# Achieving IPTV Service Portability through Delegation

Davide Proserpio, *Member*, IEEE, Daniel Díaz-Sánchez, *Member*, IEEE, Florina Almenárez, *Member*, IEEE, Andrés Marín, *Member*, IEEE, and Rosa Sánchez Guerrero, *Member*, IEEE

**Abstract** — *IPTV Set-top boxes rely on tamper proof hardware to cope with content protection but hampers enjoying an IPTV subscription in other devices. There are solutions that share the IPTV subscription using the home network but there is no approach to make the IPTV subscription portable. This article describes a solution to delegate IPTV rights to any STB using an inexpensive piece of hardware and the OAuth protocol*[1].

**Index Terms — IPTV, delegation, content protection, digital right management.**

## I. Introduction

In recent years, TV over IP (IPTV), a mean of delivering live TV and video on demand (VOD) over the Internet through conventional TV sets, has attracted considerable attention from an increasingly diverse set of elites. This interest goes way beyond the inevitable investment from telecommunications providers looking to extract new revenue streams from their existing markets. In contrast to last-century, top-down methods of communication such as magazine and TV advertising, IPTV uniquely offers a two way channel of engaging with stakeholders. It provides organizations the ability to deliver high-impact, tailored, broadcast quality content, in a cost effective fashion to a potentially global audience.

From the user′s point of view, the attractions are equally profound. It offers them the opportunity to communicate on their own terms, building and participating in a community of like-minded constituents based on their own interests and business needs. They can view their chosen content on any Internet-enabled device with an adequate broadband connection, or transfer the content to a traditional TV set via a set-top box.

The delivered content has to be protected from illegal access, thus only the authorized users (those who have a subscription or account to the IPTV service) can access the content. Digital Right Management (DRM) addresses this problem. DRM comprises several access control technologies frequently used to impose limitations on the usage of digital content and devices. It aims on avoiding illegal access during acquisition, i.e. joining the right multicast group of an IPTV channel, and once the content has been acquired. This sort of protection guarantee that broadcasted content would be accessed only by entitled users. To prevent service theft, tamper proof hardware is mandatory. This hardware securely retains rights and any cryptographic material used to decrypt protected content.

There are many scenarios in which users would like to enjoy their personalized content in more than one place. For instance, a user has a business travel during the Super Bowl and he wants to watch the match in the hotel with his personalized content. Unfortunately, as the reader may infer, DRM mechanisms have a high dependency with the underlying hardware. Thus, in practice, protected content can only be accessed using the device where the subscriber module is plugged in. There are some solutions as those presented in [1] and [2] that enable sharing the subscription using the home network. However, there is no mechanism to easily export/import the subscription that works out-of-the box. This can be considered a disadvantage for IPTV providers since they lose a chance to sell more pay-per-view contents when the user is, for instance, on holidays.

To overcome this problem, this article proposes a solution to introduce the *delegation* paradigm in the IPTV architecture in order to achieve *service portability*. Delegation is a powerful mechanism to express flexible and dynamic access control decisions. The term service portability is defined as the ability to access services using any devices, anywhere, continuously with mobility support and dynamic adaptation to resource variations as described in [3].

Thus, the article describes how a device containing an inexpensive tamper proof hardware, as a mobile phone or, as we propose, a universal TV remote, can be used to delegate IPTV rights. The tamper proof hardware inside the remote can be used to create and export an Open Authorization (OAuth) protocol [4] delegation token in order to enable access to IPTV personalized contents anywhere. The solution supports different service providers and set-top boxes and it brings a higher degree of freedom to users when it comes to enjoying their IPTV content.

The reminder of this article is organized as follows: section II present the basis of content protection, section III introduce

[1] This work has been partially supported by the State of Madrid (CAM), Spain under the contract number S2009/TIC-1650.

Davide Proserpio is with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: dproserpio@inv.it.uc3m.es).

Daniel Diaz Sanchez with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: dds@it.uc3m.es).

Florina Almenárez Mendoza with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: florina@it.uc3m.es).

Andrés Marín López is with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: amarin@it.uc3m.es).

Rosa Sanchez Guerrero is with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: rmsguerr@it.uc3m.es).

Contributed Paper
Manuscript received 04/05/11
Current version published 06/27/11
Electronic version published 06/27/11.

the concept of delegation defining the parties involved in the process. The main features of the OAuth protocol are outlined in section IV. Section V analyzes some related works. In section VI our proposal is introduced defining the architecture and the functionalities of the OAuth module. A scenario of application is described in section VII including prototype implementation details. Finally, section VIII summarizes the problem we overcame and the benefits of our solution.

## II. IPTV SECURITY

The objective of this section is to provide a background on IPTV security topics with a brief description of their objectives, how they are traditionally grouped together and how IPTV security technologies handle them.

### A. IPTV Security Topics

IPTV security comprises several protocols and technologies, and involves different participants from the provider to the equipment manufacturer. Nevertheless, the security topics directly related to commercial content distribution over IPTV can be enumerated as service protection, content protection, key distribution, rights expressions, user management, device protection and network protection.

A *service* is a collection of video and 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. However, once acquired, contents must remain under the boundaries defined by the license. To cope with that task, IPTV relies on *Content protection* techniques to protect contents against unauthorized copy, distribution or manipulation.

*Privacy* is an important topic in IPTV security, so any information about users (name, payment mechanism, or address) should be disclosed carefully protecting it by encryption and policy enforcement. Privacy affects also to user habits, so traceable information, as content identifiers that might reveal service type preferences or habits, must be obfuscated.

The user equipment plays an important role in IPTV security. Visualization devices, Set Top Boxes or home gateways, are active participants of the security infrastructure. *Device protection* aims on avoiding attempts to tamper with devices. IPTV devices can be located in hostile environments where a possible attacker has physical access to it. To protect devices effectively against tampering, IPTV standards rely on cryptographic material stored in tamper proof hardware to perform security primitives.

Broadcast only technologies, as Digital Video Broadcasting (DVB) satellite or terrestrial TV, bear with the most complex situation since the majority of security functions are delegated to the devices. The lack of a return channel that acknowledges security message reception or that allows managing the device, forces TV providers to broadcast security messages frequently to avoid desynchronisation due to transmission failures. So if a device is compromised, the entire content stream could be accessed and shared illegally without provider knowledge.

Devices play also an important role regarding *Content export* technologies that permits to move a content from one protected device to another preventing eavesdropping.

Besides there is a high cross-layering in IPTV security, the aforementioned security topics can grouped together in three major functional groups: *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*.

### B. Related IPTV Standards

There are many standardization bodies contributing to IPTV Security in either acquisition or post-acquisition scenarios. DVB Conditional Access (CA) Systems [5]-[7], Open IPTV Forum [8] and Open Mobile Alliance (OMA) Broadcast Services Architecture [9], defines techniques to prevent unauthorized usage during acquisition. Content protection technologies in general require dedicated hardware for achieving their goals. In DVB, a combination of a descrambler, a Conditional Access Module, and a smart card is necessary in every device. OMA BCAST supports a smart card or DRM (smartcard less) profile. The European Telecommunications Standards Institute (ETSI) Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN) group has utilized DVB security mechanisms also for Next Generation Networks (NGN) based IPTV trying to reuse the existing service protection and content protection standards.

The post-acquisition scenario starts after content acquisition. Contents must remain within the bounds of the contract until the content lifecycle ends. Contracts, or licenses, can be enforced using DRM and Copy Protection techniques as Content Scramble System (CSS) (used in DVDs). These specifications dictate how a legally acquired content may be converted to other codec, edited, redistributed, or exported to other devices. The foundations for any copy protection system are rights expression languages as Copy Control Indicator (CCI) field, Moving Picture Experts Group (MPEG) Multimedia framework (MPEG-21) Rights Expression Language (REL) [10], Usage State Information (USI) described in DVB Content Protection Copy Management (DVB-CPCM) [11], Open IPTV forum [8] or OMA DRM.

### C. Content Acquisition

Our solution enables content acquisition in other devices than the one holding the subscriber module. For that reason, we briefly describe the acquisition scenario. Typically, content protection uses a three level hierarchical key schema for protecting contents. Content is protected with a combination of scrambling and encryption. A given media stream is scrambled with an unpredictable key that changes frequently.

We will call it Content Key (Ck). The content key stream must be conveyed to subscribers with enough anticipation but the key distribution must be protected. Usually, the content key stream for a given service is encrypted with a Service key (Sk) and distributed using special signaling. In IPTV, these messages can be sent within the content or by any other means since the receiver can send an acknowledgment upon reception. However, in broadcast only systems, those messages must be distributed as part of the content, for instance, DVB uses Entitlement Control Messages (ECMs) for that purpose. In a broadcast service, the Ck and Sk streams are common to every subscriber acquiring the same service.

The final key hierarchy level targets individual subscribers. Ongoing changes in both Ck and Sk must be notified to subscribers so they can decrypt Sk and then the sequence of Cks. Since the access to a given service depends on the subscription, Sk must be delivered in a per subscriber basis. Every subscriber has its own Subscription Key (Suk), a shared secret known only by the provider and a tamper-proof hardware, hence providers make use of special signaling for sending the Sk encrypted with the Suk so that only one customer can decrypt each message.

Sending individual messages to subscribers is not the resource consuming it seems to be since Sk changes after a big period of time. DVB uses Entitlement Management Messages (EMMs) to update Sk. EMMs contain the Sk and DRM information. An EMM is encrypted with a Suk. Other key hierarchy systems might rely on several levels to target groups of subscribers.

Signaling messages are consumed and processed inside tamper proof hardware to prevent service theft. The hardware dependency makes IPTV subscriptions difficult to share with other legitimate devices and for that reason the delegation paradigm that does not require compromising the Suk, is an appropriate solution to the problem.

## III. THE DELEGATION PARADIGM

Delegation is a mechanism for assigning privileges, as well as other attributes, to users. The user who performs a delegation is referred to as a *delegator* and the user who receives a delegation is referred to as a *delegatee*. A privilege attribute will be *delegatable* if it can be successfully granted or transferred from one user to another.

From the administrative perspective, there are two types of delegation: *administration (administrative delegation)* and *user delegation* (*ad hoc delegation*). Administration is the basic form of delegation in which a security administrator or authority assigns privilege attributes to users. User delegation occurs among two or more users who do not necessarily possess any special administrative authority. Specifically, user delegation allows a user to assign the whole or a subset of his/her rights to other users.

From the operational transaction, *direct delegation* is defined as the delegation in which the delegator directly sends the delegation assertion to the delegatee. In contrast, *indirect delegation or multi-step delegation* is performed with the involvement of one or many intermediate parties which can forward the delegation assertion from the delegator to the delegatee.

There are other entities involved in the delegation process: the *Authorization Authority,* which is able to verify authorization decision regarding access request from users, and the *Service Provider,* which controls and provides a service to users. The Service Provider renders services according to the authorization decision of the Authorization Authority. The Service Provider and the Authorization Authority can be collocated in a single entity.

## IV. OAUTH PROTOCOL

With the increasing use of distributed web services and cloud computing, third-party applications require access to server-hosted resources. These resources are usually protected and require authentication using the resource owner's credentials (typically a username and password). This creates several problems of security and privacy. OAuth addresses these issues by separating the role of the client from that of the resource owner.

In the traditional client-server authentication model, the client uses its credentials to access its resources hosted by the server. OAuth introduces a third role to this model: the resource owner. In the OAuth model, the client (which is not the resource owner, but is acting on its behalf) requests access to resources controlled by the resource owner, but hosted by the server.

In order for the client to access resources, it first has to obtain permission from the resource owner. This permission is expressed in the form of a token and matching shared-secret. The purpose of the token is to make it unnecessary for the resource owner to share its credentials with the client. Unlike the resource owner credentials, tokens can be issued with a restricted scope and limited lifetime, and revoked independently.

### A. Client, Server and Resource owner

OAuth defines three roles: client, server, and resource owner. These three roles are present in any OAuth transaction; in some cases the client is also the resource owner.

The protected resource is stored on (or provided by) the server which requires authentication in order to access it. Protected resources are owned or controlled by the resource owner. Anyone requesting access to a protected resource must be authorized to do so by the resource owner (enforced by the server).

### B. Credentials and Token

OAuth uses three kinds of credentials: client credentials, temporary credentials, and token credentials.

The client credentials are used to authenticate the client. This allows the server to collect information about the clients using its services, offer some clients special treatment or provide the resource owner with more information about the clients seeking to access its protected resources.

Token credentials are used in place of the resource owner's username and password. Instead of having the resource owner share its credentials with the client, it authorizes the server to issue a special class of credentials to the client which represent the access grant given to the client by the resource owner. The client uses the token credentials to access the protected resource without having to know the resource owner's password. Token credentials are usually limited in scope and duration, and can be revoked at any time by the resource owner without affecting other token credentials issued to other clients.

Temporary credentials are used to identify the authorization request. In order to accommodate different kind of clients (web-based, desktop, mobile, etc.), the temporary credentials offer additional flexibility and security.

### C. OAuth protocol flow

Fig. 1 describes the overall protocol architecture and includes the following steps: (1) the client requests authorization from the resource owner. The authorization request can be made directly to the resource owner, or preferably indirectly via an intermediary such as an authorization server. (2) The client receives an access grant which represents the authorization provided by the resource owner. (3) The client requests an access token by authenticating with the authorization server using its client credentials, and presenting the access grant. (4) The authorization server validates the client credentials and the access grant, and if valid issues an access token. (5) The client makes a protected resource request to the resource server by presenting the access token. (6) The resource server validates the access token, and if valid, serves the request.

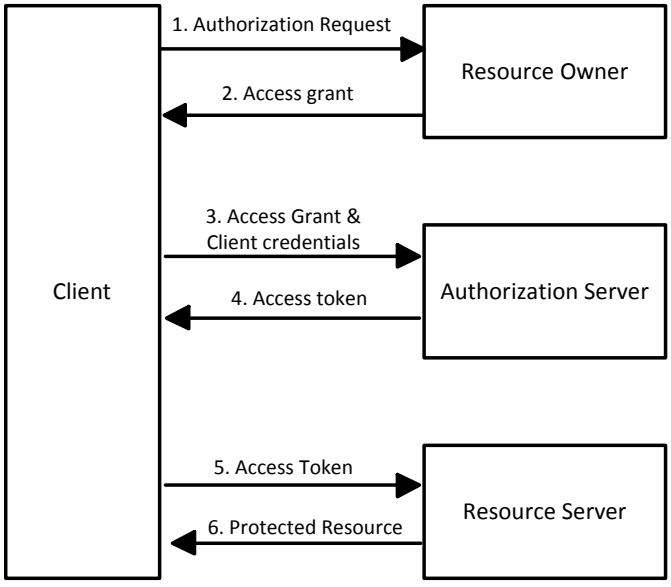


**Fig. 1. OAuth protocol flow. The picture shows the message exchange to access protected resources by a client that is not the resource owner.**

## V. Related Work

Many solutions have been presented in the recent years to overcome the limitation imposed by the IPTV when it comes to enjoying protected content anywhere and anytime without moving the subscription module.

Most of them try to enable sharing IPTV subscription within the home domain. Solutions as those discussed in [12] adopt the concept of Authorized Domain, as described in [2] and [13], to share protected content between family members and home devices. Examples of these architectures are OMA DRM [14] and Open IPTV Forum [8].

References [15] and [16] introduce the concept of Identity Management to enrich IPTV service. Along with this concept, the delegation service is introduced but by means of sharing of a single subscription among family members and with different types of restrictions.

Other like that defined in [17] proposes an answer to export the IPTV subscription using a Global Identification: the E.164-based telephone number. The solution seems to be acceptable because the identification selected is widely used by government as identification as well as to do accounting, charging, and billing. However, the proposed scheme presents great shortcomings since it is bound to a specific protocol, the Session Initiation Protocol (SIP), and does not take into account that most E.164 resources are managed by telecommunication companies and, thus, not opened.

## VI. Introducing Delegation in IPTV Architecture

As we stated before, the basis of our proposal relies on the definition of a delegation mechanism that allows users to make their IPTV subscription portable. To create the delegation token our proposal count on the simplicity and security of the OAuth protocol. We propose a secure solution, which, requiring affordable minor changes in the IPTV architecture to support the aforementioned protocol, allows users to enjoy their personalized content out of the home domain without moving the subscriber module hardware.

In the next section, we analyze comprehensively the architecture we have defined in order to countenancing IPTV subscription delegation.

### A. Entities and roles

A typical horizontal IPTV architecture comprises the Content Provider, the IPTV provider, the Set Top Box (STB) and the end user, which interacts with the STB.

In a standard situation, a user access contents from the same place, for instance his home, using the same device that will be called Home STB. The IPTV provider is usually the one that operates the STB that will be called Home IPTV Provider.

The problem appears when the user moves and needs to use a different STB that will be called Foreign STB. The case can be more complex if the provider operating the Foreign STB is not the same as the Home IPTV provider. The first provider will be called Foreign IPTV provider.

We will consider that an IPTV provider, for instance, the Home IPTV Provider, acts both as Authorization Authority and Service Provider during normal operation. Thus, when a user access Home IPTV Provider contents using the Home STB, the Home IPTV Provider serves the content (resource) to the Home STB that acts as a client.

In the case in which the user wants to access IPTV contents using a Foreign STB, he needs to provide a credential (a delegation token) to the Foreign STB (client) that will send it to the Foreign IPTV Provider before asking for content. If both IPTV providers have a cooperation agreement, the Foreign IPTV Provider, acting as a Service Provider will send the token to the Home IPTV provider to validate it. So the Home IPTV Provider acts, in this case, as an Authorization Authority. If the token is valid the Foreign IPTV provider will deliver the content to the Foreign STB.

According to the aforementioned definitions, we will map OAuth protocol roles to the participants: the IPTV subscription owner, the user, is the resource owner. The STB acts as a client (or consumer). The IPTV provider acts as Authorization Server and Resource Server under normal operation. However, when using a Foreign STB, the Foreign IPTV provider will act as Resource Server and the Home IPTV provider as Authorization Server.

### B. *Architectural changes and user equipment*

Regarding the architectural changes, our solution requires a new module to be instantiated within the IPTV architecture: the OAuth Module. This module is capable of handling OAuth messages to derive and verify an OAuth token upon request.

An OAuth token must be kept secret since directly authorizes access to a restricted service. For that reason, the OAuth module will deliver tokens to devices over an encrypted channel, avoiding eavesdropping and thus, service theft. However, that sort of protection does not prevent the token to be stolen once received if an attacker tampers with the device retaining the token.

To keep the token safe a device equipped with a programmable tamper proof hardware is needed in order to securely import, retain and export the delegation token. The device retaining the token can be whatever device equipped with a programmable tamper proof hardware and a communication interface. The architecture of our solution is shown in Fig. 2.

### C. *OAuth module*

The OAuth module resides in the IPTV provider and it is, thus, the entity that handles delegation messaging. The OAuth module supports Hypertext Transfer Protocol (HTTP) over a secure channel as Transport Layer Security (TLS) to prevent reply attacks that would be possible if the token were transmitted in clear text. Moreover it also supports the transmission of OAuth messages as payloads of SIP.

The module provides several primitives that can be executed by users to enable service portability using delegation. Those primitives are:

#### 1) *Fetching the Request Token*

When a user decides to make his subscription portable, he needs a delegation token that will be exported to the Foreign STB to access the service. The user must fetch a Request Token from the OAuth Module of the Home IPTV Provider since the provider plays the role of Authentication Authority.

After the Request Token is issued, it must be retained in a tamper proof device and eventually exported to the Foreign STB. The Home STB has a trust relationship with the Home IPTV Provider through the subscriber module that holds shared secrets that authenticates the Home STB against the Home IPTV Provider.

After the Request Token has been acquired by the Home STB, it is securely transmitted to the tamper proof equipped hardware that will retain the delegated rights.

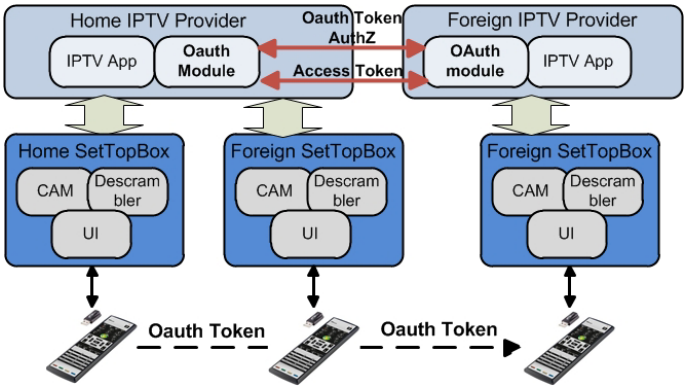


**Fig. 2. IPTV Service portability architecture. The service offers solution for delegation between the same IPTV service provider and between different IPTV service providers.**

#### 2) *Request Token Authorization*

The Request Token, once exported to a Foreign STB, must be conveyed to the Foreign IPTV Provider for validation. The Foreign IPTV provider requests validation to the Home IPTV Provider (Authentication Authority). Upon reception of the Request Token, the Home IPTV Provider might ask for authentication to the user before validating the token.

To simplify the operation, the mechanism used to accomplish this authentication is the generation of a one-time username and password associated to the token. These credentials are generated when the delegation service is defined by the user. The objective is to avoid the misuse of a token if the device retaining the token is stolen or lost.

#### 3) *Fetching the Access Token*

Once the Request Token has been authenticated, the Foreign STB, acting as consumer, can obtain an Access Token. The latter can be used to retrieve the delegated IPTV content in a Foreign STB as if they were consumed by the Home STB.

## VII. Scenario of Application and Implementation

In this section we present the scenario we have implemented to validate our solution. The objective of this section is to clarify the OAuth module behavior including a detailed explanation of the messages exchanged during the

IPTV delegation process. For a better understanding, we consider the case in which the Home IPTV Provider is different from the Foreign IPTV Provider. Notwithstanding, the same flow can be applied to a case in which both IPTV providers are the same.

In this scenario there are two tokens in play: the *Request Token,* also known as OAuth *Token,* used, once authorized, to retrieve the *Access Token;* and the Access Token which will be used to retrieve the protected resource.

### A. Assumptions

The user does not need to further authenticate with the IPTV provider in order to create the delegation service since the subscriber module in the STB univocally identifies the user.

Once the Foreign STB obtains the Access Token from the Request Token, the first can be temporally stored in the Foreign STB until deleted by the user.

The tamper proof hardware can be univocally identified and it has been registered with the IPTV provider beforehand.

Along with the Access Token, information concerning how to retrieve the content might be included in the message, especially when the Home IPTV Provider differs from the Foreign IPTV provider. Otherwise, it is assumed that IPTV providers are federated and know how to access others' services beforehand.

OAuth messages are exchange over a secure channel as TLS o using an inter-provider secure interface.

### B. Message flow

Fig. 3 depicts the message flow during the delegation set up and usage. When the user wants to use the delegation service to enjoy a specific event outside his home, he first selects through the STB's User Interface (UI) the corresponding function. This specific interface allows the user to define the scope of the delegation including the subscription to be delegated, the type of content, the period of the delegation, the Home IPTV operator, the delegation requester and a friendly name for the operation. Additionally, to enhance the security and to authorize the token that will be exported, a one-time username and password must be defined.

Once the delegation is defined, the Home STB sends a request to fetch the Request Token that will be handled by the Home IPTV Provider's OAuth module. The Request Token is returned to the Home STB and hence transmitted to the tamper proof hardware of the device that will store the token.

After this step, the user can use the Request Token in any Foreign STB supporting the delegation service while his family continues enjoying the IPTV service at home.

Let us suppose that the Foreign STB is located at a friend's home. Using the Foreign STB, the user selects the delegation function in order to export the token. An interface is presented to the user to select the Home IPTV Provider and to export the Request Token. Once the Request Token is delivered to the Foreign STB, the latter forwards it to the Foreign IPTV Provider's OAuth module. The Foreign IPTV Provider will redirect the token to the Home IPTV Provider to start the authorization process.

The Home IPTV Provider parses the token, verifies it and, if the Request Token is still valid, generates a request for token authorization. The request will be forwarded to the IPTV Foreign IPTV Provider and eventually the Foreign STB.

At this point, an interface is presented requesting authentication. If the user is successfully authenticated, the Request Token can be authorized and used to retrieve the Access Token. Depending on the scope of the delegation the Access Token could be stored in the foreign STB for further requests of the delegated content.

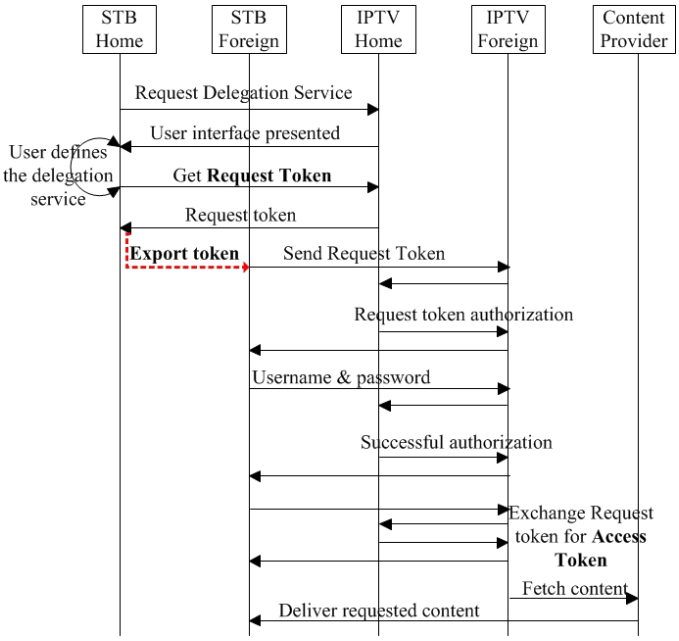


**Fig. 3. Message flow to create the delegation service. The figure depicts a scenario where the IPTV providers, home and foreign, are different.**

### C. Prototype Implementation

We have developed a complete scenario including the Home and Foreign IPTV providers and STBs. The IPTV provider has been implemented as an IP Multimedia Subsystem (IMS) service. IMS is an NGN architecture heavily based on SIP and, thus, we relied on an open source IMS core implementation to simulate a Telco operator signaling and orchestrate access to the IPTV application. The IPTV application that handles IPTV signaling has been implemented in Java and deployed to an application server able to interact with an IMS network by means of the SIP Servlet 1.1 specification.

The content streaming headend, part of the operator, has been implemented by modifying an open source streaming application. To protect the content during the process we implemented the Common Scrambling Algorithm (CSA) widely used in DVB in software.

As the core of the OAuth module we used OpenAM, an open source access management, entitlements and federation server platform, since provides a full OAuth implementation.

Concerning the tamper proof hardware, we used a secure hardware-encrypted flash drive to securely retain the OAuth token. This key will be encapsulated in a remote in a future.

## VIII. CONCLUSION

An IP-based platform offers significant opportunities to make the TV viewing experience more interactive and personalized, facilitated by a broadband connection and a STB that can handle viewer requests to access a myriad of media sources. However, the strong dependency between service provider and STBs becomes a constraint for those users who want to enjoy their personalized services out of home. This is a clear drawback for service providers that want to increase their revenues.

There are some approaches to this problem that enables a way to enjoy the IPTV protected content in different home devices creating a sort of Authorized Domain. However, few proposals try to address the IPTV portability in an easy and user friendly way that works out-of-the-box.

We have presented a straightforward mechanism to achieve IPTV subscription portability exploiting the easiness and security of the OAuth protocol. With the use of a tamper proof hardware the user will be able to export a token in order to access his personalized content in a secure fashion.

We have demonstrated how to carry out a complete service delegation defining a message flow among the involved parties and we have also implemented a prototype for testing our proposal. Moreover, our solution requires tiny invest from operator side since the module that manage the delegation can easily implemented in software and requires inexpensive hardware from user side.

## REFERENCES


[1] D. Diaz-Sanchez, A. Marín, F. Almenárez and A. Cortes, "Sharing conditional access modules through the home network for Pay TV Access," *IEEE Trans. Consumer Electron.*, vol. 55, no. 1, pp.88-96, Feb. 2009.

[2] D. Diaz-Sanchez, F. Sanvido, D. Proserpio and A. Marín, "DLNA, DVB-CA and DVB-CPCM integration for commercial content management," *IEEE Trans. Consumer Electron.*, vol. 56, no. 1, pp.79-87, Feb. 2010.

[3] E. Maler and D. Reed. "The Venn of Identity: The Venn of Identity: Options and Issues in Federated Identity Management," *IEEE Secur. Privacy Mag.*, vol. 6, no. 2, pp. 16-23, Mar. 2008.

[4] E. Hammer-Lahav, "The OAuth 1.0 Protocol", Internet Engineering Task Force (IETF), RFC 5849, Apr. 2010.

[5] European Telecommunication Standards Institute, "Support for use of scrambling and Conditional Access (CA) within digital broadcasting system," ETSI, Sophia Antipolis, France, Tech. Rep. ETR-289, Oct. 1996.

[6] European Telecommunication Standards Institute, "Implementation Guidelines of the DVB Simulcrypt Standard," ETSI, Sophia Antipolis, France, Tech. Rep. DVB TR 102 035 V1.1.1, 2004.

[7] *Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications*," European Standard EN-50221, 1997.

[8] Open IPTV Forum, "Authentication, Content Protection and Service Protection," Open IPTV Forum e.V., Sophia Antipolis, France, Tech. Rep. Rel.2-Vol.7-V2, 2010.

[9] Open Mobile Alliance (OMA), "Mobile Broadcast Services Architecture," OMA, Tech. Rep. OMA-AD-BCAST-V1_1-20091013-C, 2009.

[10] Xin Wang, "MPEG-21 Rights Expression Language: enabling interoperable digital rights management", *IEEE Multimedia*, vol. 11, no. 4, pp. 84-87, Oct. 2004.

[11] DVB Project, "Digital Video Broadcasting Content Protection & Copy Management (DVB-CPCM)", Bluebook Document A094R2, 2008.

[12] P. Koster, F. Kamperman, P. Lenoir1, and K. Vrielink, "Identity-Based DRM: Personal Entertainment Domain," *in Lecture Notes in Computer Science Springer*, vol. 4300, pp. 104–122, Oct. 2006.

[13] S. van den Heuvel, W. Jonker, F. Kamperman, and P. Lenoir, "Secure content management in authorized domains," in *Proc. of the International Broadcasting Convention IBC 2002*, 2002, pp. 467–474.

[14] Open Mobile Alliance (OMA), "OMA Digital Rights Management (DRM) v2.0", 2006.

[15] D. Díaz-Sánchez, F. Almenárez, A. Marín, E. Mikoczy, P. Weik and T. Magedanz, "An Identity Management Infrastructure for Secure Personalized IPTV Services," in *Proc. of Testbeds and Research Infrastructures. Development of Networks and Communities*, LNICST, Vol. 46, Part 13, pp. 668-683, 2011.

[16] F. Winkler, D. Abbadessa, J. Da Silva, J. Girao and M.Schmidt, "Enriching IPTV Services and Infrastructure with Identity Management," in *Proc. of IEEE Globecom*, 2008.

[17] H. Jin Park, J. Hong Yang, J. Min Lee, and J. Kyun Choi, "E. 164 based Global Identification scheme for IPTV Service Portability," in *Proc. of Asia Pacific Conference on Communications*, 2008.


## BIOGRAPHIES

**Proserpio, Davide** received a Telecom. Eng. degree from Technical University of Milan in March 2008 and a MSc degree in 2010 from the University Carlos III de Madrid. Currently he is a PhD candidate in the Telematic Engineering department of the Carlos III University. His research topics include security in NGN and Digital Identity Management.

**Díaz-Sánchez, Daniel** (M'07) received a Telecom. Eng. degree from Univ. Carlos III de Madrid in 2002. He graduated as Master Telematic Engineering (2004) and obtained his PhD (2008) from Univ. Carlos III of Madrid. He works as researcher and teacher at Universidad Carlos III. His research topic is distributed authentication, authorization and content protection.

**Almenárez Mendoza, Florina** (M'07) received the Computer Engineer degree from the University Autónoma of Bucaramanga (Columbia) in 1999, and her Ph.D. degree from the University Carlos III of Madrid (Spain) in 2006. She currently works as an associate professor and researcher in the University Carlos III of Madrid. Her research interests include distributed trust management models for dynamic environments, security architectures in pervasive devices, and security for ad hoc networks.

**Marín López, Andrés** (M'07) received a Telecom. Eng. degree and PhD from the Technical Univ. of Madrid in 1992 and 1996 respectively. He lectures in Computer Networks and Ubiquitous Computing in the Univ. Carlos III de Madrid, as an associate professor. His research interests include ubiquitous computing: limited devices, trust, security services, and security in NGN.

**Sánchez Guerrero, Rosa** received a Telecom. Eng. degree from Univ. Carlos III de Madrid in 2009. In September 2010 she started her MsC studies in the Univ. Carlos III of Madrid. Currently, she combines her studies with a position as researcher at the Department of Telematics Eng. in the Univ. Carlos III of Madrid, working within the Pervasive Computing research group. Her research topics include the problem of identity management, security, and privacy in healthcare.