White Paper

The OTA Platform in the World of LTE

Giesecke & Devrient

Creating Confidence.

The OTA Platform in the World of LTE

3GPP LTE (3rd Generation Partnership Project Long Term Evolution) is the de facto standard for the next generation of mobile access networks. Wireless operators can offer high-speed IP networks satisfying the rapidly growing subscriber appetite for e-mail, social networking and news, anywhere, anytime. While the prospect of a high-capacity network designed to deliver data at the lowest cost per bit is appealing, it is critical to leverage a Subscriber Identity Module (SIM) Over-the-Air (OTA) platform to take advantage of both legacy networks as well as the emerging next generation systems.

Table of Contents

Executive Summary

As the wireless industry has evolved, there has been a dramatic shift in how subscribers use their devices. What initially started out as a mobile voice service has progressed beyond the imagination of those original pioneers of mobile telephony. Today's smartphones and other sophisticated handsets are rapidly becoming fully functional Internet terminals that enable access to a variety of payment, information, entertainment, news and social networking services and applications.

In order to support the quickly emerging need for more wireless bandwidth not only from smartphone users but emerging data-only devices, mobile operators need to invest in expanding the capability of their networks. LTE as a fourth generation IP-based mobile access network is probably the best long-term alternative for mobile operators to gain more capacity, while keeping network and maintenance costs in check.

In this growing world of smartphones, data-only devices and wireless Internet usage, there is an enormous potential for expanding the role of both the Universal Integrated Circuit Card (UICC) as an identity token and the OTA platform within the network. With the increased use of mobile banking and near field communication (NFC) services, there is an undeniable need for a secure global mobile identity. This can be provided by UICC-based solutions.

OTA platforms therefore have a key role to play in ensuring mobile network operators get the most out of their LTE investment.

For more information about Giesecke & Devrient, please visit our web site at www.gi-de.com

Introduction

As the wireless industry enters a new era of even more intensive usage of mobile data, the promise of a network that supports more data at higher speeds over a cost effective all IP based network is truly appealing. LTE represents the fourth generation of mobile access networks. While traditional text and voice offerings remain and operators continue to utilize their existing second and third generation networks the continuing growth of smartphone and data modem sales has driven the need for networks to accommodate data traffic at a lower cost per bit.

LTE was specified by the standards body 3GPP as a highly effective radio interface for wireless communication providing data speeds of up to 100 Mbps with the potential for speeds up to 1 Gbps through advanced LTE systems. The architecture in which LTE is presented is referred to as 3GPP EPS (Evolved Packet System). It is an all-IP flat architecture, integrated with 2G and 3G wireless networks, resulting in low costs both for network investments and maintenance.

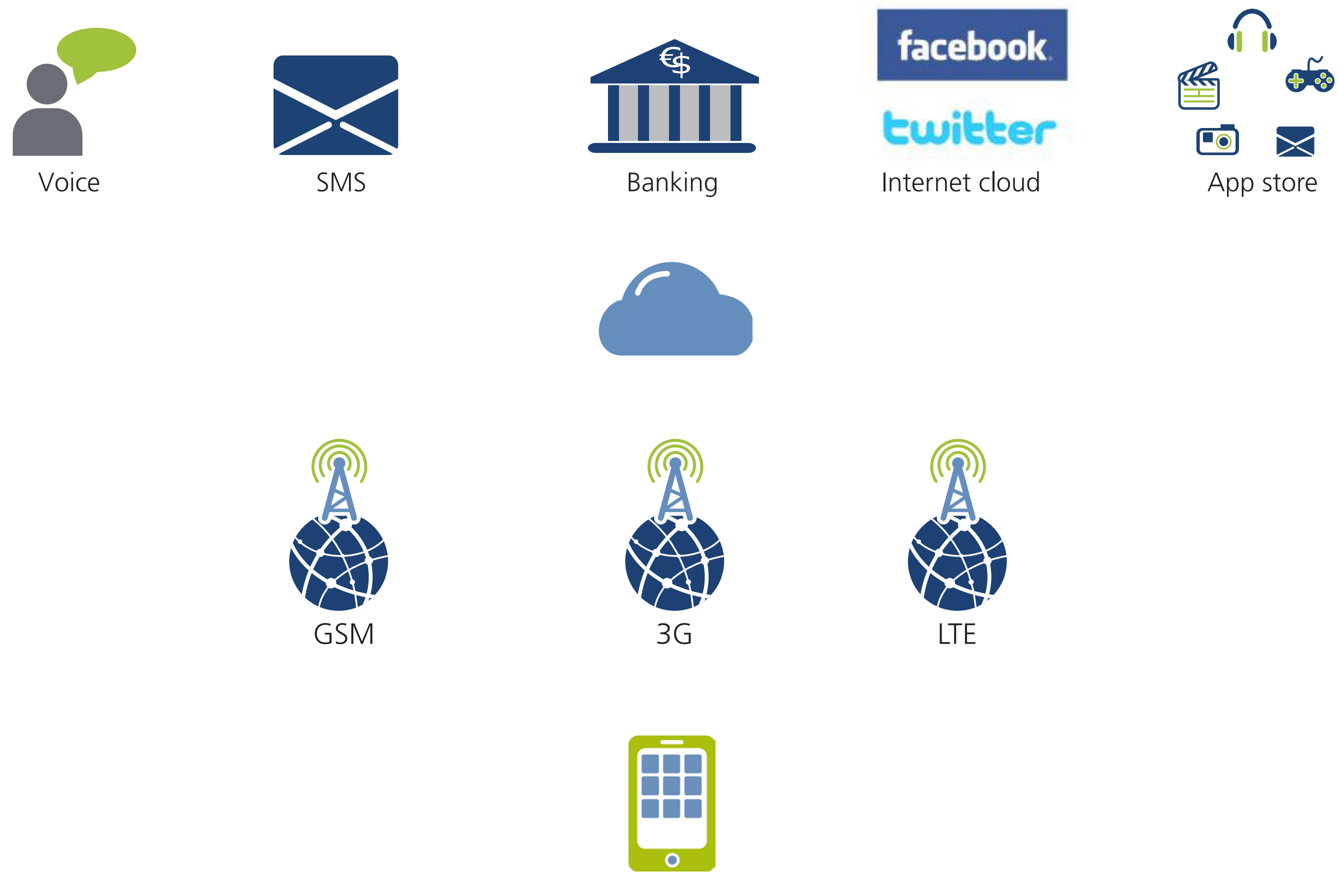
LTE networks will not operate in isolation. Just as its name states, LTE is an evolution of today's mobile networks. The personal nature of the SIM and the ability to manage it over-the-air contributes to ensuring a seamless experience for subscribers regardless of whether they are enjoying the wireless broadband offered by LTE or using 3G / GPRS data networks when outside of LTE coverage areas.

The progression to LTE seems somewhat natural given the continuing development particularly as smartphones are evolving into fully functional Internet terminals and application platforms. As a result, new business models for wireless operators have emerged. Smartphones give full access to the Internet "cloud" and a variety of payment services, infotainment, news, and social networking offerings. This is a change that the entire mobile ecosystem must understand and address although this shift not only impacts devices and mobile networks but also SIM cards and OTA platforms.

New UICCs are available in multiple gigabyte formats allowing a rich array of application software and data to be stored locally for a superior subscriber experience. OTA platforms in the LTE network can rapidly update and maintain the software and data ensuring that all information and applications are up to date.

The OTA platform benefits as well from a fully-fledged mobile IP infrastructure. Large bandwidth, Internet protocols, client-server architecture and UICC-based OTA clients will improve the ability to successfully implement new and old OTA solutions. Benefits include higher delivery capacity, higher delivery success rate, improved scalability and ability to dedicate resources to critical use cases.

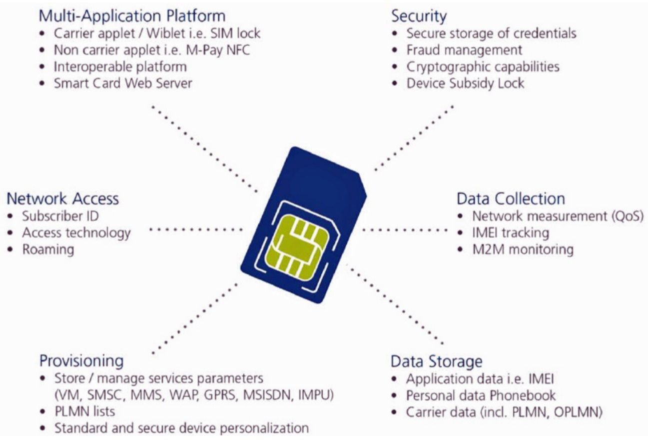
There is clearly a large potential for leveraging the UICC as identity token while the OTA platform enables secure remote management of the subscriber personal information and credentials. In the fusion between mobile services, NFC services and Internet services there is a definite need for a secure global mobile identity. This can be provided by UICC-based solutions.



The role of the UICC and OTA platform

A clear place for the UICC and OTA in the LTE world

The UICC



Today, the most prominent role of the UICC remains network authentication. The UICC comes in a number of different variations as well including the use of a SIM for GSM networks, a USIM for 3G systems, the ISIM for IMS operations and a CSIM for CDMA2000 offerings.

LTE has an evolutionary rather than revolutionary impact on the UICC utilizing the same USIM application that is used in 3G networks and remaining a central network element as the mobile operator's key to the subscriber.

The UICC card is not just about identity and network access, though. It is used for a multitude of other uses including a platform for the mobile operator's applications, using SIM toolkit applications, SmartTrust Wib or Java for example, or using a Smart Card Web Server (SCWS). The card can also be used for data storage for contact information, organizing a roaming priority list, or as a memory resource for music and pictures (mega-SIM). The UICC can also be used to collect data related to a subscriber's Quality of Service (QoS). It has a clear role in the implementation of security applications, such as mobile banking and as a secure element for NFC applications. Many believe NFC applications have the highest potential for revenue generation among all UICC use cases.

As LTE matures so will the UICC. Tomorrow's UICC will have its own IP address and communicate with the handset via a high-speed USB interface. The traditional byte-oriented SIM Toolkit protocol will be replaced with Ethernet interfaces. The architecture for OTA management will change to be client-server based using HTTP. All these improvements will make the UICC a more central and integrated part of the Internet world with industry-standard protocols, using a reliable high-capacity channel. This will in turn drastically improve the possibility of implementing OTA use cases that have previously been limited by the shortcomings of the SMS bearer.

The OTA platform

An IP-integrated UICC provides strong benefits for an operator's OTA platform. An IP-based bearer not only has higher capacity but is more reliable, especially when compared to large (multi-SMS) downloads. An IP bearer increases the data download capacity as well as improves the delivery success rate.

In cases where the UICC acts as a secure element for NFC services, applications and provisioning, IP-based OTA management is well motivated and may even be a prerequisite in many cases due to the amount of data involved in such activities.

Many mobile operators use their OTA platforms for **activation and provisioning**. In this case, provisioning parameters such as MSISDN, voicemail number, roaming priority lists and SMS service center addresses are downloaded over the air when a subscription is activated. Applications based on Java, SmartTrust Wib or SCWS can be downloaded depending on subscriber category. It is even possible that much of the UICC profile is downloaded OTA at activation. OTA downloads at activation are not only used to download parameters that are not known before activation, but are also used to enable the use of a single UICC personalization profile, to keep down logistics costs.

Within an LTE environment IP-integrated UICCs will make it easier for the mobile operator to always keep the UICC updated with compelling applications, meeting the subscriber's specific needs. The OTA platform may use information about the subscriber at activation to select and download the best-fit portfolio of applications to the card, without needing to consider the limitations of the bearer technology. Then, at a later time, the application portfolio can be updated when the subscriber signs up for a certain service, for example NFC, or new updated versions of their applications become available.

SIM Toolkit and SMS-based technologies like Java and SmartTrust Wib are well proven and widely deployed and still serve an important role as a means to deliver applications. However, SCWS technology is evolving and brings with it new advantages. It is better integrated to the mobile handset's browser, which gives a more compelling and accessible user interface for SIM-based applications. It is based on industry standard Internet protocols and high-capacity bearers rather than SIM-specific protocols. This makes it easy to build services with components not only on the SIM, but also fully integrated to Internet services.

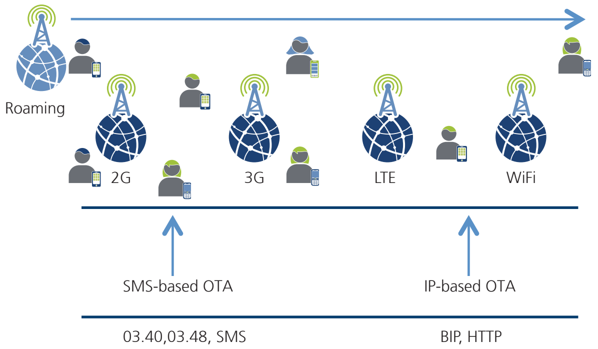
Mass updates benefit from IP based OTA, because of the size and volume of these. If the number of subscribers or the size of the update is large, the amount of SMS messages in the network will start to represent a significant load on the signaling network as well as a potential for a considerable failure rate. An IP-based bearer is better fit for such large operations and uses delivery channels through the network that are designed for data downloads. This approach also provides a better way to manage temporarily unavailable subscribers.

In a client-server architecture for IP-based OTA, because of its configurability on the server side, it is relatively easy to dedicate resources for critical use cases. This allows an operator to more easily maintain QoS levels independently of other uses of the OTA platform. For instance, it is possible to dedicate software and hardware to NFC management or activations, making these independent of mass updates of roaming lists.

Requirements on an OTA platform

How does the OTA platform change

The multi-access-technology network



When a mobile operator builds an LTE network, the normal situation is that this results in multiple parallel access networks. The mobile operator's subscribers are spread between the networks, and they may also move between them, for example when the coverage is lost or roaming outside of their home network.

The specifications for LTE networks are all IP-based, and many operators plan to launch data-only services. Nevertheless, virtually all mobile operators will have an option for voice and SMS on their LTE networks. Mobile operators are making organized efforts to outline and implement alternatives for SMS and voice implementation in LTE. It is safe to say that SMS and voice will be available for foreseeable future within the mobile networks.

For each new access network that is built, there will be higher bandwidth, more data traffic, lower latency times and a lower cost per bit. There will be less SMS traffic and in some cases no SMS service at all. Some smartphones may heavily utilize Wi-Fi networks. One can also imagine a low-cost mobile operator with an all-IP LTE network and a VoIP solution for voice.

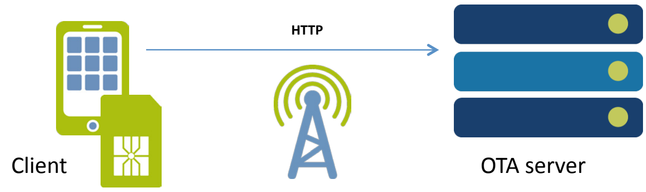
A SIM OTA platform must address these new situations and look beyond just the LTE network.

The traditional system is an ***SMS-based OTA*** in which the OTA messages are carried by SMS with special formats.

An ***IP-based OTA*** system utilizes the data and IP bearers of the mobile network and that approach becomes more and more central as network technology evolves. It uses technologies such as BIP and HTTP to set up and convey OTA messages.

For delivery of OTA messages, SMS and IP services will remain the two main interfaces for an OTA platform. The network will be responsible for delivery of such services. The access technology being used is transparent to the OTA server.

Client-server architecture for IP based OTA



While SMS-based OTA is pushed by the server to the card, a different architecture is used for IP-based OTA. In mobile networks, data connections are traditionally set up from the handset, in a client-server architecture. This is valid not only for the SIM OTA but also for mobile email, FOTA, OMA DM, and many other smartphone applications.

An IP-based OTA solution in a client-server architecture relies on applications or functionality on the UICC to initiate and manage the connection.

There are three cases associated with OTA communication:

The ***pull*** case, for instance a subscriber browsing for new e-mail with a smartphone, the ***push*** case, for example when device settings are sent to the device independent of subscriber activity, and the ***poll*** case, which is often for FOTA solutions, where devices check periodically (e.g. once per month) for new firmware.

When it comes to SIM OTA, the ***activation use case,*** a ***pull*** case, fits well a client-server architecture. In this case, the mobile operator wants to download certain items such as provisioning parameters, roaming priority lists, and/or applications, to the UICC when the subscription is activated. An activation application on the UICC is run when the handset is first switched on, and is responsible for retrieving the OTA message from the OTA platform, using a data connection and secure HTTPS protocol.

There are several advantages to this scenario compared to using an SMS carrier. The first advantage is that the capacity increases. It is possible to download more data to the UICC including exciting new applications, roaming lists and even large parts of the UICC profile in an on-demand personalization use case scenario.

When the HTTP protocol is used, it is possible to reuse commercial solutions such as web servers, routers and DNS. It becomes easier to change the network configuration and parameters, add more capacity using additional Web servers and allocate QoS pipes for certain use cases.

The delivery success rate for activations increases when using IP based OTA. This is because the client on the UICC is only activated when the handset and UICC are available to receive the update. This will drastically reduce the amount of failed transmission attempts compared to sending through the SMSC and using traditional SS7 based OTA.

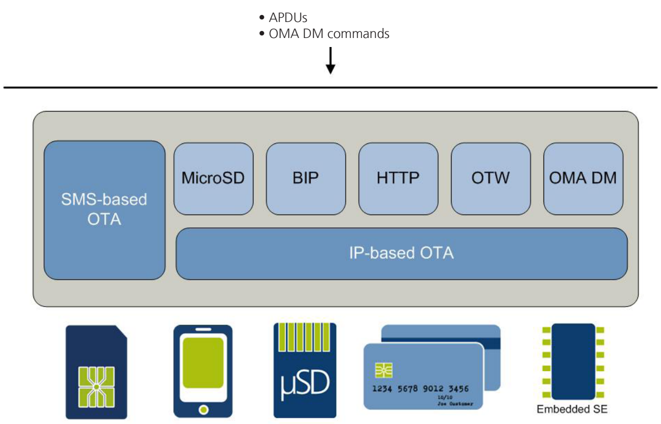
A client-server OTA solution is often a prerequisite for NFC where a UICC is used for a secure element due to the capacity and bandwidth required. This is often a ***push*** case. For payment applications, the size of the application and activation data requires a data connection for OTA operations. However, NFC is different from activations in that the use case is initiated from the server side for immediate update of the UICC. Therefore NFC requires that the OTA session be initiated using a push message from the OTA server, normally with a traditional OTA SMS. As a result, NFC applications require a combination of IP and SMS-based OTA.

Mass updates benefit from a client-server architecture. For large-scale mass updates, especially when the download itself is large, SMS may not be the best bearer alternative, due to the amount of short messages that would be required to be transmitted. The use of an IP-based OTA in a client server scenario provides several advantages, including higher capacity, fewer delivery problems and better delivery success rate. The use of data connections for remote management of SIM cards has been shown in existing networks to multiply the download capacity by at least 40 times. In an LTE network with handsets supporting a USB interface, the capacity improvements will be even more pronounced.

An IP-based OTA allows implementation of a ***poll*** scenario. In this case, an application on the UICC periodically connects to the OTA server and checks for updates. Updates may be performed using a higher capacity delivery channel, naturally distributed and throttled, but without the need for managing retransmissions. Having the application on the UICC allows for deployment of business logic, for example, to only attempt a download when not roaming or when attached to an LTE network.

As an alternative, mass updates can be implemented as in a ***push*** scenario, which will provide an immediate download. The update can either be sent SMS-only, or, if the update is large, by invoking an IP-based OTA UICC client with a single SMS.

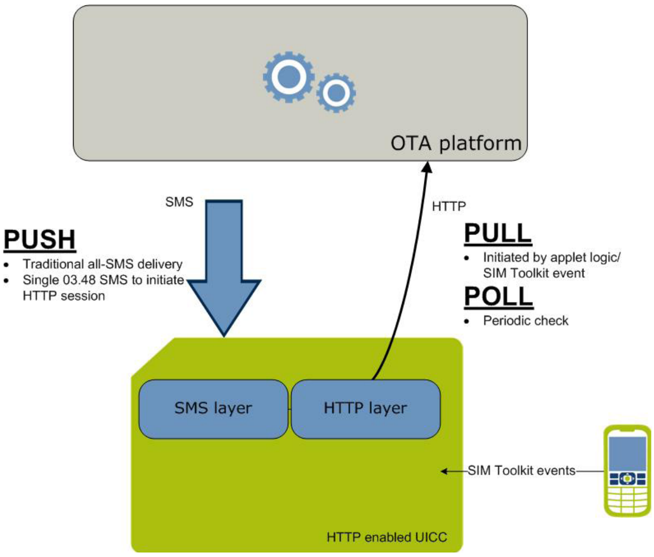
IP-based OTA for multiple Secure Elements



Several of today's OTA solutions require seamless management of multiple secure elements including NFC where there is a mixture of different secure elements. An OTA platform must manage a variety of approaches with the understanding that some subscribers use MicroSD cards for NFC while others use UICCs or embedded secure elements.

A complete OTA platform is also able to manage the device itself using OMA DM for device configuration and management, application download, diagnostics and other use cases.

Push still needed



A complete IP-based OTA solution relies on a combination of delivery approaches with push capability, normally implemented using SMS. However, it still needs to be possible to select a preferred bearer when initiating the download. Some use cases such as activation can be solved with an IP–only platform, but many use cases still need to be initiated with a push message including NFC downloads and different provisioning updates such as MSISDN or IMPU changes that only SMS can perform today. It is almost always necessary to keep a capability to manage non-IP UICC cards, for example legacy cards or UICCs in low price segments.

Always-on using the new USB interface

Initially, IP-based OTA will make use of the traditional ISO interface and the APDU-based SIM Toolkit interface between handset and SIM. This functionality is available in today's handsets. SMS is the main mechanism to push OTA updates to the card, including push initiations of IP-based OTA sessions from the server.

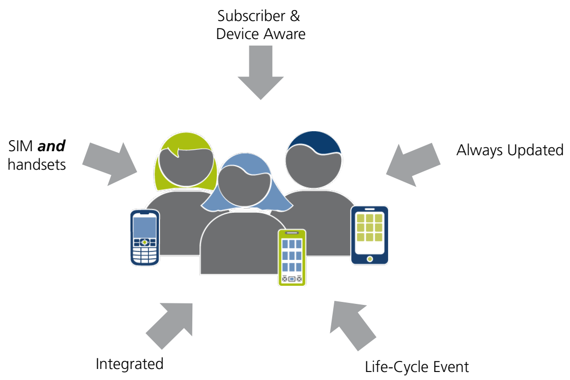
When handsets are deployed and have become widely available that make use of the new, faster ETSI TS 102.600 USB interface between handset and UICC, new possibilities will arise.

Over the USB interface, it is possible to have an IP termination directly on the UICC, and even use the Ethernet and mass storage protocols instead of the limited SIM Toolkit and APDU interfaces. This would make the UICC a fully-fledged Internet node with high-speed connection and Internet protocols, making it possible to seamlessly deploy, for instance, SIP agents, FTP servers, and HTTP servers on the UICC.

With LTE, the ability to perform push messaging to the handset via generic IP access is possible. Push messaging is normally implemented using IMS but this is not an absolute requirement. Different techniques can be used to circumvent IMS, for example standing IP connections or that the server makes direct connection to the mobile data network.

Today's ISO/APDU-based SIM/ME interface is not very well suited to forward such messages to the SIM. Push messaging requires a new application framework in the handset that is able to launch an application on the UICC and forward incoming messages to it. An alternative would be to have a standing connection between UICC and server.

Situation-aware business logic

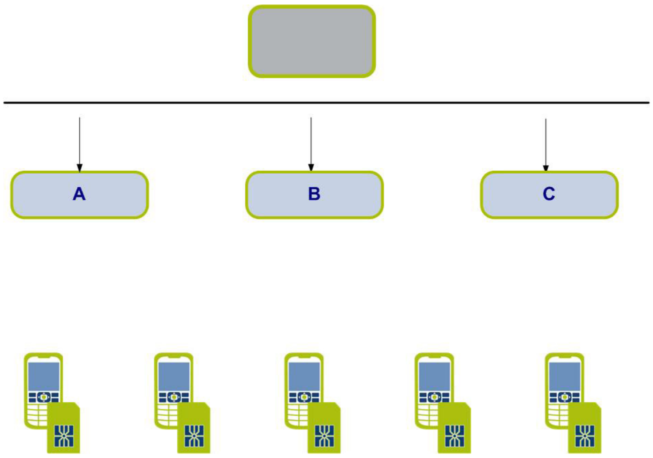


OTA solutions that are integrated in the mobile network operator environment should not be standalone islands of device and SIM management. The business logic of many SIM OTA use cases will depend on a subscriber centric situation. When implementing OTA use cases that are focused on subscriber satisfaction it is critical to be in control of not only of the subscriber's SIM, device and their combined capabilities but also location of the subscriber, and the currently used access network.

The business logic of many use cases in SIM OTA is dependent on this information. As a result, the OTA platform must be able to use this type of information, and provide it to its clients.

SIM-based roaming management for instance depends on the location, access technology (what roaming list to use, how much data is possible to deliver), device capability and device type. Within NFC, what OTA bearer to use and other parameters are dependent on UICC / device capability and the currently used access technology. For subscriber activation: it may not be desirable to download large amounts of data while roaming outside of the home network.

Flexible server configuration



A client-server architecture using HTTP becomes more flexible in terms of the server configuration. Different scalability and redundancy options become easier to implement in line with existing Internet concepts, and it is relatively straightforward to change configurations on the fly.

It is possible to include multiple sites (geographically different or co-located) for the OTA platform. The UICC may for example attempt connection to one alternative. If this fails, it will connect to a second alternative. UICCs may be divided in groups belonging to different sites. With a standard architecture, it is relatively simple to add more sites or change the configuration based on redundancy or horizontal scalability requirements as well as maintenance issues.

It is also possible to allow one single UICC to use multiple OTA platforms, in a more flexible way than SMS. One example of this is when the mobile operator uses a certain partition of the UICC for NFC services that are OTA managed by a third party, but at the same time wants to manage own partitions for traditional OTA. The mobile operator may also want to manage its own NFC services in parallel with independent parties.

Conclusion

LTE will support the continually growing appetite of subscribers for high-speed wireless networks. New feature-rich handsets, devices and data-only modems will require an ever increasing ability to access services through wireless data connections. The best answer to this development is LTE as it allows operators to build and maintain a high-capacity data network in a cost-effective way.

The UICC has a clear role in the IP-centric Internet landscape that is evolving not only in its very fundamental ability to authenticate the subscriber to the network but as a global identity token for authentication in IMS and WiFi networks as well as Internet services such as mobile banking.

An IP-centric network brings new possibilities for the OTA platform. By using the IP bearer for remote management of the UICC, the OTA platform will have the required delivery capacity to implement compelling use cases such as NFC and UICC application management, in addition to extending traditional use cases such as subscriber activation with more features.

The IP channel will bring a better delivery success rate as it is more reliable than SMS. Also, the industry-standard client-server architecture in HTTP, with all its already available and well proven solutions, not only facilitates implementation and maintenance of OTA but also brings new options for scalability and redundancy.

About Giesecke & Devrient

Giesecke & Devrient (G&D) is a leading international technology provider headquartered in Munich, Germany. Founded in 1852, today G&D is a global market leader and pioneering innovator in banknote production and processing, smart card solutions for telecommunications and electronic payment, and security documents and identification systems.

With our innovative technologies, mobile operators can implement new services quickly and efficiently, and gain knowledge about the needs of subscribers. Over 200 mobile network operators rely on us for SIM-, device-, and value added service management as well as dynamic roaming steering. Our customers range in size from new start-ups with fewer than 100,000 subscribers to well-established operators with more than 75 million subscribers. Our technology touches more than 1.5 billion people every day and has been implemented by all major SIM vendors.

We were the first vendor to build and deliver an integrated platform for SIM, device and value added service management. Our unique approach enables our customers to reach each and every subscriber in their network regardless of how they choose to use your services. We turn the diversity of SIMs and devices into your advantage.

This is my potential

It reflects who I want to be, and defines my mobile capabilities and the services open to me.

+

This is my identity

It tells you who I am, and is the key to the mobile services I want to use.

=

This is your opportunity

The capability of my phone coupled with my ability to pay is your potential.

Key Dates in G&D's SIM and Device Management History:

1991 – SIM Card Personalization System

1995 – SIM Point of Sale Personalization

1997 – SIM OTA Management

1999 – SmartTrust Wib™ first released

2002 – 3G SIM Life Cycle Management

2002 – SIM Based Dynamic Roaming Steering

2002 – Terminal Capabilities Program initiated

2003 – Fully Automatic Terminal Configuration

2004 – Ultra-high Capacity OTA (> 50 million subscribers)

2005 – Bearer Independent Protocol (BIP)

2005 – Event Triggered integrated SIM & handset management

2007 – On-Demand Activation of SIMs

2008 – 1 Billionth SmartTrust Wib™ enabled card issued

2008 – SmartTrust Wib™ 2.0 specification released

2009 – Nearly 2 billion Wib™ enabled cards issued

2009 – Provisioning of Single Wire Protocol SIMs

2009 - SmartTrust joins the Giesecke & Devrient Group

Areas of our expertise include:

- Over-the-Air server platforms, pioneered by us in 1997 and serving over 200 mobile network operators globally.
- SIM management of cards from any manufacturer covering the entire SIM lifecycle.
- Intelligent and automatic device management for facilitating the initial handset configuration and continual support and servicing of the device.
- Roaming steering solutions to help boost profitability.
- Dynamic SIM Toolkit (DSTK) including SmartTrust Wib™, the leading smart card based application execution environment that is the de facto industry standard.
- SIM card certification, ensuring correct implementation of Smart Card technologies including SmartTrust Wib™, RFM, and RAM. The certification program is open to all SIM card vendors.
- Comprehensive knowledge about device characteristics from physical properties and available capabilities to SIM and NFC support.

For more information, please visit www.gi-de.com

About the author

Daniel Ericsson

Daniel works as a Product Management Director within Giesecke & Devrient. Since joining the company in 1998, he has worked in numerous roles leading the development and standardization of the smart card in mobile telephony. He has worked as a Solution Architect, architecting and delivering customer solutions based on SmartTrust products to some of the world's largest mobile operators. Before starting at Giesecke & Devrient, Daniel worked in the defense industry with mission critical Air Defense Command & Control systems.

Daniel is a leading innovator and designer within new technology areas. His work has resulted in a number of new products. He was instrumental in the development of the first version of the SmartTrust Wib™ , the world's most widely deployed smart card application execution environment. He was a key player in the development of the patented SmartTrust SmartRoam™ dynamic roaming steering management product. He has been actively participating in ETSI and 3GPP standardisation for the SIM card in mobile telephony since end of 1999.

Outside of the office, Daniel enjoys spending time with his family, skiing, skating and photographing. He has a Masters of Science degree in Engineering Physics from the Uppsala University in Sweden.

Glossary

3GPP
Third Generation Partnership Project, www.3gpp.org

APDU
Application Protocol Data Unit

BIP
Bearer Independent Protocol

CDMA
Carrier Division Multiple Access

CSIM
CDMA Subscriber Identity Module

DM
Device Management

DP
SmartTrust Delivery Platform

EPC
Evolved Packet Core

EPS
Evolved Packet System

ETSI
European Telecommunications Standard Institute

FOTA
Firmware OTA update

FTP
File Transfer Protocol

GPRS
General Packet Radio Service

GSM
Global System for Mobile communications

HTTP
Hypertext Transfer Protocol

HTTPS
Secure Hypertext Transfer Protocol

IMPI
IP Multimedia Private Identity

IMPU
IP Multimedia Public Identity

IMS
IP Multimedia Subsystem

ISIM
IP Multimedia Services Identity Module

LTE
Long Term Evolution

ME
Mobile Equipment "device" "handset"

MSISDN
Mobile Station ISDN Number

NFC
Near Field Communication

OMA DM
Open Mobile Alliance Device Management

OTA
Over-the-Air

QoS
Quality of Service

RAM
Remote Application Management

RFM
Remote File Management (OTA)

SAE
System Architecture Evolution

SCWS
Smart Card Web Server

SD
Secure Digital

SIM
Subscriber Identity Module

SMS
Short Message Service

SMSC
Short Message Service Center

SS7
Signaling System number 7 according to ITU-T Q.700 series

UE
User Equipment (Mobile Equipment + USIM)

UICC
Universal Integrated Circuit Card

UMTS
Universal Mobile Telecommunications System

USB
Universal Serial Bus

USIM
Universal Subscriber Identity Module

Further reading

UICC in LTE: A Guidance from SIM Alliance (http://www.simalliance.org)

(This page intentionally left blank)

Giesecke & Devrient
Server Software and Services

Fredsborgsgatan 24,
Box 47154
SE-100 74 Stockholm
Sweden

Phone: +46 8 685 93 00
Fax: +46 8 685 65 30

For more information about us, please visit us at www.gi-de.com