysis approach, using the ISO/IEC 15408 [ISO 05] standard to identify the main elements to protect, and EBIOS to obtain the security risks and goals. We briefly recall below the principles of those two methodologies.

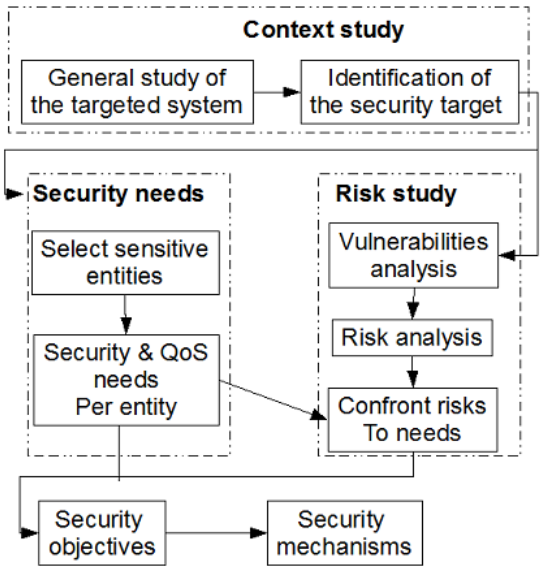

Figure 6.1. *Risk analysis methodology*

The *"asset table" methodology* identifies the different assets that belong to the system. It then describes how they should be protected from the point of view of the customer and the developer. It also investigates how they should be attacked from the point of view of a malicious third party. From the two resulting tables, it is possible to categorize the different security requirements. Although the original methodology focuses mainly on confidentiality, integrity, and authentication, other security aspects need to be taken into account, such as availability, traceability, and privacy.

Risk analysis-oriented methodologies perform a perhaps more thorough derivation of the security objectives. After a preliminary phase where the context of the security analysis is defined, the idea is to identify the security needs (e.g., critical functions, services, and information) and the risks (e.g., vulnerabilities which can be exploited by attackers, security threats). The risks are mapped to the needs to identify the critical entities that must be protected. In a second step, the security objectives and functions that should be considered to overcome the risks and protect the security target are identified. These functions are directly chosen from the Common Criteria (ISO/IEC 15408). This approach is well adapted for security certification processes. Finally, to satisfy the identified security objectives, a number of suitable mechanisms are proposed to be deployed to secure the system under analysis. Figure 6.1 shows the main steps and activities of this methodology.

After performing such an analysis for the extended home network, we obtained properties regarding user and device authentication, access control, communications security, and privacy (mainly in terms of anonymity), for different types of assets (photos, videos, etc.). For more legibility, we categorized the requirements in four main groups as follows: (1) *device requirements*; (2) *user requirements*; (3) *information requirements*; and (4) *privacy requirements*. Privacy might be seen as belonging to the user requirements category, but due to its importance for acceptance of home networking technologies, it will be considered as a separate category. The next four sub-sections present the requirements of each category in more details.

6.2.2 Device Requirements

The main protection requirement is related to the *authentication of the devices* of a household, to avoid the existence of malicious outsiders that may compromise sensitive home resources. In other words, there must exist some security mechanisms (e.g., shared keys, certificates) for authenticating a device that joins the home network. When such a device communicates with other devices of the network, it must already be authenticated. For instance, one may require a device to belong to a single home environment: the device must then be able to prove whose household it belongs to.

Another important requirement is related to *authorization*: the internal information stored within the device must be accessed and manipulated only by those devices and users that are authorized to do so. In particular, sensitive hardware (such as a mobile phone containing critical information) should be *protected against theft*.

Additional requirements concern *traceability*, notably in case of security incident. For instance, there should be in the network or in the home gateway a logging system that reports unusual situations such as anomalous communications of a device to detect if it is being controlled by an adversary. Similarly, as a number of specific devices such as the home gateway will be regularly updated (*device management*), for instance by the network operator, such updates should be identifiable and justifiable. Traceability also covers validity of the licenses of software installed on the devices, and may be guaranteed by mechanisms such as a *Digital Rights Management (DRM)* system. Note that variations of such schemes may also be used to manage privacy in the home network [KEN 02].

Finally, home devices may also be expected to present some *self-healing abilities* in case of failures, i.e., there must be some safety mechanisms that detect and react against extreme conditions in the device. This type of mechanisms may also prove useful if the device is being tampered with, although the mechanisms are then more

related to device *self-protection abilities*. A number of such security schemes have for instance been proposed for SIM cards or RFID tags.

6.2.3 User requirements

Here again, the base line requirements are *user authentication* and *authorization* to protect home resources against malicious users. Mechanisms (e.g., user/password pairs, mobile IDs) for authenticating a user of the extended home are thus required, before giving him access to home services. Such security functionalities may mean defining *user groups* (of friends, family,...): being member of a group then becomes the credential which gives access to a number of services (i.e., to view only the contents of my friends, of my family...), without necessarily disclosing user identities.

Of course, the home network should be *self-managed* as much as possible, for instance, for self-configuration of home resources, safety, or security. In other words, information provisioning should be adapted whenever the physical state of the household changes. In this regard, *context-awareness of security* is particularly important. In the home network, due to embedded constraints, security mechanisms (e.g., chosen cryptographic algorithms) must be able to be adapted (e.g., weakened) to improve quality of service when required by the context (e.g., high system load) [ALI 10].

However, in all those adaptations, the user should still be part of the loop. More than that: the user should take an active role in security management of his home network, thus entailing a number of *usability requirements*. The user must thus be able to configure a number of security parameters (e.g., who is authorized to access his contents, which level of security is suitable for exchanged contents, etc.). The management interface must be easy to understand and easy to use. The user should thus be provided with simple hints regarding the actual level of security, the state of the system, and more generally, any internal information relevant for improving the *user perception of security*.

6.2.4. Information requirements

Those requirements mainly deal with *authorization* from an information perspective, contrary to user- or device-oriented authorization. This means that the information contained in the extended home network must be accessed only by devices and users that are authorized to do so. A way to realize this is to define

"sticky" security policies [MYL 03]: access permissions are associated (an stored) with the information, and travel with it throughout the home network and beyond.

Information requirements also deal with *protection of communication channels*. The system must guarantee security (i.e., confidentiality, integrity, authentication, availability) of the transmission of control and data information. Similarly, data retention issues should be taken particularly care of: information must be stored permanently only in those devices that need to. For others, deletion of contents in remote systems should be performed once they are used.

6.2.5. Privacy requirements

This class of requirements is perhaps the most difficult to enforce, as private data is manipulated by all stakeholders of the extended home, such as users, service, content, and communication providers. Examples include direct identifying information (e.g., name, e-mail), contact lists, group membership information [MAN 08], presence data, histories of service access (e.g., visited Web sites), or personal contents (music, photos, videos, etc.). The user may also be identified using network operator data, or any of the partial identities and attributes disclosed to service providers (which are already used to build detailed user profiles).

Unfortunately, in the home network, the frontier between public and private spheres is no longer the same as the border between inside and outside the home. The very amount of personal data that is manipulated (and its automatic collection) has been raising deep privacy concerns among users. The general perception is that users completely lost control over their private data, and are now totally unaware of where, why, how, and by whom information is being gathered. To win back user trust, exchange and use of personal data should be controlled by enforcing some fundamental privacy principles (as mentioned in section 1.1.2), such as *sovereignty* (the user should remain in control of his data) and *data minimization* (information should be disclosed only to those who need to know). No more data should be collected than necessary, only for a legitimate purpose, and with explicit user consent.

The following points should be checked carefully:

– *Enforceable privacy agreements*: the user should negotiate with service providers conditions of manipulation of private data [PRI 05]. This means giving explicit consent to whom and for which purpose private data is released, by clearly stating user preferences for private data collection, disclosure, and transfer. These preferences should then be enforced with authorization mechanisms. Similarly,

obligations on data usage by third parties should be explicitly stated and enforced by service providers.

– *Multiple identities*: to weaken the link between user and private data, authentication should not be about verifying a single user identity which could be leaked, but about establishing the validity of attributes certified by third parties. This approach [BRA 00][CAM 01] allows users to disclose information about themselves (e.g., age > 21) without need to reveal their real identity (e.g., name) or all their attributes (e.g., age).

– *Anonymous communications*: all links between the user identity and attributes (e.g., the IP address) should be removed to avoid user profiling. Anonymous users should notably be supported in the home network architecture.

– *Flexibility*: in the digital home, the heterogeneity of device, networks, and protocols, and induced collection of conflicting security requirements can only be tackled with a highly customizable security infrastructure. For instance, several cryptographic protocols and formats of certificates will need to be supported. Variable user privacy preferences are also desirable, such as tunable degrees of anonymity. Along the same lines, authorities which certify user attributes may be organized in a combination of different network topologies, leading to architectures ranging from centralized to completely decentralized. The home network security infrastructure must thus provide enough flexibility to support those complex relationships.

6.2.6. Towards service-oriented home network architectures

Home network architectures are increasingly becoming service-oriented [UPN 10][OME 09]. The security requirements identified in the previous sections then become protection requirements to address at the service level. Among a few examples, one can cite:

– *Trusted source*: a home network service should have an origin which is trusted, and which may be checked.

– *Access limitations*: a service must only access parts of the home network that are authorized, and that are needed (principle of purpose limitation to guarantee privacy, e.g., to avoid unwanted collection of personal data). Such limitations may be specified by *contracts*, so that users may be aware of how the home network is going to behave, anytime, anywhere. Contracts may also help to address compliance issues in terms of business and legal requirements.

– *Availability*: A home network service should be available whenever it is needed by the user. This implies dealing with failures, performance bottlenecks, or changes in the environment. It also means performing device and service management

(software packages installation and updates) gracefully so that it has no impact on usability nor security

6.3 A Conceptual Security Architecture

6.3.1 Introduction

From the requirements described in section 6.2 (Requirements for the Digital Home), we can identify a set of security services needed to guarantee those requirements, which together form a Digital Home functional security architecture. The elements of this abstract security architecture, explained in section 6.3.2, could be integrated in an existing digital home architecture. In fact, we will show how to map this functional security architecture to a network architecture that makes use of home gateways (HGW) and operator networks in section 6.3.3, yielding a Digital Home organic security architecture.

6.3.2 Functional architecture

The requirements described in section 6.2 can be classified in three major categories:

– *User requirements*. They not only refer to the definition of different users and groups that implement the information access controls within the Digital Home architecture, but also refer to usability mechanisms that allow users to perceive the actual state of the system. Other aspects such as user authentication and privacy are considered within this category.

– *Information requirements*. They mainly specify user authorization and communication channel protection. The information contained within Digital Home must be accessed only by those devices and users that are authorized to do so. Also, the system must assure the security (i.e. confidentiality, integrity, authentication, availability) of the transmission of control and data information. Other information requirements identify the need of adapting the security mechanisms for improving the quality of service, and the deletion of contents in remote systems once they are used.

– *Device requirements.* The most important requirement is related to the authentication of the devices that belong to a certain Digital Home household, in order to avoid the existence of malicious outsiders that could influence over the system. The existence of logging systems and self-healing systems is also considered, since it is

also possible that one of the devices could be either malfunctioning or being controlled by an adversary.

The requirements identified previously can be addressed with the security components presented in Figure 6.2 (shown as an UML component diagram). We distinguish a core set of security components (user authentication, device authentication, authorization, and cryptographic services), and also a number of extensions (identity management, privacy management, trust management, and context and personalization infrastructures).

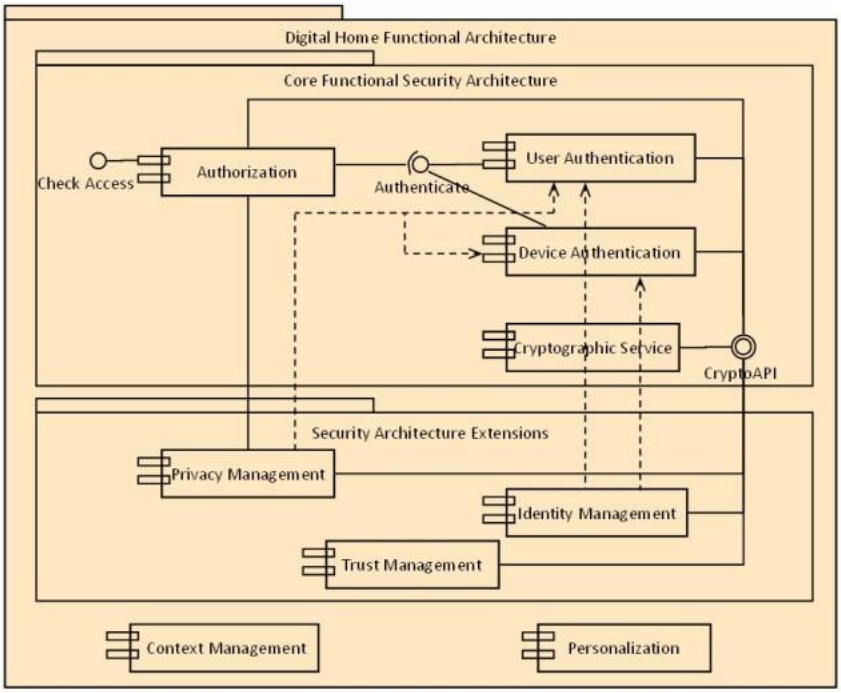

Figure 6.2. *Digital Home functional security architecture*

– The **User Authentication** component identifies and authenticates the different members of the Digital Home platform. It should support the notion of users without credentials (users that do not have any credentials but can access certain parts of the Digital Home platform when working in a local environment) and anonymous users (users that are allowed to access the system but do not want to be explicitly identified). It is used by many other components, such as the Identity Management component.

– The **Device Authentication** component manages the identities of the different devices that belong to a single Digital Home system.

– The **Authorization** component manages the access control rights of each user/group of the Digital Home system regarding to shared contents.

– The **Cryptographic Services** component provides cryptographic mechanisms to protect the interactions between the different Digital Home entities.

– The **Privacy Management** component allows anonymous access to the Digital Home system. It manages users that do not want to disclose their identity and remain anonymous.

– The **Trust Management** component allows the members of the Digital Home system to know the internal state of the system and to manage trust relationships between Digital Home entities.

– The **Identity Management** component allows to manage user identities within a given domain. It is particularly relevant in a multi-operator setting, where users may have their identities managed by several heterogeneous telcos.

– Finally, the **Personalization and Context Management** components are required to address context-awareness in a secure manner.

6.3.3. Organic Architecture

After defining the abstract security architecture, we can show how its different building blocks can be deployed in a specific Digital Home architecture. In this architecture, a home gateway behaves as the interface between the household and the outside world, and a telecommunications operator provides the necessary infrastructure to connect various digital homes.

We now specify where the security building blocks will be deployed and their interrelations. The security architecture is defined at two levels:

– A core architecture focusing on authentication and authorization is presented in section 6.3.3.1.

– An extended architecture enhances the core architecture with security services like identity / privacy management, personalization, or trust management, and is described in section 6.3.3.2.

6.3.3.1. Core Architecture

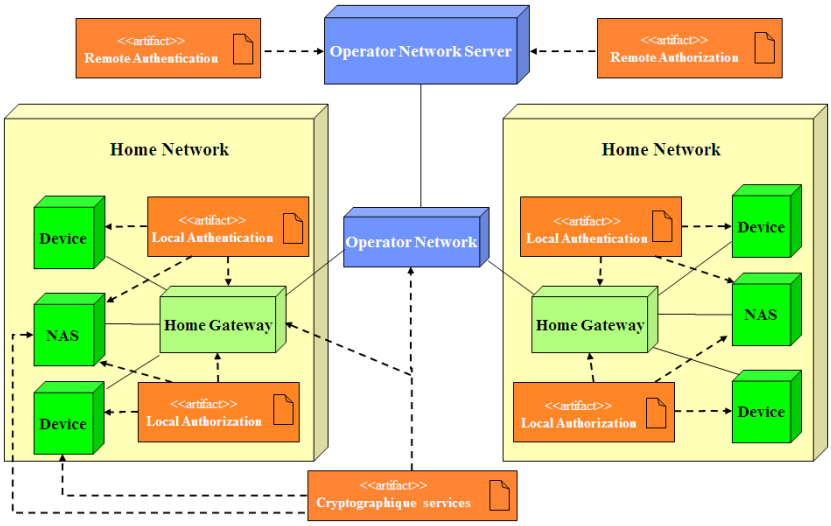

Figure 6.3. *Core Digital Home organic security architecture*

The core Digital Home security architecture, dealing only with authentication and authorization is shown in Figure 6.3. It consists of the following components:

– The *LocalAuthentication* component allows a user or a device to be authenticated to the Digital Home system. This component is located inside the house (in the gateway, behind the gateway or in the user devices).

– The *RemoteAuthentication* component also allows a user or device to be authenticated to the Digital Home system, and is closely synchronized with the LocalAuthentication component. This component is located in the operator network.

– The *UserAuthorizationManager* (also called *LocalAuthorizationManager*) component enforces access control on communications between users. It determines which user (or which house) may establish communications with which other user (or house). This component is located in the operator network.

– The *ContentAuthorizationManager* (also called *RemoteAuthorizationManager*) component enforces access control on contents. This component is located inside the house (in the gateway, behind the gateway, or in the user's devices).

– The *CryptographicServices* component is used by all network entities of the Digital Home architecture to establish secure communications. It thus resides in the devices, gateways, and operator network.

6.3.3.2. Extended Architecture

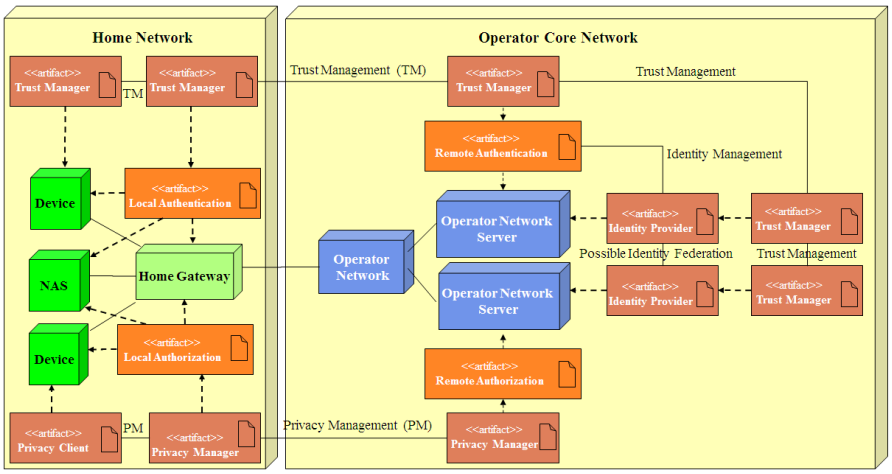

Figure 6.4. *Extended Digital Home security architecture*

The extended Digital Home security architecture enhances the core architecture by adding components for identity management, for privacy management, for personalization and for trust management, as shown in Figure 6.4.

– *Privacy Management*: This component enables anonymous user access to shared contents, simply on the basis of being a member of a group (of users, of friends, of family...). It manages credential issuance (i.e., a user asks to join a group and is given the credentials proving that he is a member) and credential show (a user proves he may access content by showing a proof of his group membership, but without disclosing his identity in a "zero-knowledge" manner). To avoid abuse, credentials may be revoked, or limited in use. Anonymity may also be lifted under special conditions.

The different sub-components of this privacy management infrastructure may be mapped to the Digital Home network architecture as follows.

- *The user* component (privacy client) will generally be located on the user device, and contain an identity selector, directly operable by the user.
- *The Identity provider* component will be responsible for issuing identities as well as credentials such as group memberships. A typical identity domain managed by a single identity provider is built from the identifiers issued by a given telco-several domains being present when multiple operators aim for interoperability of their identity management infrastructures. This component will thus typically be on the network operator side, for instance

in a dedicated server. As credentials may also be issued locally in the home network, in the most general case, this component will include a network part and another directly in the home network, for instance inside or behind the home gateway.

- *The relying party* component verifies the validity of presented credentials. In the Digital Home architecture, its location will be typically identical to that of authorization components, in order to make privacy management transparent to authorization. In the most general case, this component will thus be split in a network part to verify group membership at the user level, and a home network local part in charge of content-related privacy management.
- *The judge* component in charge of conditionally lifting anonymity will typically be embodied by the telco, or by a third party such as a regulatory or police authority. This component will thus be located inside the operator network, or in a dedicated server over the Internet.

– *Trust Management*: Given that there exist many entities in the system (different devices and users), it is necessary to provide certain level of trust among them, in such a way that one entity A can be sure that another entity B will behave as A expects, decreasing the degree of uncertainty in the collaboration between these entities. In order to describe how the trust management model fits in the extended architecture, it is first necessary to locate the different entities of the Trust Management component within Digital Home. The mapping can be done in the following way:

- *CA*: The Certification authority is in charge of generating the certificates given the identity of the user and the public / private keys. It is advisable to put this element in the operator network side (centralized model: operators provide services to homes).
- *RA*: The Registration authority verifies the user requests for a digital certificate, and if the verification is correct, requests the CA to issue that certificate. As with the CA, it is advisable to locate this element in the operator network side.
- *Directory*: The directory acts as a repository for the certificates of all members of the Digital Home, so any user can access it to acquire the certificates of other users. The directory should be located in the operator network side.
- *Client*: The client obtains and makes use of the different certificates, using the cryptographic components to perform asymmetric key operations. This element must be located in the local Digital Home system.

– *Personalization Management*: For personalization management, user profiles are stored in a local home system. That database will be synchronized with an operator

database, which contains more data about each user. Access to contents will be managed in a similar manner, using an operator database storing the permissions for users to access contents, allowing to share content among users.

6.3.4. Discussions

One of the main objectives of the previously explained functional and organic architectures is to provide a secure platform where the members of a particular household could store, access and share their digital personal life. Therefore, it is vital to assure that such information will not be accessed or tampered by unauthorized entities. This subsection will provide some discussions on the robustness of the architecture against potential attackers.

In terms of traffic manipulation, we consider that the network operator acts as a trusted third party. Therefore, an adversary cannot attack the operator core network, although he can be able to attack the home network and the access network, to eavesdrop and to inject traffic. In order to make a complete analysis of the security of the proposed architecture, we will also consider that the attacker can be able to enter the home of the user (e.g. as a guest in a party).

While an attacker may be able to access to the information flow of a Digital Home, he must not be able to manipulate such information. Therefore, on the home side, all communications between Digital Home devices must be protected using existing wireless security standards such as WPA2-AES. Note that a malicious user with physical access to the household could retrieve the security credentials of the wireless channel and access to the information flow. Nevertheless, the attacker still needs to authenticate himself in the Digital Home system in order to use its services (including access to external homes), because all interactions between users and the gateway are protected through the use of the authentication mechanisms and session establishment protocols. Moreover, the attacker cannot create fake media servers, because the gateway is in charge of storing the access permissions. Therefore, the attacker can only access the unprotected entities inside the digital home.

On the side of the access network, the existing standard mechanisms included in the home gateway, together with the authentication and access control mechanisms used to allow only the interaction between authorized Digital Home households, avoid any attacks on the network level. Note, however, that the previously defined architecture does not provide explicit protection to external attacks such as Denial of Service attacks. This must be carefully considered when developing and deploying home gateways in real-world environments.

Precisely, the home gateway is one of the most vulnerable components of a Digital Home. Therefore, it is possible for a well-prepared attacker to physically access a particular household and manipulate the contents of its home gateway. Nevertheless, the attacker will only be able to impersonate the members of that household. Besides, the operator network can make use of intrusion detection systems to detect anomalous activities when a certain gateway tries to connect to other digital homes.

Finally, another aspect that must be taken into account is the status of the operator network and its entities as a trusted third party. As there exists an extremely low chance that one disgruntled employee of the operator network may try to falsify their internal logs, it is necessary to use the public key cryptography mechanisms of the gateway to provide an unforgeable signature of the high-level interactions between households.

6.4 Relevant Security Mechanisms

6.4.1. Authentication

This section provides an enumeration of authentication and access control solutions for telecommunication and Internet services in general, and in particular with respect to the IP Multimedia Subsystem (IMS). All these solutions make use of different “proofs of identity” in order to perform the authentication process.

When implementing authentication, it is necessary to know the difference between message authentication and client authentication. Client authentication ensures that the end points of the communication are legitimate and who they claim they are. Message authentication, on the other hand, ensures the authenticity and integrity of the data during the communication. Client and message authentication are related. For example, it is common that the client authentication process produces temporary session specific credentials (e.g. Master session keys, message authentication keys, message confidentiality keys etc.). These credentials are used to provide message authentication, protecting the authenticity of the data in the subsequent communication.

Also, there are different items that can be used as “proof of identity”. The items used to authenticate an entity include “something you know”, “something you have” and/or “something you are”. “Something you know” is typically a password, while “something you have” can be a private key on a smartcard and “something you are”

is a biometric or similar property that is unique for everyone. The combination of two or three of these items is referred to as two-factor or three-factor authentication.

6.4.1.1. Basic Mechanisms

6.4.1.1.1. Challenge-Response Authentication

Challenge-response authentication is a family of client authentication protocols in which one party presents a question ("challenge") and another party must provide a valid answer ("response") to be authenticated. A simple mutual authentication sequence, where a server and a client authenticate each other using "something they know" (e.g. secret) is as follows:

– The server sends a unique challenge value **sc** to the client.

– The client generates a unique challenge value **cc**.

– The client computes **cr = hash(cc + sc + secret)** (where '+' indicates concatenation).

– The client sends **cr** and **cc** to the server.

– The server calculates the expected value of **cr** and ensures the client responded correctly.

– The server computes **sr = hash(sc + cc + secret)**.

– The server sends **sr**.

– The client calculates the expected value of **sr** and ensures the server responded correctly.

6.4.1.1.2. IPSec

IPSec (IP Security) is a security protocol suite that aims to provide security in the network layer. IPSec consists of AH (Authentication Header and ESP (Encapsulation Security Payload) headers. AH and ESP are headers in IP headers at network layer. AH provides authentication: IP packets with AH headers allow to prove the identity of the packet owner. ESP provides data encryption: IP packets with ESP headers will be protected from other users reading or modifying the packet. Both AH and ESP are security protocols that do not specify the method to perform signature (e.g., message digest with private key). It does not either specify cryptographic algorithms (e.g., 3DES-CBC) and keys for encryption. These protocols will get those parameters from SAs (Security Associations) which include the key exchange protocol (e.g., Internet Key Exchange - IKE) or manual configuration by administrators. In fact, using the

previously shown nomenclature, the AH headers provide message authentication, while IKE and others provide client authentication.

6.4.1.1.3. TLS

The Transport Layer Security (TLS) protocol, which runs in the transport layer, provides confidentiality, integrity, and authentication to client/server applications. It encapsulates application-specific protocols such as HTTP (HTTPS), FTP, and SMTP. The TLS protocol itself can be divided into two layers. The first layer is the Handshake Protocol Layer, which is focused on providing client authentication and consists of three sub-protocols: (1) The Handshake Protocol, which allows the server and client to authenticate each other and to negotiate session information between the client and the server. (2) The Change Cipher Spec Protocol, which is used to change the keying material used for encryption between the client and server. (3) The Alert protocol, which is used to indicate a change in status or an error condition to the peer. The second layer is the Record Protocol Layer, which provides message authentication (among other uses). It receives and protects data from the application layer and delivers it to the Transport Layer.

6.4.1.1.4. Diameter

Diameter is a AAA protocol that is intended to provide an Authentication, Authorization and Accounting framework for applications such as network access or IP mobility. Diameter is also intended to work in both local AAA and roaming situations. Diameter is developed from RADIUS (Remote Access Dial-In User Service) to resolve problems about mobility in WLANs, QoS (Quality of Service) for VoIP (Voice over IP), etc. Diameter operates on top of reliable transport protocols like TCP and SCTP, and assumes that its messages are secured by using either IPSec or TLS, but is not bound to a specific application running on top of it. In fact, it focuses on general message exchanging features, since authentication and authorization are dependent on applications.

6.4.1.2. IMS Authentication

6.4.1.2.1. SIP authentication overview

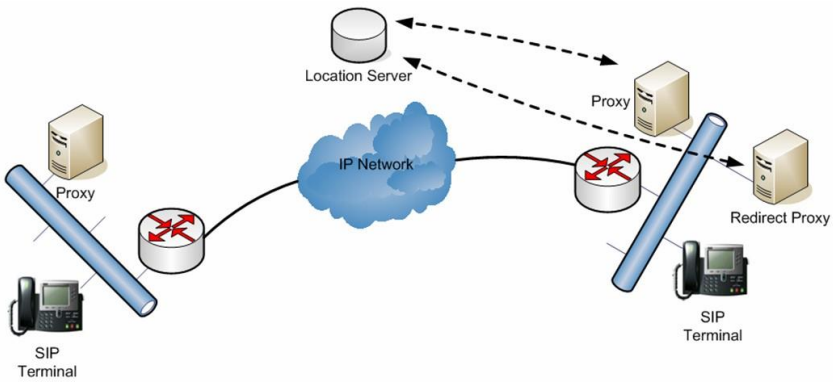

Figure 6.5. *Example of a deployment of SIP*

Session Initiation Protocol (SIP) supported by the Internet Engineering Task Force (IETF) is the backbone of IMS. SIP is a signaling protocol, widely used for setting up and tearing down multimedia communication sessions, such as voice and video calls over the Internet. Other feasible application examples include video conferencing, streaming multimedia distribution, instant messaging, presence information and online games. The SIP architecture defines two main types of devices: clients and servers. A client is described in RFC 3261 as a network element that sends SIP requests and receives SIP responses. Similarly, the server is a network element that receives requests in order to service them, and then responds to those requests. An example of a SIP deployment is shown in Figure 6.5.

The components related to authentication in SIP are less well defined than the authentication components of IMS. Authentication is performed between a SIP User Agent Client (UAC) and a SIP server, e.g. a SIP Registrar. However, there is no specialized security device (like the SIM card in IMS) used in the authentication process. Instead, the authentication is based on username/password authentication, using HTTP Digest authentication (RFC 2617). In a SIP-based network, the authentication can take place between the user agent client and the server (e.g. a proxy, a registrar or a server of another user agent), where the server requires a user agent to authenticate itself with a (user,pass) pair before processing the request. Similarly, a user agent client can request authentication of a server (leading to a two-way mutual

authentication). Note that the use of HTTP Basic authentication (RFC 2069) is not allowed in SIP (cf. RFC 3261).

In a SIP-based system, authentication measures can be enabled at different layers, such as at the application layer, at the transport layer and at the network layer. The typical protocol for security used at the network layer is IP security (IPsec), while Transport Layer Security (TLS) is often used at the transport layer. These two can be used to encrypt the message in transmission. Finally, message authentication schemes based on username/password (such as HTTP Basic Authentication and HTTP Digest Authentication) belongs to the application layer.

Actually, the cryptographic security services from the transport and network layers are not part of the SIP specification. The reason is that SIP is an application level protocol, and according to the latest SIP standard RFC3261 it only provides Digest Authentication service. Using this mechanism the UAC can identify itself to a User Agent Server (UAS) or registrar server, or to a next-hop proxy server. In addition, Digest Authentication supports mutual authentication, where the server also authenticates itself to the UAC. Therefore SIP authentication applies only to user-to-user or user-to-proxy communications; proxy-to-proxy authentication should rely on other mechanisms, like IPsec or TLS.

6.4.1.2.2. IMS authentication overview

The IP Multimedia Subsystem (IMS) is an architectural framework for delivering internet protocol (IP) multimedia to mobile users. It was originally designed by the wireless standards body 3rd Generation Partnership Project (3GPP), and is part of the vision for evolving mobile networks beyond GSM. IMS is intended to provide the access of multimedia and voice applications across wireless and fixed terminals. IMS is explained in other chapters of this book, but here we will provide a small summary of it.

The core functional components for call control, that play a role in the authentication of entities, include Proxy Call Session Control Function (P-CSCF), Interrogation Call Session Control Function (I-CSCF) and Serving Call Session Control Function (S-CSCF). There are also other two major components that manage client authentication in IMS: the user equipment part (client device, UE) and the Home Subscriber Server (HSS) in the core network. The Home Subscriber Server (HSS), or User Profile Server Function (UPSF), is a master user database that supports the IMS network entities that actually handle calls. It contains subscription-related information (user profiles), performs authentication and authorization of the user, and can provide

information about the user's physical location. It is similar to the GSM Home Location Register (HLR) and Authentication Centre (AUC).

Authentication and registration process. For a client to complete its registration (initiated by the REGISTER request) in the system, both the client and the network must be authenticated (mutual authentication). This authentication process, which is explained below, makes use of the Authenticated Key Agreement (AKA) protocol, defined in RFC 3310.

IMS authentication is based on a shared secret and a sequence number (SQN), which is only available in the HSS and the ISIM application on the Universal Integrated Circuit Card (UICC) in UE (i.e. a ISIM card in a mobile phone). As the HSS never directly communicates with the UE, the S-CSCF performs the authentication procedures and all security-related parameters that are needed by the S-SCSF.

When receiving the REGISTER request, the S-CSCF downloads the so-called Authentication Vector (AV) from the HSS. The AV does not include the shared secret and the SQN itself, but does include certain parameters that enable the S-CSCF to perform authentication without knowing the shared secret or the SQN:

– A random challenge (RAND);

– The expected result (XRES);

– The network authentication token (AUTN);

– The Integrity Key (IK); and

– The Ciphering Key (CK).

In order to authenticate, the S-CSCF rejects the initial REGISTER request from the user with a 401 (Unauthorized) response, which includes the RAND, the AUTN, the IK and the CK. When receiving the 401 (Unauthorized) response, the P-CSCF removes the IK and the CK from the response before sending it to the UE. The IK is the base for the SAs (Security Association) that get established between the P-CSCF and the UE immediately afterwards.

After receiving the response, the UE hands the received parameters over to the ISIM application, which:

– Verifies the AUTN based on the shared secret and the SQN - when AUTN verification is successful the network is authenticated (i.e. there is mutual authentication);

– Calculates the result (RES) based on the shared secret and the received RAND;

– Calculates the IK, which is then shared between the P-CSCF and the UE and will serve as the base for the SAs.

Afterwards, the UE sends the authentication challenge response (RES) in a second REGISTER request back to the S-CSCF, which compares it with the XRES that was received in the AV from the HSS. If the verification is successful, the S-CSCF will treat the user as authenticated and will perform the SIP registration procedures.

Whenever the UE sends out another REGISTER request (i.e., due to either re- or de-registration), it will always include the same authentication parameters as included in the second REGISTER request, until the S-CSCF re-authenticates the UE.

6.4.1.2.3. IMS authentication schemes: SIM-based

– *Traditional SIM authentication*. A Subscriber Identity Module (SIM), also known as a SIM Card, is a type of a removable smart card ICC (Integrated Circuit Card). The use of SIM cards is mandatory in GSM devices. Smart cards have been around for several decades and are also used for a range of other - mostly telecom related - applications. The authentication of the subscriber is based on the challenge response mechanism.

– *USIM authentication*. A Universal Subscriber Identity Module (USIM) is an application for UMTS mobile telephony running on a UICC smart card which is inserted in a 3G mobile phone. For authentication purposes, the USIM stores a long-term pre-shared secret key K, which is shared with the Authentication Centre (AuC) in the network. The USIM is in charge of generating the session keys CK and IK to be used in the confidentiality and integrity algorithms of the in UMTS.

– *ISIM authentication*. An IP Multimedia Services Identity Module (ISIM) is an application running on a UICC smart card in a 3G mobile telephone in the IP Multimedia Subsystem (IMS). It contains parameters for identifying and authenticating the user to the IMS. The ISIM contains a private user identity (a NAI address), one or more public user identities (a SIP address) and a long-term secret used to authenticate and calculate cipher keys.

– *Early-IMS authentication*. There are some early IMS implementations that do not fully support the requirements of the 3GPP specification ‘Access security for IP-based services’ (TS 33.203), mainly because of the lack of USIM/ISIM interfaces. For this situation, to provide some protection against the most significant threats, 3GPP defines some security mechanisms, which are informally known as “early IMS security”, in ‘Security aspects of early IP Multimedia Subsystem’ (TR 33.978). The early IMS security works by creating a secure binding in the Home Subscription Server (HSS) between the public/private user identity (SIP-level identity) and the IP

address currently allocated to the user at the GPRS level (bearer/network level identity).

6.4.1.2.4. IMS authentication schemes: non-SIM

– *Username/password*. The use of a username and a password as an authentication mechanism is widespread. It is used in the HTTP 1.0 Basic Authentication, where a client/web browser provides credentials through the use of these two (often small) string values in the HTTP request. The advantages of the username/password-scheme include ease of implementation, ease of use for the clients, and support in nearly all current web browsers. Disadvantages include the need to trust the communication channel (as the transport is done in plaintext) and the human factor of creating easy passwords (or writing hard passwords down on a piece of paper).

– *Smart Card authentication*. The smart card consists of integrated circuits (ICCs) embedded in a pocket-sized card. A smartcard contains a security system with tamper-resistant properties. This may include a secure crypto processor, a secure file system and the capacity to provide security services like confidentiality of information in the memory. This can be combined with biometrics to create two -or three- factor authentication. There are also contactless variants of the smart card. Contactless smart cards use near-field wireless communication (such as RFID) and might allow a user to have the smart-card in the pocket while authenticating.

– *SMS-based authentication schemes*. A SMS-based authentication scheme involves providing the user with a secret key in an SMS, carried through the mobile network. The advantage compared to other username/password-scheme is that the user does not have to remember any password. The key can then be arbitrary complex without the user making a note of it - outside his mobile phone. These improvements in security come at the expense of ease of use: the user needs to copy the secret key using the clipboard of his mobile phone. The SMS can here be regarded as the 'something-you-have' factor in the authentication scheme.

– *Network Access Subsystem (NASS) & bundled authentication*. With the NASS-IMS bundled authentication, the authentication of the access level is re-used at the IMS level. NASS-IMS bundled authentication is very similar to “Early IMS” authentication, and the solution enables authentication at the IMS level by re-using the already authenticated IP connectivity session. A difference from “Early IMS” is that the solution is based on a binding between the IMPI and the user's IP address instead of a binding between the IMSI and the user's IP address. Otherwise, the solutions are in principle similar.

– *MAC address authentication*. An authentication scheme based on MAC addresses uses the quasi-uniqueness in a network device as an authentication token. That is, the security system accepts only authentication requests from a certain set of MAC addresses. Advantages include ease of use and implementation. Disadvantages

include ease of spoofing by sniffing MAC addresses of authorized devices and using it for authentication requests.

6.4.2. Trust Model

6.4.2.1. Trust Model Concept

The ITU-T defines the trust in the area of information technology as follows: “Generally an entity can be said to 'trust' a second entity when the entity first makes the assumption that the second entity will behave exactly as the first entity expects.” [SHI 07]. To ensure the trust between two entities it is necessary to build a trust model that allows two or more entities to communicate in a safe and reliable way.

A trust model could be defined as the set of mechanisms to ensure security against a threat from the system. It is also very important to note that one of the main objectives of a trust model is to accomplish the explicit or implicit validation of an entity's identity or the characteristics necessary for a particular event or transaction to occur. For example, if entity A knows entity B, then A can trust B on forwarding information to other entities (credential-based trust management system). Moreover, if entity A knows that entity B provides a fast and reliable communication channel, A can trust B on sending urgent information (behaviour-based trust management system). This way, and as shown in section 6.1.3, the problem of uncertainty can be solved. Note that we also have to take into account the trust of an user on the system (perceived trust), although this is not based on a single model, but on the combination of various models and elements (e.g. trust, usability, privacy).

6.4.2.1.1. Trust Types

– **Third party trust**: Third-party trust refers to a situation in which two individuals implicitly trust each other even though they have not previously established a personal relationship. In this situation, two individuals implicitly trust each other because they each share a relationship with a common third party, and that third party vouches for the trustworthiness of the two people (Figure 6.6a). Third-party trust is a fundamental requirement for any large-scale implementation of a network security product based on public-key cryptography.

– **Cross certification**: Cross certification works as third-party trust through a certificate authority, but trust can be transferred between domains. If the domain certificate authorities are trusting each other, then users who are under the responsibility of certificate authorities are trusted automatically (see Figure 6.6b).

– **Direct trust**: Users may also establish direct trust relationships between two domains. User accepts as true all (or some subset of) the claims in the token sent by the requestor (see Figure 6.6c).

– **Web of trust**: A web of trust is similar to the direct trust case, but the difference is the relation which continues in a trust chain. This approach is good for scalability since there is no single central server (e.g., certificate authority) to be compromised. Its weakness is that if a node inside the trusted chain is compromised, the remaining nodes will not be trusted. This concept is interesting as it does not require a central server to issue the certificate. The typical example of web of trust is Pretty Good Privacy (PGP) [ZIM 95], often used for signing, encrypting and decrypting e-mails to increase the security of e-mail communications.

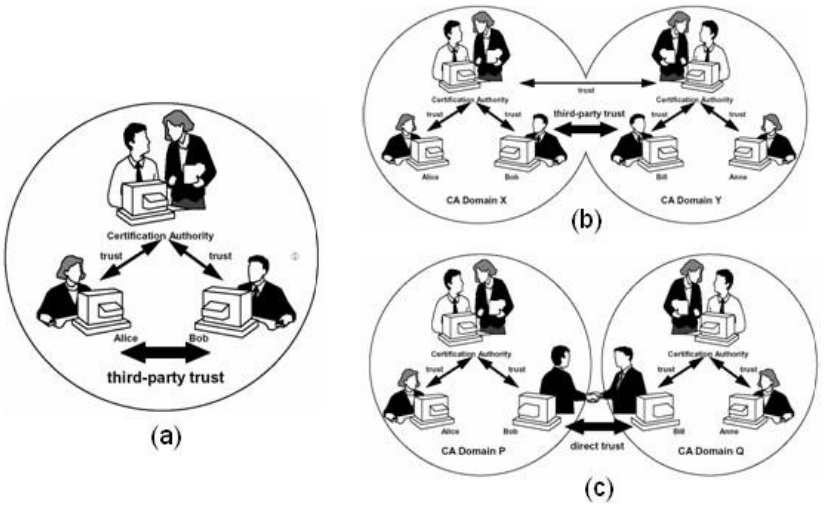

Figure 6.6. *(a) Third party trust through a certificate authority, (b) Extended third-party trust through cross-certification, (c) Direct trust between individuals*

6.4.2.2. PKI trust modeling

This section is focused on the definition of PKI trust model, its key features and the different PKI trust models that are mainly used nowadays. The PKI trust model is a credential-based trust management system that can be used for solving the "entity A knows entity B thus it can trust it" problem.

6.4.2.2.1. Public Key Infrastructures and Certificate Authorities

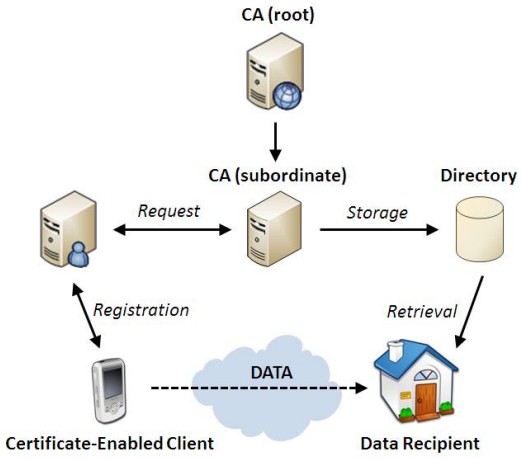

Figure 6.7. *Simplified structure of a PKI*

A public key infrastructure (PKI) is a set of applications and services that allow us to use public key cryptography (certificates) in an easy and effective manner. PKI is based on public key cryptography and its most common usage is reflected in the digital signature. However, how can we be sure that the public key of a user who we found for example in a directory or a website, is really that person and has not been forged by another? How do I trust this public key before we entrust any secrets? The most widely adopted solution is the trusted third party known as Certificate Authority (CA). The basic function of a CA lies in checking identity of applicants for certificates and to create and publish lists of revoked if they are unused. The certificate contains structured information about the identity of its owner, its public key and the CA that issued it.

Hence a PKI can be used to: (1) Key management that enables us to create, revise or revoke keys, and manage confidence levels, and (2) Key publication. Once the keys are created, the PKI can spread our public key and locate the public keys of other users with their state (key revoked, active, etc). PKI facilitates the use of the key once is retrieved. An overview of the structure of a PKI is shown in Figure 6.7.

6.4.2.2.2. PKI Components

A Public Key Infrastructure is formed by the union of several elements that allow the management of the following processes: (1) Key management (create, revise or revoke keys), and (2) Key publication. In particular, a PKI should consist of:

– *Policy Certification Authority (PCA)*: The PCA contains the rules that govern the PKI. A PCA can be represented by one company or several, but usually there is just one representation authority. The PCA sets the security level in an organization, as well as certain procedures (e.g. registration, validity of certificates, key size, encryption types) an policies.

– *Certification Authority (CA)*: The certificate authority is perhaps one of the most important parts of the PKI. A CA consists of a set of tools and files, to verify the identity of a person or server program. The main function of a CA is to validate the information in a certificate issued by the PKI. The CA must be a trusted CA (i.e. a CA that has a globally recognized authority) or secured by a superior CA.

– *Certificate Practice Statement (CPS)*: The certificate practice statement translates certificate policies into operational procedures on the CA level. The certificate policy focuses on a certificate; the CPS focuses on a CA. CPS is defined as a statement about the way that a CA issues certificates.

– *Registration Authority (RA)*: A registration authority provides the interface between the user and the CA. It captures and authenticates the identity of users and delivers the certificate request to CA.

– *Distribution System Certificate*: The digital certificate creates a link to a person, entity, service, etc, with a public key, etc. Then the digital signature ensures the veracity of the link between the certificate we received and the person named in it.

6.4.2.2.3. PKI Functionalities

As described in the previous section, the main function of a PKI is to generate a certificate associated with an entity. The main tasks involved in the PKI are:

Registration and key generation. The generation and registration of keys is essential in security procedures: if a person wants to digitally sign messages or receive encrypted information, he/she must have a pair of keys (a private key and a public key) within a public key system. These keys are generated through a key generation application. Note that the identity of a person is based on the confidentiality of the private key. Therefore, private keys should never travel through the network, and they always should be distributed through reliable channels. Once the key generation process is completed, the user sends the public key and a document signed with the private key to the RA, so that it can complete the registration. In order to make a valid registration, the person that sends the request must attach a digital certificate that proves his/her identity.

Issue of certificate. After receiving a registration request from a certain user, the RA checks if such request meets all requirements and conditions set out in the certificate policies. The RA then forwards the request to a CA, which generates the certificate associated with this particular user. This way, the public key of a user is given validity within the system. The types of certificates that are often used are X509 certificates, which provide multiple fields that are useful in the management of the certificate (e.g. distinguished name (DN), certification path, security policy). The certification authority must know all the time about the status of each certificate. This state storage is known as *lists of revoked certificates* or CRL's. These "black lists" are used to publish the revoked certificates. Thus the entity is exempt from liability for the trust that someone has put on a certificate that has been revoked.

Storing a CA key. Since the CA performs the role of "signer", it must contain a private key. The private key is an extremely important element and must be protected with extensive security measures. To achieve an optimal level of security for CA private keys, it is necessary that this key is generated and stored permanently in a high-security hardware unit, which has been subjected to sophisticated security measures from physical and electronic intrusion. These storage units are known as *certificate signing unit* CSU. The CSU also have mechanisms that destroy the private key if the security was compromised in order to ensure the protection of the information.

Directive service. A directory service is used to store information about users of a network, its resources and also allows administrators to set rules for access to resources for each user. One of the directory service models is the X500 which simplifies operations for storage, obtaining certificates and CRL's management. Each entity is represented by its X500 DN that indicates which is their entry in the directory. X500 defines the required attributes to store the certificates in the corresponding location. If the entity is a CA it's possible to store not only certificates but also CRL's. When an entity wants to obtain access to information or other certificates or CRL's, the first step is to identify the DN of the entity to be consulted and then make a request to X500 directory.

Certification services. In a security environment, the digital signature is one of the most used security techniques. This mechanism makes use of asymmetric keys. To verify the digital signature is necessary to use a public key. Furthermore, in order to verify the identity and reliability of the public key is necessary to check the veracity of the associated certificate. To check the validity of a certificate is required to continue the certification path until reaching a CA that generates trust in the person who is checking the certificate. The process of validation and certification can be done through the following steps: (1) Obtaining the certificate to validate or certify, (2)

Identification of the necessary certificates in the process to establish trust between entities involved and (3) Obtaining certificates identified.

Certificate revocation service. Revoked certificates, as it has been described in the previous sections, are those that in spite the fact that their validity period still active are revoked by the CA. The main causes for which a certificate is revoked are: (1) the associated key has been compromised, (2) the activity for which the certificate was issued has ceased. (3) The owner of the certificate has changed, and (4) the CA decided it due to other causes. The entity to revoke the certificate is the CA but it is also possible that a user generates a request for revocation, but in this case the CA must verify the reasons of this request. Revocation of a CA certificate or its renewal causes that any certificate that depends on it is revoked or renewed in the same way.

6.4.2.3. Other Trust Management Systems

6.4.2.3.1. Experience-based Models

As mentioned before, it is also possible to create a trust model where an entity trusts another entity based on past experience or behaviour. Thus, entities can perform evaluation on the other entities based on these features. These systems are known as behaviour-based trust management systems, and are mainly based on the concept of reputation, which is quite related to the concept of trust. There are several definitions of reputation: Abdul-Rehman and Hailes [ABD 00] define reputation as an expectation about an individual's behaviour based on information about or observations of its past behaviour, while Jøsang et al. [JOS 06] define reputation as a mean of building trust; one can trust another based on its good reputation.

There are some basic properties that any reputation-based trust model should fulfill regardless their field of application:

– *Type of reputation feedback*. Usually an entity A collects behavioral information about other entity B. The information collected can be positive or negative. Some systems are based on negative or positive information whereas others are based on both types.

– *The model of computation*. When A observes the behaviour of B, it needs to update B's reputation accordingly. Besides, by evaluating and storing the reputation of B, it is possible to calculate if B can be trusted for performing certain operations.

– *The metrics*. Usually these values are ranged between 0 and 1 or -1 and 1. They express the reputation of an entity as it is provided by a reputation manager. The values given can be discrete or continuous. Continuous values are considered more expressive than discrete ones.

– *Reliability*. The results provided by the trust model must be consistent with the behaviour of the entities and their expectations.

6.4.2.3.2. Trust and Privacy principles

The privacy technologies, which will be described in the next section, can also be considered as central to the trust-establishment between the user and the system itself. In fact, the following privacy principles are directly related to the perceived trust:

– Explicit privacy rules govern system usage. On top of the anonymous or pseudonymous base system, technical policies determine how to use the system, including policies for trust establishment and reputation establishment, as well as privacy preferences and privacy authorization policies.

– Privacy rules must be enforced, not just stated. Privacy policies are enforced at the receiving end by technical means. The use of personal data and the enforcement of the policies produces enough evidence so that users can actually trust the enforcement and proper use of their personal data.

– Privacy enforcement must be trustworthy. Trust is motivated by building on a trustworthy computing platform and by using assurance methods. Furthermore, external trust mechanisms are implemented that audit data controllers' systems with respect to compliance to legislation and agreed privacy policies.

– Users need easy and intuitive abstractions of privacy. To be useable by nonexpert users, intelligible and intuitive user interfaces are needed that are based on metaphors and mental models that hide technicalities like pseudonyms, linkability and privacy policies.

– Privacy needs an integrated approach. All technical components are integrated into user-side and services-side tools for privacy-enhancing identity management.

6.4.3 Privacy and Anonimity

6.4.3.1. Current Privacy-Enhancing Technologies (PETs)

A considerable amount of research has been carried out to solve the privacy challenges and meet the corresponding requirements shown in section 6.2.5. In order to guarantee privacy in the home network, many building blocks have been available for a long-time but in separate contexts [DES 06]. We will now enumerate these technologies, and afterwards we will provide a detailed explanation of them.

– *Anonymous Communication Systems*. Allow clients to stay anonymous in their communication with other systems.

– *Advanced Cryptography*. Cryptographic primitives used to implement privacy protocols and algorithms.

– *Privacy Policy Languages*. Specify privacy preferences and policies in machine-readable form.

– *Location Privacy*. Protect the location where the information was generated.

– *The DRM Approach*. Use digital rights management technology to provide a privacy management infrastructure.

– *Other Privacy Middleware*. Other PETs such as space-based privacy, tunable degrees of anonymity, and so on.

Anonymous Communication Systems. Most systems providing anonymous communications services over Internet are based on the mix technology introduced by Chaum [CHA 81] for anonymizing emails. The anonymizing network is built from a set of mix nodes, where a node accepts incoming messages and discards all sender identification information from the message headers. Upon some "trigger" condition, the mix node forwards a batch of messages to recipients or to other mix nodes. This approach provides unlinkability between the messages entering and leaving the mix. A number of systems have implemented the mix network architecture (e.g. successive generations of anonymous remailers [MIX 08][DAN 03]). A mix cascade was also implemented in the Crowds [REI 98] architecture for surfing on the Web anonymously.

An alternative to mix-based systems is proposed in the onion routing strategy [GOL 96]. A message (the "onion") traveling through a chain of network routers is encrypted multiple times. A node can only decrypt/process ("peel off") one encryption ("onion") layer at a time. The message is encrypted in the reverse order in which the nodes will receive it, thus setting up a kind of virtual circuit, quite difficult to compromise. This approach to anonymous communications was implemented in the TOR ("The Onion Router") [DIN 04] system for anonymous Web browsing.

Advanced Cryptography. Advances in cryptography are a cornerstone of privacy-enhancing technologies. Many cryptographic primitives such as anonymous credentials [CAM 01], blind signatures [CHA 82], fair-blind signatures [STA 95], group signatures [CHA 91], traceable signatures [KIA 04], or ring signatures [Reiter1998] have been proposed to build privacy-preserving mechanisms - e.g., see [BEN 07] for a comparison of their anonymity guarantees. For instance in group signatures, anonymity is provided by hiding the user inside a group, signing being performed in the name of the group but without being able to link the signature to the user identity. Another example is the anonymous credentials primitive, which offers the possibility to prove properties on private information such as possession of a

credential without actually revealing it (zero-knowledge protocols). Precisely, some of these cryptographic primitives were introduced into certificates to provide anonymity guarantees, e.g., the private certificates explained in [BOU 00], or the extension of the PMI X.509 attribute certificates with anonymity [BRA 00][CAM 01][BEN 06], where the link between identities and attributes is based on pseudonyms.

Privacy Policy Languages. A number of policy languages have also been defined to specify privacy preferences and policies in machine-readable form. The most prominent of these attempts is P3P (Platform for Privacy Preferences) [W3C 07] to define rules for handling of personal information (storage, collection, and usage). The user can be informed of release of private data using a P3P agent. P3P lacks enforcement mechanisms, although a middleware called PawS (Privacy Aware System) [LAN 05][LAN 02] was proposed for negotiation of privacy contracts by checking privacy policies of Web sites against the user privacy preferences. Several P3P agents have been implemented (JRC P3P Proxy, AT&T Privacy Bird). Yet, the P3P expressive power remains limited and its semantics ambiguous. The EPAL [EPA 03] policy language suffers from the same limitations, and is more targeted to enterprise environments.

XACML is a general purpose XML-based access control policy language, which also specifies and architecture for policy decision and enforcement. It is quite comprehensive, with implementations from Sun and Google, and should be one of major building blocks of privacy management systems. Another XML-based description language is WS-Policy, which can serve to specify general policies for Web Services in a domain independent manner using assertions. It could also be used for specification of privacy policies, but privacy assertions are not yet standardized. Finally, the PRIME Project [PRI 08] defined a number of policy languages for privacy-preserving control of resource access, release (from the user side), and data handling (from the service provider side). Targeted applications include e-commerce, health-care systems, and LBS. A user Digital Assistant for policy presentation and processing was also implemented to control private data in an intuitive manner.

Location Privacy. Technologies like contactless and RFID systems raise deep privacy concerns, since they allow fine-grained user tracking. Many protection schemes have thus been investigated [JUE 06]. To protect location information specifically, current techniques include obfuscation by adding noise to location data,

hiding it into dummy traffic [SWE 02]. However, this degrades severely location-based services, accuracy being decreased. Pseudonyms are changed frequently to prevent tracking. Another technique is location cloaking: in the Mist system [CAM 02] a hierarchy of specialized routers forms an overlay network providing a customizable level of privacy, depending on the extent of the zone covered by the router. Space can also be divided into regions connected by "mix zones" [BER 03] where location-based services cannot be used and pseudonyms can be changed to guarantee unlinkability between location and identity. Yet, this model remains complex to implement in practice. In GeoPriv [MYL 03], objects are manipulated both with their location data, and corresponding privacy policy for more efficient enforcement. This type of "sticky" policy is typical of the Digital Rights Management (DRM) approach to privacy management described next.

The DRM Approach and Other Privacy Middleware. Several attempts [KAL 07][KEN 02] have been made to extend the DRM protection model to Privacy Rights Management (PRM). The main idea is that since DRMs allow controlling distribution of digital content, they could also be used to control distribution of private data. For instance, a DRM solution for content shared inside the home was defined in [KEN 02]. Here, a DRM server is defined as control point for accessing contents from inside/outside the home: only devices authenticated as members of a specific domain may access such content. The SIM card of a mobile phone is used as tamper-resistant hardware and to perform cryptographic computations, linked with user devices with a near-field communication (NFC) link. Such ideas could be applied to define a privacy gateway for the home network, the SIM card playing the role of a secure identity selector.

A number of other middleware have also been defined for privacy management for ubiquitous computing environment. One example is the Context Fabric toolkit [HON 04], PSIUM [CHE 05], where personal information is hidden in dummy traffic. Another example are Information Spaces [JIA 02], which defines different spaces containing private data, violations occurring when unauthorized border crossing (social, physical, etc.) occurs between the spaces.

Finally, in [TEN 05] is defined the notion of Quality of Privacy (QoP), similarly to the Quality of Service (QoS), or of context information (QoC). Privacy contracts are defined which specify trade-offs between the value of a service, and the privacy the user is willing to sacrifice to access the service. Thus, tunable degrees of anonymity can be defined between the user and the service provider. Some frameworks like Sentry@Home were designed specifically for the home network [BAG 07].

Standardization Activities. Overall, as of 2011, privacy-preserving infrastructures for the home network are still in their infancy, and standardization activities are only just starting. Among the main standardization bodies active on privacy are ISO/IEC, W3C/OASIS, and ITU.

In ISO/IEC the working group JTC 1/SC27/WG 5 on "Identity Management and Privacy Technologies" is relatively active with frameworks for identity management (24760), for access management (29146), and for privacy (29100, 29101), the latter describing privacy principles for private data handling. In this subcommittee, working groups WG 1 on "Information Security Management Systems", and WG 3 on "IT Security Evaluation Criteria" are also relevant, the notion of privacy being defined explicitly along with different notions of anonymity. Smart cards with contact are also addressed in SC 17/WG 4, but privacy issues are ignored. SC 25 on "Interconnection of Information Technology Equipments" has addressed the definition of security requirements for the home network [ISO 08]. Finally, sub-committee SC 37 addresses biometrics in terms of interfaces, data formats, applications, and integration with smart cards, notably to find the right trade-off between biometrics and privacy.

W3C (World Wide Web Consortium) is the main other active body in privacy management for the home network. The main privacy-relevant specification is P3P [W3C 07]. The many standards for Web Services (XML, SOAP, etc.) are also directly of interest to the home network regarding interoperability between devices, e.g., WSPolicies to define privacy policies. W3C also defined the standards of the Semantic Web such as RDF (Resource Description Format), SPARQL, and OWL which can be used to describe, query, or exchange privacy-related information on resources. In fact, many of these W3C specifications were also transferred to the OASIS standardization organization.

ITU and IETF were also been very active on certificate management infrastructures (X.509 [ADA 99], CRLs [COO 08], PMI [FAR 02], and OCSP [MYE 99]) notably with the PKIX Working Group [PKI 08]. A number of recommendations have also been defined by the ITU-T for authentication (X.8113), authorization X.1114) in the home network, along with home device profiles (X.1112). Finally, other relevant standardization activities include: strong authentication for mobile networks at the 3GPP, NFC and mobile payment in the GSMA, privacy aspects of RFIDs in the M2M Forum, and in the TCG, the specification of the TPM (Trusted Platform Module) to provide hardware security.

6.4.3.2. Privacy at home: privacy and anonymous credentials

Certificates are very useful in a digital home environment, as they attest that users have a given identity ("I am Moyano") or characteristics ("I work for Malaga University"). In fact, digital certificates are one of the most common "proof of identity" tokens that are used by the authentication technologies described in section 6.4.1. However, certificates may contain highly sensitive personal data. They may also be used to track individuals, for example by embedding unique identifiers such as a social security number. In order to address this issue, some PETs were introduced (e.g. the notion of privacy-preserving certificate and PKI [ARD 10][BRA 00]) in certificate management infrastructures.

As a consequence, in this section we will focus on surveying available solutions for privacy-enhanced digital certificate management. We will propose a taxonomy to classify the different families of solutions. Moreover, after explaining the different solutions, they will be analyzed in terms of security, privacy, usability, and implementability properties expected from a user-centric privacy management infrastructure.

6.4.3.2.1. Identity Certificates

Pure Digital Certificates. A digital identity certificate provably binds an individual with his public key through signature by a Certification Authority (CA). X.509 certificates [COO 08] are the most well-established certificates in use today, and the foundation of modern PKIs (as shown in section 6.4.2.2). Standard extensions include policies for certificate and key usage, certification path constraints (such as path length or delegation policies), and improved Certification Revocation List (CRL) management. Pure identity certificates satisfy integrity, verifiability, and unforgeability properties due to the CA digital signature - the holder is also the only party knowing his private key. Also, proof of ownership is possible by signing a message with the private key. However, the main problem is the lack of privacy properties, such as anonymity, unlinkability, and selective disclosure.

Privacy Extensions. A number of extensions to identity certificates were proposed to solve the previous issues [KIM 05]. For instance, the Privacy-Enhanced Permanent Subject Identifier (PEPSI) proposed by the Korean Security Agency (KISA) [LEE 06] provides a privacy-preserving answer to the ambiguity of identification of subjects with distinguished names (DNs): several subjects may have the same DN if several Certification Authorities are involved, making user authentication difficult. In order to lift this ambiguity, instead of using a unique identifier (UID) or permanent identifier

[PIN 05], PEPSI makes use of a double-hashed value of a user sensitive information and of a secret random number generated by the user.

6.4.3.2.2. Attribute Certificates

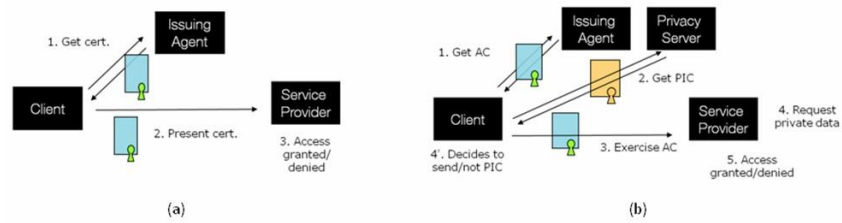

Figure 6.8. *(a) SPKI Access Control; (b) Saito et al. Scheme*

X.509 Attribute Certificates. Besides defining the PKI infrastructure, the PKIX working group [PKI 08] also proposed a PMI (Privilege Management Infrastructure) infrastructure for authorization and attribute management. The main element of this PMI is the Attribute certificate (AC). These ACs, signed by Attribute Authorities (AAs) establish the relationship between the holder identity and a number of attributes [COO 08]. Those attributes generally contain authorization information such as access rights or security clearances.

SPKI Authorization Certificates. The PKIX approach raises privacy issues since user identity information is explicitly encoded in attribute certificates. Separation of authentication from authorization is thus not totally achieved. SPKI (Simple Public Key Infrastructure) [ELL 99] proposes to fully decouple the two functionalities using authorization certificates instead of attribute certificates: authorizations are bound to the holder public key instead of his identity. This approach is more privacy-friendly since the user identity does not appear in access control enforcement, and thus may not be inferred so easily.

An SPKI certificate thus only includes the holder public key and access rights signed by the issuer. Figure 6.8a shows how access control is enforced using SPKI certificates: an Issuing Agent manages identity information independently from the Service Provider and issues authorization certificates to the client after registration. The Service Provider delegates the authority to issue certificates to the Issuing Agent, which plays the role of an attribute authority in the PKIX model, the Service Provider being the Source of Authority. Authorization certificates are then presented to the Service Provider by the client to access the requested resources. SPKI certificates are a first step forward towards anonymous access since the user identification does not appear explicitly. However, further improvements are possible.

SPKI Privacy Extensions. Saito et al. [SAI 01][SAI 03] propose a privacy-enhanced access control scheme using SPKI authorization certificates to manage private information. In addition to authorization certificates, a private information certificate (PIC) is introduced to guarantee the safety of the client's private data, linked with his public key. A new authority, the Privacy Server is added which issues PICs, while authorization certificates are issued by the Issuing Agent as in the original SPKI scheme. The scheme is summarized in Figure 6.8b.

6.4.3.2.3. Anonymous Attribute Certificates

Blind vs. Fair-Blind Certificates. The two main issues to solve with pure attribute certificates are weak anonymity and the absence of conditional release of anonymity. Those issues may be tackled with the two following types of certificates, which may be referred to anonymous or pseudonymous certificates [CRI 04], since the link between identities and attributes is based on pseudonyms.

Blind certificates are based on cryptographic primitives such as blind signatures [CHA 82][CHA 85] where a signer entity does not know anything about the message it signs, and may not link the signed message with its sender. The certificate contains an authenticated token without any identity information. This class of certificate provides very strong anonymity and unlinkability, since external parties may not determine the ownership of the certificate. However, it does not provide any accountability, and is an open door for malicious behaviors. Fair-blind certificates are similar, but a trusted third party may “unblind” the certificate to break anonymity under well-specified conditions, hence providing more traceability to the holder identity. These certificates may for instance be realized using fair-blind signatures [STA 95] where under those conditions a signed message may be linked with its sender. Thanks to this conditional release of anonymity, this class of certificate may for instance be used to prevent money laundering.

Anonymous Attribute Certificates with Fair-Blind Signatures. The University of Malaga proposed a scheme to realize anonymous attribute certificates (AACs) using fair-blind signatures [BEN 04][BEN 06][STA 95], enabling to enhance PMIs with anonymity services. A special type of Attribute Authority (AA), an Anonymous Attribute Authority (AAA), is introduced to issue AACs. Once users have applied for an AAC to the AAA, the AAC can be used to enforce their privileges in the same manner as a regular attribute certificate (AC), except that the process is performed anonymously. This approach thus makes anonymity completely transparent to the authorization process.

The scheme relies on the fact that an AC may be linked to any data structure by introducing a hash value of the structure in the certificate holder field (see Figure 6.9). A pseudonym structure is defined which contains the user (private) pseudonym, the name of the Trusted Third Party (TTP), the conditions for disclosure, and a public key which is a proof, obtained anonymously, that the user satisfies the conditions to obtain the certificate. The structure is signed by the user to prove knowledge of the corresponding private key. The resulting conditionally anonymous X.509 attribute certificate is signed by the AAA.

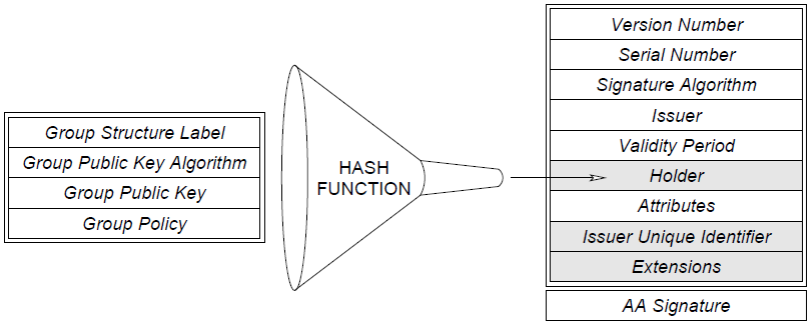

Figure 6.9. *Structure of an Anonymous Attribute Certificate*

Unifying Signature Schemes: Anonymity 2.0. Another design of pseudonymous attribute certificate based on group signatures may be found in [BEN 06]. More generally, many cryptographic primitives such as ring signatures [RIV 01], group signatures [CHA 91], or traceable signatures [KIA 04] have been proposed to build privacy-preserving mechanisms. How to overcome such diversity? The Anonymity 2.0 framework [BEN 07] aimed to support those different signatures schemes within the X.509 standard. It extended the semantics of identity certificates by binding a public key to a concept (e.g., a ring, a group, etc.) grouping a number of entities holding private keys. All entities in the concept may sign messages with their private keys. The signature may be verified using the concept public key. Attribute certificates are bound to identity certificates as before, authorization attributes now regarding concept entities. In fact, this vision to unify identified and anonymous authentication is realized in the X.509 standard through certificate extensions.

Veiled Certificates. Veiled certificates [GER 09] tackle the problem of privacy-preserving multi-credentialing: how to aggregate credentials coming from different independent issuers into a single credential. Veiled certificates are based on the notion

of VC token, a signature by the user of his identity attributes and certificate public key K_p thanks to a dedicated veiled private key k ($VC = E_k(ID,K_p)$). The corresponding veiled public key k_p is only shared with the issuer to enable verification of the VC token ($D_{kp}(VC) = ID, K_p$). The VC token is embedded in a veiled certificate (VC) signed by the issuer, which also contains the user public key and the certificate life-time. The scheme is easily implementable within X.509 certificates by inserting the VC token in an extension field and leaving the subject field blank. Moreover, the computation overhead is comparable to X.509-handling PKIs and is compatible with limited devices.

6.4.3.2.4. Anonymous Credentials

The certificates used in standard PKIs for authentication and authorization provide little anonymity guarantees. Anonymous attribute certificates partly solve this problem. However, it may be feasible to trace a particular user if he uses the same certificate multiple times. Above all, it is not possible to select just a subset of the attributes. Anonymous credentials solutions go one step beyond: only a proof of possession of the credential is communicated to the service provider, for instance by proving a property on the attributes contained in the certificate. In fact, the certificates themselves - also called private certificates - are never transmitted. In the following, we show the design and properties of the two main available schemes as of 2011, namely UProve from Microsoft, and Idemix from IBM.

Credentica/Microsoft U-Prove. The scheme developed by Stefan Brands [BRA 00] is at the core of the U-Prove technology developed by Credentica [CRE 07], now property of Microsoft. U-Prove credentials called ID tokens are cryptographically-protected containers of user identity assertions, and may be seen as privacy-friendly certificates, either short- or long-lived. The token contains a unique random token identifier and its privacy behavior may be tuned thanks to several fields to disclose (resp. unconditionally hide) attributes when showing the ID token to a service provider (Token Attributes resp. Embedded Info fields). Another field (User extensions) allows to hide attributes from the issuer but to disclose them to service providers. This scheme is attractive because of its implementability: integration is possible with frameworks such as Liberty, SAML, CardSpace, or Web Services. The token may be split between the device and a secure hardware element (e.g., TPM) and should be implementable in the mobile phone and/or the SIM card.

IBM Idemix. Idemix is a Java middleware developed by IBM which implements the Camenisch and Lysyanskaya [CAM 01][CAM 06] anonymous credential system. It allows attribute-based authentication and authorization with strong anonymity thanks to the credential multi-show unlinkability property. In Idemix, users are

identified with different organizations by unlinkable pseudonyms. Using those pseudonyms, they obtain credentials from those organizations certifying a set of attributes. Users may then prove knowledge of properties over selected attributes to verifying organizations to access services. A de-anonymization authority allows to recover the pseudonyms or the real identities in case of abuse.

6.4.3.2.5. Analysis and Conclusion

	Properties	**Identity certificates**		**Attribute certificates**	
		Standard Identity Cert. (X.509)	Privacy-ext Identity Cert. (PEPSI)	Attribute cert. (PKIK, SPKI)	Privacy-ext attribute cert. (Saito)
Identity Theft	Integrity	yes	yes	yes	yes
	Unforgeability	yes	yes	yes	yes
	Verifiability	yes	yes	yes	yes
	Non-replay	yes	yes	yes	yes
Privacy	Anonymity	no	yes	limited	limited
	Unlinkability	no	no	no	no
	Selective disclosure	no	no	no	limited
	Multiple credentials	no	no	no	no
Accountability	Pooling prevention	possible	possible	limited	limited
	Accountability	yes	yes	yes	yes
	Revocability	yes	yes	yes	yes
	Cond. release of anonymity	no	no	no	no
Usability	Implementability	simple	simple	simple	simple
	Efficiency	high	high	high	high

Table 6.1. *Properties of Existing Solutions: Identity and Attribute Certificates*

After explaining the different solutions, we will analyze them by considering the following four sets of properties:

– **Identity Theft Prevention**: To avoid identity theft, the following properties should be guaranteed Integrity, Unforgeability, Verifiability, Stealing prevention and Non-replay.

– **Privacy**: For enforcement of the “need to know” principle, the following properties must be guaranteed: Confidentiality, Anonymity, Unlinkability, Selective disclosure, Support of multiple IdPs and Credential aggregation.

– **Accountability**: The following properties are also desirable to guarantee accountability: Pooling prevention, Non-transferability, Revocability, Conditional release and Auditability.

– **Non-Technical Properties**: Finally, the infrastructure must fulfils a number of non-functional requirements which are not security-related but concern more the architecture of the infrastructure, and its relation to the user and environment: Implementability, Usability, Efficiency, Regulatory compliance and Privacy policies.

	Properties	**Blind certificates**	**Fair-Blind certificates**		**Anonymous credentials**	
		E-cash (e.g. Chaum)	Fair-blind cert. (Anonimity 2.x)	Veiled cert.	UProve	Idemix
Identity Theft	Integrity	yes	yes	yes	yes	yes
	Unforgeability	yes	yes	yes	yes	yes
	Verifiability	yes	yes	yes	yes	yes
	Non-replay	yes	yes	yes	yes	yes
Privacy	Anonymity	yes	yes	yes	yes	yes
	Unlinkability	yes	yes	no	yes	yes
	Selective disclosure	no	no	limited	yes	yes
	Multiple credentials	no	no	yes	no	yes
Accountability	Pooling prevention	no	no	yes	yes	yes
	Accountability	no	yes	yes	yes	yes
	Revocability	difficult	yes	yes	yes	yes
	Cond. release of anonymity	no	yes	yes	yes	yes
Usability	Implementability	simple	simple	yes	fairly	fairly simple
	Efficiency	medium	medium	high	medium/low	medium/low

Table 6.2. *Properties of Existing Solutions: Blind, Fair-Blind Certificates and Anonymous Credentials*

Tables 6.1 and 6.2 show an overall view of explored solutions for privacy-enhanced certificates, and their properties. All families of certificates appear well-protected against identity theft, essentially due to the digital signature of the issuer, and to the inclusion in the certificate of a validity date (e.g. expired credentials cannot be used or replayed).

In terms of privacy, as expected, conventional digital identity certificates offer no guarantees whatsoever - although some extensions provide weak anonymity properties. The uses of certificates remain linkable, for instance due to unique identification numbers that are embedded in the certificate. The same assertions

remain true with attribute certificates. Privacy guarantees get stronger with blind and fair-blind certificates, but still lack the selective disclosure of attributes, an essential feature for users really to feel in control of their private data by exercising informed consent. Some pseudonymous attribute certificates also present linkability problems. Those issues are solved with anonymous credentials which offer the strongest privacy properties, for instance with zero-knowledge show protocols. The veiled certificates solution supports multi-credentialing, also possible with anonymous credentials schemes.

Regarding accountability, most types of certificates are generally in some way traceable and revocable in case of abuse. Only blind certificates offer users full immunity for their actions by failing to satisfy those properties. Conditional release of anonymity has little sense for identity and attribute certificates since the anonymity guarantees are weak. The novelty of fair-blind certificates is to be able to lift user anonymity under well-agreed conditions, limiting fraudulent user behaviors. Conditional de-anonymization is also guaranteed by anonymous credentials schemes. Pooling of credentials may only be prevented with the most advanced schemes.

Finally, usability properties are also critical for adoption. Low-privacy solutions have already been widely deployed in existing PKIs. Pseudonymous attribute certificates may generally also be easily inserted in the X.509 standard[2]. Anonymous credentials were theoretically designed to be integrated with open frameworks for easy implementation. Unfortunately, in practice the interface with an external PKI to realize a "privacy-preserving PKI" is not so clear[3]. The performance overhead seems to be the main limitation of those solutions, far from original public announcements. Both Idemix and U-Prove may be implemented on limited devices, which is interesting for the Digital Home context to realize a privacy-preserving PKIs in the SIM or on the mobile. In the Digital Home were actively explored solutions with the strongest privacy properties such as fair-blind certificates and anonymous credentials.

---

[2] Performance might be slightly decreased compared to conventional signatures due to the use of more advanced signature schemes.

[3] For instance, Idemix mostly focuses on the cryptographic layers, the interface with the external PKI not being so very well-defined.

One problem still little considered in all those solutions is how to express user privacy preferences through explicit privacy policies[4]. First policies were already defined [ARD 10][PRI 11]. However, how to integrate privacy-enhancing certificates with attribute-based access control to achieve privacy-preserving authorization [KOL 07] remains for the moment unsolved, and requires much further research [ARD 08][KOL 07].

6.4.4. Usability

6.4.4.1. Exploring the Concept of Usability

There are multiple definitions for usability. According to [LIN 06], it "*refers to the efficiency, comfort, safety and satisfaction with which a wide range of people and under a variety of conditions can perform their tasks with a product (i.e., a good or a service). It is much more than a measure of how easily a thing can be used, and it encompasses all aspects of the product and its use, including the hardware and software interfaces, the documentation, the packaging and even the services associated with the product*"}. In [ROZ 04], it is stated that "*usability is the measure of the quality of a user's experience when interacting with a product or system - whether a Web site, a software application, mobile technology, or any user-operated device. Usability is a combination of factors that affect the user's experience with the product or system, including ease of learning, efficiency of use, memorability, error frequency and severity, and subjective satisfaction*".

So, usability is an important feature to achieve, and from different point of views [USA 11]. From the user's perspective usability is important "*because it can make the difference between performing a task accurately and completely or not, and enjoying the process or being frustrated*". From the developer's perspective usability is important "*because it can mean the difference between the success or failure of a system*". From a management point of view, "*software with poor usability can reduce the productivity of the workforce to a level of performance worse than without the system*". In all cases, "*lack of usability can cost time and effort, and can greatly*

[4] To express obligations when controlling access to private data, either a single policy language may address both access control and privacy issues, or two separate policy languages may be needed, one for access control, and the other for privacy.

determine the success or failure of a system. Given a choice, people will tend to buy systems that are more user-friendly".

6.4.4.2. User Interfaces: Usability and Security Considerations

Given that a (graphical) user interface (GUI, or UI) is the entry point for a user into an application or system and that the user is the weakest link in the security chain, it is indisputable that a secure GUI can improve considerably the whole system security. So, most of the proposals for usable security mechanisms focus on making well-defined, secure interfaces.

From the user's perspective, an UI is usable if the users a) are reliably made aware of the tasks they can perform in the system, b) are able to figure out how to successfully perform those tasks, c) do not make dangerous errors, and d) are sufficiently comfortable with the interface to continue using it. In order to achieve this, usability must fulfill the following goals [CRA 06]:

– *Learnable*: users should be able to learn the basics of the UI once they have interacted with it.

– *Memorable*: users that have previously worked with the interface should be able to remember how to use it. This goal is closely related with intuitiveness.

– *Flexible*: there should be multiple, non-exclusive ways to perform a certain task.

– *Efficient*: the interface provided by the UI should allow users to perform their tasks in a productive way (i.e. as fast as possible).

– *Robust*: the basic operation of the interface should be provided with minimal error rates. If the system fails, the interface is supposed to provide good feedback, so the user can easily recover from the error.

– *Pleasing*: user should be satisfied with the functionality of the UI.

– *Fun*: users must not think that learning and using the UI is a cumbersome task. Instead, users should think that the UI is fun and easy to use.

Any human user making use of a UI that fulfils the previously shown goals can be able to know and trust the system they are interacting with. As a matter of fact, usability is closely linked to trust, as user interfaces play an important role on fostering trust between the user and the system: the UI allows the system to know what the user expects from it, and the UI also allows users to both interact with the system and know its internal behavior.

Nevertheless, knowing how to efficiently interact with the system is not enough to trust it. There is one non-functional aspect that must be taken into account when designing a usable system: security. The digital home provides certain security

mechanisms to users (e.g. file permissions and preferences, credentials for accessing the system), but users must be able to properly perceive and apply these mechanisms when interacting with the system. In order to fulfill the goals of usability (learnable, memorable, flexible, etc) in the area of security, and to gain the trust of the user, any UI must comply with the following principles [JOH 03]:

– *Visibility of system status*: This principle refers to the possibility of observing the internal state of the system. One example of this is the padlock displayed in the botton right-hand corner of some web browsers such as Internet Explorer when visiting a secure web site. The padlock is informing the user about the status of the site.

– *Aesthetic and minimalist design*: It is required to consider a tradeoff among different types of user and the amount of information shown to each of them. Whilst a first-time user will need enough information, too much of it could be unpleasent for an experienced user, and that is why irrelevant information should not be displayed, but just the minimum necessary avoiding technical, complex terms.

– *Help users recognise, diagnose and recover from errors*: It is quite frustrating for an user when an error occurs and no clear information about it is explained. As an example, we could think of an error happening during a banking transaction and one of the following error messages being displayed: 'Your interactive session is no longer active' or 'Error 204'. Obviously, the user would be concerned about the result of the transaction. Besides, it is required to pay additional attention to those errors related to security functions as they tend to have more lethal consequences, so users must be able to know the actual state of the security mechanisms and security state of the system after an error takes place.

– *Satisfaction*: Users often think of security as a very technical, not primary activity topic. Thus, it is necessary that their experience with security features to be satisfying or they will not use them. This could be achieved by means of graphics or humour, as well as designing easy-to-use security functions.

– *Convey features*: The user should be informed by the interface about the availability of security functions. If the user can use some sort of confidentiality feature, the interface should inform him/her that this possibility indeed exists, by means of graphical information. The difference of this criterion with the visibility of system status lies in the fact that the latter informs whether a security issue is being used.

– *Learnability*: Since security is often not a priority for a user, a secure HCI should be as easy-to-learn as possible in such a way that a casual user who has not used the software for some time, should have no need of learning all again. Some guidelines to achieve these goals are the use of metaphors (icons that represent real objects) and the use of conventions and standards. For example, users are in the habit of hearing

the word ‘password’, so it would be confusing to change from this convention to other name such as ‘access code’.

6.4.4.3. Usability dimensions

There are different mechanisms and best practices that can be used to implement or improve the usability in the area of security. To facilitate the analysis of these mechanisms, it is possible to classify them into dimensions, which we could define as features of usability which needs to be analyzed, addressed and measured. According to this definition, usability can be classified into three dimensions in the context of security:

– **Security Mechanisms Usability**: the UI related to the security mechanisms offered by the system must be usable (e.g. which are the usable ways of authenticating a user?). This dimension also refers to the usability of the security mechanisms themselves (when used by network and application designers), but we will focus only on human user-machine interactions.

– **Security Perception / Feedback**: the user must be able to know that a security mechanism is being properly applied (e.g. how does the user know he/she is authenticated?), receiving feedback on this matter.

– **System Status Perception**: the internal state of the system should be known by the user. It is different from the security perception dimension in the sense that it provides an overview of the system as a whole (e.g. are my movies being accessed by someone?), instead of focusing on the feedback provided by a single security mechanism.

6.4.4.3.1. Security Mechanisms Usability

As regards the security mechanisms dimension, its great importance is due to the fact that it is useless and nonsense having, say, a very secure and sophisticated authentication mechanism if the user does not know how to utilize it, because it may happen that she does not use it ever or that she uses it wrongly, turning it into an insecure mechanism.

Some guidelines have previously been given to build well-defined interfaces [JOH 03]. Another proposal in a similar direction is in [HEI 08], where noticeability of messages depends on the salience with which they are displayed. So, given any message, the required salience for that message can be calculated as a function of the message relevance and the confidence with which the relevance was determined. Another interesting approach is the so-called smart, security-aware GUIs [BAS 10].

A security-aware GUI does not display options to users for actions that they are not authorized to execute on application data.

One of the security mechanisms that has been more intensively studied and widely discussed is user authentication [CRA 05]. Traditional authentication mechanisms are based on the "what the user knows" motto, and the most used instance of this principle is the user / password pair. Nevertheless, there are other interesting instances of the "know" principle that try to be more usable: challenge questions (system ask users about information they only know), image recognition (the password is composed by a set of images), tapping (users tap regions of an image in a particular order), and drawing (a sketch drawn by the user becomes the password).

Other authentication mechanisms are based on the "what the user is" motto. Actually, the field of biometrics studies how to identify a user based upon his physical traits (such as his iris or his fingerprints) or his behavioural traits (his typing speed). All these mechanisms can improve the usability of the system: they do not require the user to memorize or write anything, as the token that proves the identity of the user is the user himself. Finally, there are authentication mechanisms based on the "what the user has" motto. Users can carry certain objects such as mobile phones, smart cards, and ATM cards. These objects are supposed to belong only to one particular person, thus a computer system can detect the presence of a certain human being based on the existence of those objects. Note that all these authentication mechanisms are not mutually exclusive. In fact, it is suggested that authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods [FED 05].

On the other hand, the usability of access controls has received limited attention in both the UI and access control communities [BEZ 09]. Classic access control mechanisms such as Access Control Lists (ACL: assigns lists of permissions to an object) and Role-Based Access Control (RBAC: assigns permissions to operations, rather than objects) have some problems. Users seem to not understand the implications on changes in ACL UIs, and RBAC techniques are difficult to understand by non-experts. Still, there are some approaches that can be used to improve the usability of access control systems. Access control UIs should be designed in a way that allow users to easily create a mental model of the actual permissions of a certain object or set of objects, either by improving the visualization of the access controls mechanisms or by representing them textually. Moreover, access control mechanisms should take into account that it is possible to access the elements of a digital home from two different contexts (inside and outside the home).

Also, as privacy is, in most cases, a major concern for users of digital homes, it is also necessary to enhance the usability of all the mechanisms that are related to it. Fortunately, there have been some discussions regarding the usability of privacy [CRA 05]. One solution is to improve user awareness: users should know about how the system is going to manage their data, so they can make well-informed decisions when interacting with the system. Once they make a decision, users should also be able to change the configuration of the system in order to further protect their privacy, and privacy tools should provide the user with feedback about what preventive features are operational. The system should also have some detection features that may discover some potential privacy threats, although these features are not usable if they do not lead the user towards an adequate response. Finally, it is also necessary to analyze what are the elements of the system that, when interacted with, may lead to a privacy leak, and develop some prevention measurements. For example, whenever a user wants to give access rights to a certain user whose identity he knows, the system should provide a photograph of that user next to his name and nickname. This way, the risks of providing access rights to the wrong user is reduced.

6.4.4.3.2. Security Perception / Feedback

As for the security perception dimension, in order for a user to feel confident whilst using a system, he/she must be sure about the degree of security of that system. At first, expressing security to an unexperienced user can be thought to be a hard task. Usually, users do not understand basic, well-known concepts such as confidentiality. Generally solutions are based on both training the users in very basic security concepts and using symbols and procedures which they feel comfortable with.

In [CRA 06] the concept of metaphor is presented as a very useful way of providing the user with security information seamlessly. A metaphor is a visual symbol, an icon that links a security concept with an existing concept in the real life. For example, in some web browsers a small padlock icon is presented in a corner of the window. This padlock can be locked if the website is secure (e.g. if it is using SSL/TLS) or unlocked if it is not. Likewise, in [HOS 00] a comprehensive list of icons for visualizing risks and attacks is presented. Other proposals try to make the users aware of the consequences on acting irresponsibly, making use of approaches such as well-defined alerts and information dialogs [CRA 07], audited dialogs [BRU 07] and peripheral notification [KOW 05] approaches. The first one argues that in order for users to understand the use of security mechanisms, it is necessary to use well defined alerts with enough information about the implications of an action. The second one proposes thwarting false user answers by (1) warning users that their answers will be forwarded to auditors, and (2) allowing auditors to quarantine users who provide unjustified answers. The third approach is peripheral notification and consists of

presenting information leaks in a peripheral display (maybe in the user's screen itself). This way, a user can immediately know what kind of personal information can be accessed by anyone.

Two different approaches which we could categorize into the security perception dimension although they tackle more specific problems are those in [LIE 07] and [NEW 06]. The first one, named Facemail, is an extension to a web mail system that shows pictures of the selected recipients in a peripheral display while the user is composing an email message, preventing users from sending emails to wrong recipients mistyping an email address or getting a wrong email address, what could lead to a potential security or privacy violation. As regards the second one, it deals with trust problems in scenarios where many different devices from different manufactures must communicate with each other. The authors propose two modes of operation for these devices, secure and simple mode, so as to prevent malicious devices from gathering private data.

6.4.4.3.3. System Status Perception

Regarding the system status perception dimension, it is not directly related to any security mechanism, but it can help users to ensure that their systems are behaving as expected. A way to allow users to know and understand the internal state of a system is to show them the underlying mechanisms and activities of that system. This way, users can be able to visualize the existing connections and relationships between different components. Moreover, the connections between internal networks (e.g. the digital home) and external hosts can also be shown. Note that opening the internal behaviour of the system to the users may increase the trust between those users and their systems, but such knowledge may lead to privacy problems as the behaviour of some users can be inferred from the state of the system. Therefore, it is necessary to achieve a balance between being able to perceive the actual state of the system and protecting the privacy of the different users of the system. Nevertheless, it is important to point out that part of the research community [DIG 05] considers that opening the system to the user is important since only end users are effectively capable of determining what counts as secure or insecure, as those users are continuously interacting with their system.

So, in order to obtain a correct, global perspective on how security is deployed on a system, it is important to provide the user with certain information about the system workings and some examples are extracted from the literature next. In [KIN 08], light and sound indicators are proposed for RFID devices so that users can better understand how they work or when they are accessed. [BAL 04] proposes VISUAL (Visual Information Security Utility for Administration Live), a network security

visualization tool that may assist users in seeing the activity of hosts within a network, displaying their relative positions and revealing the ports and protocols used. Finally, a similar tool is presented in [LAK 04], called NVisionIP, which goal is providing a graphical representation of a class-B network current state.

6.5. Applying the Security Architecture

In this section, we describe how the previously defined security architecture (cf. section 6.3) could be instantiated in a IMS digital home architecture and a VPN digital home architecture. Note that these instantiations make use of some of the security mechanisms introduced in section 6.4.

6.5.1. IMS Embodiment

In the IMS embodiment of the Digital Home security architecture, the security components are refined as follows, as shown in Figure 6.10. For access control, the Remote Authorization Manager is implemented in the operator network by a dedicated IMS application server (called AVSIP in the figure), directly linked to the core network. Its main security function is to enforce user-level access controls, i.e., to identify the users and the homes that are authorized to talk to one another. This component may also be extended to manage user groups.

Local authorization as performed by the Local Authorization Manager is refined into an application server behind the Residential Gateway, or RGW (called LAN-AVSIP in Figure 6.10). It provides a high-level view of the contents inside the home shared to outsiders (content catalogue), and manages content-level permissions. Note that such security mechanisms are defined at the middleware level, and rely on standard IMS security for network-level authentication and authorization.

Additional access control mechanisms are also present in the firewall management component to open/close the right RGW ports in order to only accept authorized Digital Home IMS communications after authentication. To manage the private IP addressing scheme inside the home network, the firewall component also performs NAT operations to map the private IP address of a device to the public IP address of

the RGW, and back to deliver incoming packets to the right device. By default, only incoming packets belonging to an outgoing connection will be authorized.

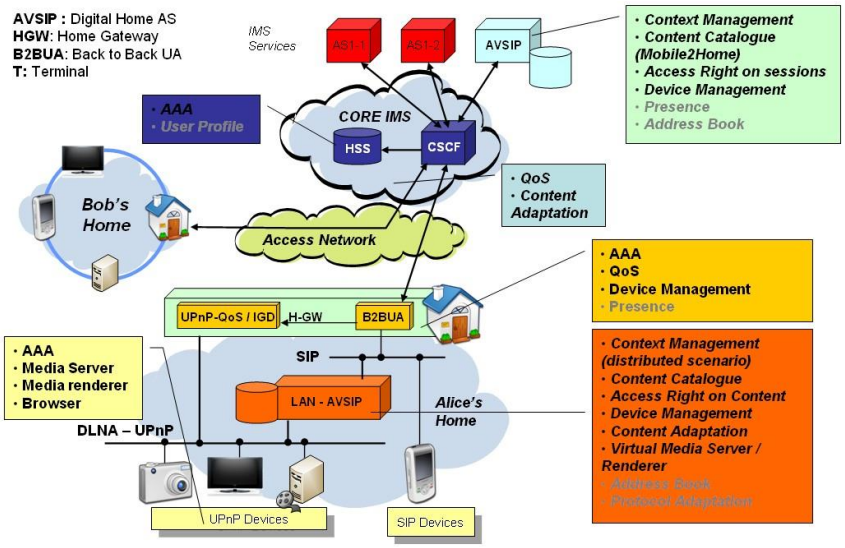

Figure 6.10. *Security components in the IMS solution*

If privacy is not considered at all (i.e., no users are anonymous), privilege enforcement (both in the IMS application server and gateway security server) may be realized using standard access control mechanisms such as capabilities lists or access control lists. The use of authorization/attribute certificates is also possible, but requires the different elements of a PKI/PMI to be deployed in the operator network (e.g., attribute authorities to issue the certificates), and on the client devices (e.g., a privilege verifier to assess the validity of certificates) [PKI 08]. While this approach may seem costly, it offers great flexibility to introduce privacy management features without great modifications inside the infrastructure as shown next.

The abstract view of user-centric privacy management is realized through a privacy-enhanced PKIX-compliant AAI (Authentication and Authorization Infrastructure) called AMISEC [LAC 09] based on anonymous attribute certificates (AAC) [BEN 07][BEN 06]. The Identity Provider part of the privacy infrastructure is implemented by an anonymous attribute authority (AAA) inside the AVSIP application server which issues AACs to anonymously access contents. This component may also lift user anonymity in case of abuse. The Service Provider part is implemented inside the Local Authorization Manager behind the RGW to verify the AACs presented by the user to grant him access to shared content. Finally, an

identity selector on the user's device lets him choose which credential to present to the remote Digital Home system, notably to determine whether access should be anonymous and with which strength.

While such a privacy architecture could have been implemented using anonymous credentials infrastructures [IDE 11][BRA 00], the advantage of the adopted approach is to fully decouple authorization from anonymity management, as privacy management functionalities are just a simple extension to a standard AAI. The AMISEC component-based architecture enables to support different anonymity policies through the use of several types of AACs for different cryptographic schemes (e.g. Traceable Signatures [KIA 04]). Thus, the user may choose its degree of anonymity depending on the type of AAC presented - or no anonymity using a standard attribute certificate, processed by the AAI without involving the privacy management extension.

6.5.2. VPN Embodiment

The second solution to provide remote access to the home contents is based on VPN tunnels created between the considered home and an external server in the operator's network. In order to implement the VPN tunnel, a VPN server is needed so that it manages the connection to the clients. In this architecture, the VPN server is located in the External Server and all the different homes implement a VPN client. The explained distribution guarantees that all the communication (both control and data) travels through the External Server which is a design objective to be able to control the access to the multimedia contents. To create the VPN server and the VPN clients, the software used is OpenVPN.

The External Server is the core of the VPN connection since it processes all the VPN tunnels of the Digital Home external communications. To do so, the External Server incorporates the VPN server and a MySQL database which contains the basic information for the connection to the home environment. The information required by this External Server will be:

– Unique name of the house

– Virtual IP of the house that is, the VPN internal address, to be able to connect to it when requested by the user. The database will make the link of the unique name of the house with its virtual IP

– Public Certificate of the house, used to implement bidirectional authentication in OpenVPN or credentials for user authentication.

The process of registering this information in the External Server is initiated by the residential gateway (RG) or PC in the home. The first time the RG is initiated at home, it establish the VPN connection with the server and sends to it all the information required: the unique name of the house and its VPN address, and the public certificate of the residential gateway that is used to access the house or the credentials used to authenticate different users at home. This process must be done periodically to avoid unwanted events in case of connection loss or changes in the configuration at home. When a user wants to remotely access to his multimedia contents, it should first connect to the external server, which has a known public IP and then it is redirected to the desired home.

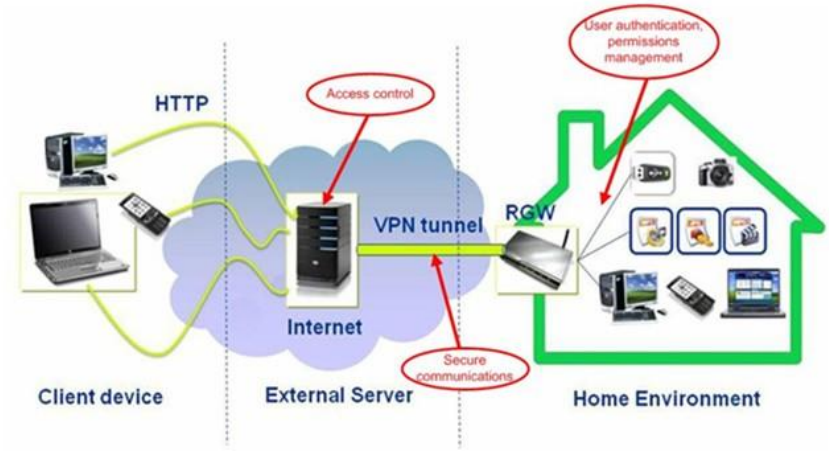

Figure 6.11. *Security aspects to take into account in the VPN scenario*

The main security aspects to take into account are depicted in Figure 6.11.

When accessing remotely, the user should be authenticated. This can be easily done with username and password, although the user can make use of different authentication mechanisms. The process is as follows: the client device will open a connection to the external server, and select an authentication mechanism (e.g. user/password pair). The external server will collect the authentication credentials, and will send it to the RG. Afterwards, the security components contained in the RG will check the validity of the credentials. If the authentication is successful the RG will open a session with the External Server, and the External Server will provide the user with an authenticated session (e.g. through web cookies).

There is also a need of secure communications when the data is traveling over the VPN tunnel to avoid the intrusion of an unknown user. The main reasons to provide security at this stage are the following:

– The fact that the home is regularly sending configuration information to the server. If a malicious user is monitoring the communication, he would be able to obtain this configuration.

– A database poisoning could be performed. In this case, the wrongdoer could send the periodical registration on behalf of the house and in case of success, the user would be sent to a false IP address stored in the database.

Both problems can be easily solved encrypting the communication that travels within the VPN tunnel using a RSA algorithm. The first problem is solved due to the encryption of the data. It is impossible to break the encryption without the private key, which would be securely held by the server. The second problem is also solved with the RSA algorithm since a private key must be used to encrypt the message. If the server receives a message encrypted using other key, the message would be unreadable after decryption and yet the server would not be able to process it. The software that is being used (OpenVPN) implements this kind of security method through the bidirectional authentication mechanism, thus it is a good option. Besides, with this particular configuration, we achieve device authentication, as both the External Server and the RG must provide valid certificates in order to open the secure channel.

Secure Communication is not only limited to the VPN connection, but it also must be taken into account while connecting the clients and the External Server. Since the clients will be using HTTP to connect to the External Server, it is possible to use standard mechanisms such as SSL/TLS in order to protect the communication channel. An additional benefit of this configuration is that we achieve server (device) authentication, as it is necessary to authenticate the server in order to create the channel. Note that with this configuration we do not need client (device) authentication, as the users may connect the External Server from any client device (e.g. a computer in a hotel), and such users must authenticate themselves before accessing the services of the Digital Home.

Also inside the home, an authentication component will be needed to be able to provide multimedia recommendations based on user profile. The External Server will query the RG on the multimedia contents that the user can access, and the RG will filter the contents according to the outputs of the authentication component.

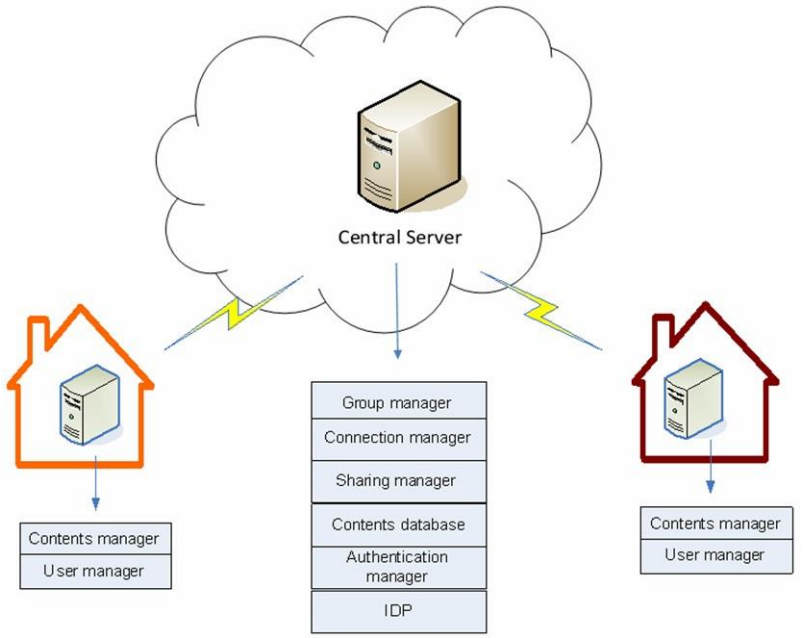

Figure 6.12. *Architecture of the components in the network*

The previous security components explained above can be deployed in the VPN scenario as shown in Figure 6.12. Both, central server and home server, implement several modules which execute all the actions involved in the communication. Regarding the home server, the contents manager, in addition to storing all the multimedia items discovered within the home network, keeps track of which of them are shared and does the task of updating the sharing manager and the contents type database. The user database, stores the usernames belonging to that home and some registration fields. It also updates the authentication manager and the group manager and checks that the username is unique via the IDP.

The central server database integrates 6 different modules that perform specific tasks.

– *Group manager*: It takes care of the groups and homes where the user is included. It must be aware of the updates made at homes and of the communication with other central server modules like the sharing manager.

– *Connection manager*: It manages all the connections process between house and central server. It stores information about how to reach a user and must be able to save that information when missing.

– *Sharing manager*: It incorporates the information that relates the shared content with the owner and the user who the content is shared with. It must keep track of the updates in the content manager of all homes.

– *Contents type database*: It keeps information about the shared content (name, type ...). Note that this DB does not store the contents themselves (e.g. music, video…), but only the different types of contents defined by the user.

– *Authentication manager*: It supplies the security to the system when remote access is exercised.

– *IDP (Identity Provider)*: It has a security goal as well but in this case the IDP deals with the preservation of the unicity of usernames and home names.

Bibliography

[ABD 00] ABDUL-RAHMAN A., HAILES S., "Supporting Trust in Virtual Communities", Proceedings of the 33rd Hawaii International Conference on System Sciences, 2000.

[ADA 99] ADAMS C., FARRELL S., KAUSE T., MONONEN T., "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, http://tools.ietf.org/html/rfc4210, September 2005.

[ALI 10] ALIA M., LACOSTE M., HE R., ELIASSEN F., "Putting Together QoS and Security in Autonomic Pervasive Systems", Proceedings of the 6th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet), 2010.

[ARD 08] ARDAGNA C., CREMONINI M., DE CAPITANI DI VIMERCATI S., SAMARATI P., "A Privacy-Aware Access Control System", Journal of Computer Security, 16(4):369-397, 2008.

[ARD 10] ARDAGNA C., CAMENISCH J., KOHLWEISS M., LEENES R., NEVEN G., PRIEM B., SAMARATI P., SOMMER D., VERDICCHIO M., "Exploiting Cryptography for Privacy-Enhanced Access Control: A Result of the PRIME Project", Journal of Computer Security, 18(1):123-160, 2010.

[BAG 07] BAGÜÉS S., ZEIDLER A., VALDIVIELSO F., MATIAS I., "Sentry@Home: Leveraging the Smart Home for Privacy in Pervasive Computing", International Journal of Smart Home, 1(2):129-146, 2007.

[BAL 04] BALL R., FINK G. A., NORTH C., "Home-centric visualization of network traffic for security administration", Proceedings of the ACM workshop on Visualization and data mining for computer security (VizSEC/DMSEC), 2004.

[BAS 10] BASIN D. A., CLAVEL M., EGEA M., SCHLÄPFER M., "Automatic Generation of Smart, Security-Aware GUI Models", Second International Symposium on Engineering Secure Software and Systems (ESSoS), 2010.

[BCS 07] BCS: The Chartered Institute for IT, "What makes software dependable?", February 2007. http://www.bcs.org/content/conWebDoc/9933

[BEN 04] BENJUMEA V., LOPEZ J., MONTENEGRO M., TROYA J.M., "A First Approach to Provide Anonymity in Attribute Certificates", International Workshop on Practice and Theory in Public Key Cryptography (PKC), 2004.

[BEN 06] BENJUMEA V., LOPEZ J., TROYA J.M., "Anonymous Attribute Certificates based on Traceable Signatures", Internet Research, 16(2):120-139, 2006.

[BEN 07] BENJUMEA V., CHOI S.G., LOPEZ J., YUNG M., "Anonymity 2.0 - X.509 Extensions Supporting Privacy-Friendly Authentication", International Workshop on Cryptology and Network Security (CANS), 2007.

[BER 03] BERESFORD A., STAJANO F., "Location Privacy in Pervasive Computing", IEEE Pervasive Computing, 2(1):46-55, 2003.

[BEZ 09] BEZNOSOV K., INGLESANT P., LOBO J., REEDER R., ZURKO M. E., "Usability meets access control: challenges and research opportunities", Proceedings of the 14th ACM symposium on Access control models and technologies (SACMAT), 2009.

[BOU 00] BOUDOT F., "Partial Revelation of Certified Identity", Conference on Smart Card Research and Advanced Applications (CARDIS), 2000.

[BRA 00] BRANDS S., "Rethinking Public Key Infrastructures and Digital Certificates", MIT Press, 2000.

[BRU 07] BRUSTOLONI J. C., VILLAMARIN-SALOMON R., "Improving Security Decisions with Polymorphic and Audited Dialogs", 3rd Symposium on Usable Privacy and Security (SOUPS), 2007.

[CAM 01] CAMENISCH J., LYSYANSKAYA A., "Efficient Non-Transferable Anonymous Multi-Show Credential System with Optional Anonymity Revocation", Advances in Cryptology (EUROCRYPT), 2001.

[CAM 02] CAMPBELL R., AL-MUHUTADI J., NALDURG P., SAMPERMANE G., MICKUNAS M., "Towards Security and Privacy for Pervasive Computing", International Symposium on Software Security, 2002.

[CAM 06] CAMENISCH J., SOMMER D., ZIMMERMANN R., "A General Certification Framework with Applications to Privacy-Enhancing Certificate Infrastructures", IFIP TC-11 International Information Security Conference (SEC), 2006.

[CHA 81] CHAUM D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981.

[CHA 82] CHAUM D., "Blind Signatures for Untraceable Payments", Advances in Cryptology (CRYPTO), 1982.

[CHA 85] CHAUM D., "Security without Identification: Transaction Systems to Make Big Brother Obsolete", Communications of the ACM, 28(10):1030-1044, 1985.

[CHA 91] CHAUM D., VAN HEYST E., "Group Signatures", Advances in Cryptology (EUROCRYPT), 1991.

[CHE 05] CHENG H.S., ZHANG D., TAN J.G., "Protection of Privacy in Pervasive Computing Environment", International Conference on Information Technology: Coding and Computing (ITCC), 2005.

[COO 08] COOPER D., SANTESSON S., FARRELL S., BOEYEN S., HOUSLEY R., POLK W., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". RFC 5280, http://tools.ietf.org/html/rfc5280, May 2008.

[CRA 05] CRANOR L.F., GARFINKEL S., "Security and usability: Designing secure systems that people can use", Proceedings of the 2nd symposium on Usable privacy and security (SOUPS), 2005.

[CRA 06] CRANOR L.F., GUDURU P., ARJULA M., "User interfaces for privacy agents", ACM Transactions on Computer-Human Interaction, 13(2):135–178, 2006.

[CRA 07] CRANOR L.F., HONG J., REITER M., "Teaching Usable Privacy and Security: A guide for instructors", 2007, http://cups.cs.cmu.edu/course-guide/

[CRE 07] CREDENTICA, "U-Prove SDK Overview", Credentica White Paper, 2007.

[CRI 04] CRITCHLOW D., ZHANG N., "Security-Enhanced Accountable Anonymous PKI Certificates for Mobile E-Commerce", Computer Networks, 45(4):483-503, 2004.

[DAN 03] DANEZIS G., DINGLEDINE R., MATHEWSON N., "Mixminion: Design of a Type III Anonymous Remailer Protocol", IEEE Symposium on Security and Privacy (SP), 2003.

[DES 06] DESWARTES Y., AGUILAR-MELCHOR C., "Current and Future Privacy Enhancing Technologies for the Internet", Annales des Télécommunications, 61(3-4), 2006.

[DIG 05] DIGIOIA P., DOURISH P., "Social navigation as a model for usable security", Proceedings of the 2005 symposium on Usable privacy and security (SOUPS), 2005.

[DIN 04] DINGLEDINE R., MATHEWSON N., SYVERSON P., "Tor: The Second-Generation Onion Router", USENIX Security Symposium, 2004.

[ELL 99] ELLISON C., FRANTZ B., LAMPSON B., RIVEST R., THOMAS B., YLONEN T., "SPKI Certificate Theory". RFC 2693, http://tools.ietf.org/html/rfc2693, September 1999.

[EPA 03] Enterprise Privacy Authorization Language (EPAL). http://www.w3.org/2003/p3p-ws/pp/ibm3.html

[ESA 00] ESA: European Space Agency, "Software dependability techniques", 2000.

[FAR 02] FARRELL S., HOUSLEY R., TURNER S., "An Internet Attribute Certificate Profile for Authorization", RFC 5755, http://tools.ietf.org/html/rfc5755, January 2010.

[FED 05] Federal Financial Institutions Examination Council, "Authentication in an Internet Banking Environment", 2005, http://www.ffiec.gov.

[FTC 98] Federal Trade Commission, "Fair Information Practice Principles, Privacy Online: A Report to Congress", June 1998.

[GER 09] GERDES J., KALVENES J., HUANG C.-T., "Multi-Dimensional Credentialing Using Veiled Certificates: Protecting Privacy in the Face of Regulatory Reporting Requirements", Computer and Security, 28(5):248-259, 2009.

[GOL 96] GOLDSCHLAG D., REED M., SYVERSON P., "Hiding Routing Information", International Workshop on Information Hiding, 1996.

[HEI 08] HEINER A., ASOKAN N., "Using salience differentials to making visual cues noticeable", Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC), 2008.

[HON 04] HONG J., LANDAY K., "An Architecture for Privacy-Sensitive Ubiquitous Computing", International Conference on Mobile Systems, Applications, and Services, 2004.

[HOS 00] HOSMER H.H., "Visualizing Risks: Icons for Information Attack Scenarios", 2000, http://csrc.nist.gov/nissc/2000/proceedings/papers/050.pdf, National Institute of Standards and Technology.

[IEE 98] IEEE STD 830-1998, "IEEE Recommended Practice for Software Requirements Specifications", 1998.

[IDE 11] Idemix (Identity Mixer): Pseudonymity for e-Transactions, 2011, http://www.zurich.ibm.com/security/idemix/

[ISO 05] ISO/IEC 15408-1:2005, "Information technology - Security techniques - Evaluation criteria for IT security", 2005.

[ISO 08] ISO/IEC 24767-1, "Information Technology - Home Network Security - Part 1: Security Requirements", Final Draft, 2008.

[JAA 08] JAATUN M., TONDEL I., "Covering Your Assets in Software Engineering", Proceedings of the 3rd International Conference on Availability, Reliability and Security (ARES), 2008.

[JIA 02] JIANG X., LANDAY J., "Modelling Privacy Control in Context-Aware Systems", IEEE Pervasive Computing,1(3):59-63, 2002.

[JOH 03] JOHNSTON J., ELOFF J.H.P., LABUSCHAGNE L., "Security and human computer interfaces", Computer & Security, 22(8):675–684, 2003.

[JOS 06] JØSANG A., ISMAIL R., BOYD C., "A Survey of Trust and Reputation Systems for Online Service Provision", Decision Support Systems 43(2), 2007.

[JUE 06] JUELS A., "RFID Security and Privacy: A Research Survey", IEEE Journal on Selected Areas in Communications, 24(2): 381-394, 2006.

[KAL 07] KALMAN G., NOLL J., "Right Management Infrastructure for Home Content", IST Mobile and Wireless Communications Summit, 2007.

[KEN 02] KENNY S., KORBA L., "Applying Digital Rights Management to Privacy Rights Management", Computers & Security, 21(7):648-664, 2002.

[KIA 04] KIAYIAS A., TSIOUNIS Y., YUNG M., "Traceable Signatures", Advances in Cryptology (EUROCRYPT), 2004.

[KIM 05] KIM S., WON D., "Privacy-Enhanced Public-Key Certificate: How to Embed an Individual's Sensitive Information into a Certificate", Trends in Mathematics, 8(1):21-28, 2005.

[KIN 08] KING J., MCDIARMID A., "Where's the beep?: security, privacy, and user misunderstandings of RFID", Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC), 2008.

[KOL 07] KOLTER J., SCHILLINGER R., PERNUL G., "A Privacy-Enhanced Attribute-Based Access Control System", Annual IFIP WG 11.3 Working Conference on Data and Applications Security Data and Applications Security, 2007.

[KOW 05] KOWITZ B., CRANOR L., "Peripheral Privacy Notifications for Wireless Networks", Proceedings of the ACM Workshop on Privacy in the Electronic Society (WPES), 2005.

[LAC 09] LACOSTE M., "Architecting Adaptable Security Infrastructures for Pervasive Networks through Components", International Conference on Future Generation Communication and Networking (FGCN), 2009.

[LAK 04] LAKKARAJU K., YURCIK W., LEE A. J., "NVisionIP: netflow visualizations of system state for security situational awareness", Proceedings of the ACM workshop on Visualization and data mining for computer security (VizSEC/DMSEC), 2004.

[LAN 02] LANGHEINRICH M., "A Privacy Awareness System for Ubiquitous Computing Environments", International Conference on Ubiquitous Computing (UBICOMP), 2002.

[LAN 05] LANGHEINRICH M., "Personal Privacy in Ubiquitous Computing - Tools and System Support", PhD thesis, ETH Zurich, 2005.

[LEE 06] LEE J., PARK J., KIM S., SONG J., "PEPSI (Privacy-Enhanced Permanent Subject Identifier) Embedded in X.509 Certificates", International Journal of Computer Science and Network Security, 6(6):204-208, 2006.

[LIE 07] LIEBERMAN E., MILLER R. C., "Facemail: showing faces of recipients to prevent misdirected email", Proceedings of the 3rd symposium on Usable privacy and security (SOUPS), 2007.

[LIN 06] LINFO.ORG, "Usability", http://www.linfo.org/usability.html, 2006.

[MAN 08] MANNAN M., VAN OORSCHOT P., "Privacy-Enhanced Sharing of Personal Content on the Web", Proceedings of the International World Wide Web Conference (WWW), 2008.

[MIX 08] Mixmaster Project Development Page. 2008, http://mixmaster.sourceforge.net/

[MYE 99] MYERS M., ANKNEY R., MALPANI A., GALPERIN S., ADAMS C., "Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol – OCSP", RFC 2560, http://tools.ietf.org/html/rfc2560, June 1999.

[MYL 03] MYLES G., FRIDAY A., DAVIES N., "Preserving Privacy in Environments with Location-Based Applications", IEEE Pervasive Computing, 2(1):56-64, 2003.

[NEW 06] NEWMAN R., GAVETTE S., YONGE L., ANDERSON R., "Protecting domestic power-line communications", Proceedings of the second symposium on Usable privacy and security (SOUPS), 2006.

[OEC 80] OECD, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", 1980.

[OME 09] OMEGA IST PROJECT, "OMEGA Architecture Model", 2009, Project Deliverable D6.1, http://www.ict-omega.eu/.

[PIN 05] PINKAS D., GINDIN T., "Internet X.509 Public Key Infrastructure Permanent Identifier". RFC 4043, http://tools.ietf.org/html/rfc4043, May 2005.

[PKI 08] IETF PKIX Working Group. http://datatracker.ietf.org/wg/pkix/charter/

[PRI 05] PRIME IST PROJECT, "Privacy and Identity Management for Europe", 2005, White Paper.

[PRI 08] PRIME IST PROJECT, 2008, http://www.prime-project.eu/

[PRI 11] PRIMELIFE IST PROJECT, 2011, http://www.primelife.eu/

[REI 98] REITER M., RUBIN A., "Crowds: Anonymity for Web Transactions", ACM Transactions on Information and System Security, 1 (1), 1998.

[RES 08] RESEARCH AND TECHNOLOGY ORGANIZATION, "Improving Common Security Risk Analysis", September 2008, RTO Technical Report RTO-TR-IST-049.

[RIV 01] RIVEST R., SHAMIR A., TAUMAN Y., "How to Leak a Secret", International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), 2001.

[ROZ 04] ROZINOV K., "Are Usability and Security Two Opposite Directions in Computer Systems?".

[SAI 01] SAITO T., UMESAWA K., OKUNO H., "An Access Control with Handling Private Information", International Parallel and Distributed Processing Symposium (IPDPS), 2001.

[SAI 03] SAITO T., UMESAWA K., KITO T., OKUNO H., "Privacy-Enhanced SPKI Access Control on PKIX and its Application to Web Server", International Conference on Advanced Information Networking and Applications (AINA), 2003.

[SHI 07] SHIREY R., "Internet Security Glossary, Version 2", RFC 4949, http://tools.ietf.org/html/rfc4949, August 2007.

[SRI 07] SRINIVASAN A., TEITELBAUM J., LIANG H., WU J., CARDEI M., "Reputation and Trust-based Systems for Ad Hoc and Sensor Networks", On Trust Establishment in Mobile Ad-Hoc Networks, Wiley & Sons, 2007.

[STA 95] STADLER M., PIVETEAU J.M., CAMENISCH J., "Fair Blind Signatures", Advances in Cryptology (EUROCRYPT), 1995.

[SWE 02] SWEENEY L., "k-Anonymity: A Model for Protecting Privacy", International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10:557-570, 2002.

[TEN 05] TENTORI M., FAVELA J., RODRIGUEZ M., GONZALESV., "Supporting Quality of Privacy (QoP) in Pervasive Computing", Mexican International Conference in Computer Science, 2005.

[TON 08] TONDEL I., JAATUN M., MELAND P., "Security Requirements for the Rest of Us: A Survey", IEEE Software, vol. 25, num. 1, p. 20-27, 2008.

[UPN 10] UPNP, "The Universal Plug and Play Forum", 2010, http://www.upnp.org/.

[USA 11] "Why Usability Is Important", http://www.usabilityfirst.com/about-usability/introduction-to-user-centered-design/.

[W3C 07] W3C, "Platform for Privacy Preferences (P3P) project", 2007, http://www.w3.org/P3P/

[WES 67] WESTIN A., Privacy and Freedom, Bodley Head, 1967.

[ZIM 95] ZIMMERMANN P., "The Official PGP User's Guide", MIT Press, 1995.