ACCELERATE IMS SERVICE ROLLOUT WITH REMOTE DEVICE MANAGEMENT
Accelerate IMS Service Rollout with Remote Device Management

For mobile operators, IMS service rollout, with few exceptions, is a complex process. The reasons for this are many: IMS implementation is complex in itself; adding the migration of legacy consumer services and a multitude of roaming scenarios provides much for mobile operators to think about. Not only does this complexity increase rollout time and staffing costs, it can have a detrimental impact on the consumer experience if not handled effectively. Employing remote device management to enable IMS services and enforce IMS policies on the customer devices allows operators to cut through this complexity and frees them from many of the headaches of their legacy systems and roaming partners. This enables operators to focus on the rapid rollout of IMS services, and the gains in profitability and cost reduction these services can bring.

About IMS-based Services

IMS (IP Multimedia Subsystem), first conceived in 1999, has been around for quite a while now. Its original aim — providing a communication architecture that is independent of access type and relies on IP-based protocols — provides a sound basis for the types of network topographies that are emerging today.

Second- and third-generation (2G and 3G) mobile networks have their roots in the public telephone system, and have relied on signaling protocols oriented around the Signaling System No. 7 (SS7) standard as defined by the ITU, ANSI, ETSI and the IETF. Developing in SS7 (compared to IP) is complex, expensive and time-consuming, and the skilled manpower for developing in this technology is diminishing year by year.

The advent of all-IP LTE networks, along with the competitive drivers of Over-The-Top (OTT) IP services, provides an opportunity for replacing SS7 with IMS and bringing mobile networks into the IP mainstream. This provides not only the additional services themselves but also an
opportunity to phase out legacy technology while gaining the cost savings and spectral efficiency of a single radio technology.

The two key services where IP is making headway in mobile telephony are Voice-over-LTE (VoLTE) and Rich Communication Services (RCS), as well as subsets of the functions of each.

RCS is a set of services designed to combat the threat of OTT providers such as Skype and Whatsapp by integrating tightly with the device phone book and allowing cross-network interoperability for multi-media data services. RCS currently comes in two flavors, RCS-e and RCS 5.x:

- RCS-e is a minimal subset of the RCS and is marketed under the joyn brand name. It provides dual and multi-party instant messaging as well as multimedia content sharing supporting the sharing of pictures, videos and files during a voice call.

- RCS 5.x, of which RCS-e is a subset, supports all of the RCS-e services as well as IP voice and video communication with presence and location sharing.

RCS 5.x requires significantly more investment in infrastructure compared to RCS-e, and RCS-e is seen as a stepping-stone to the full IP-based video and messaging infrastructure that full implementation of RCS 5.x will bring.

### Management Challenges for IMS-based Services

All IMS services require that certain information must be available on the device. This information may be necessary to enable specific services within IMS, fundamental to the operation of the IMS service itself, or simply provide more optimal operation of an IMS service. This information includes credentials, service activation settings, a number of settings that enable the smooth running of IMS services, and service data having to do with communication continuity, media handling and service accessibility.

#### Credential Management

Credentials are required in IMS to authenticate that the user can connect to the network, and that the network to which they are connecting is valid.

There are two key approaches to providing a device with credentials: 1) the credentials are derived from the SIM card, or 2) the credentials are inserted into the device at service inception.
There are two key mechanisms available for using the SIM card to provide credentials. One technique, termed GPRS IMS Bundled Authentication (GIBA), works by comparing the IP addresses allocated to the subscription with the IP address used in the incoming SIP Registration message. The other technique, termed Authentication and Key Agreement (AKA), operates as a challenge-response protocol between the SIM card and the mobile operator’s HSS, using the mechanism within IMS.

Both GIBA and AKA create significant architectural impacts on the mobile network and require that the IMS network be integrated with the mobile network. GIBA also has the significant disadvantage of only operating when the device connects via a GIBA-enabled mobile network. This not only creates roaming complexities, but also denies access to the service from non-3GPP networks such as Wi-Fi. This contradicts the major aim of IMS, which is to provide an access-independent communication solution. It is also a cost to the deploying operator.

AKA has some advantages over GIBA as it will operate over any access network, but it does require that the device provide the IMS application with access to the credential information on the SIM card. For embedded IMS clients, this is not an issue, but when the IMS capability is downloaded and installed as an application after the device is manufactured it is unlikely that this will be available, as it may compromise the security of the SIM.

Rolling out AKA authentication can present challenges, particularly in the early phases of an IMS service take-up. Obviously it is better to have the IMS service tightly integrated into the device at manufacture, as AKA Authentication will be available and the customer experience can be more seamless. But at the initial stages of a rollout, this may not be possible; at a minimum, the IMS service on the client may have to be installed as a pre-integrated application or a downloadable aftermarket application. To support this, the network must support multiple authentication types. This implies that the provisioning server can differentiate between embedded and non-embedded IMS applications.

Inserting the credential information in the device when the SIM is inserted into the device overcomes these shortcomings. The credentials used apply to the Digest Authentication protocol and are acceptable for SIP. There are two key ways of doing this: 1) using the HTTP/S protocol as described within the RCS standards and prescribed by GSMA or 2) using OMA DM.

Using the HTTP/S protocol has the disadvantage of requiring access to the mobile network. This is because the device needs to be authenticated in the network, either by the network enriching the HTTP messages with subscriber information or by SMS. As IMS is oriented to
be access-independent, this may not always be possible and may cause disturbance to the device user if the SIM is inserted but a mobile network is not available.

When using a pre-bootstrapped OMA DM-enabled device, the device can connect to the target management server at SIM insertion, enabling it to pull the credentials it needs regardless of the access type it is using. This does not require any integration with the operator network and has the added benefit of not requiring that the customer have an MSISDN, which is optional in an all-LTE network.

Regardless of whether OMA DM or HTTP is used by the remote management system, provisioning the credentials directly into the device can bring IMS solutions to market more quickly by freeing the service planner from legacy equipment concerns, and allowing them to focus on the revenue opportunities and cost savings associated with the IMS services themselves.

**Multiple Devices**

The traditional model of one device per subscription is threatened by OTT service providers. Skype and Apple, for example, provide services where it is possible to have multiple devices per subscriber account. This is attractive to consumers because many of them have multiple devices and are used to moving between them, using the most appropriate device for their circumstances.

Having multiple devices per subscriber presents challenges to (3GPP) operators because their subscriptions are oriented around SIM cards. This affects their costs, as they do not need to actively consider the device (with regard to the subscription at least). It also provides considerable freedom for the consumer in terms of device selection.

The RCS 5.1 standard provides a mechanism to allow multiple devices per subscription that involves the primary device allowing secondary devices to share the same identity as the primary device. There are a number of schemes to enable this, the simplest being the sending of a one-time password to the primary device via SMS. The one-time password is entered on the secondary device and, from that point on, the secondary device will share the identity of the primary device and can use the services and make video and voice calls.

Although having additional devices for a subscription is attractive to the customer, for the operators it can present some significant security challenges. Once the secondary devices have the identity of the primary device they have, in IMS terms, the same access rights as the primary device and can use the services as desired. Even if the services are free to use and there is no loss of revenue to the operator, a malicious user of that secondary device may be
able to impersonate the customer and commit fraud. With paid-for IMS services, this could have revenue impacts on both the deploying operator and the customer being impersonated.

To mitigate this, management capability is required that can allows the suspension/resumption and cancellation of access rights on devices. At the simplest level this capability would have to be provided by the operator so that they can resolve issues and address incoming customer care traffic as quickly as possible. But to reduce this cost further a self-care mechanism is required such that the customers can manage their own devices independently. Ideally, device actions should be performed in real time so that the customer is confident in the security of their devices and does not feel the need to further contact the operator.

Service Activation

The critical setting for activating IMS services is the address of the Proxy Call Session Control Function or P-CSCF. The P-CSCF is used as the anchor point for establishing IMS sessions.

The P-CSCF should be set on a per-network basis; in a roaming scenario, a local P-CSCF is optimal, enabling the traffic to be managed as locally to the customer as possible, and providing as optimal an experience as possible.

There is a number of different ways to set the P-CSCF value in the device:

- Store the P-CSCF address in the iSIM card
- Use a DHCP procedure to determine the P-CSCF address
- In LTE, download the P-CSCF in the PDN Connectivity Request or Bearer Resource Allocation Request
- When on GPRS, download the P-CSCF address as part of the PDP-Context establishment
- Insert the P-CSCF address in the device as part of device management activity

A Greenfield deployment, with no legacy phones or legacy SIM cards, is well suited to using the iSIM for P-CSCF determination. The challenge is that many operators, particularly those with existing GSM and UMTS technologies, will find it logistically challenging to replace their SIM cards at service launch. Additionally, services that are initially rolled out using an aftermarket application will not have access to the iSIM and will not be able to read the P-CSCF.
The mechanisms for retrieving the P-CSCF address from the network include a range of different techniques, depending on the deployed equipment. It is possible, for example, to use DHCP as part of PDP context establishment or as part of an LTE bearer establishment. Both the device and network must both support the mechanism used. However, networks and devices are evolving at different rates and come from different vendors, so in some cases the GPRS network may support a particular mechanism, but when the customer moves to LTE, that network may not support it. This is very complex to manage, particularly when dealing with roaming scenarios, for example when the target network may not even have considered IMS and may be actively competing to stop the device using IMS. Aftermarket IMS applications are an issue also, as the APIs to read the P-CSCF address are not readily available. The most obvious disadvantage to having the network download the P-CSCF is that it must be standardized to achieve this. This is unlikely to be the case in locally connected Wi-Fi networks, which would deny access to the IMS service over Wi-Fi.

The ability to remotely insert the P-CSCF into the device or application overcomes the disadvantages of having to access the P-CSCF via iSIM or network download. Additionally, it is possible to remotely insert multiple P-CSCF values so that the device can decide which to use depending on the network that it finds itself in. Focusing on managing the data for the IMS application in the device facilitates freedom of movement when dealing with complex network and roaming scenarios, enabling faster time to market for IMS services.

As with credential management, using a remote management system to provision the P-CSCF directly into the device avoids all of the concerns of multi-network and multi-roaming scenarios, and enables the fastest route to getting IMS services to market.

**Settings Management**

Although the credentials and P-CSCF address are fundamental to the launch of IMS services, other settings are needed to make IMS services to work effectively. If the operator has enough influence over the supply of devices, these values can be burnt into the device or IMS application. Pre-configuration, however, does have significant logistical challenges and is not well suited to changing environments. Change is a big part of IMS rollouts, particularly during the initial rollout period, when a step-wise approach to deployment is optimal.

Within IMS itself, there are a number of settings that are significant to the smooth running of IMS services, specifically:

- Access Point Names
- PDP context for SIP signaling
- T1, T2 and T4 timer values
- Private user identity
- One or more public user identities
- Voice domain preferences
- SMS over IP usage
- Keep alive
- Mobility management preferences
- Best-effort voice and video settings

In certain cases, some of these values may be provided by the iSIM, but when no iSIM is available (as in the case of a legacy SIM base) another mechanism is required to set these values in order to activate IMS services effectively. This is particularly significant for VoLTE and SMS over IP.

For RCS services, the problem is increased multi-fold, as the number of settings is much greater (compared to VoLTE) and there is no standard for providing the settings values via an iSIM card. Depending on the subset of RCS services to be launched, the following settings need to be configured on the device, in addition to the IMS settings, including:

- Presence server and settings
- Chat server and settings
- Document Management server and settings
- Capability Management preferences
- File Transfer Content server and settings
- Localization Sharing server and settings
- Address Book Backup server and settings

The sheer number of settings — well over 180 items — means that it is only practical to set these values remotely when they are needed. With the absence of any network or SIM
standard to do this, the only practical way is to use remote management. This facilitates rapid service rollout and handles service change with no impact on the customers.

**Service Management**

IMS services are complex in themselves, especially when compared to legacy SS7 services; they provide more functionality and run over multiple topographies. When IMS services are rolled out with legacy services, possibly as part of step-wise replacement program, the complexity is increased multi-fold. This means that during the rollout process, features may change and services will need tuning. This is important — to gain adoption and to avoid regulatory attention, the customer experience during this process needs to be as smooth as possible.

The types of service data that are pertinent during service rollout are:

- Communication continuity
- Media handling and interaction
- Service accessibility

The data required for these services is dynamic and usually set on a per-customer basis. The data also changes throughout the lifecycle of the device. This makes it well suited for management within the device on behalf of the customer.

**Communication Continuity**

The path from circuit-switched voice to IMS Voice over LTE is not a simple migration. Only in the rare cases of a Greenfield VoLTE deployment will it be possible to go straight to VoLTE for all customers. The reality for most operators is that they will be migrating in a step-wise way as the network and devices migrate over time to IMS, and the 2G/3G spectrum is freed up for LTE. During this migration, customers need to roam and use their services on 2G/3G and 4G without any disturbance of their service levels.

The transfer of calls between 2G/3G and 4G is handled by a “Service Continuity Transfer Number” or STN; when transferring back, a “Service Continuity Transfer URI” is used. These values are fundamental to communication continuity and can only be downloaded if a Core Services application server is present. When this server is not available, remote configuration of these values ensures that “service continuity” is achievable. The 3GPP has provided remote management objects to achieve this.

At the network, the network operator needs control over how their devices behave in terms of which access types are selected for connection continuity. For example, certain access types
being phased out may need to be disallowed (e.g. 2G/GSM), or new access types such as Wi-Fi may be capable of carrying VoLTE traffic and should be preferred. The 3GPP has provided remote management objects to enable the management of these values on the device:

- Restricted access types
- Preferred access types
- Preferred technology for voice, which is either SS7 or IMS
- Transfer into preferred technology as soon as it is available
- Disallow transfer to IMS
- Disallow transfer to SS7
- Disallow transfer for waiting calls
- Disallow transfer of different media types

**Media Handling and Interaction – Media Negotiation**

Within IMS, the Multimedia Telephony Service for IMS (MTSI) is defined for the purpose of increasing multi-operator interoperability for multimedia telephony services, including 2G/3G services as well as different IMS services. Although the session is established in a well-defined IMS network, the actual communication path is between the endpoints — the devices. However, devices are constantly being developed, upgraded and enhanced, so a session negotiation among the endpoints is required in order to negotiate an agreeable set of codecs, quality of service, bandwidth, possible alternative media types and versioning information. This is termed MTSI Network Preferences or MTSINP.

The decision on which preferences the device should use is not only limited by the capabilities of the device, but also by the capabilities of the network and the operator policy. A simple example is video quality, where the customer will always want the highest bandwidth, but may need to be restricted based on their billing profile. Restricting the bandwidth in the network will disrupt the customer experience, but if the device is forced to negotiate a lower bandwidth level at session establishment, the customer will still be able to use the service.

The 3GPP provides a management object to manage the MTSI Network Preferences. Using remote device management, devices can be updated as and when the network need
increases or decreases, or according to the policy and charging rules for individual customers.

**Media Handling and Interaction – Media Adaptation**

Mobile networks, by their very nature, imply variability of network characteristics. Customers may roam between access types or vary their distances between radio towers while engaged in a media session. This provides significant challenges for media handling in IMS. Setting up the MTSI Network Preferences assumes that the network conditions are good, but during the lifetime of a media session on a mobile network, actual conditions can easily change.

To ensure that the best possible experience is provided to the customer, the media session can be adapted to the conditions in real time. Examples of what can be done include:

- Change the bit rate used
- Change the packet rate used
- Change the error resilience, such that more checking is performed over a less reliable network

The 3GPP provides a management object to manage the MTSI Media Adaptation Settings Preferences. Using remote management, it is possible to set and change these values on the device. This can happen relatively infrequently, as and when the network grows and evolves, or in real time, in response to adverse network characteristics such as high congestion.

There are a number of critical services associated with IMS that optimize both the customer experience and network utilization. It is likely that these services will grow and change over time. All of these services need policies, and to work effectively, these policies have to come from the directly from the operator. The only effective way to do this is via standardized remote management.

**Service Accessibility**

With the rollout of IMS, the device will have to make multiple decisions about which services to register for and in what networks. At one level, these decisions can be quite complex, but in many cases the decisions can be simplified by restricting or limiting specific services for particular devices or customers. This is valuable, as it may not be desirable for particular devices and services to access radio and signaling resources if they are not entitled to or if the resource is not fully available.
The benefit to the customer is particularly critical in a roaming scenario, when they will be incurring unanticipated additional charges and possibly experiencing degraded performance for a service that they may not require.

To address this need, the 3GPP has specified a management object to allow a remote management server to activate and deactivate these services within a device.

The services that can be controlled in this way are:

- Call control functions
- Supplementary services, e.g. multi party calling, call waiting, etc.
- Emergency calls
- SMS, via circuit-switched and packet-switched
- LCS, via circuit-switched and packet-switched
- GPRS-based services
- Multicast service
- IMS

This remote management provides the operator with a means of controlling the resources used by a customer in accordance with the policy and charging rules for that customer and in line with the resources available within the network.

Managing access of the devices to the service is a key part of the migration from legacy voice to Voice-over-LTE. To ensure that the customer is not impacted, the services need to be activated and deactivated in line with their availability. The only effective way to do this is via standardized remote management.

**Conclusion**

Modern mobile networks are becoming tremendously complicated. Multi-generational wireless standards combined with all-IP IMS core services, all of which need to be seamlessly interoperable, are providing a number of challenges for mobile operators in the coming years.
The importance of non-3GPP access types such as wireless LAN further complicate things, as operators (and standards bodies) no longer have control over the capabilities of the infrastructure to the extent to which they had previously become accustomed.

Multiple devices per identity are an attractive feature for IMS services but the security issues surrounding its deployment, if not properly addressed, could overwhelm a customer care facility.

Employing iSIM cards can help with the some IMS service deployment issues. However, except for Greenfield deployments, it is not usually practical to upgrade the customer base if alternatives exist, if for no other reason than that the expense is not justifiable. Additionally, the deployment of iSIM for many IMS services only provides a basic set of capabilities and does not provide for RCS settings, VoLTE continuity, media handling or service control, all of which are necessary for deploying the value-add services and capabilities customers are demanding.

The use of remote device management can overcome all these issues. It provides a simple mechanism for activating services, providing service settings, and setting policies and preferences. Based on mature standards, remote device management is a proven mechanism that has many clients available to support the numerous use cases needed for delivering IMS services.

With remote device management, IMS services can be rolled out rapidly, while many of the concerns about deployment topographies and technologies are reduced or eliminated altogether. Huge savings can be achieved from avoiding the deployment of new SIM cards, eliminating the need to integrate cellular and IMS technologies, and removing all the clutter of multiple legacy and roaming scenarios.

The use of remote device management by both operator customer care agents and end-user self-care mechanisms can reduce the security impacts, and therefore the costs, of an IMS rollout, while also providing functional parity with OTT service providers.

Launching new IMS-based services may represent a significant investment to an operator, but there are also risks associated with being left behind as new services take off in the marketplace. Remote device management provides a low-investment alternative for enabling IMS services. In fact, the value of an investment in remote device management increases the more it is used. Once remote device management is employed for credential management, then it is only a short step to settings management, and from there only a small step to communication continuity management and so on. In addition, remote device management can enable you to accelerate the benefit from IMS services. When a device connects to a
server to enable one service, the impact of enabling further services is lessened, as the infrastructure has already been put in place. Thus solving one IMS service rollout issue provides an escalator to addressing multiple IMS service rollout issues from single solution.
CONTACT US

If you would like to receive additional information on our company and our innovative mobility management solutions, please feel free to contact us.

Mformation Software Technologies, LLC
581 Main Street, Suite 640
Woodbridge, NJ 07095
Tel: +1 732 692 6200
Fax: +1 732 549 7542

www.mformation.com

info@mformation.com

© Mformation Software Technologies LLC. All rights reserved