Your media everywhere, anytime. This summarizes end-user expectations when ever-wider broadband and ever-lower flat-rate tariffs combine with users’ thirst for digital content.

The authors describe Ericsson’s end-to-end solution for remote access services, which builds on the IMS and UPnP families of standards, along with the Home IMS Gateway (HIGA), which serves as an intermediary gateway for connecting the device-centric consumer electronics space with the user-centric telecommunications world. The gateway approach leaves the consumer electronics and telecommunications business models unaffected, while at the same time creating synergies between the two.

Connecting users to their home networks

TV sets, set-top boxes, game consoles, stereos, cameras and other entertainment appliances now routinely come with built-in communications capabilities that enable them to upload, download, and display data from other devices in the home. The Digital Living Network Alliance (DLNA), for example, develops device interworking profiles for home-based media-sharing services.\(^1\)

DLNA is based on the Universal Plug and Play (UPnP) family of standards.\(^2\) UPnP also standardizes other services, such as the control of home appliances. Now widely accepted in the industry, with more than 100 devices being certified each month, DLNA will soon enable interworking for all sorts of devices across home networks.

Once users have their media devices connected and running at home, they will soon also want to access their content from remote locations. A mobile phone with WiFi connectivity can easily serve as a peer in a home network, but connecting to this network remotely is an entirely different matter. At present, to access the home island from outside, users must either choose a proprietary, service-specific system or lower their security and run the risk of making their home networks vulnerable to external attacks.

In our example scenarios (Box A) Mr. and Mrs. Martin will expect specific features of the remote access service. Opening a connection into the home means opening a back door into a network that is otherwise “secure by obscurity.” And without end-to-end bandwidth and delay guarantees, the user experience suffers from contention in both the home (LAN) and wide-area (WAN) networks. This can translate into poor sound quality and pixellated artifacts in video signals. Over-provisioning the network is not an option for operators; the only workable solution is to manage the quality of service (QoS) in the wide-area access and core networks, and all the way into the home network and end devices.

Most users are unwilling to buy a separate box just to enable remote access. By the same token, separate boxes represent a significant outlay to operators who would carry the bulk of the costs and would need to further subsidize users for making good use of investments in broadband infrastructure.

Consumer electronics companies prefer a solution that extends the DLNA standard outside the home via UPnP Remote Access. Notwithstanding, this approach falls short in terms of usability and quality of service. What is more, it does not permit users to access their home services from an unknown peer to the home network, such as a friend’s PC or via a hotel TV (Box A).

Ericsson’s target architecture for remote access combines the strengths of

- IMS (IP Multimedia Subsystem); and
- UPnP and DLNA.

It takes the best of both worlds and melds them into one coherent solution. This solution, which does not require additional boxes in users’ homes, reuses existing operator IMS infrastructure to authenticate users, to set up secure media sessions, to perform routing, and (optional) to ensure the establishment of end-to-end QoS.

The core element in this architecture is the Home IMS Gateway (HIGA, Box B), a functional block in the residential gateway that has been under development at Ericsson since 2005. HIGA is currently being standardized in HGI, ETSI TISPAN and the Open IPTV Forum.\(^3\)

As an interworking function that resides in users’ homes, HIGA serves both as a termination point for IMS signaling from the operator backend and as a UPnP peer towards the home network (Figure 1). HIGA provides control over the home network connection and enables devices residing inside the home to connect to peers and services in the WAN using the IMS security and QoS. By using HIGA for remote access, operators can deliver trusted connections with maintained control over the managed network.

**UPnP Remote Access**

The UPnP Forum is in the process of standardizing the UPnP Remote Access architecture. The specification is close to approval,
but not presently included in the DLNA interoperability guidelines.

UPnP Remote Access specifies mechanisms that make it possible to extend the home network so that it logically includes remote devices outside the home LAN. Devices may thus communicate among themselves using UPnP procedures (specified, for example, in the UPnP Device Architecture).

The main functional components of the UPnP Remote Access architecture are the
- Remote Access Transport Agent (RATA);
- Remote Access Discovery Agent (RADA).

These two components are applied in both the Remote Access Server (RAS) and Remote Access Client (RAC). The corresponding RATAs establish secure communication channels between remote devices and the home network, while the RADAs synchronize UPnP device information and content exchanges between RACs and the home network.

At present, UPnP Remote Access cannot support QoS management over the wide-area link. It can only support best-effort delivery of media. Also, to exchange credentials during the initial pairing process, the remote access server and client must be attached to the same LAN. This effectively prohibits remote access devices – in particular non-portable ones – from establishing a remote access session with an arbitrary remote server.

Ericsson’s goal has been to enhance standard UPnP Remote Access functionality with support for setting up an IMS-based remote access tunnel. Non-IMS-enhanced RASs and RACs may still use the tunnel establishment as described in the UPnP architecture. The proposed IMS enhancements provide particular benefits in managed network environments. Ericsson is also studying additional extensions that use IMS provisioning mechanisms to enable a remote pairing process between client and server.

**IMS-assisted remote access**

The main flow for establishing a remote-access session is based on IMS and supports the UPnP/DLNA 2-box model. The remote access service is invoked between a Digital Media Renderer (DMR – implemented in our scenario on a mobile device such as a mobile phone or laptop) and a Digital Media Server (DMS) in the home network. The HIGA functions as both the IMS User Agent and termination point of the virtual private network (VPN) tunnel in the home (Figure 2).

For the flow shown in Figure 3, the mobile device and HIGA must already have connected to and registered with the IMS network. HIGA can therefore be reached through its default IMPU (for instance, sip:martin-family@operator.com). Furthermore, it is assumed that HIGA has, via UPnP ceremonies in the RADA listener, collected information about and built up a device database for DLNA-compatible devices in the residential network. In our example flow below, this database holds an entry for the NAS, which is assumed to support a DLNA DMS profile.

**Phase 1: Connection request**

Using his mobile phone, Mr. Martin wants to access a video clip located on the NAS in his home network. The remote-access application on his mobile device sends an IMS
3-box streaming:
Ordinarily, Mr. Martin’s commute to work takes about 30 minutes, but today the roads are packed. He pulls out his phone and logs on to his media portal. He then selects his home server as source and the car stereo for output. Music from his favorite playlists is immediately streamed to his car speakers.

2-box download:
Mrs. Martin unexpectedly runs into an old friend while shopping in town. As the two begin talking about their summer vacations, Mrs. Martin pulls up some images from her home media server and displays them on her phone.

2-box upload:
Having no recent photos of her friend, Mrs. Martin uses her phone to take a snapshot of the two of them together. She then uploads the image to a digital photo frame at home, annotating it with a message to her husband: “I’ll be out a little longer than expected!”

2-box remote control:
Mr. Martin, realizing that he’s going to miss the Champions League final due to a late customer meeting, logs on to his home server from his laptop. With a few simple clicks, he programs his digital video recorder (DVR) to record the match.

2-box remote control:
A few minutes later, Mr. Martin receives a message on his phone indicating that somebody has rung the doorbell at home. Mr. Martin connects to the door system to find that the “visitor” is his son, who forgot his keys. Mr. Martin approves entry and the door opens.

3-box streaming:
Finishing work rather late, Mr. Martin and some colleagues decide to watch the Champions League final at a friend’s place. Using his mobile phone, Mr. Martin connects to his home server and directs the recorded game to be played via his friend’s big-screen TV.
INVITE message to HIGA, which authenticates the request by comparing the P-Asserted-ID (inserted by the home operator in the INVITE message) with the values of allowed user identities. In short, home access control is delegated to established IMS mechanisms, whereas the user (Mr. Martin) maintains control of the access control list. Optionally, the operator backend can manage access control and operation.

The session description protocol (SDP) included in the IMS signaling, is used to inform the RAS and RAC of the IP addresses and ports for the remote access tunnel. It is also used to negotiate VPN profiles and the key management protocols used to establish the tunnel. This negotiation ensures agreement on a common secure mechanism supported by both HIGA and the remote client. It also allows for continuous updates as new security schemas emerge.

### Phase 2: Peer-to-peer VPN setup over the IMS media plane

Once Mr. Martin is successfully authenticated and authorized, the remote client sets up a secure media control session between itself and HIGA.

For tunnel setup, UPnP Remote Access specifies an out-of-band connection-establishment procedure. Ericsson’s solution employs a corresponding connection-establishment profile based on operator-managed IMS network procedures, with HIGA functioning as the VPN server. After tunnel setup, the connection between Mr. Martin’s remote device and the NAS in the home network appears as a local UPnP connection.

### Phase 3 – UPnP discovery

Because UPnP was originally designed for use in local area networks, there are some challenges associated with extending it for use in wide area networks. For example, the UPnP device-discovery mechanisms are based on the exchange of multicast messages that internet routers typically discard. UPnP Remote Access solves this by filtering relevant messages in the remote access server and by forwarding them to remote peers via unicast.

By applying the standard UPnP RADA mechanism for synchronizing Mr. Martin’s remote mobile client with the remote access server (co-located with HIGA in Figure 2), the mobile device can retrieve a list of home media servers and their UPnP service

---

**BOX B, HOME IMS GATEWAY**

The Home IMS Gateway (HIGA) is a logical function that collects information about users, devices and services in the home, and manages IMS sessions on behalf of non-IMS-capable home devices.

HIGA is registered to the IMS core based on secure authentication, for example, using a soft or hard ISIM with a family identity. Through a back-to-back user agent (B2BUA) and a SIP user agent (SIP UA), home devices can interact and interwork with the IMS core. SIP devices that contain a SIP UA, such as a VoIP phone, can directly register with HIGA. The B2BUA then translates SIP control signaling into IMS-specific messages that it relays to the IMS core.

For IP devices, such as DLNA-compatible media servers and renderers, a SIP UA inside HIGA acts as a proxy. To support remote access, HIGA deploys a Remote Access Server (RAS) and (optionally) a UPnP control point for QoS policy control in the home network.

HIGA functionality can be deployed anywhere in a user’s home network. From a practical perspective, it is easiest to co-locate it with the user’s residential gateway (RGW) – that is, with the router in the home. While it is possible to manage network address translation (NAT) and firewall control through the use of the UPnP internet gateway device (IGD) profile even when HIGA and the gateway are not co-deployed, co-deployment avoids relying on this interface, which is considered insecure in IGD v1.0. It also makes provisioning and firewall management more natural, since the HIGA–gateway combination serves both as operator termination and entry point.
descriptions. RADA is also used to dynamically inform remote clients about device updates, for example, when a media server is switched on. Given the IMS identity of the remote user, HIGA can be configured to perform additional filtering of UPnP devices made available to the remote client.

Phase 4 – Content selection
Mr. Martin selects his home NAS as content source, browses through the list of available media items (based on the UPnP Content Directory Service profile), and selects a video clip either for download or streaming. The UPnP/DLNA control points manage all media access and trickplay functions. HTTP (the default transport protocol in DLNA) as well as RTP (optional in DLNA) can be used to transport media through the VPN connection over the IMS media plane.

Phase 5 – IMS media plane QoS upgrade
UPnP does not support QoS management beyond the home LAN. However, one can support the requirements that real-time-critical media services put on delay and bandwidth by applying standard IMS procedures, which facilitate QoS control between the remote client and HIGA (Figure 4).

In the example flow, Mr. Martin’s remote-access application sees the need for a QoS upgrade from the existing best-effort connection and issues an IMS re-INVITE or a session UPDATE to the IMS network and Mr. Martin’s HIGA. Based on the session description protocol (SDP) in this SIP message and the confirmation from HIGA, the IMS Core provides the policy and resource control and enforcement functions (PCEF/RCEF). Optionally, to ensure full end-to-end quality of service, UPnP QoS management may be applied in the residential network, thereby bridging the QoS management procedures on the WAN and LAN sides through HIGA.

Phase 6 – Content playout
The video clip is played on Mr. Martin’s mobile device.

Placeshift – 3-box remote access
Apart from setting up an authenticated, authorized and secure tunnel with a mobile remote device, HIGA can, in the same way, facilitate connections between two homes, effectively creating a peer-to-peer network with managed QoS. Assisted by IMS, HIGA can prevent unauthorized file sharing and unlawful access to content, since content requestors and providers can be identified in a trusted manner.

In a 3-box remote access or “placeshift” scenario, remote DLNA media renderers (DMR) are used as the endpoints of remote access sessions – for instance, when Mr. Martin accesses content from his friend’s TV (Box A). While the secure control channel is established just like in the 2-box case between the mobile client (now functioning as a digital media controller, DMC) and HIGA, the media session must now be set up between the DMR in the TV and the home network. In this case, the remote access client is only used to authenticate and authorize the DMR, and instructs HIGA to set up a VPN tunnel that it can use to deliver the media.

Standardization
The UPnP Forum and DLNA have made good progress in delivering standards for interoperable consumer equipment. So far, however, support is limited to services in the home network. A standardized solution that enables DLNA devices to access wide-area services without the need for specialized
telecommunications software offers a significant value-add to the consumer equipment industry and paves the way for economy of scale and market uptake.

In Ericsson’s approach, the Home IMS Gateway (HIGA) provides a generic mechanism for connecting consumer equipment to IMS-based operator infrastructure, and via a virtual private network (VPN) to remote user equipment. Although any type of service can generally be supported through such a tunnel, we outline how one can realize UPnP Remote Access with the help of IMS.

HIGA is currently being standardized in the Home Gateway Initiative (HGI) and ETSI TISPAN. In TISPAN, Ericsson is actively engaged in the standardization of customer premises network equipment that supports, for example, IMS Multimedia Telephony and IMS-based IPTV; and defines requirements and the architecture for next-generation customer network gateways and services, including remote access.

HGI is defining requirements for coming generations of residential gateways that will serve as a hub between a home network and a remote environment. Ericsson has a driving role in HGI.

The UPnP Remote Access standard supports the coexistence of various tunnel-setup mechanisms in the remote access server and client. Ericsson is defining profiles suitable for IMS-based tunnel setup, allowing the client and the server to negotiate security schemas for the tunnel. For the solution to be fully compliant with UPnP RA and to ensure broad acceptance for IMS-based tunnel establishment in the CE industry, Ericsson is actively participating in UPnP Forum and DLNA standardization.

**Conclusion**

In an all-connected world, remote access is a key scenario. The simple user proposition is that user-created and commercial content will be available anywhere, anytime and on any device. Remote access also applies to other application areas, such as home monitoring & control and sensor networking.

Ericsson’s solution consists of an architecture that enables secure remote access with telecom-grade performance. The solution builds on the IMS standard for user authentication and authorization, for routing remote access control messages, and for negotiating end-to-end QoS. What is more, the architecture is fully compliant with the consumer equipment industry’s standards for media-sharing services.

Ericsson has, together with Sony and Sony Ericsson, demonstrated the described target solution at leading industry events such as GlobalComm 2006, IBC 2006, Broadband World Forum 2007 and Mobile World Congress 2008. The solution is now being prepared for consumer trials with key operators and leading consumer electronics and gateway partners. The architecture is also being brought forward in standardization, in particular within ETSI TISPAN and the Home Gateway Initiative.

**REFERENCES**

1. DLNA: http://www.dlna.org/en/industry/home
2. UPnP Forum: http://www.upnp.org
4. ETSI TISPAN: http://www.etsi.org/tispan
5. Open IPTV Forum: http://www.openiptvforum.org