Phone-controlled Delivery of NGN Services into Residential Environments

Andreas Fasbender[1], Stefan Hoferer[2], Martin Gerdes[1], Takeshi Matsumura[3],
Andreas Häber[4], Frank Reichert[4]
[1]Ericsson Research, Ericsson GmbH, Germany,
[2]Department of Communication and Distributed Systems, RWTH Aachen, Germany,
[3]Ericsson Research, Ericsson Nippon K.K., Tokyo, Japan,
[4]Agder Mobility Lab, University of Agder, Grimstad, Norway

Abstract

The horizontally layered architecture of the IMS/NGN standards family enables the delivery of services independent of access network and requesting device. In this article, the authors propose a further separation of service control and delivery, allowing the requesting device – in particular a user's mobile phone – to invite other devices (we will focus on DLNA appliances) into the service delivery, enhancing both user experience and service design flexibility. The proposed solution builds on exploiting proximity technologies (e.g. barcodes, NFC) for pairing the control device with a remote environment. Motivated by scenarios, the architecture concepts are explained and a prototype that was implemented for validation is described. Selected findings and a short overview of related standardization efforts conclude the paper.

1. Introduction

Entertainment devices such as set-top boxes, game consoles, music players, and cameras today routinely come with built-in networking capabilities that enable them to upload, download, and render media from other devices in the home. The Digital Living Network Alliance (DLNA) is since 2004 publishing interworking guidelines for home media sharing services [1] based on the Universal Plug and Play (UPnP) standards family [2]. DLNA is now widely accepted in the consumer electronics industry and will soon enable advanced interworking services for all sorts of devices in (local) IP network islands.

In parallel, fueled by a rapidly growing broadband penetration both in fixed and mobile scenarios, consumers are increasingly adopting online media download and streaming services such as music portals, mobile TV and fixed IPTV. Operators on the other hand have started to prepare for an increasing media mix by rolling out next-generation network (NGN) infrastructures and services based on IP Multimedia Subsystem (IMS) for service control and IP transport. Standardization bodies, such as the 3rd Generation Partnership Project (3GPP) [3], Open Mobile Alliance (OMA) [4] and the Open IPTV Forum [5], are specifying basic services and enablers to deliver operator-managed and 3rd party services via this infrastructure.

Many telecommunication services today have in common that they are designed and optimized for a single consumption device, for example a mobile phone, an IMS Multimedia Telephony (IMT) terminal, or a set-top box (STB). Devices are typically securely coupled to the user's identity and subscription by Subscriber Identity Module (SIM) cards or conditional access modules, consequently restricting service delivery to a specific consumption device and often even location. Mechanisms such as placeshift (e.g. Orb, Slingbox) have to be put in place to support the user's growing demand for access to content and services, everywhere and anywhere.

The user's phone as a personal device holding the identity, service portfolio and personal data (such as address book, media files, and service credentials) is today heavily under-utilized as a service control device, one important reason being limitations in screen size and input facilities. In this paper, we propose a new service delivery concept, which relaxes the tight coupling of service control and delivery through the use of IMS, and allows users to initiate and control their services on for example a mobile phone, while delivering the services to a most suitable consumption device. This leads to a triangular relationship between user, the user's services (aggregated from multiple sources), and the devices used for service play-out and

978-0-7695-3333-9 /08 $25.00 © 2008 IEEE
DOI 10.1109/NGMAST.2008.71

interaction. Our proposed architecture combines the benefits of operator-guaranteed trust, security, charging and quality of service based on NGN technologies with the consumer electronics (CE) industry perspective of launching attractive end user devices.

We start by describing sample scenarios in Section 2, motivating the requirements on a flexible end-to-end solution. In Section 3 we present our proposal for an architecture that addresses these requirements, providing a description of all functional elements required and explaining the signaling flows. Our prototype media portal implementation, based on IMS, DLNA and QR Codes for proximity detection, is described in Section 4, followed by a summary of lessons learned and a short overview of ongoing standardization activities in related areas in Section 5. Section 6 concludes the article and points to open issues and potential future research.

2. Scenarios & requirements

2.1 Example scenarios

Remote music access: Carol is on a business trip, visiting a conference. On the way to the hotel she accesses the media portal of her service provider to listen to music with her mobile phone. After she has checked in, she decides to listen to her music in her hotel room and connects to her media portal again. Using her mobile phone she discovers all available media devices in the hotel room, with the stereo system and a TV set among them. This time she wants to enjoy the better sound quality of the hotel stereo system. Therefore, she selects the stereo system as target device for the music from the media portal, and her songs are immediately played on the stereo system in her room.

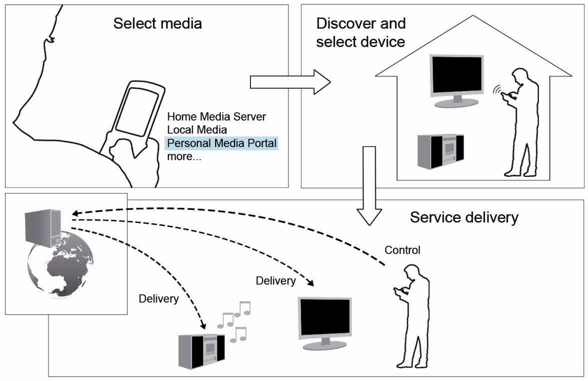

Figure 1. Separating service control and delivery

Remote DVR and Placeshift TV: The next day, Carol realizes that she will probably miss her favorite TV program in the evening. The *Placeshift TV* feature of her home IPTV subscription would actually allow her to redirect the TV media delivery from her IPTV provider through the hotel network and her room TV. But she expects to return late after the conference dinner. Therefore she prefers to log into her own residential control device at home from her phone, and to program her digital video recorder (DVR) with a few simple clicks to record the TV program for her.

2.2 Requirements

Considering above examples and similar user scenarios, a number of requirements for a widely applicable solution have been identified [6]:

For delivery of user services to devices in a remote environment a trust relationship between the user's identity, the service provider and the remote device selected for service consumption needs to be established. This relationship shall not depend on the source of the service, such as the user's home network, an operator application server, a 3rd party service provider, or the mobile device itself.

The intended solution should support interaction with any kind of remote device, such as UPnP/DLNA or SIP devices. Modifications to the software and hardware environment and the behavior of these devices shall not be required.

In order to provide an acceptable user experience, the user shall not be required to have any deep networking knowledge. Consequently, the user shall not be required to enter lengthy addresses, user names or passwords on the mobile phone or any remote device, an inconvenient and time consuming task.

For both, the network owner and its users, security is an important aspect of an acceptable solution. Most consumer appliances, including DLNA devices, lack a proper security implementation due to their restricted use in local network environments. Disclosing device information and other details shall only be allowed to trusted external peers in our solution.

The administrator of the visited network shall be able to grant access to selected devices and services, and restrict access for visitors. It must be possible to revoke access to any device at any point in time.

3. Architecture

The proposed architecture for the phone-based delivery of NGN services into residential environments is based on the following main principles: Connectivity and accessibility information about residential devices and their services is published to a presence server. A URL is transmitted to the mobile phone, pointing to the presence instance where the connectivity and accessibility information for the residential devices can be retrieved. This URL is forwarded to application servers or other peers that subsequently use it for requesting detailed device and service descriptions. These details are then utilized for establishing a service delivery session into the residential network, using the phone for service control.

In Figure 2, the logical components of our architecture are illustrated. Functionalities and signaling flows are explained subsequently, under consideration of the *remote media access* use case. The signaling flows may vary in certain details for other use cases, but the same general principles are applicable.

3.1 Functional architecture

Because UPnP and similar service discovery protocols are designed to work in local IP networks, a *Residential Control Device* is necessary to make external nodes aware of the status and capabilities of devices within the local environment. In addition, the Residential Control Device must manage the access and connectivity of these devices through the residential gateway. Thus, the Residential Control Device allows using devices from the local network with external services, such as media delivery services from a portal to a local media player.

Essentially, the Residential Control Device provides the following functionalities (compare Figure 2): A *DLNA Control Point* (DLNA CP) is used to discover DLNA devices such as Digital Media Renderers (DMR) or Internet Gateway Devices (IGD) within the residential network. Corresponding device profiles are exposed from DLNA devices like TVs and music players, while the IGD device profile is provided by the residential gateway. After a device has been discovered, more details about device capabilities and supported services can be fetched from the respective device. This information is later required to access and control the offered services. To present the information on a DMR (e.g. in form of a barcode image shown on a DLNA TV) a *HTTP server* may also be deployed that serves as source for this information.

An *IMS Client or B2BUA* registers the Residential Control Device in the IMS core and hence connects the residential network to the NGN service infrastructure. This is used to publish detailed device and service information from the residential environment to the NGN Presence Server and to establish a secure and QoS enabled media tunnel between the *Application Server* and the residential control device for the service delivery into the residential environment. The B2BUA in the Residential Control Device also supports the handling of inbound session requests to SIP devices (or nodes with SIP UAs) within the residential environment [7].

The *Residential Environment Control Logic* contains the use case dependent functionality for the publication of device and service connectivity and accessibility information, and for the control of inbound service delivery sessions. It includes a management console for the selection of DLNA devices that are made available to the user for the delivery of an NGN service from the external service network, creates NAT-bindings at the residential gateway for inbound service delivery, publishes the required information for the inbound service delivery to a presence server, and transmits a reference to this information to the mobile phone. Different options can be supported for this transmission, including NFC, Bluetooth, or 2D barcodes displayed on the DLNA-TV and decoded by the mobile phone.

The *User's Phone* is the central service access and control device. It hosts an *IMS Client* required for

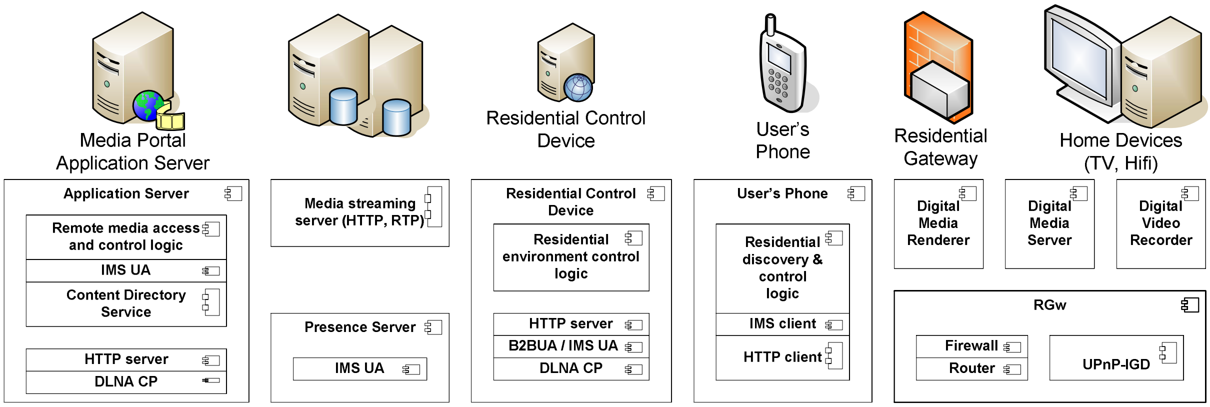

Figure 2. Functional end-to-end architecture

authentication to the NGN, accessing the NGN Application Server (the media portal in our example use case), and forwarding the reference to the device and service information (that has been published to a presence server) to the NGN Application Server. The *HTTP client* is used for any HTTP-based service control GUIs provided by an NGN application server. Through this control GUI the actual service delivery (e.g. streaming to a DMR) is decoupled from the service control on the user's phone. The *Residential Discovery & Control Logic* retrieves the device and service information reference from the residential control device and forwards it to the Application Server.

In order to deliver services into a residential network, the *Application Server* offers the following functions: It handles user authentication and authorization for personalization, coupling between user's service control point such as mobile phone and the service delivery target device, delivering the requested service to the target device securely with appropriate quality of service, and optional charging for the service. In our architecture, it hosts the service portal as the entry point for a user to select and request a service from the user's personalized menu. Through the IMS UA, it also implements a SIP interface to the IMS core over a standard ISC interface (IMS Service Control). Before allowing the user to access the services, the AS authenticates the user and authorizes service requests. Here, the IMS based architecture takes advantage of the Generic Bootstrapping Architecture (GBA) mechanism [8] to provide a single sign on (SSO) experience to the user. The DLNA Control Point (CP) controls UPnP/DLNA devices by sending UPnP actions to them over a secure tunnel.

A *Remote Media Access and Control Logic* establishes a secure tunnel used by the DLNA CP (IMS remote access, [9]). The residential network can delegate authentication of the AS or the user requesting access to it to the IMS network and authorize remote access for service delivery based on the authentication result. The *Content Directory Service* provides content lists such as video files or music albums that the user can watch or listen to. It also provides search functionality so that the user can easily find the desired content.

In the following we briefly explain the application of GBA mechanism to this architecture [8]: The IMS operator deploys a Bootstrapping Server Function (BSF), and the AS works as Network Application Function (NAF). If a User Equipment (UE) requests a service from the AS for the first time, the AS will demand that the UE must be authenticated using GBA. Thereafter, the UE and the BSF mutually authenticate using a shared secret. As a result, a pair of session keys is generated by the BSF, and one of the keys is delivered to the UE. The UE responds back to the AS with the received session key, where after the AS requests the BSF to authenticate the user by providing the session key. The BSF returns the authentication result and finally the AS approves that the UE is authenticated. Besides high security, this process has the advantage that it can be completed without the user having to type in a password.

Another component of the operator NGN infrastructure is a *Presence Server* that operates as information relay for device and service connectivity and accessibility information between the residential environment and the application server, which requires support for enhanced presence information formats.

Finally, a *Media Streaming Server* provides media storage and delivery through HTTP or RTP streaming.

3.2 Service delivery issues

In standard home environments, devices are connected to a residential gateway, which provides a mapping between the private IP address space used in the home and the publicly routable IP address space. In order to deliver end user services to residential devices, those devices first have to be known by the service provider and also be capable of interacting with the service. One option for device discovery is to rely on direct connectivity to the residential environment (e.g. using WiFi or Bluetooth). Besides the fact that not all mobile devices may be capable of or allowed to directly connect to the LAN, another disadvantage is that continuous listening for presence updates would drain the batteries of a mobile device rather quickly.

In any case, mobile devices that only have access to cellular connectivity need to discover local device information by other means. For this purpose, new proximity technologies such as barcodes or Near Field Communication (NFC) can be used. Here, the information is retrieved by reading so-called tags attached to the remote environment. To prevent the user from identifying each available device by a separate tag, it is reasonable to expose a central device and service repository located in the remote environment.

Furthermore, the lack of direct connectivity to the local network requires a solution for the user to control local devices via the service backend. This requires mechanisms to traverse firewall and NAT in the residential gateway. One possible solution is to use the port management mechanisms offered by the UPnP Internet Gateway Device (IGD) profile [10]. IGD is widely deployed on off-the-shelf gateways; however, due to inherent security flaws it is not always available.

3.3 Signaling flows

High-level signaling flows are provided in Figure 3 to the right, consisting of three main phases as described in the following. Parts of the standard signaling with the IMS core has been omitted from the figures and explanations in the following, including the procedures for authentication and registration of the IMS entities.

In the *service presence publication* phase, the Residential Control Device publishes the presence information of devices and services in its local environment to the Presence Server.

In the *media selection and service awareness* phase, when the phone retrieves the initial page of a service, it passes an argument for the IMPU of the service presentity. This IMPU is acquired by the phone using a proximity solution, such as NFC or barcodes. Next, the Remote Media Access and Control Logic node receives the service information through having subscribed to the presentity of this IMPU. In case of static setups this flow can be optimized, e.g. by using a so-called one-shot SUBSCRIBE (expiration set to 0). Thereafter, media and playout device selection is carried out between the user's phone and the application server.

In the *remote service usage* phase, the Remote Media Access and Control Logic node establishes a remote session with the Residential Control Device, including the opening of a port at the Residential Gateway firewall for the media playout. Using this port mapping, the user can control the Digital Media Player with his phone through a GUI provided by the Remote Media Access and Control Logic. In the final step, the Digital Media Player fetches the content from the Media Streaming Server.

4. Prototype implementation

A simplified prototype based on the described architecture has been developed in collaboration of Ericsson Research, University of Agder and RWTH Aachen. This prototype supports a scenario where the user is a guest at a hotel providing Digital Media Players and retrieves media from a Media Portal. The prototype focuses on the implementation of the service delivery functionality and builds on HTTP signaling for remote service awareness instead of SIP/IMS.

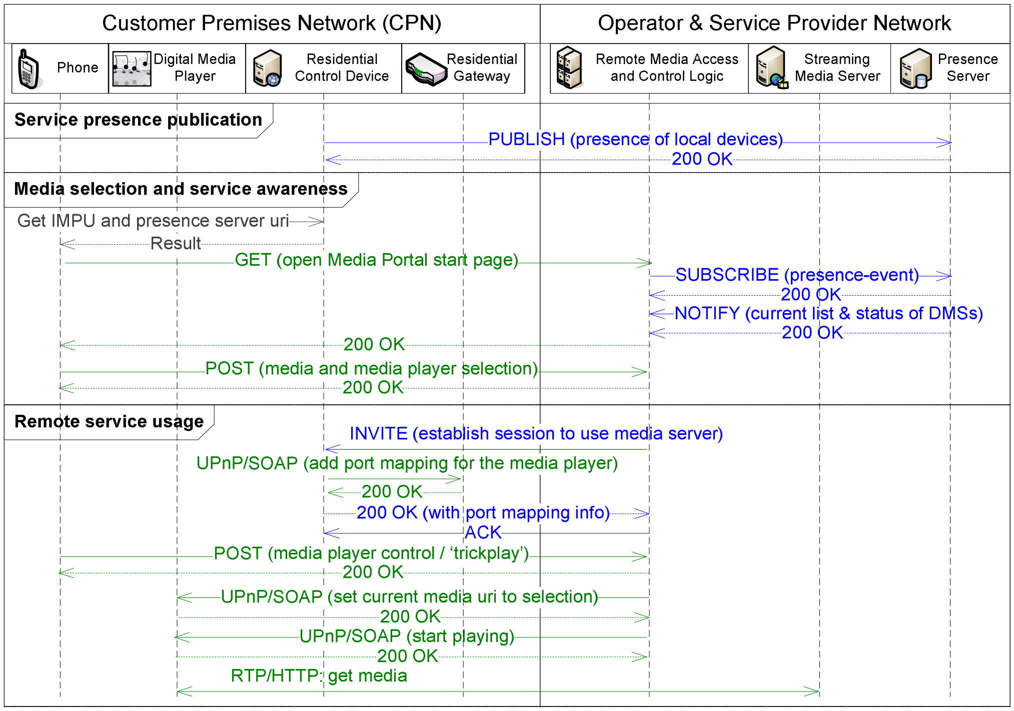
Customer Premises Network (CPN)
Operator & Service Provider Network
Phone
Digital Media Player
Residential Control Device
Residential Gateway
Remote Media Access and Control Logic
Streaming Media Server
Presence Server
Service presence publication
PUBLISH (presence of local devices)
200 OK
Media selection and service awareness
Get IMPU and presence server uri
Result
GET (open Media Portal start page)
SUBSCRIBE (presence-event)
200 OK
NOTIFY (current list & status of DMSs)
200 OK
200 OK
POST (media and media player selection)
200 OK
Remote service usage
INVITE (establish session to use media server)
UPnP/SOAP (add port mapping for the media player)
200 OK
200 OK (with port mapping info)
ACK
POST (media player control / 'trickplay')
200 OK
UPnP/SOAP (set current media uri to selection)
200 OK
UPnP/SOAP (start playing)
200 OK
RTP/HTTP: get media

Figure 3. High-level signaling flow for remote media access on DLNA renderers

4.1 Barcodes

For the prototype, barcodes were used to transfer an initial set of information from the hotel network to the user's phone. Unlike traditional barcodes such as EAN-13 which is widely deployed on consumer products, modern barcodes can store up to several hundreds of bytes of data. The mapping between a barcode and the stored information is described by a barcode symbology. To date, more than 1000 symbologies exist, differing e.g. in data density, maximum capacity, available readers or distribution.

QR Codes (Quick Response Codes) are two-dimensional codes released in 1994 and standardized in ISO/IEC18004 [11]. They provide sufficient capacity to encode the required data set. Due to their availability as an open standard, several SDKs exit for encoding and decoding QR Codes with acceptable performance.

In our initial implementation, the connectivity information was encoded in a 2D barcode and included a globally routable address and a unique identifier for each user device, generated and published by the Residential Control Device. This flow was later extended to retrieve only the address where the list of available home devices could be fetched. Prior to encoding, information could optionally be encrypted, i.e. requiring the user to enter an access code on the phone, to prevent it from being misused.

4.2 Implementation

The prototype architecture is shown in Figure 4. The multimedia content, made available through the Media Portal, is stored in the *Digital Media Server* (DMS). Based on Java Servlet technology [12], the *Media Portal* was implemented as the web application used by clients, such as the phone client as described below. After requesting users to login to the web site, it offers a personalized menu for the selection of media content and media renderer that shall be used to playout the selected content. In addition, playback control is provided.

We used a commercial off-the-shelf gateway in a routed setup and supporting NAT control through UPnP IGD. A Java MIDlet was implemented on the phone to decode the QR Codes. Information about available media renderers, obtained from the QR Codes, is submitted to the Media Portal when accessing the user's home page in the phone's browser. We used UPnP-compliant *Digital Media Renderers* located in the hotel network, such as a DLink DSM-320.

The *Residential Control Device* used in the hotel network for the access provision to local DMR:s has been implemented on a standard Linux PC. It performs the discovery of DMR:s in the hotel network by means of UPnP, and creates a provisioning web site. Here devices available for the hotel guest can be pre-selected, together with a mapping between DMR:s and

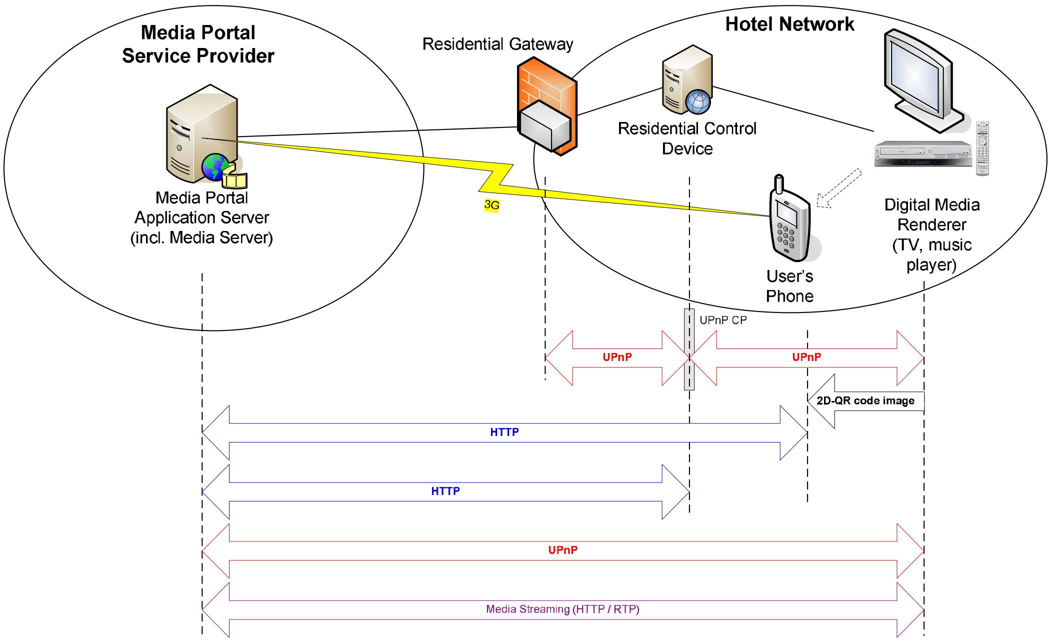

Figure 4. End-to-end prototype architecture for Online Media Portal

the guest's hotel room. The control functionality also generates the QR Code and displays it on the guest room TV via UPnP Audio-Video (AV) service.

4.3 Lessons learned

To start with, the demonstrator worked as expected and the Online Media Portal could indeed be realized as anticipated. This proofs that our architecture concepts generally hold. However, several issues have also been identified during implementation, which we summarize in the following.

The phone QR Code reader implementation as Java MIDlet yielded poor barcode recognition performance with an average delay of 6 seconds per decoding attempt. This delay can be significantly decreased to less than 2 seconds by e.g. using Symbian-based implementations. While the Java-based reader makes it necessary to manually take a snapshot of the barcode, the Symbian application allowed continuously scanning the environment for barcodes and notifying the user or an application once a code is captured. This is due to a more flexible access to the camera. The integration of barcode recognition engines into the camera API as seen for recent Japanese mobile phones is expected to further increase recognition performance.

One disadvantage of using UPnP/DLNA appliances is that only HTTP streaming is specified as mandatory, while support for RTSP/RTP is only optional. For HTTP, standard media renderers buffer parts of the media before playback. Therefore, a delay is introduced between selecting play and the actual media playout, depending on the channel capacity and required bandwidth. Our measurements show that for example for a 128 Kbps mp3 music playout at 1 Mbps access capacity around 2 seconds are spend on buffering. At 0.2 Mbps the experienced buffer delays were already in the order of eight seconds.

The timing of setting up and releasing IMS session for remote access needs to take scalability into account. In addition to the session establishment, when device control is requested as in Figure 2, the establishment may be triggered by the startup of the Residential Control Device or by the user's sign-in/sign-out to the service portal. The former may consume unnecessary resources in the network and in the AS regardless how many home devices are accessed, and the latter requires a timer based session management, since the user may leave a session without explicitly signing out. A different approach is to use SIP MESSAGE for delivering UPnP actions to home devices, without establishing a remote access tunnel. However, the user may experience longer latencies before the action is executed on the target device, because the SIP MESSAGE is routed via the CSCF.

Support for non-UPnP devices (e.g. Apple Bonjour or SIP devices) requires a new functional entity in our architecture. Currently the service provider in the AS is tightly coupled to the UPnP protocol used by the home device where the service is delivered. The new entity would be expected to provide a common interface to control home devices in order to keep service provider's logic independent from the protocol or standard used by the home device.

In case the Residential Control Device is not collocated with the Residential Gateway, the proposed solution requires support of UPnP IGD in order to establish port mappings. Since malicious software exists that exploits loopholes in IGD, several gateway vendors and operators mandate UPnP IGD to be disabled by default. The gateway working committee of the UPnP Forum is already addressing these security issues. It is likely that next IGD specification will require use of a default authentication and authorization mechanism. Alternatives to IGD are for further study.

5. Standardization

Work in several standardization bodies is ongoing that addresses most parts of our proposed architecture.

The Home Gateway Initiative (HGI, [12]) is in the process of specifying the next generation requirements on residential gateways, including an IMS Proxy function that terminates the operator NGN signaling and translates it to home network internal SIP/UPnP signaling. Our proposed HIGA architecture matches closely with HGI specifications.

ETSI TISPAN [13] is working on similar features within WG5 (Home Networks) on the Consumer Network Gateway (CNG) specifications, in close collaboration with HGI.

The UPnP Forum has been since 2006 working on specifying an architecture for remote access, basically extending the UPnP network to include remote clients via a VPN tunnel. Similarly, DLNA has recently started a task force on remote access. Both solutions can be applied to perform end-to-end signaling between a remote client (e.g. mobile phone), and UPnP/DLNA devices residing in a remote environment.

Finally, the Open Mobile Alliance (OMA) [4] is working on standardizing profiles for proximity solutions such as NFC and barcodes.

6. Conclusions & outlook

We have shown how NGN technologies, UPnP/ DLNA and new proximity solutions can be applied to separate service control from delivery. Using standard technologies available today, services can be delivered to consumer devices in broadband-connected local network islands, with the user's phone staying in control of service access and delivery. This allows operators to further adopt the role of a service and trust broker for users. This role may be further extended by offering hosting services for the access control logic to providers of network islands, such as hotels, hotspots or conference venues.

Besides architectural details and signaling flows, we have described a proof-of-concept implementation of our solution that showed that the proposed mechanisms work as expected.

We also pointed to some areas for improvements, for example the fact that proximity technologies are not yet properly integrated into the mobile phone software stack. Our prototype implementation also did not yet make use of the in-built QoS policy management and control mechanisms of IMS/NGN. For improved experience and reduced end-to-end delays, the user should be able to decide if content is streamed over a reserved channel or where best-effort delivery is sufficient, which may correspond to different charging schemes. Similarly, the use of RTP is expected to yield quality gains over HTTP streaming.

References

[1] Digital Living Network Alliance: Interoperability Guidelines v1.5, March 2006.

[2] UPnP Device Architecture 1.0, July 2006.

[3] 3GPP – http://www.3gpp.org

[4] OMA – http://www.openmobilealliance.org

[5] Open IPTV – http://www.openiptvforum.org

[6] Stefan Hoferer: Design, analysis, and prototyping of an architecture for bootstrapping of user, device, and service relationships in heterogeneous networks, diploma thesis, RWTH Aachen, March 2008.

[7] Torbjörn Cagenius, Andreas Fasbender, Luis Barriga: An IMS Gateway for Service Convergence in Connected Homes, 45th FITCE congress, Athens, August 2006.

[8] Generic Authentication Architecture and Generic Bootstrapping Architecture, 3GPP TR 33.220.

[9] Andreas Häber, Martin Gerdes, Frank Reichert, Ram Kumar: Remote Service Usage through SIP with Multimedia Access as Use Case, PIMRC 2007, Athens, September 2007.

[10] Internet Gateway Device (IGD) v1.0, November 2001.

[11] ISO/IEC. Information technology: Automatic identification and data capture techniques – QR Code barcode symbology specification, ISO/IEC 18004, August 2006.

[12] J2EE Java Servlet Technology – http://java.sun.com/products/servlet

[13] Home Gateway Initiative – http://homegatewayinitiative.org

[14] ETSI TISPAN – http://www.etsi.org/tispan