R. Roman, et al., "Advanced Secure Multimedia Services for Digital Homes", *Information Systems Frontiers*, vol. 14, pp. 527-540, 2012.
http://doi.org/10.1007/s10796-010-9258-9
NICS Lab. Publications: https://www.nics.uma.es/publications

Advanced Secure Multimedia Services for Digital Homes

Rodrigo Roman · Javier Lopez · Olivier Dugeon · Marc Lacoste · Pierre Plaza Tron · Marta Bel

Abstract Our society is becoming increasingly more IT-oriented, and the images and sounds that reflect our daily life are being stored mainly in a digital form. This digital personal life can be part of the home multimedia contents, and users demand access and possibly share these contents (such as photographs, videos, and music) in an ubiquitous way: from any location and with any device. The purpose of this article is twofold. First, we introduce the Feel@Home system, whose main objective is to enable the previously mentioned vision of an ubiquitous digital personal life. Second, we describe the security architecture of Feel@Home, analyzing the security and privacy requirements that identify which threats and vulnerabilities must be considered, and deriving the security building blocks that can be used to protect both IMS-based and VPN-based solutions.

Keywords Digital Home · Content Sharing · Multimedia · Security · Privacy

1 Introduction

Wherever we look, we find that technology surrounds us, becoming part of our daily lives. Even the pieces that store our personal memories, such as photographs and videos, are stored in digital form. As human beings, we like to watch and share these pieces of our lives with other human beings: the rise and impact of social networking tools such as Facebook are an example of this particular need.

Precisely, linking our digital personal life with the capabilities of a smart, digital home is the main objective of the Feel@Home project (F@H 2010). By taking advantage of the technologies and protocols that are available as of 2010, the Feel@Home project envisions an environment where a human being can access his own multimedia contents from any place, whether inside or outside the home. Moreover, this vision also includes accessing remote contents (e.g. looking the photos of relatives or friends). As all multimedia information will be stored within the digital home of the user, we need to provide an architecture and certain protocols that can support content access and sharing.

However, the security and privacy of the overall architecture and the members of the household is an essential element that must be taken into account. Therefore, the purpose of this article is not only to present the Feel@Home system and how it can be implemented with technologies that are already available, such as IP Multimedia Subsystem (IMS) and Virtual Private Networks (VPN), but also to describe which are the security building blocks that must be created in order to create an interoperable security architecture. The structure of this article is as follows. Section 2 introduces the Feel@Home system and its abstract architecture, including how it can be instantiated to make use of IMS and VPN technologies. Section 3 provides the security requirements of Feel@Home and the specification of its security architecture. Section 4 describes how the security architecture can coexist with VPN and IMS networks. Finally, section 5 concludes the paper.

R. Roman, J. Lopez
University of Malaga
E-mail: {roman, jlm}@lcc.uma.es

O. Dugeon, M. Lacoste
France Telecom
E-mail: {olivier.dugeon, marc.lacoste}@orange-ftgroup.com

P. Plaza, M. Bel
Telefonica I+D
E-mail: {pierre, martabm}@tid.es

2 Feel@Home

2.1 Smart Homes, Multimedia, and Feel@Home

The evolution of smart homes has not been happening as fast as the analysts had predicted, but several factors are now enabling the advancement of the internet-enabled smart homes and its associated products. For example, most of the devices for home automation, entertainment and security are, as of 2010, integrating networking capabilities at cheaper prices. Also, Home Gateways (also known as Residential Gateways - HGW) (HGI 2008) could be used to handle and manage the services from the broadband public accesses into the homes, taking into consideration the mix of technologies in the home networking arena (e.g. WiFi, Ultra Wide Band, Home-Plug, G.hn). In fact, there is already a market for HGW in Europe, with commercial products such as BT Home Hub (BT), Livebox (France Telecom), and Alice Gate (Telecom Italia).

It is necessary to consider that smart homes must not be limited to the acquisition of contents from traditional service providers (e.g. through IPTV (Mas et al 2008)). One traditional example falls within the realm of home automation: a smart home can include intelligent devices that are capable of monitoring the state of the household and react against changes in the environment (e.g. turning off certain lights to save energy). There also exist a certain aspect that must be taken into account when developing services for smart homes: our *digital personal life*. Everyday, we create memories that are stored in digital form (e.g. photographs, videos), and we like to share this information with relatives and friends, as proven by the success of social networking sites.

Precisely, the main objective of the Feel@Home system is to fulfil these needs. A certain part of the users' multimedia information (e.g. their digital personal life) will be stored in the smart home, and it will be possible to access that information in an ubiquitous way. Besides, services will be adapted depending on the context and without basically any intervention, no matter the terminal or network users are connected to. In particular, the main services that the Feel@Home system will provide are as follows:

- *Local access to multimedia home library*: From inside his home, a user will be able to retrieve all multimedia content stored in any device (e.g. PC, server, hard drive) and play it in any available player (e.g. TV, HI-Fi, mobile phone).
- *Remote access to multimedia home library*: When a user is outside his home environment, he will be able to access all the multimedia contents stored at home. It will be also possible to simultaneously watch a multimedia content with a relative or friend and comment on it.
- *Sharing content with relatives and friends*: A user can provide access rights to friends and relatives so that they can access the multimedia contents the main user has given permission to.

2.2 Feel@Home and the State of the Art

As of 2010, there are many services in the market that deal with digital content. We can classify them into two major categories: Internet Services (e.g. Flickr, Youtube, iTunes) and Home Systems (e.g. Commercial Home Media Centers (by manufacturers such as HP and Microsoft), Freevo).

- *Internet Services* allow users to store their digital personal life without relying on physical devices located in their households. Such digital information can be accessed anytime and anywhere through the use of web interfaces. Nevertheless, there is no unified service to share contents (e.g. audio, video, pictures), they usually cannot be used to discover contents located at the home, and the location of information is based mostly on tags.
- *Home Systems* are physical devices that usually connect to the home network of the users in order to provide access to their digital personal lives. In addition, they are able to offer other services such as remote access, content sharing, and support for home automation. However, most of these systems are not able to discover other media players located at the home, and many of them are difficult to configure, and provide limited metadata support.

In comparison with these systems, the aforementioned Feel@Home architecture will unify in one application the discovery of contents at home (servers at home) and the ones shared by other users with us. It will be able to discover all players and renderers available at home, and will also provide the possibility to share contents with friends or family in a secure way and access the contents from any location. Furthermore, the content management system being developed will be able to store metadata along with the content, allowing browsing and searching content conveniently by useful characteristics that are not available in state-of-the-art systems. Finally, Feel@Home allows the addition of new services regarding external internet services, local home automation systems, Quality of Service (QoS) and security and privacy.

2.3 Feel@Home Architecture: An Overview

The Feel@Home architecture aims to support various underlying technologies that are already in the market, like IMS, VPN, Digital Living Network Alliance (DLNA), and Universal Plug and Play (UPnP). Such technologies are able to set up and link home networks, and allow customers to share contents. In addition to content sharing, the architecture must allow customers to access to its own contents from anywhere, that is, in nomadic and mobility access. By nomadic we mean an access to the network from a hot spot (e.g. hotel, airport, railway station) and by mobility we mean an access from a mobile terminal i.e. 3G UMTS. Moreover, the Feel@Home architecture must allow visitors (i.e. people who are physically visiting a Feel@Home-powered household) to access the contents as if they were accessing remotely.

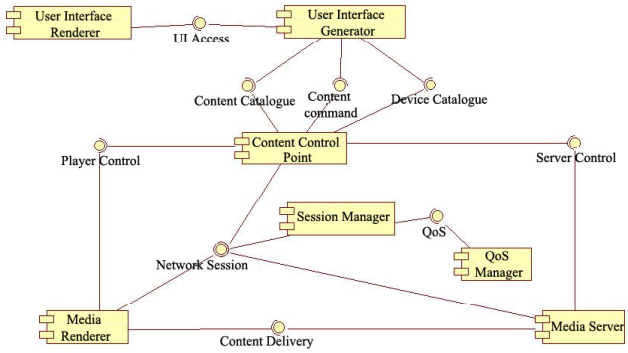

Fig. 1 Feel@Home Abstract Architecture

2.3.1 Common Framework and Abstract Architecture

For the development of the Feel@Home architecture, the first task was to define a *common framework* where customers could be able to easily share multimedia content. An overview of this framework is as follows: A Home network is composed of UPnP and/or DLNA devices which store and render multimedia contents. All are linked to a HGW which allows devices to access outside the Home Network. This HGW has several functions (HGI 2008) and manages the Home Network address scheme within a private IP subnet. From an external point of view, the Home Network is protected with a firewall, and a private address schema is handled through network address (port) translation (NAT(P)).

As we need to establish a connection or a session between two Home Networks, we must handle both firewall pinhole controls as well as linking two private address zones which could potentially share the same subnet. Besides, setting up a session may not be enough to create a successful connection: sharing content could potentially require a huge amount of network resources like bandwidth, low delay, low packet loss, etc. These requirements have a direct and great influence on the Quality of Service. Note that the Feel@Home consortium considers the use of the recent UPnP QoS v3 (van Hartskamp 2008) specification to manage the QoS on the Home Network, linking this QoS control with the one done in the Network Operator to guarantee end-to-end QoS.

After defining a common framework, the next step was to abstract the different technologies in order to produce a *generic architecture*. By using the Unified Modeling Language (UML) to draw a first abstract view of the architecture, we identified the generic building blocks necessary to share and access to the multimedia contents (cf. Figure 1). Feel@Home is designed around a Content Control Point, a Session Manager and a QoS Manager. The Content Control Point collects and manages the list of all multimedia contents of the customers located in the Home Network devices through a Catalogue. It also offers a User Interface to the customer in order to manage its catalogue, share and retrieve multimedia contents. The Session Manager role consists of establishing the session between the two Home Networks in order for the Media Server (i.e. container of multimedia information) to send content to the Media Renderer (i.e. player of multimedia information). It is solicited by the Content Control Point when the customer wants to view a content (local or remote) or by its peer when a remote customer want to access to a remote content.

The Session Manager could also request the help of the QoS Manager to guarantee end-to-end QoS. Once the Content Control Point needs QoS, it must use the Session Manager together with the QoS Manager, as the QoS setup is linked to the notion of session. Indeed, controlling and enforcing QoS imply that the 'start', 'end' and 'where' parameters (i.e. the parameters associated to a certain multimedia content) must be known in addition to standard QoS parameters such as bandwidth and class of service. Note that the Content Control Point could request a content sharing between a Media Renderer and a Media Server without using the Session Manager. This is the case when the media is shared inside the Home Network without QoS.

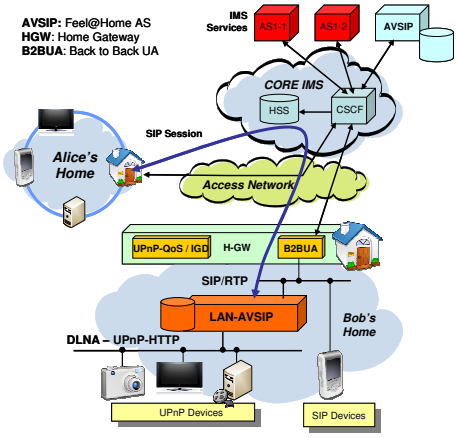

Fig. 2 IMS Scenario Architecture

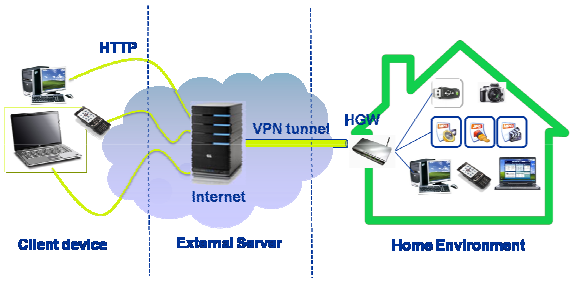

Fig. 3 Overview of the VPN Scenario Architecture

2.3.2 IMS and VPN implementation

From the specific use cases and implementation technologies analyzed in the Feel@Home project, the use case that considers the *IP Multimedia Subsystem (IMS)* alongside with the Session Initiation Protocol (SIP) has numerous advantages. First of all, SIP/IMS allows native session establishment, which takes into account the NAT(P) and firewall problem (i.e. link between public and private addresses, opening ports for incoming connections). In fact, the HGW includes a SIP proxy, and this SIP proxy can modify the Session Description Protocol (SDP) context according to the NAT(P) configuration, and can also open a pinhole in the firewall whenever a new SIP session is set. The second main advantage of SIP is to natively interact with QoS. Indeed, the IMS specification has standardized the Resource Allocation Control Function (RACS) to perform Call Control Admission and QoS setup in the Network Operator, which allow QoS guarantee.

Nevertheless, as stated in the beginning of section 2.3, Feel@Home aims to support technologies such as UPnP and DLNA. With these technologies, SIP IMS can not be used "as is": SIP and UPnP are not only two different protocols, but also are too far in their philosophy to envisage a one-to-one mapping of messages. In addition, SIP can negotiate a session for a specific application (i.e. RTP for voice), while UPnP is also a web services framework that allows a specific application to give a service in the Home Network. As a result, the mapping between SIP and UPnP could only be feasible at the application level (Chintada et al 2008).

In the IMS scenario, the Content Control Point takes the form of an IMS Application Server (AS). This AS is present in both home and operator networks, and an overview of this solution is presented on Figure 2. In the operator network it acts as a normal AS, triggered when a SIP session is initialized by a customer to access sharing content. On the other hand, The AS in the home network has a double stack, and it can support both SIP and UPnP. It can act as a Virtual Media Renderer or Virtual Media Server for the UPnP side, and can also act as a Back-to-Back User Agent (B2BUA) for the SIP side. A transport protocol adaptation is also provided by the AS: SIP uses RTP, while UPnP uses HTTP for media transport. Note that this adaptation could be avoided for DLNA devices using the RTP option for media transport. Finally, regarding QoS, the local AS can act as a UPnP QoS control point to manage QoS in the home network, detailing in the SIP SDP context the needed QoS for the operator network.

Another possible solution to offer remote access to the home contents from any location is to establish a *Virtual Private Network (VPN)* between the remote client device and the home where the contents are stored. In that case, the remote client device would become one more device in the home network and would have the ability to perform all available operations as if it was located inside the home. However, just establishing a VPN between the remote device and the home network would imply that all possible remote devices will have to implement a VPN client, which is not portable due to the huge amount of possible client devices and that is a very hardware-dependent solution.

That is why the proposed solution also introduces an external server that would be located in the operator's network and which is used to overcome the NAT(P) problem by establishing a VPN connection between itself and the home environment. The process should be initiated by the HGW located inside the home by registering itself in the external server and running a VPN daemon to connect to the external server. Whenever a customer wants to access remotely the digital home contents, he should contact the external server. As customers will use PCs and mobile IP-enabled de-

vices which normally include a browser, the external server incorporates a web server responsible of listening to the client requests and calling the appropriate home environment though the VPN connection established before to gather the digital home contents. Figure 3 actually shows a global overview of the VPN solution architecture.

Although IPSec may provide basic secure (at network-level) connectivity between digital homes, a richer set of protection features such as content-based authorization and privacy management are required for a secure extended home experience. However, both VPN and IMS solutions may naturally use IPSec for enhanced network layer security: while more natural in a VPN setting since a tunnel is already established between the two homes, IPSec may also be used in the IMS design, as shown by ongoing work at ETSI and 3GPP where IPSec is used to protect the IMS media plane (ETSI 2010).

3 Conceptual Security in Feel@Home

3.1 Security Requirements

Security is a central aspect of the extended home concept. The whole Feel@Home system must assure that the digital personal life of the members of the household, that is, their photos, videos, and data that reflect their daily lives, are protected from unauthorized parties that would misuse them. In order to create a secure Feel@Home system, it is mandatory to obtain and analyze the security requirements of the application scenarios. From those security requirements, it is possible to identify both the importance and the risk associated to the different assets that belong to the system. Afterwards, we can infer which security mechanisms should be used to protect the architecture. Note that we also considered the requirements for home automation and intelligent households for the sake of completion.

There are standard documents for defining system requirements (such as IEEE Std 830-1998 (IEEE 1998)), but there are not many concrete techniques for eliciting security requirements (Tøndel et al 2008). Due to the importance of the assets (e.g. information), we firstly followed the academic-based "Asset Table" methodology (Jaatun and Tøndel 2008). Moreover, we also followed a risk analysis approach, using the ISO/IEC 15408 (2005) standard to identify the main elements of the Feel@Home system and the EBIOS methodology (2004) to evaluate and obtain the security risks and goals. As a result, we obtained three major categories of security requirements: Information requirements, Device requirements, and User requirements. Note that user privacy belongs to the user requirements, but due to its importance it will be considered as a separate category.

- *Information requirements.* They mainly specify user authorization and communication channel protection. The information contained within Feel@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 Feel@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.
- *User requirements.* They not only refer to the definition of different users and groups that implement the information access controls within the Feel@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 are considered within this category.

As a key requirement for user acceptance of Feel@Home technologies, privacy may be viewed as a class of requirements in itself and is discussed in the following section.

3.2 Privacy Requirements

Private data is manipulated virtually by all stakeholders of a smart home: users, and service, content, and communication providers such as network operators. Examples include direct identifying information (e.g. name, e-mail), lists of friends and contacts, group membership information (Mannan and van Oorschot 2008; Zheleva and Getoor 2009), presence information, histories of service access (e.g. visited Web sites), or personal contents (music, photos, videos, etc.). The user may also be identified using operator data, or any of the partial identities and attributes disclosed to service providers, already used to build detailed user profiles.

Unfortunately, the frontier between public and private is no longer the same as inside/outside the home:

many devices can be accessed remotely from outside the household to share contents, and some services are also managed remotely by multiple operators or services providers. The very amount of such data and its automatic collection raises deep privacy concerns: the user becomes totally unaware of where, why, how, and by whom information is being gathered, loosing control over his private data.

To win back user trust, exchange and use of personal data should be controlled enforcing some fundamental privacy principles 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) (OECD 1980). No more data should be collected than necessary, only for a legitimate purpose (e.g. context-awareness at a household level), and only with explicit user consent. Moreover, the following requirements should also be satisfied:

- Enforceable privacy agreements: the user should negotiate with service providers conditions of manipulation of private data (PRIME 2005). The user should thus give explicit consent to whom and for which purpose private data is released by clearly stating his 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 (Benjumea et al 2006; Camenisch and Lysyanskaya 2001) allows users to disclose information about themselves (e.g. age>18) 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.
- 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, Feel@Home security will need to support different cryptographic protocols and formats of certificates. Variable user privacy preferences are also desirable, such as tunable degrees of anonymity and the willingness of the user to disclose personal data.
  Finally, 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 security infrastructure must thus provide enough flexibility to support those complex relationships. For example, links between authorities can be based on certification. This gives rise to chains of trust and chains of delegation. It can also be possible to establish and revoke P2P links between authorities dynamically. Note that a combination of these approaches may also be adopted, by distributing functionality (Zhou and Haas 1999) or by using clusters (Bechler et al 2004).

3.3 Security Architecture

After defining the requirements of the Feel@Home system, we can specify the security architecture that will be used to fulfill those requirements. Firstly, we define a *functional security architecture* in which the security countermeasures needed to meet the requirements identified previously are identified. These countermeasures take the form of security components. Secondly, we map the functional security architecture to the Feel@Home network architecture, yielding the *organic security architecture*. At this level, the organic security architecture may be described independently of the particular Feel@Home embodiment (IMS or VPN solution). This will greatly facilitate the interoperability between the IMS and the VPN solutions from the security viewpoint.

The very first component of the functional security architecture is the *Cryptographic Services* component. The role of this component is to provide interfaces to cryptographic primitives such as encryption and hashing. This component is used by all the other components in the Feel@Home architecture, and one clear example of that is the *Trust Management* component. This component provides a certain level of trust among Feel@Home entities, 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. Trust between entities is achieved by using inherent trust, i.e. by using public key certificates to ensure that a set of entities belong to the same Feel@Home system. Note that we also consider gained trust in this component, that is, trust that a device has in other devices because of their past and current behavior.

The architecture also provides two authentication components. The first component, the *User Authentication* component, authenticates users in a Feel@Home system so that they can receive personalized multimedia content and check for shared content. As Feel@Home

aims to support different types of authentication mechanisms (e.g. (user,password) pairs, smartcards), there is support for different authentication subcomponents that can receive as input the corresponding credentials and will then make use of the authentication policies to return an "access" or "deny" output. Regarding the second authentication component, the *Device Authentication* component, it allows devices that belong to the same Feel@Home system to authenticate themselves. It is quite similar to the user authentication component, as it also provides different mechanisms for authentication. Nevertheless, it also has its own characteristics. This component can make use of the trust management component to create a "circle of trust", where a device knows that its neighbors really belong to a Feel@Home system. Moreover, any device can take the role of authenticator, as devices tend to use mutual authentication.

The *Authorization* component is a complex component aiming to guarantee that only authorized users may access only the contents which are shared. In Feel@Home, the general approach to access control is to enforce authorization at two levels: (i) at the household/user granularity, that is, enforce the rights for a home (resp. a user) to open a connection to another home (resp. to access the catalogue of another user) to view / download content; and (ii) at the content granularity, that is, enforce access rights of users on a particular content (music, video). The first layer of access control may typically be translated at the level of the HGW into a firewall management component to determine which ports to open/to close to establish a remote home-to-home connection. The second layer of access control is closer to DRM enforcement or management of access control lists and other access control policies specifying "which user has the right to access which content shared by which user". Note that using the authorization in conjunction with a privacy management component enables to enforce access control not only based on user identities but on the basis of being member of a group.

The *Firewall Management* component introduced in the previous paragraph should guarantee protection of the Home Network of the customer while leaving the possibility to accept the Feel@Home data once authenticated. In addition, due to private IP address scheme used in Home Network, the Firewall is also coupled to the NAT(P) function that also protects devices inside the Home Network. Internally, the Firewall and NAT(P) are generally based on Netfilter (2010), where rules are created to authorize new sessions, add new redirection rules to reach a Media Server, and block all unsolicited incoming IP packets.

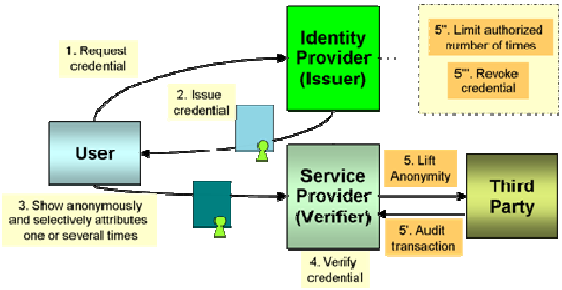

Fig. 4 Stakeholders of User-Centric Privacy Management

Finally, the *Privacy and Identity Management* component aims to prevent identity theft, maintain full user control over private data, while guaranteeing accountability. We adopt the user-centric vision of digital privacy (Bhargav-Spantzel et al 2007) where credentials are mainly stored locally on the user device, are issued by identity providers, and are presented to relying parties (a.k.a. service providers) to access anonymously services (see Figure 4). This Feel@Home 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.

After defining the different components of the functional security architecture, we can introduce the elements of the organic security architecture. These elements make use of the security components of Feel@Home, and are integrated either in the home network or in the operator network. They are as follows:

- *Located in the Home Network*
  - *Contents database*: This element keeps information about the shared content and its related policies (e.g. who owns it, who can be able to access it).
  - *Local Content Manager*: This element enforces access control on contents. It implements the authorization components, and access the contents database.
  - *Local Authentication Manager*: This element allows any known user or device to be authenticated to the Feel@Home system. It implements the authentication components and policies, and can be located in the gateway, behind the gateway or in the user devices.

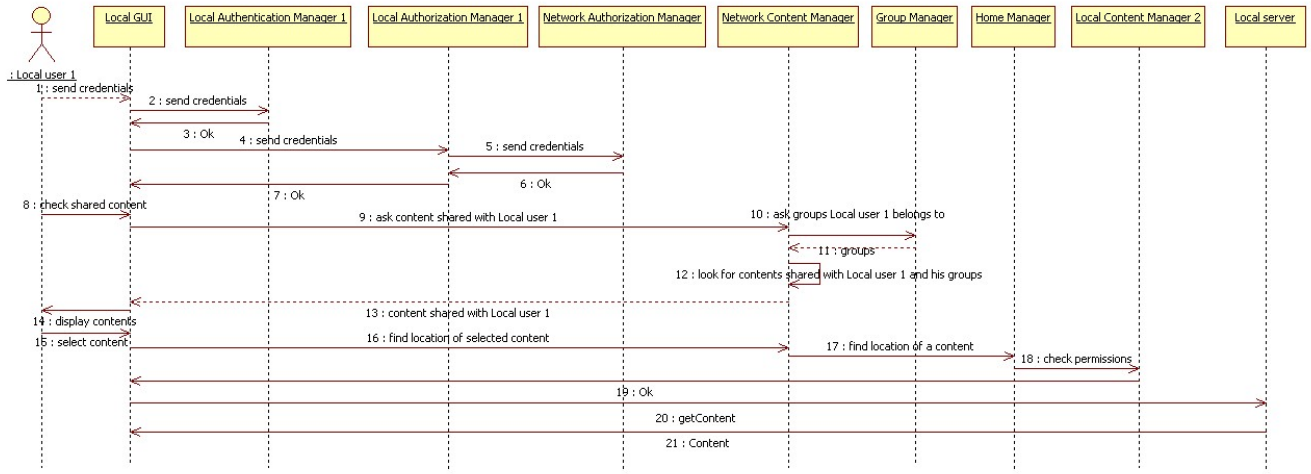

Fig. 5 Simplified Sequence Diagram of Content Sharing Between Homes

- *Located in the Operator Network*
  - *Network Content manager*: This element stores the information that relates the shared content with both the owner and the user whom the content is shared with. It must keep track of the updates in the content manager of all homes.
  - *Authorization Manager*: This element enforces access control on communications between users. It determines, through the use of certain policies, which user (or which house) may establish communications with which other user (or house). This component can be also replicated inside the home network.
  - *Group manager*: This element takes care of the groups and homes where the user is included. It must be aware of the updates made at homes, and also of the contents of other central server modules like the sharing manager.
  - *Home manager*: This element manages all the connections between homes and central servers. It also stores information about how to reach a particular user.
  - *Identity Provider*: While this element manages the identity of the users, actually its main goal is the preservation of the uniqueness of usernames and home names.

An example of the interaction between these elements is shown in Figure 5, where one user in his home uses his Feel@Home system to access certain contents located in a remote Feel@Home system. First, the user is authenticated in his own home through the Local Authentication Manager, and then the Authorization Manager checks if he is authorized to access the contents of a certain household. Once a user is authenticated and authorized, he can check which contents are shared with him. For that purpose, the system checks the Network Content Manager to look for any multimedia item the local user has permissions to. The system also uses the Group Manager to check if this user belongs to a group, in order to also look for the contents shared with that group. Once the user knows the contents shared with him, he can select one to be played at his home. At this point, the system uses the Home Manager to locate the remote home, and after checking the validity of the connection through the Local Content Manager the information is displayed in the user's player.

4 Secure Convergence of Networks in Feel@Home

In this section, we describe how the previously defined security architecture is instantiated in both the IMS solution and the VPN solution. Moreover, we also provide a small discussion on whether or not interoperability between the IMS-based solution and the VPN-based solution is possible from the security point of view. Note that we summarize in Table 1 how the different security components are mapped to the security requirements and the IMS/VPN instances of the architecture.

4.1 Securing the IMS infrastructure

In the IMS embodiment of the Feel@Home security architecture, the security components are refined as follows. For access control, the Authorization Manager is implemented in the operator network by a dedicated

Table 1 Link between Security Components, Requirements and Implementations

Security Components	Requirements	IMS Instance	VPN Instance
Cryptographic Services, Trust	Comm. Channel Security Adaptation Anonymous Communications	Distributed over the IMS Infrastructure	Distributed over the VPN Infrastructure
User Authentication	User Authentication Usability Flexibility	AVSIP, LAN-AVSIP	Managed in the HGW
Device Authentication	Device Authentication	Standard IMS Security	Using VPN Mechanisms
User Authorization	User Authorization Access Control Flexibility Logging	AVSIP, LAN-AVSIP	Managed in the HGW
Firewall Manager	Comm. Channel	Firewall component	Firewall component
Privacy, ID Mgmt.	User Authorization Multiple Identities Privacy Agreements	AMISEC Infrastructure	Managed in the HGW

IMS application server (called AVSIP in Figure 2), directly linked to the core network. Its main security function is to enforce user-level access controls, that is, 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 Content Manager is refined into an application server behind the HGW (called LAN-AVSIP in Figure 2). 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 the trust mechanisms and 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 HGW ports in order to only accept authorized Feel@Home IMS communications after authentication. To manage the private IP addressing scheme inside the home network, the firewall component also performs NAT(P) operations to map the private IP address of a device to the public IP address of the HGW, and back to deliver incoming packets to the right device. By default, only incoming packets belonging to an outgoing connection will be authorized.

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) (PKIX 2010). 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 shown in Figure 4 is realized through a privacy-enhanced PKIX-compliant AAI (Authentication and Authorization Infrastructure) called AMISEC (Lacoste 2009) based on anonymous attribute certificates (AAC) (Benjumea et al 2006, 2007). Privacy enforcement is done both on the content-provider side (using privacy-enhanced authorization mechanisms described next) and on the user side (using an identity selector to choose under which identity and with which level of anonymity the user will access contents).

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 (*conditional release of anonymity*), i.e., user identities may be disclosed under well-defined conditions when dishonest behaviors are detected. This functionality may be performed by the identity provider, or more generally by a completely separate third party (the "Judge") to avoid collusion between stakeholders with conflicting interests. In FeelHome, however, although the two components are logically distinguished to allow potential extensions and handle the general case, to simplify, in the privacy infrastructure prototype implementation, the Judge and Identity Provider functionalities are implemented together in the AAA.

The Service Provider part of the privacy management infrastructure is implemented inside the Content Manager behind the HGW 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 re-

mote Feel@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 (Credentica 2007; IBM 2010), 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 of several types of AACs for different cryptographic schemes (e.g. Traceable Signatures (Kiayias et al 2004)). 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. This last feature enables to implement the *tunable anonymity* privacy requirement, by supporting different types of AAC, each with variable anonymity guarantees based on the intrinsic strength of the advanced signature algorithm involved. The *anonymous communications* requirement is only partially addressed in this Feel@Home security architecture embodiment: the privacy middleware layer prevents linking user attributes to user identites, but not user identities to IP addresses. This last element should be handled at the network layer, for instance using mechanisms for anonymous SIP communications.

4.2 Securing the VPN infrastructure

The major goal of the VPN solution is to allow remote access to the contents stored at home. In this solution, as we explained in section 2.3.2, a remote client located outside his home will make use of an external server to connect his HGW. Regarding the location of the security elements specified in the organic security architecture (cf. section 3.3), all elements that belong to the operator network will be located in the external server, while the home network elements will be included in the HGW.

When accessing remotely, all users should be authenticated and authorized to access the contents. In the VPN solution, the *authentication* process is as follows. A client device will open a connection to the external server, and select and authentication mechanism (e.g. user/password pair). The external server will collect the authentication credentials, and will send it to the HGW. Afterwards, the security components contained in the HGW (e.g. Local Authentication Manager) will check the validity of the credentials. If the authentication is successful, the HGW will open a session with the External Server (e.g. using session tokens of Feel@Home), and the External Server will provide the user with an authenticated session (e.g. through web cookies). As for *authorization*, the External Server will query the HGW on the multimedia contents that the user can access, and the HGW will filter the contents according to the outputs of the content manager.

Another important aspect that must be taken into account for the VPN solution is to provide *secure communications* when the data is traveling over the VPN tunnel between the external server and the HGW, in order to avoid the intrusion of unknown users. This can be easily solved encrypting the communication that travels within the VPN tunnel using public key cryptography mechanisms, such as message signatures and session key negotiations. Besides, with this particular configuration, we also achieve device authentication, as both the External Server and the HGW must provide valid certificates obtained from a trust component in order to open the secure channel.

Secure Communication is not only limited to the VPN connection, but it also must be considered 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 Feel@Home.

4.3 Secure Convergence of Networks

As we have seen, the security architecture presented in Section 3.3 can be mapped easily to IMS and VPN embodiments of a Feel@Home system due to its simplicity. In fact, this simplicity also enables the establishment of secure connections between IMS and VPN-based Feel@Home systems. The main idea is to provide a common interface that can be understood by the elements of the other network at the operator network level. For example, whenever a VPN system wants to connect an IMS system, the IMS system will provide a VPN interface, and vice versa. This way, the IMS system will be considered as another element of the VPN network, although the IMS network will maintain its internal functionality.

This basic idea is shown in Figure 6. The Local Authentication and Local Authorization Managers are implemented in the HGW in the VPN solution, and in a

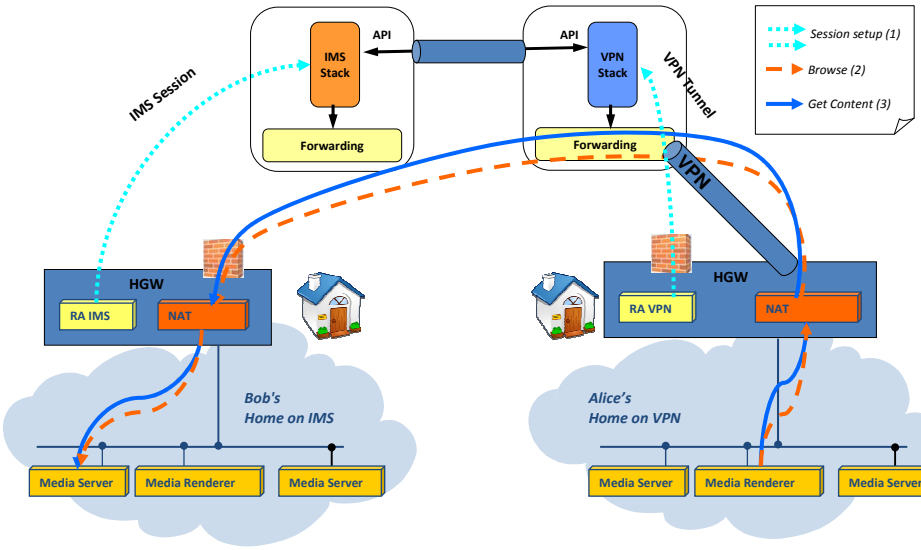

Fig. 6 Connecting a VPN solution with a IMS solution

virtual proxy behind the gateway in the IMS implementation. On the other hand, the Authorization Managers and other elements are implemented in an external server (VPN server) in the operator network in the VPN solution, and in an IMS application server in the operator network in the IMS solution. Whenever a VPN user wants to access certain contents to display them in a media renderer, it will contact its operator network, and afterwards the operator network will forward all queries to the IMS network and the media server where the contents are stored.

4.4 Security Analysis

One of the main objectives of the Feel@Home architecture was 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. While we have already shown that the security components of Feel@Home satisfy the security requirements, in this section we will provide a summary of additional security analyses performed in our project, including the threat model we have considered in such analyses.

In terms of traffic manipulation, we consider as one of the security assumptions of our architecture that the network operator acts as a trusted third party[1]. Therefore, an adversary cannot attack the core IMS network or the VPN server, although he can be able to attack the home network and the access network, eavesdropping and injecting traffic. As for user-side security, an adversary can try to manipulate the system by using the HMI interfaces provided by Feel@Home. In order to make a complete analysis of the security of our architecture, we will also consider that the attacker can have physical access to the home of the user.

While an attacker may be able to access to the information flow of Feel@Home, he will not be able to manipulate such information. On the home side, all communications between Feel@Home devices will 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 Feel@Home system in order to use its services (including access to external homes), because all interactions between users and the HGW are protected through the use of the authentication mechanisms and session establishment protocols. Moreover, the attacker cannot create fake media servers, because the HGW is in charge of storing the access permissions, and will inform any authorized user that a

[1] Note that such trusted network operators might use Feel@Home as a new source of user data, thus this situation should be carefully considered.

previously unknown data source is available. Therefore, the attacker can only access the unprotected entities inside the digital home.

On the side of the access network, the standard IMS and VPN mechanisms included in the HGW, together with the authentication and access control mechanisms used to allow only the interaction between authorized Feel@Home households, avoid any attacks on the network level, although Feel@Home does not provide protection to external attacks such as Denial of Service attacks. Another interesting target for attackers located at the outside of the household is the firewall component, because this component will open certain ports of the HGW firewall to accept previously authorized IMS connections. Still, an adversary can not known in advance which are the ports that are going to be opened in the HGW. Besides, the HGW itself can analyze the incoming IMS connections, in order to check if one particular connection is trying to manipulate the contents of the home network.

It can be easily deduced from the previous paragraphs that one of the most vulnerable components of the Feel@Home system is the Residential Gateway. Therefore, it is possible for a well-prepared attacker to physically access a particular household and manipulate the contents of its HGW. 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 HGW tries to connect other digital homes. Precisely, 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 the 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 HGW to provide a unforgeable signature of the high-level interactions between households.

5 Conclusions

In this article, we have introduced the overall architecture of Feel@Home, describing how it can be used to provide ubiquitous access to multimedia home contents, specially to the digital personal life of users. After that, we have analyzed the different security and privacy problems that can arise in a digital home environment, providing a security architecture that can be instantiated in both VPN-based and IMS-based solutions.

As for the practical feasibility of the solution presented in this paper, we should point out that in the 5th Annual Celtic Event, held from 12 to 13 April 2010 in Valencia, Spain, we showcased an early prototype of the whole architecture. This prototype implemented both IMS connectivity and VPN connectivity, and it allowed users to access multimedia contents stored at their home from any location, taking advantage of existing underlying home protocols such as the UPnP protocol.

In the Feel@Home consortium, we believe that the future of home networks will largely depend on the usefulness of home services and in their usability. Our main goal is to provide a rich experience for home users where they do not need to know what are the underlying protocols that can be used to access their information (e.g. UPnP, IMS) - they simply access their "digital personal life" in a secure an ubiquitous way. In the near future, we plan to expand our Feel@Home vision to not only consider ubiquitous access, but also ubiquitous knowledge: the state of our house and the things that can be found inside it.

Acknowledgements This work has been partially supported by the Feel@Home project. The authors would like to thank all members of the Feel@Home consortium for their much appreciated help on this paper, with special thanks to Benoit Michau for his insight on IMS security.

References

Bechler M, Hof HJ, Kraft D, Rahlke F, Wolf L (2004) A Cluster-Based Security Architecture for Ad Hoc Networks. In: Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'04), pp 2393–2403

Benjumea V, Lopez J, Troya J (2006) Anonymous Attribute Certificates based on Traceable Signatures. Internet Research 16(2):120–139

Benjumea V, Choi S, Lopez J, Yung M (2007) Anonymity 2.0 - X.509 Extensions Supporting Privacy-Friendly Authentication. In: Cryptology and Network Security Conference (CANS'07), pp 265–281

Bhargav-Spantzel A, Camenisch J, Gross T, Sommer D (2007) User Centricity: A Taxonomy and Open Issues. Journal of Computer Security 15(5):493–527

Camenisch J, Lysyanskaya A (2001) Efficient Non-Transferable Anonymous Multi-Show Credential System with Optional Anonymity Revocation. In: International Conference on Advances in Cryptology (EUROCRYPT'01), pp 93–118

Chintada S, Sethuramalingam P, Goffin G (2008) Converged Services for Home Using a SIP/UPnP Software Bridge Solution. In: 5th IEEE Consumer Communications and Networking Conference (CCNC'08), pp 790–794

Credentica (2007) U-Prove SDK Overview. White Paper

DCSSI - France (2004) EBIOS Expression of Needs and Identification of Security Objectives

ETSI TISPAN WG5 (2010) LS to 3GPP regarding Remote Access to CPNs. Retrieved from `http://www.3gpp.org/ftp/tsg\_sa/WG3\_Security/TSGS3\_59\_Lisbon/Docs/S3-100582.zip`

HGI, Home Gateway Initiative (2008) Home Gateway Requirements: Residential Profile

IBM (2010) Idemix (Identity Mixer): Pseudonymity for e-Transactions. Retrieved from `http://www.zurich.ibm.com/security/idemix/`

IEEE Computer Society (1998) IEEE Std 830-1998, IEEE recommended practice for software requirements specifications. ISBN 0-7381-0332-2

IETF PKIX Working Group (2010) Retrieved from `http://www.ietf.org/html.charters/pkix-charter.html`

ISO/IEC (2005) ISO/IEC 15408-1:2005, Information technology - Security techniques - Evaluation criteria for IT security

IST PRIME Project (2005) Privacy and Identity Management for Europe. White Paper

Jaatun M, Tøndel I (2008) Covering Your Assets in Software Engineering. In: 3rd International Conference on Availability, Reliability and Security (ARES'08), pp 1172–1179

Kiayias A, Tsiounis Y, Yung M (2004) Traceable Signatures. In: Conference on Advances in Cryptology (EUROCRYPT'04), pp 571–589

Lacoste M (2009) Architecting Adaptable Security Infrastructures for Pervasive Networks through Components. In: International Conference on Future Generation Communication and Networking (FGCN'09), pp 275–292

Mannan M, van Oorschot P (2008) Privacy-Enhanced Sharing of Personal Content on the Web. In: International World Wide Web Conference (WWW'08), pp 487–496

Mas I, Berggren V, Jana R, Murray J, Rice C (2008) An IMS-based architecture for interactive, personalized IPTV. IEEE Communications Magazine 46(11):156–163

netfilter/iptables Project (2010) Retrieved from `http://www.netfilter.org/`

OECD (1980) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

The CELTIC Feel@Home Project (2010) Retrieved from `https://rd-projet-feelathome.rd.francetelecom.com/`

Tøndel I, Jaatun M, Meland P (2008) Security Requirements for the Rest of Us: A Survey. IEEE Software 25(1):20–27

van Hartskamp, M, et al (2008) PnP QoS Architecture, UPnP Forum

Zheleva E, Getoor L (2009) To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles. In: International World Wide Web Conference (WWW'09), pp 531–540

Zhou L, Haas Z (1999) Securing Ad Hoc Networks. IEEE Network 13(6):24–30