An Identity Management Infrastructure for Secure Personalized IPTV Services

Daniel Díaz Sánchez[1,*], Florina Almenárez[1], Andrés Marín[1], Eugen Mikoczy[2], Peter Weik[3], and Thomas Magedanz[3]

[1] Telematic Engineering Department, Carlos III University of Madrid
Avda. Universidad, 30, 28911 Leganés (Madrid), Spain
[2] Slovak University of Technology, (Bratislava), Slovakia
[3] Technische Universität Berlin, (Berlin), Germany

Abstract. This article focus on IPTV security and IPTV service personalization by the introduction of an Identity Provider as new participant in IPTV service provision that deals with authentication, user profile and device profile management. The Identity Provider, integrated as part of the Telco operator, would provider user profiles with a wider scope than application specific profiles, enabling high personalization of services and improvement of user experience. Paper gives overview about existing IPTV security technologies but also describe novel architecture for secure personalized NGN based IPTV services.

Keywords: IPTV security, IdM, NGN based IPTV.

1 Introduction

IPTV is envisioned as the next step in user's TV experience with a provision of highly personalized services ranging from linear television, video on demand (VoD), near video on demand (n-VoD), personal video record (PVR) to advance blended services as messaging, chatting, presence and web 2.0 mashups.

Traditional broadcast-only content protection, as DVB Conditional Access [1], can not authorize users before they acquire the signal so contents are protected before delivered over the air. In this scenario, user authentication and content protection are performed entirely by the customer's hardware. DVB's major drawback is the absence of the concept of "user" that is substituted by the concept of customer (subscription). Customers are associated with hardware and their profiles are handled by the provider. Every user under a subscription receives the same service, thus personalization, if exists, is often poor.

IPTV provides a return channel that enables interaction as well as the separation of users and subscriptions can be provided. IPTV must be able to maintain protected contents within the boundaries of the subscription (contract) during the entire content lifecycle regardless the user equipment. In some cases, IPTV can prevent

* This work has been partially supported by "Jose Castillejo" mobility grant (Daniel Díaz) and Netlab project both financed by Spanish Ministry of Education.

T. Magedanz et al. (Eds.): TridentCom 2010, LNICST 46, pp. 668–683, 2011.

unauthorized users to acquire protected contents on demand since it can authorize them beforehand. However, some scheduled contents as linear television or n-VoD, which are broadcasted over IP using DVB-CA technology for efficiency, still require strong hardware protection.

In the article we summarize how the most relevant IPTV standardization bodies approach service and content protection, user identification and user profiling. The most innovative IPTV platforms allow users to consume IPTV services from several Content Providers; through managed and unmanaged networks; using different devices. The summary signs the fragmentation concerning IPTV content protection and user management. So, in order to achieve the provision of highly-personalized IPTV services while maintaining security it would be necessary to have a separate profile for every principal involved in the service provision. For instance, a content profile, which describes every detail about the content lifecycle; a subscription profile, managed by the IPTV provider, that express the rights a customer pays for and how he delegates them to users; a user profile for personalization; and a device profile containing protection capabilities, identifiers and cryptographic information.

It will be shown that IPTV user profiles are usually application specific, covering only IPTV related information, since IPTV users profiles are highly related to Telco-originated identities. These Telco-originated identities are based on *identifiers* and *authentication* mechanisms where the original scope is much narrower than in the case of Internet-originated Identity. We expect a user profile to be a user's Digital Identity available to many services, so rich in personal information, whose disclosure to the different services is handled by the user. In this way the user obtains the desired personalization from any service while respecting its privacy.

The article proposes the introduction of a Identity Provider (IdP) as new participant in IPTV service provision. The IdP deals with authentication and user profiles on behalf of different services including IPTV. Thus, IPTV services can be highly personalized by the use of an enriched user profile. Moreover, users are expected to store the profiles of their preferred devices under their user profile. In this way, the user can access IPTV services through several devices selecting the preferred one in every interaction. Device profiles would be used by IPTV service providers to check if a device is adequate for accessing a given content, to adapt the content protection to the selected hardware or to suggest any other user device as an alternative.

2 IPTV Security

Security topics in IPTV are: *service protection*, *content protection*, *key distribution, rights expressions, user management*, *device protection* and *network protection*. This section we will define the objectives of these security topics, how they are traditionally grouped together and how IPTV security technologies handle them. A service is a collection of video/audio contents bundle together in a package. *Service protection* ensures that subscribers are only able to gain access to services that are part of their subscription thus it governs the acquisition process. Once acquired, contents must remain under the agreement the user maintains with the content provider. *Content protection* techniques protect contents against unauthorized copy, distribution or manipulation.

Security solutions for IPTV must respect *user privacy*. Information about users as personal information, payment data or addresses must be protected by encryption and policy enforcement; also traceable information, as identifiers that might reveal service type preferences or habits, must be obfuscated. The user equipment as visualization devices, set top boxes, home gateways are part of the security infrastructure protecting contents. *Device protection* aims on avoiding attempts to hack devices, distribute virus or perform Denial of Service attacks (targeting the user or the provider network). Devices rely on cryptographic material stored in tamper proof hardware to perform some security tasks. In DVB the majority of security functions are delegated to devices. Devices are also highly related to *Content export* technologies that allows to move a content from one device to another preventing piracy.

The aforementioned security topics are grouped together in three major functional groups with some overlap among them: *Conditional Access Systems*, *Digital Rights Management* and *Copy Protection*. However, the practical realization of those security functions leads to two different scenarios, ruled by different content protection technologies, known as *acquisition and post-acquisition*.

DVB Conditional Access (CA) Systems [1-3], Marlin [4] and OMA BCAST [5] are security technologies governing acquisition. Content protection technologies might require dedicated hardware. In DVB it is necessary a combination of a descrambler, a Conditional Access Module and a smart card in every visualization device. OMA BCAST supports a smart card or DRM (smartcard less) profile. ETSI TISPAN has utilized NGN security mechanisms also for NGN based IPTV and trying to reuse the existing service protection and content protection standards. Once contents have been acquired, the post-acquisition scenario starts. Contents must remain within the bounds of the contract until the content lifecycle ends. Contracts can be enforced using *Digital Rights Management* and Copy Protection techniques as CSS (used in DVDs) or Advanced Access Content System (AACS). These specifications dictate how a legally acquired content may be converted to other Codec or format, edited, redistributed, or stored in other devices. The foundations for any copy protection system are rights expression languages. These languages have evolved from the simplest expression, as copy control indicator (CCI) field, to the complexity of MPEG21 Rights Expression Language (REL) [6], Usage State Information (USI) described in DVB-CPCM [7], Octopus DRM [8] used in Marlin (Open IPTV forum) or OMA DRM.

2.1 DVB IPTV Security

DVB specifications have been adopted by the majority of broadcasting systems during the last decades to distribute contents over satellite (DVB-S), terrestrial (DVB-T) and mobile networks (DVB-H). IPTV is expected to reuse DVB Conditional Access (DVB-CA) seizing already deployed head ends and consumer hardware. DVB-CA defines a holistic approach standardizing content format, metadata and protection procedures from the head end to the user equipment involving content providers, network operators and consumer electronics manufacturers. Fig. 1 shows the structure.

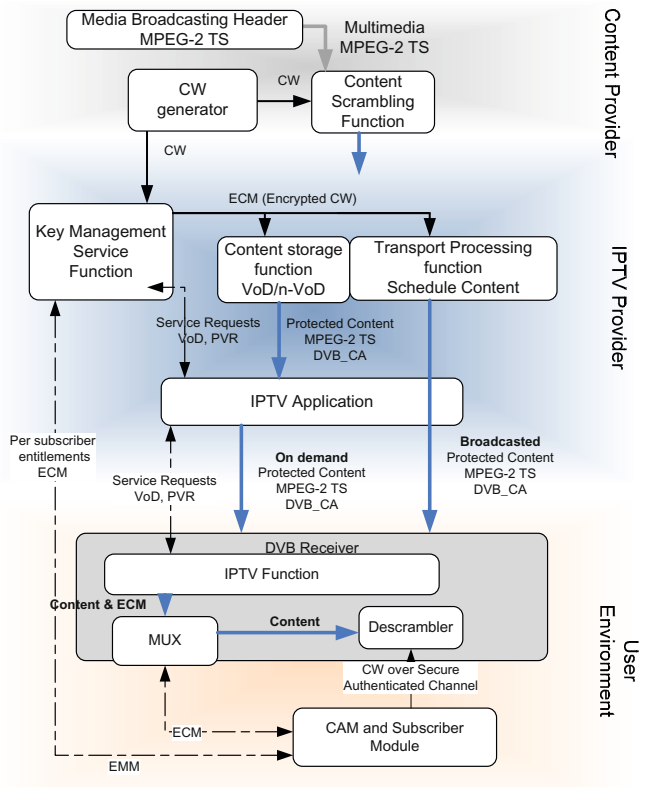

Fig. 1. Distribution networks. IPTV provides bidirectional communication and access control to the network whereas traditional broadcast networks cannot.

DVB Conditional Access (CA) Systems are defined across several specifications as DVB-CA (Conditional Access), DVB-CSA (Common Scrambling Algorithm) [1] and DVB-CI (Common Interface and CI+) [3][9].

DVB uses MPEG-2 *Transport Streams* (TS) as the preferred ***content format***. DVB IPTV encapsulates MPEG-2 Transport Streams in IP packets, reusing thus the traditional Conditional Access infrastructure and hardware. MPEG-2 TS is very useful for broadcasting over networks where errors might occur since it combines data streams with audio and video. MPEG-2 defines a *Program* as a set of *Packetized Elementary Streams* (PES) containing audio, video and clock references. It includes also data tables describing the relationships between the streams and data called Program Specific Information (PSI). There are three PSI tables related with Conditional Access: the Program Association Table (PAT), the Program Map Table (PMT), and the Conditional Access Table (CAT). The last points to *entitlement management messages* (EMMs) and *entitlement control messages* (ECMs).

Content acquisition in DVB broadcasting only networks is entirely managed by the end user hardware. DVB relies on SimultCrypt [2] which separates content encryption, content delivery and key distribution. Audio and video is scrambled with

a hardware-generated unpredictable session key called Control Word (CW) that changes frequently. DVB traditionally used Common Scrambling Algorithm (CSA) [1] for scrambling but new algorithms, based on Advanced Encryption Standard (AES), are under development, as ATIS CSA, DVB-CSAv3 or DVB-CPCM Local Scrambler Algorithm. These algorithms are inefficient in software implementations to prevent the development of software cracks.

The key distribution system is not standardized except for the messages used to convey that information to customers and the interface between hardware. CWs are encrypted with a *Service key* (SK) and distributed using ECMs. Providers send EMMs contain the SK and DRM information, encrypted with a *customer key* CK, to update SK. In broadcasting only networks ECMs and EMM are broadcasted together with the content in MPEG-2 CAT tables and repeated frequently to deal with transmission errors. Nevertheless, in IPTV the reception of ECMs and EMMs can be acknowledged thus can be sent directly to users.

DVB manages i*dentification*, *authentication* and *authorization* in user equipment in cooperation with CA ***hardware***. DVB Common Interface (CI/CI+) [3][9] defines the communication interface that every Conditional Access Module (subscriber module) must fulfil to communicate with a standard descrambler (decryption system). A CAM implements the key distribution protocol (EMM/ECM) for a given CA system provider. The most advanced version of the Common Interface specification, CI+, defines how to use the descrambler's public key to open a Secure Authenticated Channel between the CAM and the descrambler for CW delivery. As the user might infer, the CAM must be collocated with the descrambler so in order to use a different visualization device it is necessary to move the CAM from one device to another. Fortunately, some works propose to place the CAM in a gateway in order to share it with several descramblers through IP [10] or DLNA [11].

Post-acquisition process starts after the content is descrambled. During the acquisition process, decrypted contents never go out of tamper proof hardware so the final destination of the content (a digital video record or a TV) must satisfy several requirements. To protect descrambled contents from being accessed once acquired, the decryption hardware, if not integrated in the visualization device, should export contents through a High-Bandwidth Digital Content Protection [12] (HDCP, HDMI, GVIF) or a similar secure interface. Moreover, DVB defines also some specifications, as DVB-CPCM [7], to allow contents to moved, copied or exported. To identify authorized devices, DVB-CPCM supports the definition of *authorized domain*: the set of DVB-CPCM compliant devices within a household among which contents can be moved.

The reader must note that DVB lacks of ***user management*** so there is neither user authentication nor profile. *Identification, authentication* and *authorization* are performed by the user hardware thus the customer is identified by its equipment. In broadcast only networks, to demand authorization for accessing new contents, a customer uses a modem, integrated in the user equipment, or calls to the customer service. In DVB IPTV this can be handled by the return channel.

2.2 Open IPTV Forum Security

Open IPTV Forum (OITF) has developed an end-to-end solution to access enriched and personalized IPTV services that can be accessed through either managed or

unmanaged networks [13]. It aims on standardizing the user-to-network interface (UNI).The architecture of the system is depicted in Fig. 2.

The OITF content protection supports three media ***formats***: OMA DCF, Marlin IPMP and MPEG2-TS. Regarding ***content protection***, OITF describes its architecture in [14] with two different approaches: the terminal centric approach (CSP-T) and the gateway-centric approach. OITF defines three different keys for content encryption that are provided by the Content and Service Key Management Function. The Content Key is used for Marlin Content encryption and both Service Key and Program Key are used as described in section 2.1 to generate the ECMs and EMMs to cope with MPEG-2 TS content delivery. In OITF, MPEG-2 TS contents can be delivered protected as stated in DVB specifications with either a Marlin CA protection (identified with the appropriate CA descriptors) or with any other DVB CA.

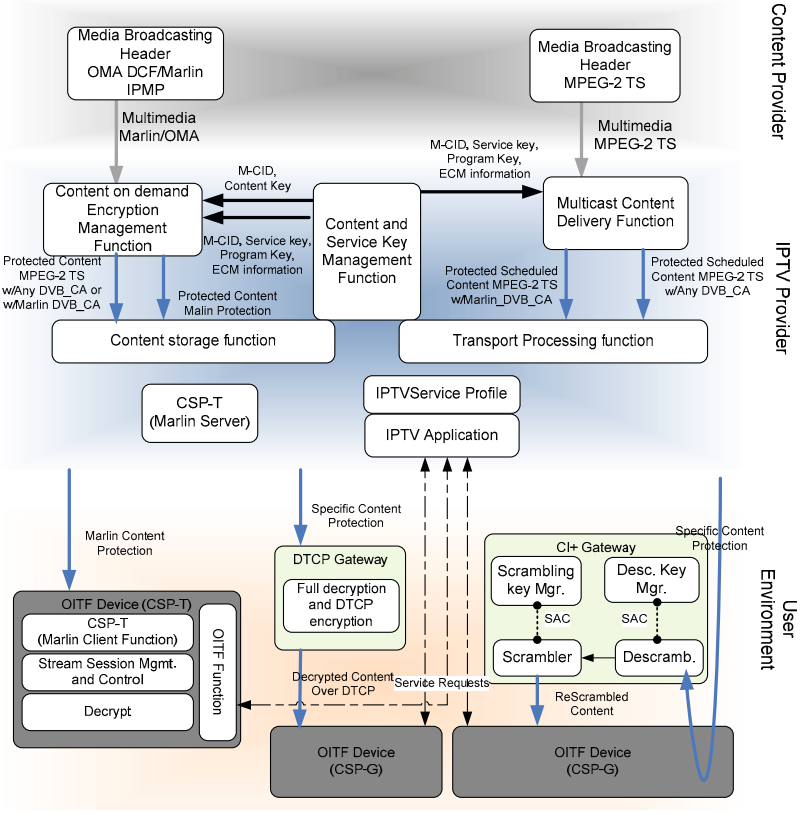

Fig. 2. Open IPTV forum functional architecture of content protection

CSP-T is based on Marlin Broadband [13] defined by the Marlin Developer Community. The CSP-T client in the OITF interacts directly with the CSP-T server function in the network to acquire protected content. The OITF function (OITF device) requests contents through the IPTV application located it the IPTV provider

network. A protected content acquisition involves the IPTV application and IPTV Service Profile function. The acquisition starts when the OITF detects the protection by the execution of Node acquisition, Link acquisition and License Acquisition Marlin protocols [14]. Marlin uses an Octopus-based DRM system such that uses Nodes and Links objects to express relationships among principals within the system (e.g., users, devices, and subscriptions). Once the OITF device obtains a Node and Link represented by a Business Token it requests a license from the IPTV application. The IPTV application requests the user profile and the business token from the IPTV Service Profile and issues a license bound to the Node that represents the user. If the user is allowed to access the requested content, it will be able to request the corresponding Content Key to the CSP-T Server so the CSP-T server can request the key in behalf of the user to the Content and Service key Management function.

The gateway-centric approach is optional in OITF. The gateway acts as a bridge between the network and the OITF device. The content protection is terminated in the gateway and a local protection system is used between the gateway and the OITF device. The OITF, upon the reception of content protected with a *CA descriptor* that it can not handle, performs discovery to find a CI+ gateway to decrypt the content. If the OITF device finds an appropriate gateway it authenticates to the gateway and redirects the content for decryption. The gateway is equipped with a DVB descrambler that opens a Secure Authenticated Channel with the CAM to receive key material. The descrambler outputs the descrambled content to a scrambler that encrypts the content into a compatible format. Finally, the gateway sources the protected content to the OITF device.

Regarding ***user management***, traditional DRM systems, as DVB, licenses are directly bound to the device that is used to obtain the rights and also to a customer identity. In Marlin, a License is typically bound to a user (more precisely, to an Octopus Node representing the user), and relationships between users and devices, or users and subscriptions, are maintained separately [14]. User management is handled differently for managed and unmanaged networks. In unmanaged networks OITF proposes, in [16], the use of HTTP Digest Authentication. The user must authenticate with the Service Access Authentication located in the IPTV provider network in order to be identified and authorized to access IPTV services. In managed networks, user identification and authorization is based on either 3GPP IMS AKA or SIP Digest. The authentication in this case is triggered when either the Internet Gateway is switched on or the user demands personalized services. Moreover, in some scenarios, Generic Bootstrapping Architecture (GBA) [17] and SAML [18] Web-based Single Sing on techniques can be also used.

The user profile is handled by the IPTV Service Profile. OITF specifications separate Subscription Profiles from User Profiles. Moreover, it manages the links between the principals as subscriptions, users and devices in a comprehensive way. Nevertheless, the user profile is still an application specific profile limited to the IPTV context; thus, it is hard to achieve a high degree of service personalization.

2.3 ETSI TISPAN IPTV Security

ETSI TISPAN works on NGN based IPTV as part of TISPAN NGN release 2/3 [18] on two IPTV architecture: NGN dedicated/integrated IPTV subsystem (non-IMS) [19] and NGN IMS based IPTV [20].

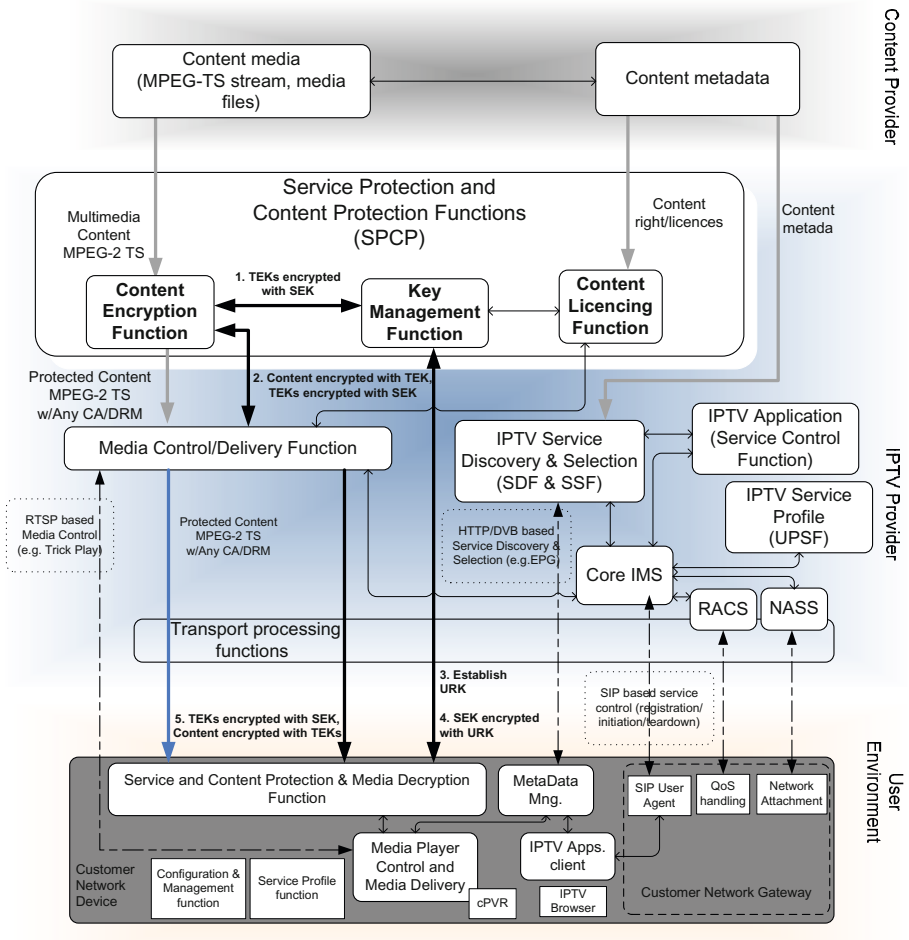

Fig. 3. TISPAN IMS based IPTV functional architecture with service and content protection

IPTV security has been part of NGN Security architecture specification [21] and TISPAN also provides deeper analyses in technical report for IPTV security for NGN release 3 [22].

TISPAN focus on two aspects of IPTV security service protection and content protection (SPCP): ***Content Protection,*** that assures a protection of content or content assets during its entire lifetime and ***Service Protection,*** that have to provide the protection of content (e.g. files or streams) and IPTV related service information during delivery which may include content already protected and meta data that the service provider adds to the content.

The generic model for service protection of IPTV as identified in [22] is based on well defined key hierarchies (3 or 4 layer hierarchies) uses a set of keys that provide cryptographic isolation of services and content for both unicast and multicast distribution of IPTV content:

User Root Key (URK) - A symmetric key used for the protected transfer of SEK in multicast service, or for protection of TEK in unicast service. This key is known only to the IPTV user and the SKMF (Service Key Management Function) and should be derived as part of an authentication and authorisation service (e.g. bootstrapping by GBA and/or IMS-AKA).

Session Encryption Key (SEK) - A symmetric key used for the transfer of traffic encryption keys on a multicast service. This key is known to the session members and to the the SKMF.

Traffic Encryption Key (TEK) - A short lifetime symmetric key used to encrypt the IPTV media within the NGN. This key is shared with all IPTV users for a specific channel or programme and with the MDF containing the CEF (Content Encryption Function).

ETSI TISPAN is re-used existing NGN security architecture and security mechanisms like NASS bunded authenification on transport layer and IMS AKA on service leayer and also bootstrapping mechanisms like GAA/GBA.

There are analyzed several candidate solutions for service protection and content protection (SPCP) for TISPAN NGN based IPTV [22]. Generally there are identified several candidates: OMA BCAST [5][23], DVB CSA/ SimultCrypt [24], 3GPP MBMS [25], OIPF Marlin [4].

TISPAN IPTV service protection model for both multicast and unicast services may be based on the 4-Layers or 3-Layers Key Hierarchy. Figure 4 shows IPTV service protection model based on 4-Layers Key Hierarchy and IPTV functional entities that are tightly related to service protection [22].

OMA BCAST solution addresses service protection and/or content protection and can take into account already deployed service protections can support DVB SimultCrypt and also MBMS. OMA BCAST DRM Profile provides solution for equipments without presence of a smart card. OMA BCAST Smartcard Profile supports using IMS UICC.

2.4 Other IPTV Solutions

A large number of IPTV providers have created and deliver own services through commercial proprietary-based vertical solutions such as Microsoft IPTV Edition (MSN TV 2 set-top box and Xbox console), Apple TV, Intel, Real player, etc.

Although Apple TV platform is not quite IPTV yet, it is just a link from the PC to the television[1] for content transfer. These solutions focus on the ***content protection*** using fully proprietary DRM solutions; for instance, Windows Media DRM [26] from Microsoft TV, or DRM Plus from Verimatrix VACS (Video Content Authority System) software for Intel.

They use DRM and PKI keys (i.e. X.509 certificates) for access and authentication stored in a dedicated chip (i.e. smart cards). The authentication required for VoD and PVR is based on network identifiers (i.e. through regional clusters) or serial numbers in the deco without tamper proof ***hardware***. So, authorization can follow two approaches. Firstly, server-side using unicast connections through Access Control

[1] http://www.iptv-watch.co.uk/2007/06/10/apple-tv-could-add-iptv-capability-in-2008/
http://www.iptv-watch.co.uk/2009/08/25/zte-and-apple-get-into-iptv/

Lists (ACLs), the subscriber record is looking up in a database before granting a given connection (i.e. VoD, PVR). Secondly, using broadcast or multicast applications by providing a subscriber's device(s) with cryptographic keys necessary to access through IGMP protocol to join or leave an IP multicast (e.g. Pay TV channels). The distribution of these keys is not specified, it can be performed as part of setting up a unicast connection for SSL, or alternatively, keys can be sent to the receiver in advance. Thus the user profile is not managed adequately.

On the other hand, 'over the top' services such as Youtube, Megavideo, Joost are using the Internet as a bidirectional channel to provide global reach. These solutions do not offer security neither services nor QoS. The access is usually anonymous.

3 Improvements for Secure Personalized IPTV Services

3.1 Motivation

The majority of user management functions as authentication attribute exchange and user profile management have been already addressed by the Internet community and standardized by relevant organizations. Identity Management technologies support the concept of a user-centric Digital ID as a set of attributes. The criteria for selecting attributes for an identity matches, among others, technical needs, roles intended to be played by the user, privacy concerns and legal constraints. Thus, an Identity Management System can be used for many purposes as *authentication, authorization, verification, uniqueness, linkage, preferences/attribute exchange, and reputation* [27] by using a set of protocols, languages and processing rules.

The integration of traditional content distribution networks with Internet Identity Management systems was inconceivable due to the lack of a return channel. Nevertheless, Next Generation Networks break this tendency allowing this integration. It can be considered one hot topic in current security and NGN research; in fact, there are several works that proposes such integration. In [28], the authors establish the requirements for the integration of Identity Management technologies in Next Generation Networks. Moreover, describes how the central notions in NGN (Telco-originated) identity management solutions are *identifiers* and *authentication* where the original scope is much narrower than in the case of Internet-originated Identity hampering the access to services when they are provided outside Telco domain. Regarding workgroups, for instance, the Focus Group on Identity Management (FG IdM) [29] or Kantara Initiative, with a broaden objective, are contributing to this integration.

For the purposes of IPTV security we concentrate in what is known as Identity Federated model. In a Telco federated model, users' data are in an Identity Provider (IdP) located in the operator domain with interfaces to Internet so the information can be easily accessed by Relying Parties (or external services). Authentication is handled by the operator or a third party depending on where the source of authentication is. This is known as a meta Identity Provider since implements many different interfaces for Relying Parties, as SAMLv2.0 [18], ID-WSF (Identity Web Services Framework) and WS-Federation; and also several authentication mechanisms around a user profile.

In section 2, we described IPTV security architectures where the concept of user is either missing or associated with a subscription or dedicated hardware. Nevertheless, user profiles are still managed by the IPTV provider.

Our meta-IdP aims on providing services for user authentication, user profile management and device profile selection. User authentication can be performed by either third parties (PKI, user/password, OpenId) or the Telco provider (GBA, IMS AKA). The user profile (Digital ID) links IPTV identifiers under a subscription to user preferences. Thus, IPTV providers can deliver highly personalized services to the user relying not only on IPTV user preferences but also on information collected by user profiling during IPTV service consumption or provided by third party Internet services through the user profile. Device profiles are stored in a list of preferred devices under the user profile. A device can be explicitly selected by the user or automatically according to the context. The subscription, user and device profile are associated under an IPTV session with specific user (user identity) and should be used for accomplish service personalization, content casting and content protection casting. The following sections describe the relation among principals, the architecture, interface and services of the proposed IPTV security infrastructure.

3.2 Relation among Principals

The Fig. 4 shows the relation among principals. The subscription profile is managed by the IPTV provider. The subscription profile stores customer's information as: payment, contract details, rights, delegation policies and authorized users. The delegation policies express how subscription rights are delegated to users (e.g. parental control, content types, playback time window…). Users are managed by the Telco meta-IdP system. The meta-IdP provides user authentication and profiles. A user profile is a collection of attributes or claims about service preferences, relation with Internet services (as social networks or communities) and preferred devices.

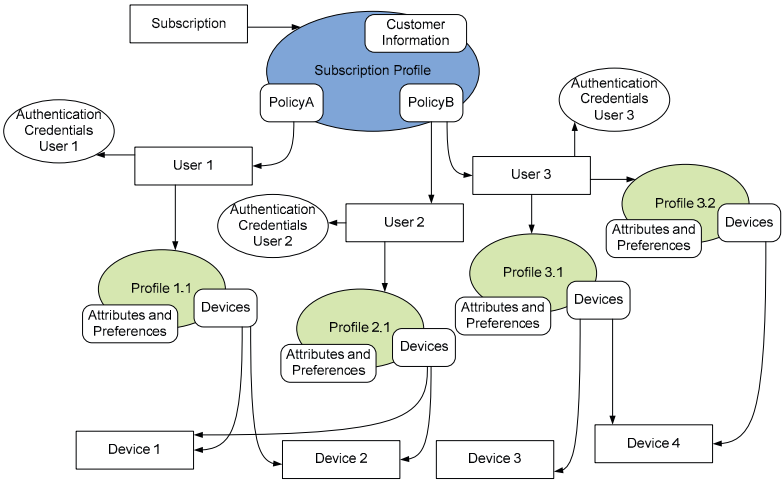

Fig. 4. Relations among principals in our Telco meta Identity Provider

A user might have more than one profile in its identity portfolio in order to separate duties or roles. The device profile contains a detailed description of the supported formats, content protection technologies, identifiers and credentials (i.e. descrambler public key).

As shown in Fig. 5, an IPTV session is characterized by a subscription profile, a user profile and a device profile. Under the scope a session a user will be able to access personalized contents if his subscription rights are enough and the device meets the requirements of the content provider. The session information will be used for adapting the content to the device (content casting) and/or to deliver the content using the most appropriate content protection technology (content protection casting).

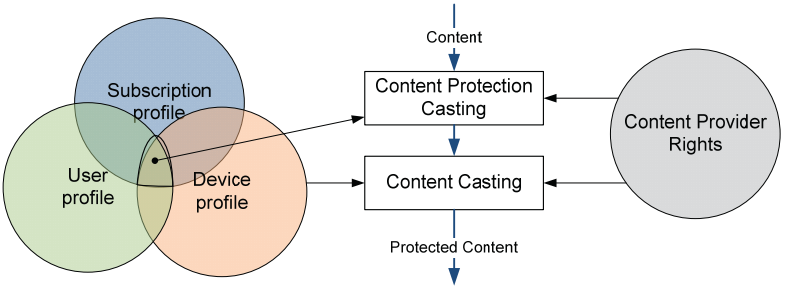

Fig. 5. IPTV Session characterization for content and protection casting

3.3 Architecture and Interfaces

In this section we describe the functional architecture of the proposed IPTV security infrastructure. Our proposal does not substitute but complements existing IPTV security solutions. The core element of our architecture is the meta-IdP located in the Telco operator domain. This element is not part of the IPTV security infrastructure itself since handles user authentication and profiles on behalf of any service including IPTV. Fig. 6 shows the architecture.

The meta-IdP exposes the Authentication Service and the Attribute Exchange and Assertion function. The Authentication function is intended to serve as the authentication endpoint for the majority of the services used by an average user (including Internet services). It must support multiple authentication mechanisms (and credentials) including Telco (GBA, IMS-AKA) and Internet (i.e. PKI, username and password or OpenId) authentication. The security assertions and attribute exchange interface conveys authentication decisions, profiles and attributes to third party services, Internet or Telco services. This interface must support many security assertion languages and protocols (SAML, WS-Federation, WS-Security, Oauth...). The idea is to facilitate authentication and user management to users and services improving user experience while reducing management costs.

The IPTV provider can take profit from the Identity Provider by using several functions as session management, service personalization, content casting and content protection casting. These functions might be implemented by IPTV platforms as DVB IPTV that lacks from an appropriate user management or mapped to existing IPTV

functions, for instance, TISPAN SPCP or Open IPTV Forum node and link acquisition. The Session Management function is in charge of retrieving the subscription profile, the user profile and the device profile. The Session Management function binds those profiles to a session identifier and may check the profiles against the license of the requested content determining the most appropriate content format (include encoding, resizing or aspect ratio modification.) and content protection .

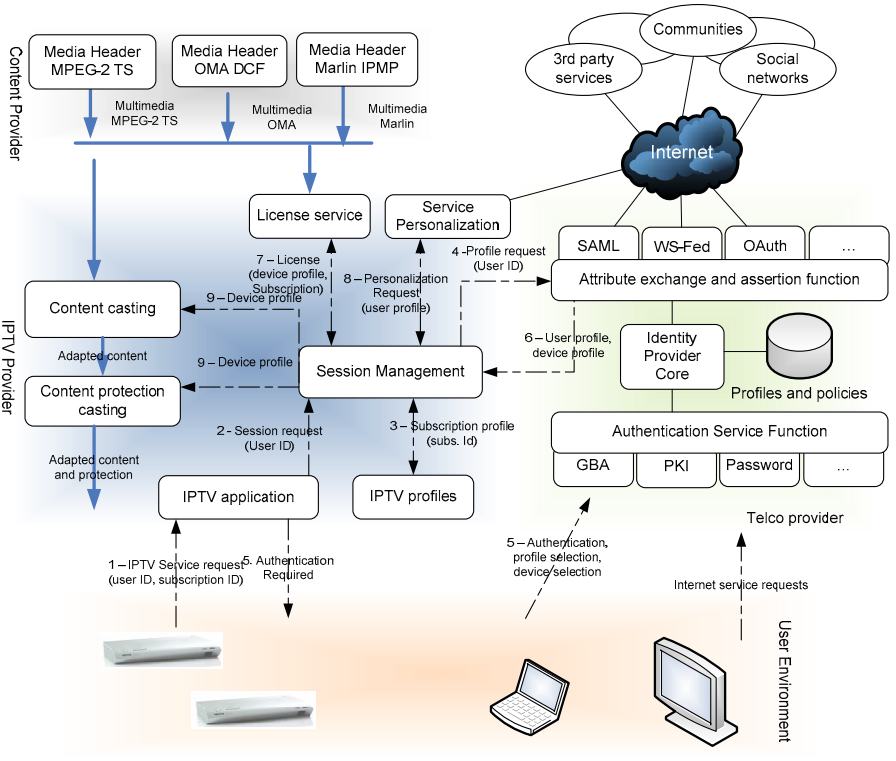

Fig. 6. Security infrastructure for service personalization, content and protection casting

The Service Personalization function receives the user profile from entities like UPSF/HSS, Session Management function IPTV application and uses it for retrieving information from service/user data and other services to personalize the IPTV service. Generally, in IPTV architecture can exist the hierarchical model of relations (as shown in Fig.7) between the internal service states of functional elements, the IPTV Service State information and Presence information and all these information could be used for user profiling and flexible IPTV service personalization [30];

- the internal service state information can be aggregated in IPTV Service State, and IPTV Service State data can be used to update Presence.
- IPTV presence may be related also to User Action Data (e.g. bookmarks) as well as used for updating user's Service Access History (for user profiling).

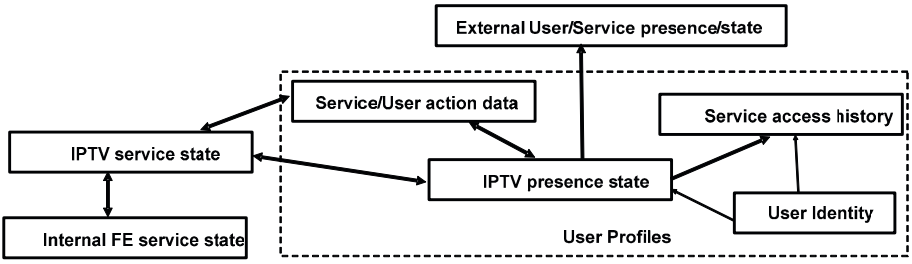

Fig. 7. Using service state and user profile and presence for IPTV service personalization

- User profile (presence state) could be updated from/to external application (including Internet social communities statuses and profiles).

The degree of personalization depends on the information disclosed by the user in his profile. Advanced IPTV services require mechanisms to personalized content and user interaction in all phases of IPTV service (service attachment, service discovery and selection, services initiation/modification/teardown and last but not least for any service interaction).

3.4 Content Acquisition

A content acquisition in the proposed architecture starts with an IPTV service request through a managed or unmanaged network. The user requests a service to the IPTV application providing his user and subscription identifier. The IPTV application sends this information to the Session Management function (e.g. core IMS). If the user has no valid session the Session Management function resolves the user identifier and finds the Identity Provider authentication function. The Session Management sends this information to the IPTV application, which redirects the user to the Identity Provider authentication function using, for instance, an HTTP redirection to an Identity Provider HTML or CE-HTML (for consumer electronics hardware) page.

Then, the user authenticates, selects the attributes to disclose in his profile (or a predefined user profile) and selects the device (or leaves it to the default). The Identity Provider asserts the user's identity to the Session Manager through the appropriate attribute exchange and assertion protocol. After that, the Session Manager requests the user profile and the device profile to the Identity Provider and matches user identity with the subscription profile delegation policy. If the user is entitled to access this content, the Session Manager checks the device profile with the content license to find out if the device fulfils content provider's requirements.

If the device is able to cope with the acquisition and post acquisition content protection requirements, the Session Manager selects the most appropriate content format and protection. Then the Session Manager sends the user profile to the Service Personalization function. The Service Personalization function might rely on user profile, service policies, presence/service state and aggregated user data from different sources as NGN Telco, third party and Internet services. The degree of personalization depends on the information disclosed in the user profile.

Finally, according to the session, the Session Manager starts the content adaptation. It triggers the Content Casting function to adapt the content to device‘s requirements as format, size, quality, bitrates... Moreover, it also triggers the Content Protection Casting function to protect the content with the appropriate technology.

4 Conclusions

This article goes through the most important efforts on IPTV content protection showing the fragmentation of the market. Every standardization organization has chosen its own content protection leaving user management and device management under a non interoperable silo that hampers personalization and scalability. This article proposes the introduction of an Identity Provider as new participant in IPTV service provision that deals with authentication, user profile and device profile management. The Identity Provider, integrated as part of the Telco operator, would provider user profiles with a wider scope than application specific profiles, enabling high personalization of services and improvement of user experience. Moreover, it can be also critical for content protection assurance since it can manage device profiles; thus helping IPTV providers to adapt the content to the device’s specific hardware. In that way, users can be able to select the device to be used, breaking the traditional tendency of binding users to devices; and content providers can be sure that their contents are under control during the entire content life cycle.

References

1. Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems, ETR 281 V1. Technical Report, Digital Video Broadcasting (1996)
2. Implementation Guidelines, of the DVB Simulcrypt Standard, TR 102 035 V1.1.1. Digital Video Broadcasting (2004)
3. Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications, EN 50221. Technical Report, CENELEC (1997)
4. Marlin Broadband Architecture Overview for Marlin Adopters. Intertrust (2007)
5. Mobile Broadcast Services Architecture, Candidate Version 1.1, OMA-AD-BCAST-V1_1-20091013-C. Technical Report, Open Mobile Alliance (2009)
6. Wang, X.: MPEG-21 Rights Expression Language: enabling interoperable digital rights management. IEEE Multimedia 11(4), 84–87 (2004)
7. Digital Video Broadcasting Content Protection & Copy Management (DVB-CPCM), DVB Project Bluebook Document A094R2 (2008)
8. The Role of Octopus in Marlin. Technical Report, Marlin Developer Community (2006)
9. CI Plus Specification, Content Security Extensions to the Common Interface V1.2. Technical Report, CI Plus LLP (2009)
10. Díaz-Sánchez, D., Marín, A., Almenárez, F., Cortés, A.: Sharing conditional access modules through the home network for Pay TV Access. Transactions on Consumer Electronics 55(1), 88–96 (2009)
11. Díaz-Sánchez, D., Sanvido, F., Proserpio, D., Marín, A.: Extended DLNA protocol for sharing protected Pay TV contents. In: IEEE International Conference on Consumer Electronics, Las Vegas, USA (2010)

12. High-Bandwidth Digital Content Protection System Revision 1.3, Technical Report (2006)
13. OITF Release 1: Vol.1 Overview. Technical Report, Open IPTV Forum (2009)
14. OITF Release 1: Vol.7 Authentication, Content Protection and Service Protection. Technical Report, Open IPTV Forum (2009)
15. Open IPTV Forum, Functional Architecture V1.2. Technical Report, Open IPTV Forum (2008)
16. Generic Authentication Architecture (GAA), Generic bootstrapping architecture, TS 33.220 V8.7.0. Technical Report 3GPP, ETSI (2009)
17. Mishra, P.: SAML v2.0. OASIS Standard. Technical Report SAML v2.0, OASIS Security Services TC (2005)
18. ETSI ES 282 001, TISPAN; NGN Functional Architecture (2009)
19. ETSI TS 182 027, TISPAN; IPTV functions supported by the IMS subsystem (2009)
20. ETSI TS 182 028, TISPAN; NGN Integrated IPTV Subsystem in NGN (2009)
21. ETSI TS 187 003,TISPAN; NGN Security; Security Architecture (2009)
22. ETSI TR 187 013, TISPAN; Feasibility study on IPTV Security Architecture (2009)
23. OMA-TS-BCAST_SvcCntProtection – v1_0: Service and Content Protection for Mobile Broadcast Services", version 1.0, Open Mobile Alliance
24. ETSI TS 103 197,DVB; Head-end implementation of DVB SimulCrypt
25. 3GPP TS 26.237, IP Multimedia Subsystem (IMS) based Packet Switch Streaming (PSS) and Multimedia Broadcast/Multicast Service (MBMS) User Service. Release 8
26. Leung, Y., Peinado, M., Strom, C.: Binding Digital Content to a Portable Storage Device or the like in a Digital Rights Management (DRM) System, U.S. Patent 7010808. Microsoft Corporation (2006)
27. Palfrey, J., Gasser, U.: Digital Identity Interoperability and eInnovation. Retrieved from Case Study (2007),
    `http://cyber.law.harvard.edu/interop/pdfs/interop-digital-id.pdf`
28. Subenthiran, S., Sandrasegaran, K., Shalak, R.: Requirements for identity management in next generation networks. In: 6th International Conference on Advanced Communication Technology, pp. 138–142. IEEE, Los Alamitos (2004)
29. ITU-T Focus Group on Identity Management. Report on Identity Management Use Cases and Gap Analysis. ITU-T (2008)
30. Schumann, S., Mikoczy, E., Podhradsky, P., Muruchi, F., Maruschke, M.: Presence management and merging presence information for NGN services" on "Wireless and Mobile Networking", WMNC 2009, Gdansk, Poland, September 9-11. Springer, Heidelberg (2009) ISBN: 978- 3-642-03840-2