IPTV Meets Delegation: Achieving IPTV Service Portability

Davide Proserpio, Fabio Sanvido, Daniel Diaz-Sanchez and Andrés Marin, Ingeniería Telemática,
Universidad Carlos III de Madrid, Avda. de la Universidad 30, 28911, Leganés, Madrid

***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.**

I. INTRODUCTION

Digital rights management (DRM) comprises several access control technologies frequently used to impose limitations on the usage of digital content and devices. DRM 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 enables 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. Delegation is a powerful mechanism to express flexible and dynamic access control decisions. The article describes how a device containing 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 OAuth [3] delegation token in order to enable access to IPTV personalized contents anywhere. The solution supports different service providers and set-top boxes. The solution brings a higher degree of freedom to users when it comes to enjoying their IPTV content.

This work has been partially supported by the Community of Madrid (CAM), Spain under the contract number S2009/TIC-1650

II. BASIS OF DELEGATION

In this section we introduce the delegation paradigm, the name of the entities involved and the OAuth protocol.

A. Delegation

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. 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. 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.

B. OAuth Protocol

The OAuth protocol allows clients to access server resources on behalf of another party (such a different client or an end user). In the OAuth model, the client (which is not the resource owner, but is acting on its behalf) requests access to resource controlled by the resource owner, hosted by the Service Provider (SP). 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 a matching shared-secret. The purpose of the token is to make unnecessary for the resource owner to share its credentials with the client. In this way, there is no need to hand out usernames and passwords. Unlike credentials, tokens might be issued with a restricted scope and limited lifetime and they can be revoked independently. Thus, this protocol modifies the traditional client-server model bringing users a better user experience when dealing with distributed web resources and cloud computing. Due to its reliability, flexibility and simplicity, we consider this protocol the best candidate for making IPTV subscriptions portable.

III. IPTV DELEGATION ARCHITECTURE

This section outlines the architecture of a STB and also the logical entities that must be present in the IPTV provider for countenancing IPTV subscription delegation. The solution assumes the existence of a device equipped with a tamper proof programmable chip. We used a universal remote control

and a USB key for testing, but it could have been implemented in a mobile phone or any other device meeting the requirements. For clarity, in the architecture we let the IPTV operator to act as both Authorization Authority and Service Provider. Nevertheless, these roles can instantiated by different stakeholders. The functional architecture of the solution is sketched in Fig. 1.

Our approach to delegation in IPTV utilizes the OAuth protocol in order to generate a delegation token. This token can be used to obtain a service delegation once checked. Thus, the IPTV provider must implement an OAuth module along with the standard IPTV architecture. The aim of this module is to deliver OAuth tokens and to authorize the service delegation by checking the received credentials.

Customer willing to enjoy the IPTV Delegation Service must have a device equipped with a programmable tamper proof hardware. This hardware is used for securely store and move the delegation token. To improve security, this device should support a mechanism to authenticate the user before releasing the token to a STB.

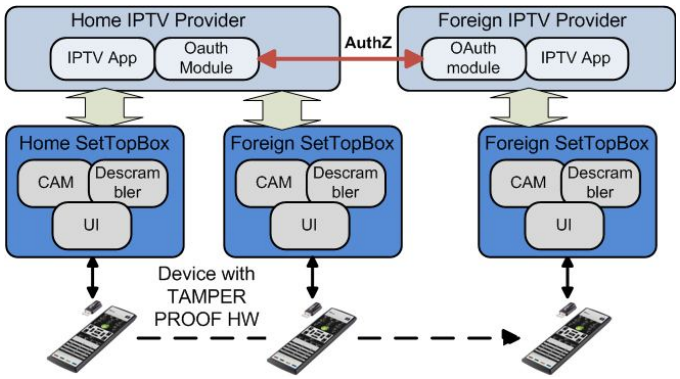

Fig. 1. Functional architecture of STB and IPTV provider.

IV. IPTV DELEGATION OPERATION

The STB user Interface offers the Delegation Service function. When the function is selected, the customers should define the scope of the delegation including the subscription to be delegated, the type of content, the period of the delegation, the IPTV operator, the delegation requester and a friendly name for the operation. Once the service is defined, the request is sent to the IPTV provider OAuth module, which is in charge of generating the OAuth token. The token is returned and stored in the tamper proof hardware of the device (remote). After this step, the customer would use the token in any STB supporting the delegation service while, for instance, her family members can continue enjoying the IPTV service.

When the user wants to move the generated token to a foreign STB, she authenticates to the device. Then she can transfer the token to the foreign STB. Once the STB receives the token, it is sent to the associated IPTV provider and the OAuth module verifies the service authorization. Whenever the STB's IPTV provider differs from the home provider, the latest would be in charge of communicating with the home OAuth module to perform the verification process. This communication should be executed over a secure interface using HTTPS protocol as OAuth protocol specifies. If a successful response is received, the foreign IPTV module can provide the requested service to the user. Depending on the IPTV architecture or the type of service, the response could contain some information about to how obtain the requested content.

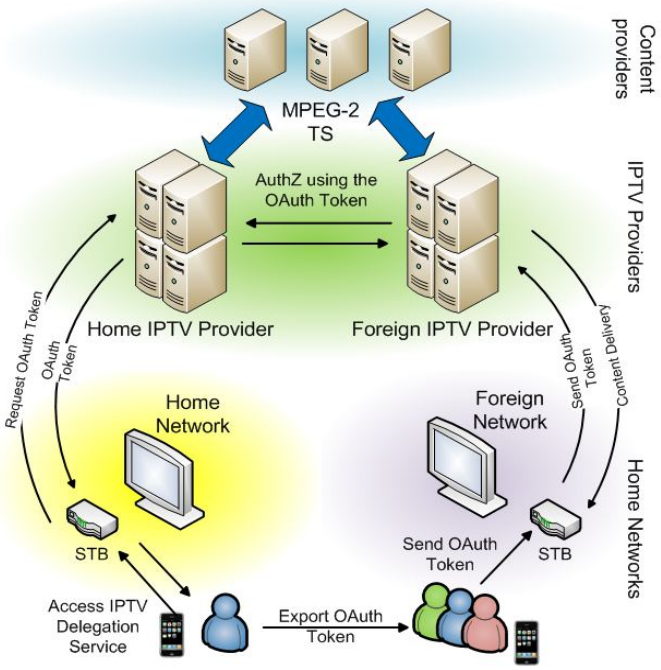

Fig. 2. IPTV Delegation operation

V. IMPLEMENTATION AND CONCLUSIONS

To test our solution we implemented an IPTV NGN architecture using Fokus Open IMS core and UCT Advanced IPTV. The content distribution has been implemented by modifying the open source application VideoLan and a software implementation of CSA scrambling algorithm. The OAuth module has been developed using OpenSSO that provides a complete OAuth protocol stack. As tamper proof device we used an IronKey 1GB Secure Hardware-Encrypted Flash Drive to securely store and move the OAuth token. This key will be encapsulated in a remote.

Our solution is an approach to IPTV subscription delegation that works out-of-the-box. It requires tiny invest from operator side and little hardware from user side. This simple solution allows customers to enjoy their IPTV service with foreign STBs without having to move the subscriber module. Moreover, some family members would be able to consume IPTV services outside whereas others keep on enjoying IPTV services at home.

REFERENCES

[1] Díaz-Sánchez, D., Marín, A., Almenárez, F., Cortés, A.: Sharing conditional access modules through the home network for Pay TV Access. In Transactions on Consumer Electronics. Vol. 55, Issue 1, pp. 88-96 (2009).

[2] 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.

[3] E. Hammer-Lahav, "The OAuth 1.0 Protocol", Internet Engineering Task Force, RFC 5849, April 2010