BECOMING A DATA-DRIVEN BROADCASTER AND DELIVERING A UNIFIED AND PERSONALISED BROADCAST USER EXPERIENCE

M. Barroco

EBU Technology & Innovation, Switzerland

ABSTRACT

Meeting audience expectations is becoming easier for broadcasters with Hybrid broadcasting. The advent of transport technologies such as Hybrid Radio and HbbTV (Hybrid broadcast broadband TV) facilitate a wide range of opportunities for custom-made content aggregation, discovery and, ultimately, consumption. In the connected world, editorial teams need to better know their audiences so as to better provide them with targeted content (format, duration, angle). To achieve this, broadcasters need to uniquely identify people across their various devices. As data privacy concerns are paramount, broadcasters need to let the user control whether he wants to be identified based on a profile, anonymously or not at all. Also, broadcasters should embark on this strategic pathway, in such a way as to avoid vendor lock-in, using open solutions and adopting standard interfaces for data exchange.

In designing a system, Authentication, Authorisation, Identity Management, Device Synchronisation, Data Collection, Data Anonymization, Analytics and Recommendation Engines need to be considered as keys to providing customised non-linear TV, Radio and Online channels.

The European Broadcasting Union (EBU) and its Public Service Media Members are working to put together a set of standards and technologies to enable broadcasters to offer a simple and smooth personalized user-experience on connected devices and ultimately across all their channels. This paper will present the required architectural elements and examples of use cases that help broadcasters embrace the personalised media future that awaits us all.

INTRODUCTION

With the new distribution opportunities offered by hybrid technologies and standards (HbbTV [1] and RadioDNS [2]), broadcasters' new challenge is to provide the right content on the right device at the right time to the right people. To embrace this digital shift requires us to challenge the way our systems are designed and to provide the right tools to our editorial teams so that the user is put at the centre of our infrastructures while at the same time keeping control over the data generated by the system.

Unlike the online players of Netflix, Google and Facebook, which all have the ability to take in account feedback, considering a user as an individual, broadcasters do not yet have this as part of their business DNA. The ability to provide a unified and simple user experience across devices is based on the capability of uniquely identifying a device connected to the broadcast channel. The idea is therefore to create a link between the devices and the broadcasters. These links can then be assigned to someone to create a group of devices where broadcasters can offer a common and consistent experience.

ETSI TS 103 407 [3], *Cross Platform Authentication for limited input hybrid consumer equipment* (CPA) is an open standard that associates online user profiles with media devices and that, in particular, enables broadcasters to offer device synchronization, to build users' profiles and to start collecting data, with subsequent leveraging of data analysis. This is the foundation of delivering a unified and personalised broadcast user experience.

First, this paper outlines the organizational milestones required to deliver a data-driven media experience, Then, it describes the basic technical concepts required to deploy a cross platform authentication mechanism including a description of the benefits in terms of user experience. Finally, it covers a few personalisation use cases employing this architecture.

DATA-DRIVEN DISTRIBUTION

From a broadcaster's strategic point of view, delivering a unified and data-driven media experience requires organization-level adoption and implementation of the following elements:

1. Open Standards and Interfaces: Broadcasters' metadata related to the channels and content shall be available to the rest of the system.
2. Analytics: Data collection to measure the audience and to track system performance.
3. Single Sign-On: A robust cross-platform authentication mechanism allowing each user to authenticate on each of their devices (Online, Radio and TV included). A good design should support identity federation and should let the user choose their preferred identity provider.
4. Recommendation: A broadcaster's ability to provide coherent non-linear access and discovery of its content catalogue.
5. Personalization: A broadcaster's ability to adapt its user-experience to the user across all platforms. This includes direct access to relevant content and preferences as well as the ability for editorial teams to target and propose tailored content to audience clusters and, ultimately, to any individual of the broadcaster's audience.
6. Business Intelligence: The ability for a broadcast organization to understand its total audience experience in order to positively impact its business.
7. Data Broker: A broadcaster acts as Identity provider in order to provide user authentication to access external services. Good examples for Public Service Media are Libraries, Mobility, etc.

A ROBUST DEVICE AND USER AUTHENTICATION

Typical Architecture

As defined in CPA (cross-platform authentication), the architecture will require different web services in order to match the broadcast industry's needs. Based on the OAuth 2.0 framework [4], CPA is adapted to the broadcast eco-system and specifies a few additions such as different levels of device association, dynamic discovery of the components of the system as well as single sign-on between channels while preserving data isolation between services. Moreover, CPA specifies several aspects left open to implementers in OAuth 2.0 to facilitate interoperability, such as endpoint URL paths. A typical architecture supporting cross-platform authentication is composed of the following web services:

Identity Providers are services that manage user identities and authenticate users on an Authorization Provider.

Authorization Providers are services that store device identities and the association between device identities and user identities. They are responsible for granting the authorization to a device to access a specific service by itself or on behalf of a user.

Service Providers are subsets of a broadcaster's experience backend. Usually this is a micro service specific to a broadcaster's personalised feature, which requires device or user identification. (e.g. playlist service including bookmarking, electronic programme guide, generic data collection service, news feed, recommendation system or advertisement).

Figure 1 shows the process of calling a service provider:

1. Dashed line: The Device discovers the Authorization Provider based either on the channel it is tuned to or on the application it is running. It requests a token which is delivered using CPA.
2. Solid line: Devices call a Service Provider with this token.
3. Dotted line: Service Provider verifies the token with the Authorization Provider. The Authorization Provider check the validity of the token and sends the device identifier and user identifier (if it exists) as well as additional metadata about the user.

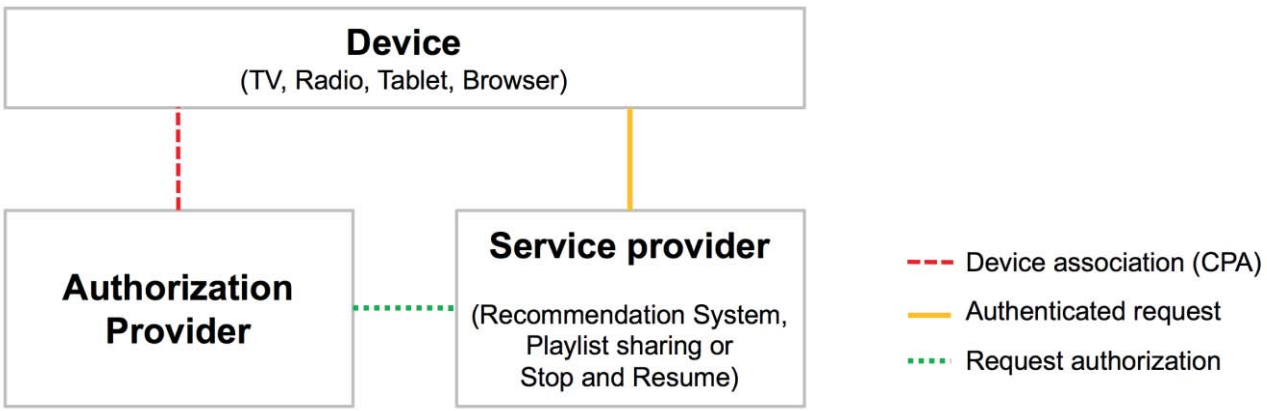

Figure 1 – Architecture overview

Level of identification

Especially with Public Service Media, data privacy is paramount and user data must be handled carefully. As defined by the Cross-Platform Authentication Protocol, the user can be offered three levels of authentication on a device:

- Anonymous; no recorded server-side data can uniquely identify the device or the user.
- Unauthenticated association ('client mode'); the device is uniquely identified on the Authorization Provider.
- Authenticated association ('user mode'); the device is uniquely identified and associated with a user profile.

The user mode allows the user to enjoy a unified media experience across all devices since his data can be linked using his user profile. Using different levels of association, users can start to use a service and later associate the device with his account. This action will link the data collected on this device with data collected on other devices associated with his user account.

Authentication and Identity Federation

To avoid lock-in with third party providers whilst keeping the login process simple, broadcasters shall offer their audience the possibility of creating a user account on their website and it will federate identities in order to let the audience login using their favourite Identity providers (Facebook, Google, …). This solution allows the broadcaster to keep control over the user's profile and leaves the possibility for the user to continue using the broadcaster's platform even if he changes his relationship with a third party identity provider. This process could require the creation of a password on the Authorization Provider.

Using this technique, Identity providers are only used to authenticate the user at the beginning of a session. Every succeeding interaction will be isolated from the Identity provider and handled exclusively by the Authorization Provider, which is under the control of the broadcaster.

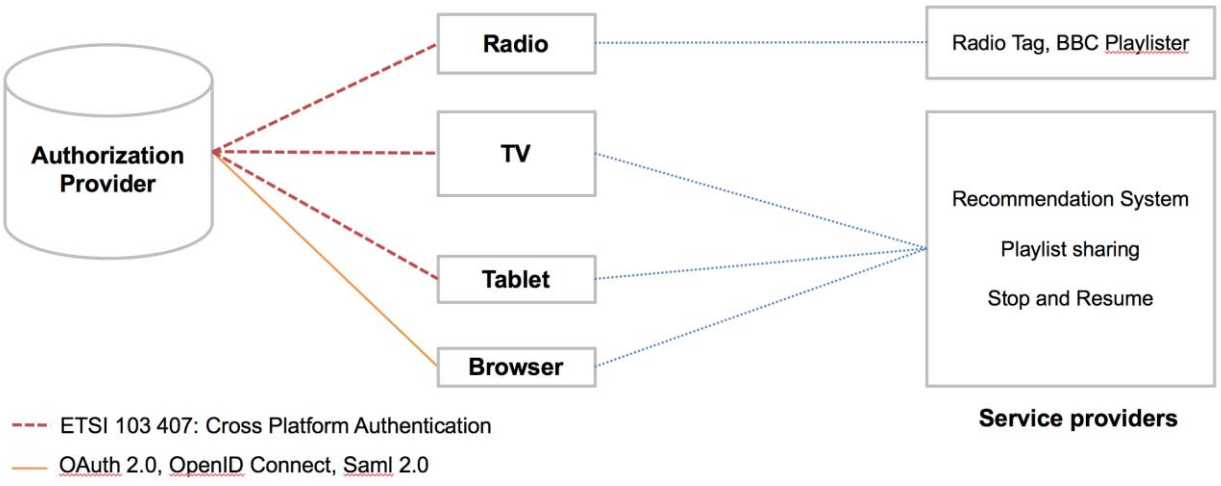

Figure 2 – Token delivery method

Bearer token

The authorization is delivered as a bearer token [5], which can be used to access a service provider on behalf of the device or the user. A different token is delivered per service or per group of services as shown in Figure 2. Depending on the type of service, the token could be used in the “Authorization” HTTP Header to access a protected endpoint.

Association and Authorization process

The association process results in the delivery of a bearer token, as described above. CPA has been specifically designed to enable limited input devices such as Radio and TV receivers to retrieve a token from an Authorization Provider without requiring users to enter their username and password on the device itself. This token can be used to access services such as playlist managers, recommendation systems and users’ profiles. In the context of websites, SAML 2.0 [6] or OAuth 2.0 Authorization Grant and Implicit Grant are examples of protocols that can be used to create a session cookie on different domains or provide a token to client-side JavaScript applications (i.e. Angular.js applications). For scalability reasons, a token-based approach is recommended since it especially allows broadcasters to serve web assets from Content Delivery Networks and provide stateless application program interfaces (API).

Broadcast Services independence and isolation

One of the key requirements of the CPA design is to preserve a clear isolation between the different services while enabling the user to authorize or deny access to his data and profile. Therefore, the broadcast signal’s metadata or the website are responsible for indicating to the device which Authorization Provider (AP) is in charge of authorizing access to a specific service. Multiple AP can co-exist. For instance, in the context of a RadioDNS service, the AP would be declared as part of the available services for a channel in the DNS records. For a HbbTV portal, the AP will be announced by the service provider serving the assets or into the metadata delivered over the air. The AP is then responsible for authorizing a device to access protected resources by providing a token per service.

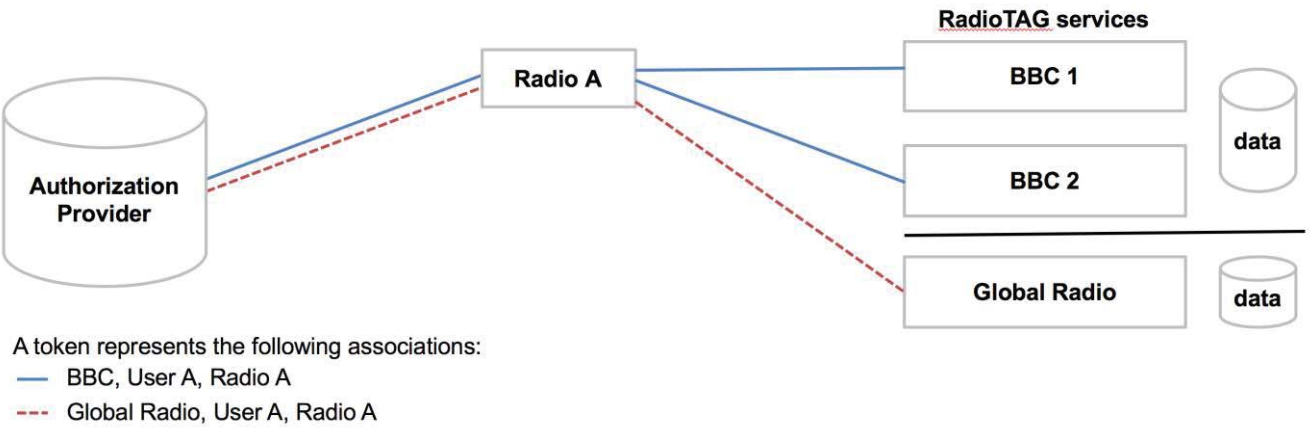

Figure 3 – Data isolation and anonymization

Data storage and anonymization

User data are sensitive. Sharing them with third party partners must be done carefully. The mechanism of token generation and verification allows a broadcaster to anonymize the data returned to the services. Indeed, when validating a token, the Authorization Provider decides what data it returns to the Service Provider. It can also anonymize some data by hiding values, by keeping track of a lookup table and swapping values or it can hash the sensitive values. Using the two last techniques, it will not be possible to join datasets between services without accessing the lookup table, as illustrated in Figure 3.

Revocation of a device or a service

Two mechanisms are available to cancel authorizations. Firstly, the user can revoke a token on the Authorization Provider side. The next time the service provider attempts to verify a token the Authorization Provider will notify it that the token has been revoked. This is useful in the context of a stolen device. Secondly, on the device side, resetting the memory of the device will delete the tokens and prevent any future usage.

Figure 4 – BBC Playlister demonstration

USER EXPERIENCE OF THE ASSOCIATION PROCESS

As shown in Figure 4, the association process starts with the displaying of a code on the device. This code must be entered on the Authorization Provider website using another browsing device in order to complete the association. It means the user doesn't have to enter his username and password on a remote control or on a small screen. The complete manipulation is shown on Figure 7.

SERVICE PROVIDER USE CASES

This section describes several personalisation use cases that are enabled by the authentication mechanism. The solid orange lines in Figure 5 show the link between a device and a user profile. As soon as this link is enabled on two devices with the same user identity it is possible to create device interactions such as pushing content from one device to another. Moreover, if the broadcaster supports the concepts of user communities, it would be possible to create social interactions and send content to another user.

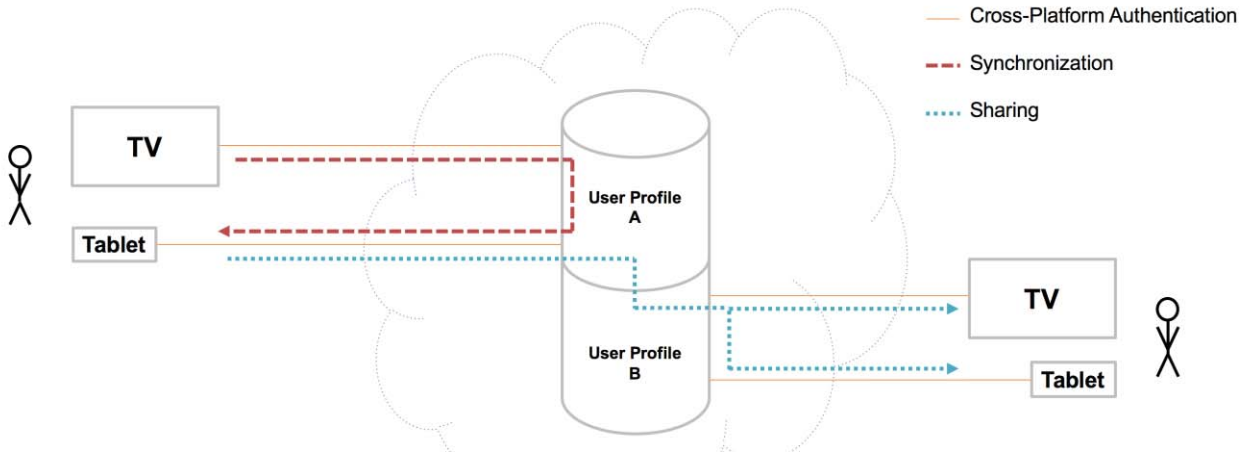

Figure 5 – Device and social interactions

Playlists and Bookmarks service

This service can be used to provide playlists to mobile devices built using a bookmarking button on radio devices. Moreover, a history playlist can be built based on the video watched by a user.

Content shifting: Play content on a device and resume it on another device at the right time

Since the broadcaster is able to collect data about a user's consumption, it is possible to store the last moment consumed by a user. This information can be used by a broadcaster to propose the same content on another device, starting from that point onward.

Recommendation systems

Based on the viewing history of devices and users, it is possible to extract consumption patterns and to retrieve recommendations based on user similarities. Using CPA, editorial teams will be able to recommend different content to the same user depending on the device he is using.

Notifications

Based on the user's profile and his consumption habits, a broadcaster can intelligently push notifications (sport results, newly available content, breaking news) to a user's device in order to engage him with live content or to increase his awareness of a specific event or show. These notifications can take different forms, such as RadioVIS personalized slide shows, HbbTV alerts on top of the red button or mobile notifications as shown in Figure 6.

Figure 6 – Notification examples (Hybrid Radio, Apple Watch and HbbTV)

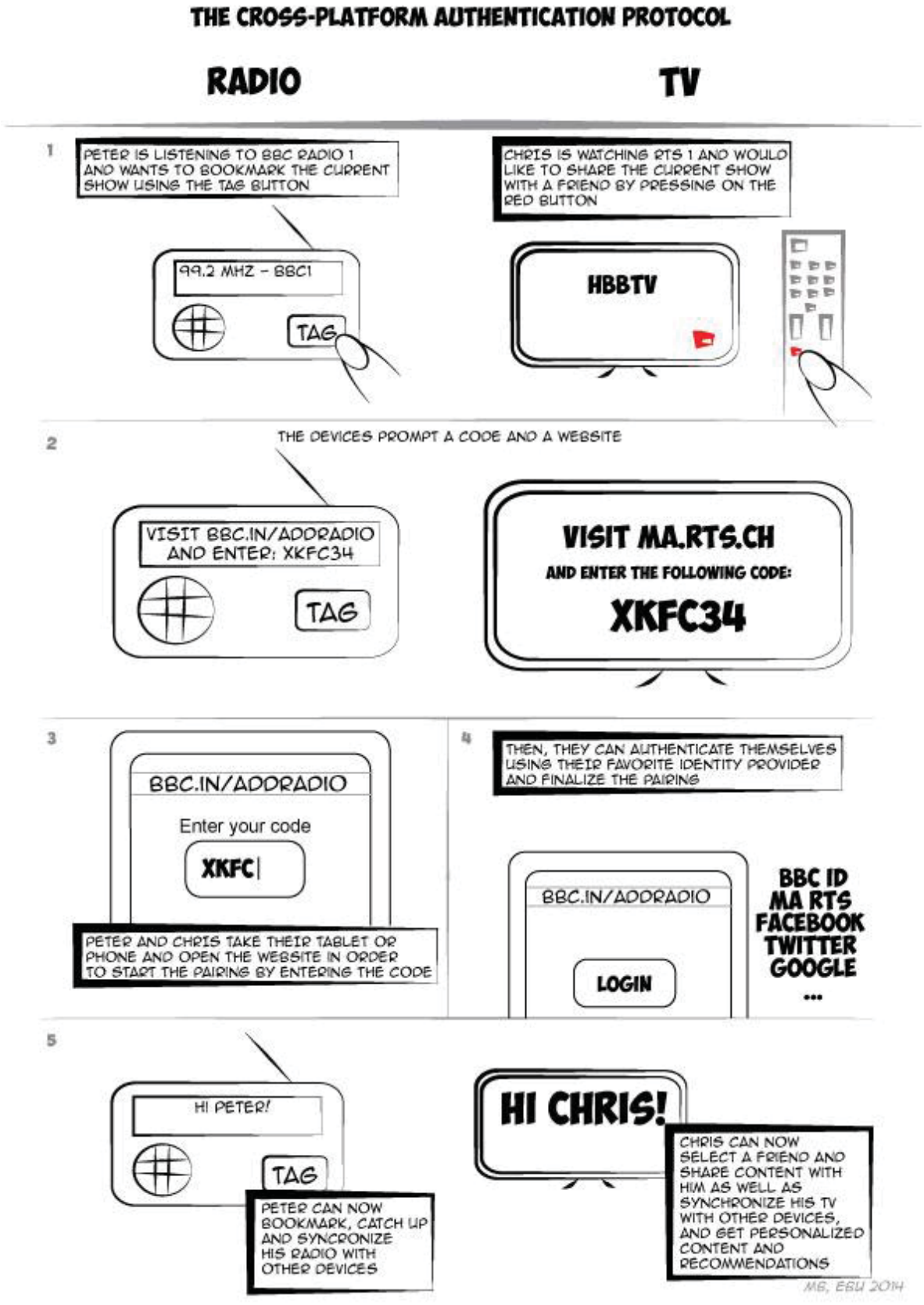

Figure 7 – Description of the association from the user's point of view

FUTURE WORK

The EBU is currently working in close collaboration with Public Service Broadcasters to roll out and optimize the operational aspects of running such systems at scale.

ACKNOWLEDGEMENT

This paper is the result of several years of international collaboration and joint work with many colleagues. I would like to especially acknowledge the outstanding contribution and help of Chris Needham, Sean O'Halpin, Sébastien Noir, Michael De Lucia, Miguel Rodriguez, Aleksi Rossi, Mathias Coinchon, Peter MacAvock and other colleagues who contributed to the work mentioned in this paper.

REFERENCES

1. HbbTV: http://www.etsi.org/technologies-clusters/technologies/hybrid-broadcast-broadband-television
2. ETSI TS 103 270: "RadioDNS Hybrid Radio; Hybrid lookup for radio services"
3. ETSI TS 104 307: "Cross Platform Authentication for limited input hybrid consumer equipment ".
4. IETF RFC 6749: "The OAuth 2.0 Authorization Framework".
5. IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".
6. N. Ragouzis et al., Security Assertion Markup Language (SAML) V2.0 Technical Overview. OASIS Committee Draft, March 2008.