

Towards personalized TV for concurrent use; challenges and opportunities for IMS-based IPTV

Ray van Brandenburg, M. Oskar van Deventer, Georgios Karagiannis, Mike Schenk

Abstract—As TV is becoming increasingly personalized, its focus has become more and more on single individual users. In this article we propose a new form of personalized TV services; personalized TV services for multiple concurrent users of the same television. We will present a number of novel use cases that fall in this category. IMS-based IPTV seems a good architecture to implement these new services on since it is based around an established service oriented infrastructure called IMS (IP Multimedia Subsystem) which features an advanced identity management framework. We will demonstrate that up until now, concurrent use has not been taken into account in IMS-based IPTV. This results in a number of challenges, particularly in the areas of identification and authentication. With a new authentication method we will present in this article, called RFID Digest, we introduce a possible solution to these issues. This new authentication method is integrated in a multi-user TV prototype that allows multiple users to simultaneously enjoy personalized services together on the same TV. The article concludes that the area of personalization for concurrent use offers possibilities for new TV services to distinguish themselves.

Index Terms—IMS, IPTV, Personalization, Concurrent TV services

I. INTRODUCTION

A Service-Oriented Infrastructure represents the infrastructure that is required to efficiently support current and future technology oriented services in areas such as registration, service discovery, provisioning, interconnection and billing. A good example of an architecture that supports these features is the IP Multimedia Subsystem (IMS) [12]. IMS was originally developed in the

Manuscript received February 12, 2010. This work was supported in part by SenterNovem, an agency of the Dutch Ministry of Economic Affairs. Its writing has been carried out in the context of the European EUREKA CELTIC RUBENS project.

Ray van Brandenburg is with TNO Information- and Communication Technology, Brassersplein 2, 2621 CT Delft, the Netherlands (email: ray.vanbrandenburg@tno.nl).

M. Oskar van Deventer is with TNO Information- and Communication Technology, Brassersplein 2, 2621 CT Delft, the Netherlands (email: oskar.vandeventer@tno.nl).

Georgios Karagiannis is with the Design and Analysis of Communication Systems group of the University of Twente, Faculty of Electrical Engineering, Applied Mathematics and Computer Science; PO Box 217, 7500 AE Enschede, the Netherlands (email: karagian@cs.utwente.nl).

Mike Schenk is with TNO Information- and Communication Technology, Brassersplein 2, 2621 CT Delft, the Netherlands (email: mike.schenk@tno.nl).

mobile telephony world as a framework to deliver multimedia services to mobile devices. In recent years the scope of IMS has been extended to also work with fixed access technologies. One example of this development is the standardization of IMS-based IPTV [5]; an IPTV architecture that uses IMS for all major SOI-related functionality such as registration, service discovery, billing etc.

IMS-based IPTV allows for a wide variety of IPTV functionality such as Electronic Program Guides (EPGs) Networked Personal Video Recording (N-PVR) and Video-on-Demand (VoD). IMS's nature as a cross-domain architecture also allows for novel combinational services such as incoming phone calls being shown on the TV screen and automatically pausing the current video. Other features include an array of 'Social TV' services which allow users sitting alone at a TV to communicate with other users elsewhere and thereby creating a feeling of 'watching apart, together' [4]. It is these kinds of services together with applications like personal recommendation engines that really show how much TV is becoming a personalized medium, adapted to the person watching.

It also shows that TV is becoming increasingly focused on the individual experience of a single user sitting in front of the TV. This is in stark contrast to the traditional situation of multiple viewers sitting next to each other on the couch and enjoying TV together, as a group. Almost everybody will be familiar with the situation of a number of family members or friends watching TV together in the living room at the end of the day. Another example is how big sports events such as the Super Bowl in the US and the World Cup in Europe have become big social events, where large groups of people get together and watch collectively. In these types of situations it is the collective experience that is important.

What we aim to do in this article is try to combine these two aspects of the modern TV experience; on the one hand the advantages of a personalized TV experience and on the other the social experience that watching TV together on the couch has always been. In order to do so, we will answer the following three research questions: (1) "In what way are services for multiple concurrent TV users taken into account in the design of current TV architectures?", (2) "Are there any viable use cases for multiple concurrent TV users, both from a user and a business perspective?" and (3) "How could a

personalized multi-user TV service be implemented?”.

This article is organized as follows. Section II will provide some historical perspective on the evolution of personalization in the TV world.

Section III will continue with a brief introduction of the TV architecture we will focus on most in this paper, IMS-based IPTV, and its underlying SOI framework IMS.

In Section IV we will answer the first research question and show that at this moment, the concept of multiple users in front of one TV is largely ignored and is not taken into account in the development of personalized IPTV architectures (i.e. IPTV architectures with an identity management system).

Section V will answer the second research question and introduce a number of use cases that show that there are indeed interesting and viable use cases in the area of personalized services for concurrent use. It will further discuss how these kinds of services are also interesting from a business point of view.

In Section VI the challenges facing the implementation of multi-user use cases in IMS-based IPTV will be discussed.

Section VII will answer the third research question by introducing a number of solutions to the challenges discussed in section VI and will present a prototype of a personalized TV service for concurrent users.

Finally, section VIII will wrap up this article with conclusions and recommendations for future work.

II. EVOLUTION OF TV AS A PERSONALIZED MEDIUM

This section provides a historical perspective, illustrating how television has become more personal over the years.

When analogue TV (PAL (Europe), NTSC (US) [1]), see Fig. 1, was introduced more than fifty years ago, it was delivered over the air using antennas. In these times, there was no form of identification whatsoever; there was no way for TV broadcasters to know how many TVs or which users would be receiving their signal. This also meant that TV set owners could receive TV channels free of charge; no identification meant no way to charge them.

Analogue cable TV introduced a simple form of identification; the physical connection from TV to provider. Now it was possible for TV broadcasters to offer bundles of television channels to individual households and (more importantly) charge them for access.

The introduction of scrambling of TV signals, such as the Conditional Access (CA) [2] method used in most DVB standards [3], provided TV broadcasters and content providers with a system to more effectively control subscriptions to television channels. By scrambling TV channels with unique keys and then distributing (by way of smartcards) these keys to subscribers in different packages it was possible for providers to offer different service levels and differentiate between households in the same neighborhood. This marked the first time that TV became ‘personal’ in the sense that

people could control which channels they received.

In parallel to these developments, early forms of interactive TV were introduced. By using a separate return channel not directly linked to the TV access technology used customers were for the first time able to interact with TV shows. In the beginning fixed telephone lines were used for this return channel, later SMS and the internet became the return path of choice. Examples of these early forms of interactive TV include SMS voting on popular TV shows such as Idols and Big Brother.

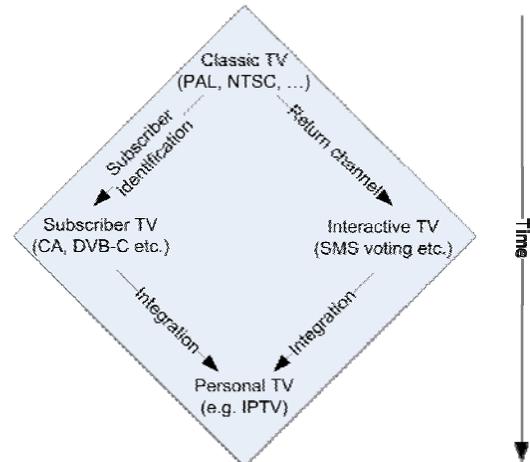


Fig. 1 The evolution of TV as a personal medium over time. Subscription TV and early interactive TV which were separate developments towards personalization have now been integrated in IPTV, which features an integrated return channel as well as means for user identification.

While subscription TV and interactive TV have been separate developments towards personalization for quite some time, the two have been growing towards each other in a relatively new technology called IPTV. The distinguishing feature of IPTV is that both the subscribed content delivery and the interactive services are provided over one and the same (in this case IP-) network. This integration enables more advanced use cases using actual user identification instead of terminal identification (as found in smartcard-based systems). Social TV applications are a good example of how IPTV further personalizes the TV experience by integrating social interaction, such as text and video chat, presence and sharing use generated content.

Another recent example of personalization in the TV world is the development of self-learning recommendation engines. These applications ‘learn’ a user’s likes and dislikes by observing his/her channel zapping behavior. This information is then used to provide personalized content recommendations.

From simple scrambling algorithms to advanced Social TV services and recommendation engines, TV has been on a path towards personalization for quite some time. All of the developments in personalization however aim at single users. In the rest of this article we will try to unify the concept of personalization with the traditional use of TV as a collective medium and aim to introduce a number of use cases that offer personalized experiences for multiple concurrent users.

III. INTRODUCING IMS-BASED IPTV

Before continuing with the concept of personalized services for concurrent use, it is useful to first have a brief introduction of IMS and IMS-based IPTV. The reason we have chosen IMS-based IPTV in the context of this paper is that from all major IPTV architectures, it has the most advanced identity management framework and is therefore the IPTV architecture best suited to provide personalized multi-user services.

A number of standardization bodies collaborate on IMS, among them 3GPP, 3GPP2 and ETSI TISPAN. IMS can be seen as a service oriented architecture that provides registration, service discovery, session control, billing and other services to a variety of services running over different access technologies. To ensure interoperability, IMS is based almost entirely on Internet Engineering Task Force (IETF) protocols such as the Session Initiation Protocol (SIP, [14]) and Diameter [15].

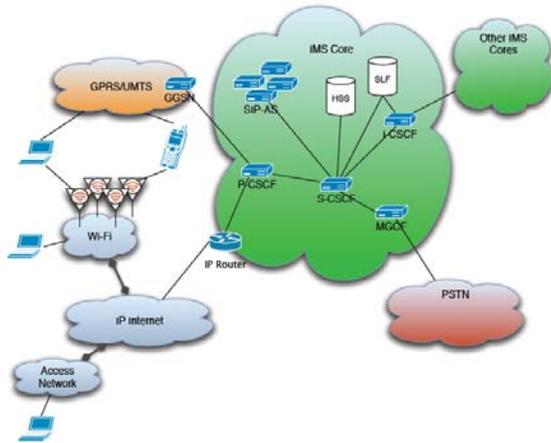


Fig. 2 An overview of the IP Multimedia Subsystem (IMS). In this figure it has been made clear how IMS brings several access technologies together and can therefore offer combinational services.

In the last few years, IMS has developed from being dedicated to mobile devices running over UMTS (hence its 3GPP origin) to a more general IP multimedia SOI that is ‘access independent’; supporting both mobile and fixed access technologies such as WLAN and xDSL. However, IMS’s origin in the mobile telephony world is still apparent when looking at its structure, components and identification system.

The core of the IMS system, see Fig. 2, is based around the Home Subscriber Server (HSS) and a number of Call Session Control Functions (CSCFs). The HSS is a master database containing subscriber information such as user profiles. In that way it can be compared to the HLR (or Authentication Center) in GSM/UMTS. The CSCFs are SIP servers processing SIP signalling packets. There are different types of CSCFs in a network; the S-CSCF which is the central SIP server which performs SIP registration and communicates with the HSS, the P-CSCF which is the SIP server closest to the user terminal and is responsible for maintaining a secure connection to the terminal and the I-CSCF which is responsible for routing to other IMS networks.

IMS-based IPTV is basically an extension to the standard IMS system. It consists of a number of IPTV functions, see

Fig. 3, which use the IMS core as an intermediary between them and the TV. All session control handling and authentication procedures are handled by the IMS core.

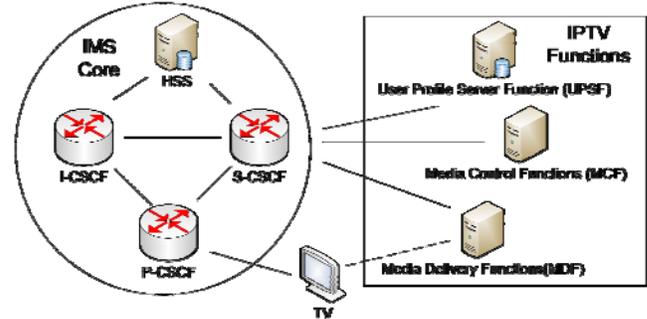


Fig. 3 The IMS core as an intermediary between the IPTV functions and the TV.

IV. CURRENT USE CASES FOCUS ON SINGLE USERS

This section will try to answer the first (1) research question: “In what way are services for multiple concurrent TV users taken into account in the design of current TV architectures?” We will do this by analyzing the use cases that form the basis of IMS-based IPTV. These use cases also form the foundation for the Integrated IPTV architecture [7].

As a result of IMS’s advanced identity management framework, IMS-based IPTV is intrinsically suited to personalized services and is also used in that way. The purpose of this analysis is to find out to what extent concurrent use has been taken into account in its design.

As mentioned, IMS-based IPTV is developed in conjunction with another IPTV architecture, called Integrated IPTV [7]. The two architectures share a document that functions as a blueprint and details the use cases and requirements for both of them. By analyzing the document TS 181 016 [6], we can get a good idea of the focus of the architecture. Which types of use cases are included and which are considered the most important? The central question of course is: what role does concurrent use play in its design?

IPTV use cases can be divided into three different categories, see Fig.4: classic TV use cases for arbitrary numbers of users (not dependent on the number of users), use cases for multiple users at different TVs (one per TV) and the concurrent use category of multiple users at the same TV (either simultaneously or at different times).

As one looks at the use cases offered in TS 181 016, it immediately becomes obvious that the majority of the use cases fall in the first category of use cases for arbitrary number of users. Examples are traditional broadcast TV and the electronic program guide (EPG), but also cases such as Video-on-Demand, Personal Video Recording and Pay-Per-View.

Use cases in the second category of multiple users at different TVs are mostly use cases that fall under the ‘Social TV’ banner such as presence, Watching Apart Together, recommendations from other users and sharing the remote

control.

The third category, use cases for several users of the same TV, is empty; no real use cases were found that are explicitly meant for concurrent use. It should be noted that if one looks very careful, a single line can be found that does refer to the multi-user situation. This line, which is related to the presence use case, is the following: “The interactive IPTV solution shall allow multiple users in front of one TV-SET to communicate their status”. What this means is that out of tens of use cases, and hundreds of requirements, there is only a single line devoted to concurrent use. Even more remarkable is the fact that in the final stage 2 document TS 181 027 [5], that describes the IMS-based IPTV architecture itself, there is no mention of this requirement and the feature is not explicitly implemented.

Situations	Use cases
Single users or arbitrary # of users	Broadcast TV, EPG, Pay Per View, Content on Demand, Personal Video Recording, Incoming calls shown on TV, Content Recommendations (using user history)
Multiple users at different TVs	Social TV(watching apart, together), User Generated Content, Presence, Sharing the remote control, Content Recommendations (from other users)
Concurrent use (multiple users at the same TV)	{none found}

Fig. 4. Use cases, which form the blueprint of IMS-based IPTV, show that the architecture was not designed with multiple concurrent users in mind.

Based on this analysis, it is safe to say that the IMS-based IPTV solution, while enabling many personalized services for individual users, has not been designed with multiple users and concurrent use in mind. It should be noted that this does not necessarily mean that the architecture does not support multiple concurrent users; it just wasn't designed with the concept in mind.

Of course the above analysis is not exhaustive and does not look at other IPTV architectures. However, a similar survey of the other main IPTV architectures such as DVB-IPTV [20] and Open IPTV Forum [19] show that these architectures suffer from the same problem encountered in IMS-based IPTV; the requirements and use cases do not include the concept of concurrency. The first (1) research question (“In what way are services for multiple concurrent TV users taken into account in the design of current TV architectures?”) can therefore be answered negatively; multi-user TV services are not taken into account.

V. PERSONALIZED MULTI-USER USE CASES

The observation that all examples of ‘personalized’ use

cases focus on single individual users, raises the question whether the combination of personalization and concurrent use is even possible or desirable, at all. Maybe there are no interesting use cases that deliver a personalized experience for multiple concurrent users. Or multi-user personalized services are simply not viable from a business perspective. This leads us to the second (2) research question: “Are there any viable use cases for multiple concurrent TV users, both from a user and a business perspective?”

In this section we will present a number of new use cases, some from a user perspective and some from a business perspective, which we have come up with. We think this set of use cases presents adequate reason to believe that personalized services for multiple concurrent users do in fact form an interesting and viable category of TV services.

- 1) *Multi-user Recommendation Engines*: In section II self-learning recommendation engines were taken as an example of how TV is becoming increasingly more personalized; the recommendation system learns by observing a user's behavior and the result is a personalized recommendation. While these kinds of systems work well when a TV is only used by a single user, when multiple users are sharing a TV, there are a number of issues. For example, if your six-year old daughter watches the Teletubbies in the afternoon, you don't want the system to recommend you all kinds of children programs when you're watching TV in the evening. Another example is that you might watch different programs when you're watching with your friends than when you're watching with your children, and the system should take this into account.
- 2) *Multi-user Targeted Advertising*: Targeted advertising is the main reason why personalization is interesting from a business perspective. Taking multiple concurrent users into account could make targeted advertising be even better adapted to the current audience. Imagine a common family of a mod, a dad and their two children. When the children are watching, it would make sense to have advertisements for children's programmes, when dad is watching, beer commercials would be a good fit. However, when dad is watching together with his children, none of the above commercials would be fitting. In this case, commercials for Disneyland would be appropriate. In the same way, when mom and dad are watching TV together, commercials for a romantic weekend to Paris would be perfect. This shows that taking multiple users into account, and possibly the relation between these users, could make advertising far more effective.
- 3) *Personal EPG/Channels*: In recent years, both in the US and Europe, the number of TV channels has skyrocketed [9][10]. This makes it increasingly

harder for users to make a selection; users are overwhelmed by choice. This results in a TV that contains hundreds of channels of which every member only watches a very small subset. A useful multi-user application would be a system in which every family member is able to choose and order his own list of channels. When this user turns on the TV, he only sees his favorite channels, in the order of his choosing. The multi-user aspect comes in when two or more members log in. In this scenario the respective sets of channels are added to each other. An additional possibility is for adult-only channels to automatically disappear when a child logs in.

- 4) *Multi-user Social TV*: Social TV applications allow users at different TVs to chat and enjoy TV shows together [4]. Taking multiple simultaneous users into account brings both additional opportunities as well as requirements to the concept of Social TV. One of those requirements is privacy; if you're not alone but watching TV with several family members it is important that users on your buddy list can see this, so that they don't send those very private chat messages (and prevent embarrassing situations). In the area of new opportunities brought by multi-user Social TV are things like how to allow multiple concurrent users to chat on the same screen without harming the TV experience for the rest of the users.

These four use cases (and others) show that there are interesting use cases that involve both personalization and concurrent use. Furthermore, they show that acknowledging the possible situation of multiple users simultaneously watching a TV also changes the way single-user applications should behave. Examples of this are the social TV and recommendation engine use cases. This shows that taking multi-user scenarios into account is not only a nice extra but a necessity to ensure privacy and correct functioning. Additionally, with the multi-user targeted advertising use case, we have shown that multi-user personalization is not only interesting from a user perspective but also from a business perspective. With this conclusion we can now answer the second (2) research question ("Are there any viable use cases for multiple concurrent TV users, both from a user and a business perspective?") positively.

VI. TECHNICAL ASPECTS OF IMS-BASED IPTV

The previous section demonstrated that personalization and concurrent use are not contradictory but can in fact add to each other. The next step is trying to implement such a use case which brings us to the technical aspects of these types of multi-user TV services. This leads to the third (3) research question: "How could a personalized multi-user TV service be implemented?"

A. Requirements

This section will focus on the technical requirements of a multi-user TV service. As we have shown earlier, IMS-based IPTV was not designed with concurrent use in mind, which poses the question if it is able to support multiple simultaneous users at all. More specifically: "does IMS's identification mechanism support multiple simultaneous users at the same terminal?"

In order to answer this question, we first need to get an idea of the kind of requirements the use cases presented in the previous section introduce.

The one thing all three use cases share is the need for identification; a method to know which users are currently using the TV. Identification can be both local as well as global. An example of local identification is an interactive TV show keeping two participants on the same TV apart from each other. Global identification is needed to distinguish users from other participants worldwide interacting with the show. Where local identification is the domain of the terminal (the TV or set-top-box), global identification needs to be taken care of by IMS.

Continuing with the example of the interactive TV show, it would make the system far more versatile if it would be possible for users to not only play together with members of their own household, but also with friends or family from other households. This introduces two further requirements: The first requiring users to be able to log in on any TV within the network. This could mean TVs in their bedroom or basement, but also TVs at a neighbor's or friend's house. Some sort of *roaming* is required. It should be noted that the term *roaming* in this context is different from the use of the same term when applied to the mobile telephony world. Here it means switching from one TV to another; in the telecom world, it means switching from one carrier to another (in a different country). The second roaming-related requirement directly follows from the first; if multiple users can log in on one TV and users are also allowed to roam between different TVs than the situation with users from different subscriptions watching TV together might also arise and this situation should therefore be supported.

As a result of this analysis, a list of seven multi-user requirements has been drawn up. We found that this list can be used as a good checklist to check whether IPTV architectures support concurrent use.

- 1) The IPTV solution should support globally unique identification of a user
- 2) The IPTV solution should support multiple consecutive users at the same terminal
- 3) The IPTV solution should support multiple concurrent users at the same terminal
- 4) The IPTV solution should support roaming between different TVs within the same household (intra-house roaming)
- 5) The IPTV solution should support roaming between different TVs in different households (inter-house roaming)

- 6) The IPTV solution should allow different users of the same subscription to be simultaneously logged in at different TVs
- 7) The IPTV solution should allow users of different subscriptions to be logged in at the same TV

B. Identifiers in IMS

Now we have defined some general multi-user requirements; the next step is to check whether IMS-based IPTV meets these requirements. In order to do so, it is useful to first know some more about IMS's identification system.

As already discussed IMS has its origin in the mobile telephony world. It is from this world where IMS gets its identification system, which is based around the use of Universal Integrated Circuit Cards (UICCs), more commonly known as SIM cards.

On the UICC, two distinct types of identifiers are placed, IMPIs and IMPUs. The IMPI, which stands for IP Multimedia Private Identity, can be compared to the IMSI found in GSM/UMTS. It is a private identifier in the form of a SIP URI that is bound to a specific subscription. The IMPI is used for authentication purposes and is only known to the UICC and the operator's authentication center.

The IMPU, which stands for IP Multimedia Public Identifier, is a public identifier in the form of either a SIP URI (sip:ray@tno.nl) or a TEL URI (tel:+31 6 123 456 78). It can be compared to a telephone number and just as with telephone numbers, a user can have multiple IMPUs associated with a single IMPI (IMSI). It is important to note that the IMPU plays no role in the authentication process; this is the domain of the IMPI.

If a user has multiple IMPUs, these can be stored together, on the same UICC, or each IMPU can have its own UICC (with associated IMPI). It is also possible for one UICC to have multiple IMPIs. Finally, it is possible for users to share an IMPU (analogue to a family having their own phone number but also a shared one; the household telephone). As one can imagine, the flexibility of the UICC-based IMPI/IMPU system allows for a wide variety of different configurations; one of which is displayed in Fig. 5.

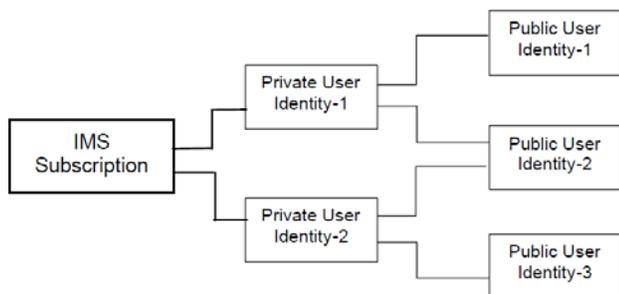


Fig. 5. Due to the flexibility offered by the IMPI/IMPU system, lots of user/group configurations are possible.

The question now is: is it possible to simultaneously register two IMPIs (possibly of different subscriptions, see requirement 7) on the same terminal? Fortunately, the IMS standards are very clear that this is indeed supported. What

this means, is that in theory, the concurrent use scenario is feasible.

However, before we can conclude by saying IMS-based IPTV supports concurrent use, we first need to look at the more practical aspects of IMS's identification system. The main issue here is: how to get two IMPIs from different households, which are therefore on different UICCs, physically on the same terminal?

In order to answer this question we need to look at IMS's authentication system.

C. Authentication in IMS

IMS's authentication system relies primarily on a UICC-based mechanism called IMS AKA (IMS authentication and Key Agreement). In order to provide authentication for terminals that do not feature physical UICC slots, two other mechanisms, SIP Digest and NBA (NASS-Bundled Authentication) are also provided.

a) IMS AKA

IMS's main authentication method, IMS AKA, is similar to AKA mechanisms found in GSM and UMTS. It is a challenge response mechanism that uses a combination of an IMPI and a shared secret K that is stored in the UICC and in the operator's authentication center (the HSS).

As already discussed, IMS allows for multiple IMPI to be placed on a single UICC. If we now assume that each user is identified by a single IMPI, there are two options for a family. The first is to give each family member a separate UICC containing their personal IMPI. The second is to have a single family-UICC containing the IMPIs of all family members.

Now consider the seven multi-user requirements introduced earlier. If the family members each have their own UICC, there is a problem when two members want to watch TV together; the terminal needs two UICC slots (where the standard terminal only has one). Of course this problem could be remedied by simply installing two UICC slots on all terminals; however this solution does not scale. What if three, four, five or more users are watching TV together? To sum up, single-user-UICCs pose a problem for requirement 3.

The second option, with a family UICC, is also not ideal. In this case, there are problems when different family members want to watch TV at different locations (either in their own house or at different households). Since there is only a single UICC, only one TV can be used simultaneously. Family-UICCs therefore do not meet requirement 6.

The main problem with IMS AKA is the physical nature of a UICC; they can be at only one place at a time and cannot be split or joined together. Of course this can be expected, in the mobile telecom world, where IMS and UICCs have their origins; there is no analogue to the concept of multiple users sharing a terminal so the physical nature of the UICC is not an issue. For multi-user TV applications however, we can safely conclude that UICCs, and with them IMS AKA, is not a viable option

b) *NASS-Bundled Authentication (NBA)*

Fortunately, IMS features two other authentication methods, specifically designed for applications where the use of physical UICC is not possible. The first of these is NBA. NBA works by linking an IMPI to a physical line identifier such as an xDSL connection identifier. When a user presents his IMPI, the physical connection over which he connects is checked against his stored line identifier in the user database (in the HSS) to check whether the user is who he claims to be. When the two match, the user is successfully identified.

The problem of NBA in the context of multi-user TV is immediately apparent; since a user can only connect through one specific connection, roaming is not possible. The inflexibility of NBA makes sure that it does not meet requirement 5 of the multi-user requirements.

c) *SIP Digest*

The final form of authentication offered by IMS is SIP Digest authentication. SIP Digest is similar to HTTP Digest, a well known form of authentication that is often used in log-in procedures on websites. Instead of being based on UICC, SIP Digest is built around a combination of an IMPI and a password. When a user registers in the IMS core network, he provides his IMPI and his password. His password is then checked through a challenge- response mechanism to check whether it matches the password stored in the user database (in the HSS).

Note that SIP Digest is intrinsically less secure than IMS AKA, so an additional layer of security (DNS-SEC, https, SSL) may be needed for its use [11][13]. For most internet applications, however, Digest-based security suffices and we believe it is also sufficient for access to IPTV services.

The main problem with SIP Digest is in the area of usability; asking users to enter their IMPI and password on a keyboard every time they turn on the TV is not very user-friendly and is not likely to be successful. In order for SIP Digest to be useful in the area of TV identification, the issue of usability will first have to be solved.

Now we have briefly discussed all three of IMS's authentication methods, we can conclude that none of them is without any issues. IMS AKA's primary issue is the physical nature of UICCs and the resulting lack of flexibility, NBA authentication does not allow roaming and SIP Digest has usability issues. This further supports the notion that IMS-based IPTV was not designed with multiple concurrent users in mind.

As for the possibility of implementing personalized multi-user use cases in IMS-based IPTV, this seems feasible, although with a number of issues. We have already shown that IMS's system of identifiers is very flexible and allows for multiple users to simultaneously log in on the same terminal. As for the method of authentication, even though SIP Digest has usability issues, technically it is perfectly capable of allowing multiple simultaneous users to log in.

Now we have concluded that multi-user use cases are in

fact both viable as well as technically feasible, the rest of this article will focus on how to implement them and minimize the existing issues.

VII. IMPLEMENTATION

A. *User-friendly authentication is possible*

At this point, the only problem standing in the way of a working prototype of a multi-user application is SIP Digest's usability issue. Users do not want to enter a username and password every time they want to watch TV; watching TV should be a simple, relaxing situation. What is needed is a new way for users to identify themselves to the TV; a user identification system that requires minimal effort from the user. Of course this system should meet all of the multi-user requirements stated earlier.

This new identification method should also work within the existing IMS framework. Now IMS has been completely standardized it is very hard to get new elements added to the standard. What this means is that whatever new form of identification or authentication is developed, it should work within the existing framework so that no changes in the IMS core, and therefore no standardization, is needed. The only way to do this is by re-using one of the three existing authentication methods. The new identification method should therefore be compatible with either SIP Digest, IMS AKA or NBA.

There are numerous forms of user identification possible today. From the very simple, typing in a username to the very complex, like facial recognition. For the purposes of the prototype discussed in the next section, we have chosen to use RFID (Radio Frequency Identification). The reason we have chosen RFID is because of its high flexibility, low cost, the fact that it is inherently suited to roaming (as opposed to for example facial recognition) and since it requires minimal effort on the part of the user. It should be noted that the prototype that we describe here could just as well have been developed using another form of identification and the choice of RFID here does not mean we believe that this will be the identification method of choice if and when multi-user TV services are rolled out in the future.

RFID is a technology that allows RFID tags (simple credit card-sized plastic cards that can hold small amounts of data) to be wirelessly read out over a small distance. The unique property of RFID is that RFID tags do not need a power supply to function; they are powered by the energy emitted by the reading device. RFID tags come in wide variety; from very small and cheap ones to ones with lots of memory and advanced security features. The simplest way to describe the ones used during this project is contactless 1Kb memory cards [17]. Using a challenge response mechanism for authentication, an RFID reader is able to read and write data to and from the RFID tag.

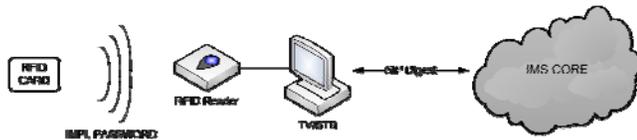


Fig. 6. An overview of the RFID Digest identification and authentication method. The user swipes his RFID card in front of an RFID reader which transfers the user's credentials to the terminal (the TV or set-top-box). The terminal then contacts the IMS core to perform regular SIP Digest authentication.

The proposed identification and authentication system for our prototype, see Fig. 6, works as follows: a user's IMPI, IMPU and password are stored on an RFID tag. When the tag is read out by an RFID reader (connected to the TV or set-top-box), the user's credentials are transferred from the RFID tag to the terminal. The terminal then initiates standard SIP Digest authentication with the IMS core, which sees no difference between this process and the regular SIP Digest procedure. Since it is combination between RFID and Digest technology, this new authentication method has been appropriately named RFID Digest.

B. Prototype development

With RFID Digest, we can now conclude that there is nothing standing in the way of a personalized TV service for multiple concurrent users. The next step in the process is proving this by developing a prototype; a prototype that demonstrates both RFID Digest as well as an interesting multi-user use case.

For this prototype we have decided to implement the Personal EPG/Channels use case. The most important reason for this is that it is very simple yet immediately shows the underlying concept of multi-user TV; not requiring a long explanation, it shows in 30 seconds how the individual experiences of several users can be combined into an improved collective experience.

The prototype includes several elements of the personal EPG/Channels use case. Every user (identified by an RFID card) has a distinct set of channels; users can watch these channels by logging in (swiping their card in front of the reader). If multiple users are logged in on the same terminal, they will have access to a union of all channels each of them is subscribed to. To clearly show the set of channels the users are able to watch, the prototype will include an Electronic Program Guide that automatically adapts to the available channels. In order to demonstrate the possibility of user information stored on the RFID cards, each RFID card will be marked adult or child. When a child logs in, the prototype will automatically remove all adult-only channels from the list of available channels.

The main problem we encountered during the development of the prototype was the lack of an IMS-based IPTV testbed. Since IMS-based IPTV is still in the standardization phase, we didn't have a functioning IMS-based IPTV test environment at our disposal.

To solve this problem we designed an alternative server-side architecture, see Fig. 7. A total of four entities are

necessary: two nodes performing the duties of the session control server and user-profile-storage server (HSS) of the IMS core and two nodes performing the IPTV-specific functions of video broadcasting and EPG generation and delivery.

In order to stress the importance of Digest authentication to RFID Digest (and through the use of SIP Digest the easy integration with IMS), it has been decided to use a Digest capable HTTP server as a replacement for the SIP-enabled S-CSCF. By replacing SIP Digest with the very-similar HTTP Digest, the general concept is maintained.

The fact that with the transformation from SIP to HTTP the very session-control nature of IMS has been removed is not considered a problem for the purposes of showing the features and advantages of RFID Digest; which is ultimately the goal of the prototype. The most important thing is that Digest authentication, which forms an integral part of RFID Digest, has been maintained in the new situation. The actual authentication process between client and server is therefore practically unchanged from the IMS-enabled situation, which should be enough in proving that RFID Digest can be seamlessly integrated with IMS.

The same reasoning goes for the fact that SIP maintains states and HTTP does not. Because of this, in the prototype it will be possible for a user to log in at multiple TVs with the same RFID card.

With the HTTP server performing the role of S-CSCF, another server-side entity is required to perform the role of HSS (UPSF). For this a simple SQL server has been chosen. Even though it is not possible to have the HTTP and SQL servers perform the exact same roles as the S-CSCF and HSS, the overall picture is the same; the SQL server performing the role of credential storage and the HTTP server handling the authentication itself (and contacting the SQL server for credential information).

For the video-broadcasting node, VLC, a streaming video server with an RTP/RTSP channel has been chosen.

The EPG node is more complex. The main issue here is that in the case of a multi-user personal EPG, there are a number of requirements not found in regular EPG applications, such as multiple customizable EPGs. It should be noted that the EPG node would also have to be newly developed, since it is probable that IMS-based IPTV's EPG system would also have failed to meet all of the multi-user requirements.

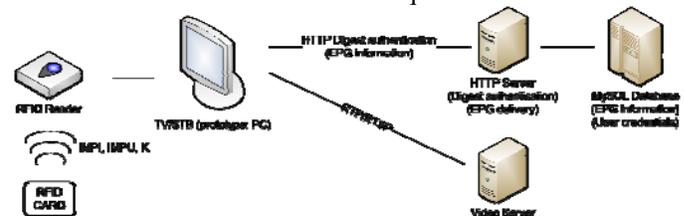


Fig. 7. An overview of the prototype's functional structure which clearly shows the IMS entities being replaced with alternative nodes.

For the RFID Digest prototype, it has been decided to have the HTTP server already in place for Digest authentication also handle EPG requests. Another SQL database provides the

necessary EPG information. The advantage of this structure is that the HTTP server can use the same credentials obtained for authentication to generate a personalized EPG.

On the terminal (the set-top-box or pc), the client has been divided into five functional block, see Fig. 8: an RFID handler which performs all RFID related tasks such as authentication and decryption, an EPG handler which creates a visual EPG from the raw data received from the EPG server, a video client which requests channels from the video server and handles descrambling and decoding, an IP communication block which is responsible for communicating with the HTTP server and performing Digest authentication and finally, a graphical user interface.

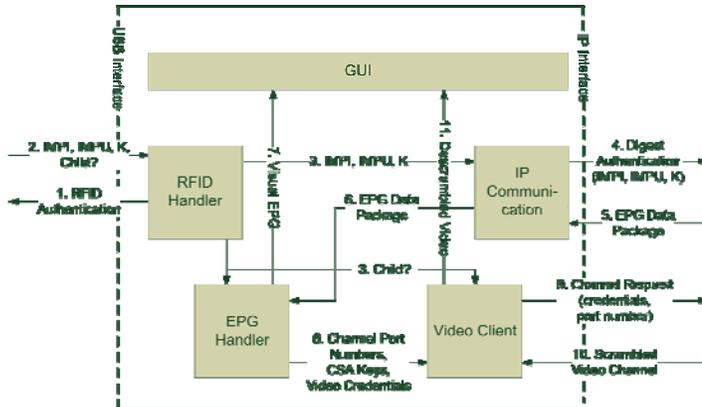


Fig. 8. An overview of the client applications which runs on the terminal. Shown are the five functional blocks and the communication channels between them.

Fig. 8 also shows the various information flows between the various functional blocks.

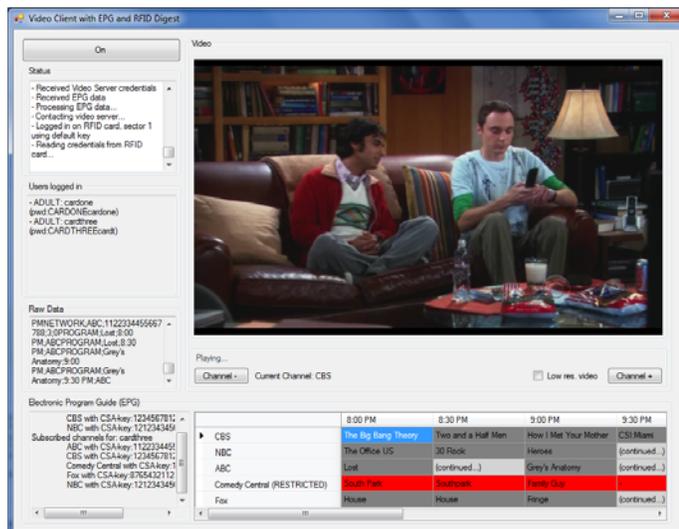


Fig. 9. Screenshot taken from the completed prototype demonstrator. In this case, two adults are logged in, both with their own sets of channels. The EPG clearly shows one network marked in red. This indicates an adults-only channel. Should a child log in, this network is removed from the EPG and the list of available channels.

For more information on the exact implementation details of the prototype, the reader is referred to [18].

The correct functionality of the personal EPG/Channels use

case prototype has been verified using a demonstrator. Fig. 9 shows an example screenshot taken from the prototype implementation demonstrator. In this specific situation two users are logged in, both with a different set of subscribed channels. Also shown is the EPG in which a specific network has been marked as restricted. Should a child log in, this network would be removed from the EPG and the available channels list.

This prototype presents one possible answer to the third (3) research question (“How could a personalized multi-user TV service be implemented?”).

VIII. CONCLUSIONS AND FUTURE WORK

Service oriented infrastructures are about effectively and efficiently supporting current and future technology oriented services. IMS is a good example of an infrastructure that fits this bill. Because of its cross-domain orientation it is well positioned to provide convergence between different types of domains and services. In the case of IMS-based IPTV it allows different types of IPTV applications to effectively share both information as well as resources. By providing service discovery and control it also facilitates innovative new applications and services to be quickly implemented and evaluated.

One such group of services are personalized services for multiple concurrent users, an area that up until now has not been properly investigated. With a number of use cases we have shown that there are interesting and viable use cases to be found that aim at multiple simultaneous users of the same terminal.

We have also shown that while IMS-based IPTV, through its reliance on IMS, has an advanced identity management framework at its disposal, it wasn’t designed with multiple concurrent users in mind. This notion is supported by the fact that in IMS-based IPTV’s requirements document, no references were found to multi-user scenarios or use cases. Furthermore, IMS’s standard authentication protocol, IMS AKA, is not well suited to provide authentication for multiple simultaneous users at the same terminal.

In order to prove that personalized services for concurrent use are in fact an interesting area of research, we have developed a proof-of-concept demonstrator of such a multi-user use case. In order to solve the identification problem we have defined a new authentication method, called RFID Digest, which combines the use of personal RFID cards with the SIP Digest authentication method. The unique advantage of this solution is that it doesn’t require any changes to the IMS core and therefore additional standardization is not necessary. In particular, we developed a prototype of the personal EPG/Channels use case that applies the RFID Digest authentication method for identification support. Using a demonstrator we have verified and shown the correct functionality of the personal EPG/Channels use case prototype. In particular, this prototype is able to support the

multi-user personal EPG/Channels use case requirements listed in Section VI.

In the future, our work will be focused on three areas. First, some research will be needed in the area of security; are there any new security vulnerabilities brought by the use of RFID? And are these vulnerabilities acceptable for the overall security level of IMS? Also, policy decisions like who is responsible for the security of the RFID cards? Should they be the property and responsibility of the IPTV provider, just like with SIM cards in the telecom world, or should the users themselves be responsible for them, like with passwords in the internet world?

Another area for future work is the implementation of additional personalized multi-user TV use cases. Specifically, use cases that incorporate ‘active concurrency’, that is, use cases in which the different users have an ‘active’ role. An example of such a use case is the interactive TV show; here multiple users will have to simultaneously communicate with the TV and this brings additional issues.

Furthermore, another future area is the implementation and performance evaluation of personalized multi-user TV use cases combined with the RFID Digest authentication method in an IMS-based IPTV testbed. These types of use cases and others will really help in (1) bringing the general concept of multiple concurrent users to the attention; (2) becoming the next step in TV personalization.

REFERENCES

- [1] International Telecommunication Union, “Conventional Television Systems”, ITU-R BR 470-7, 2005
- [2] Digital Video Broadcasting, “Framing Structure, channel coding and modulation for cable systems”, EN 300 429 v1.2.1, 1998
- [3] Digital Video Broadcasting, “Support for use of scrambling and Conditional Access”, ETR 289 v1, 1996
- [4] E. Boertjes, J. Klok, O. Niamut, M. Staal, “ConnectTV: Share the experience”, in *Social Interactive Television*, P. Cesar, D. Geerts, K. Chorianopoulos: IGI Global, 2009, pp. 187-202
- [5] ETSI TISPAN, “IPTV Architecture: IPTV functions supported by the IMS subsystem”, TS 182 027 v2.0.0, 2008
- [6] ETSI TISPAN, “Service Layer Requirements to Integrate NGN Services and IPTV”, TS 181 016 v3.3.1, 2009
- [7] ETSI TISPAN, “NGN integrated IPTV subsystem Architecture”, TS 182 028 v3.3.1, 2009
- [8] M. Sack, “iShow – An Interactive TV Show”, Thesis, Saxion Hogeschool Enschede, 2007
- [9] RNW, “Over 6,500 TV Channels in Europe, UK in top spot”, rnw.nl, Oct. 17 2008 [Online]. Available: <http://blogs.rnw.nl/medianetwork/over-6500-tv-channels-in-europe-uk-in-tio-spott-poll>. [Accessed Jan. 20 2010]
- [10] Nielsen Media, “Average U.S. Home Now Receives a Record 118.6 TC Channels”, nielsenmedia.com, Jun. 6 2008. [Online] Available: <http://www.mediabuyerplanner.com/entry/34086/us-homes-receive-a-record-1186-tv-channels-on-average/>. [Accessed Jan. 20 2010]
- [11] ETSI TISPAN, “3G Access Security for IP-based Services”, TS 133 203 v8.5.0, 2009
- [12] ETSI TISPAN, “IP Multimedia Subsystem: Stage 2”, TS 123 228 v8.5.0, 2009
- [13] M. T. Hunter, R. J. Clark, F. S. Park, “Security issues with the IP Multimedia Subsystem (IMS)”, in *Proceedings of the 2007 Workshop on Middleware for next-generation converged networks and applications*
- [14] IETF, “Session Initiation Protocol”, RFC 3261, 2002
- [15] IETF, “Diameter Base Protocol”, RFC 3588, 2003
- [16] IETF, “Uniform Resource Identifier: Generic Syntax”, RFC 2396, 1998
- [17] NXP Semiconductors, “MF1ICS50 Functional Specification”, Available: http://www.nxp.com/acrobat_download2/other/identification/M001053_MF1ICS50_rev5_3.pdf. [Accessed Feb. 10 2010]
- [18] R. van Brandenburg, “Towards multi-user personalized TV services, introducing combined RFID Digest authentication”, Thesis, University of Twente, 2009
- [19] Open IPTV Forum, “Services and Functions for Release 2”, v1.0, 2008
- [20] Digital Video Broadcasting, “DVB-IPTV standards”, Feb. 10 2010 [Online]. Available: <http://www.dvb.org/technology/standards/> [Accessed Feb. 10 2010]

M. Oskar van Deventer (M’09) was born in The Netherlands in 1965. He has an MSc degree in electrical engineering (1987) and a PhD degree in optical networking (1994) both from Eindhoven University of Technology, The Netherlands.

Oskar has been working as a Senior Scientist for KPN Research (Leidschendam, 1987-2003) and TNO Information and Communication Technology (2003-now) in the areas of Signal Transport Systems and Network and Service Control, respectively. He has published numerous articles and a book on optical communications. With over 350 contributions, he is a main contributor to the ITU-T BICC standards for Voice-over-IP over ATM (1999-2002) and the nearly completed ETSI TISPAN IMS-based IPTV standards (2006-2010), being Rapporteur for two of those standards. He was also chairman of Dutch VoIP Interconnection Taskforce (FIST) and chairman of Dutch ENUM technical working group (ENUM Innovation Platform). His current focus is interoperability and interconnection of IPTV systems and Content Delivery Networks.

Dr. van Deventer has won several international awards in the area of Mobile Gaming, a Eurescom best paper award and the Veder award for best research in electrical engineering (1997). He has also been responsible for over 40 patent applications.

Ray van Brandenburg was born in the The Netherlands in 1984. He has a BSc degree in electrical engineering (2007) and an MSc degree in embedded systems (2009) both from the University of Twente, Enschede, The Netherlands.

Ray is currently working as Innovator for TNO Information and Communication Technology in the area of Network and Service Control. In the last year his main focus has been on IPTV services and identification and authentication techniques.

Georgios Karagiannis holds an MSc and PhD degree in electrical engineering from the University of Twente, Enschede, The Netherlands. Since 2003 Georgios is Assistant Professor at the Design and Analysis of Communication Systems group at the University of Twente. From 1994 to 1998 he was working as a Researcher at the University of Twente. In 1998 he joined the Wireless Multimedia Research unit of Ericsson Eurolab Netherlands in Enschede, The Netherlands, where he stayed until April 2003. His research interests are in the fields of fixed, mobile & wireless (inter)networking, end-to-end QoS signaling and provisioning, mobility and routing in logical access (overlay) networks and performance evaluation.

Mike Schenk graduated from Delft University of Technology in 1991.

Mike is currently working as a Senior Scientist for TNO Information and Communication Technology in the area of Service Enabling and Management. On behalf of KPN, he was active in standardization bodies such as ETSI, ITU and ISO and industry for a such as the TINA Consortium (TINA-C) and the Object Management Group (OMG). His main interest is the application of generic middleware solutions for telecommunications purposes. Examples are network/service management platforms, service enabling platforms such as OSA/Parlay and JAIN and generic authentication and identity management platforms. Mike’s current focus is on validating upcoming technologies by trial implementations for customers. Based on these trials the strategic value of a technology can be estimated. He firmly believes in the added value of hands-on experience. Closely related to this is the topic of Business Continuity Management.