11th February 2011

UICC in LTE: Guidance from SIMalliance

Table of Contents

The Applications Generation

Spurred on by the exponential growth in demand for mobile data, today's mobile service providers are beginning to make the transition to the all-IP infrastructure offered by **Long Term Evolution (LTE)** – the accepted evolution path for all currently deployed mobile networks, from GSM/UMTS to W-CDMA and CDMA.

Much has already been made of the opportunities of this potential 100 mbps download pipe, and rightly so because while LTE is an **evolution** of Universal Mobile Telecommunications Systems (www.3gpp.org) it marks a **revolution** in the kind of services that mobile operators - and a much wider community of content brands - will be able to offer consumers.

Critically perhaps, LTE is also making us refine the concept of the 'connected device,' moving the emphasis away from simple connection to the mobile web via the smartphone to encompass a host of other devices; from the netbook, the connected car and even the domestic electricity and gas meter.

For the consumer

But the truly exciting element, and where evolution becomes revolution, is what the network can do for the consumer. For the very first time in a decade consumer expectations of what a mobile service can do have been met, and in many cases, exceeded. We are living in a technology-enabled application generation and the possibilities are endless.

But LTE offers so much more than conventional mobile entertainment, mobile video and business applications. By providing a true mobile broadband experience LTE is going to fundamentally change the way we will access and consume content and services on the move.

Near Field Communications (NFC) moves the game on yet further.

Often running in tandem with LTE roll-outs, NFC's ability to allow a mobile device to securely 'talk' to a similarly connected device within four or five centimeters of one another has opened up a host of contactless payment opportunities that have already found their way onto the high street. One wave of the mobile near a reader will soon be fast-tracking us through airport check-in, acting exactly as contactless cards such as the UK's Oyster and Hong Kong's Octopus travel cards. This is great news for the consumer, the transportation brand and is, through a revenue share model, an important incremental revenue stream for the operator.

For the machine

LTE offers the opportunity for Machine to Machine (M2M) communications too. In 2020 there will be 800 million connected machines (GSMA source). The most commonly quoted examples, and with good reason, are close circuit television (CCTV) for private and national security, and healthcare monitoring solutions. The operator will again benefit from a new revenue stream.

For the Operator

LTE is great news for the mobile operator community outside of providing new and enhanced revenue streams by dramatically reducing the cost-per bit through interoperability with all 3GPP and non-3GPP networks. Not only does the technology offer an enhanced radio interface to improve coverage and capacity for end-users, and the scalability of internet architectures, it also provides an opportunity to reduce financial risk and protect infrastructure investment by reusing existing network assets.

But it's the fatter pipe that will be the true winner here for operators. The greater the bandwidth the more services the operator is able to offer its customers. The more services the bigger the incentive to stay on the operator's network. The longer the user stays on the network the more comprehensive a profile the operator can develop on the individual user…and that intelligence provides huge value to the operator and to third party content providers and brands.

And it's a good job too because operators have been feeling the pinch of falling voice revenues for some years now. The commoditization of voice has of course driven down profits while mobile broadband has required a huge investment in the network and returns have yet to be realized.

But perhaps more significant than each and every point made above is the fact that the world has changed. If nothing else the Google phone and Apple's iPhone are important markers here. They are visions of the future where a whole host of so-called 'over the top' players are vying for the loyalty (and the intelligence) of the consumer. LTE gives the operator the opportunity to compete.

More worryingly, it also levels the playing field and, to a very great degree, destroys the barriers to entry these new players have faced, and operators have enjoyed, for over two decades.

It's the belief of the SIMalliance that today's generation of SIM can help to rebuild some of these walls and put the power and control of LTE back in the mobile operator hands.

Before we go into detail, let's take the opportunity to define today's generation of SIM for today's applications generation.

Today's SIM

For more than two decades the Subscriber Identity Module or SIM card has been authenticating secure access to the mobile network. It has also been constantly evolving, growing ever more powerful, with more and more features and functions. Today's generation of SIM, the one that helps operators deliver and differentiate in LTE is the UICC (Universal Integrated Circuit Card).

Anyone who has ever owned a 2G GSM or 3G UMTS mobile phone will be familiar with the SIM card. For the consumer it's the portable chip that contains their phonebook. For the industry of course it has a more critical purpose; not only securely authenticating the subscriber to their chosen network but also offering secure access to voice, basic data such as SMS and a host of operator value added services (VAS) and applications.

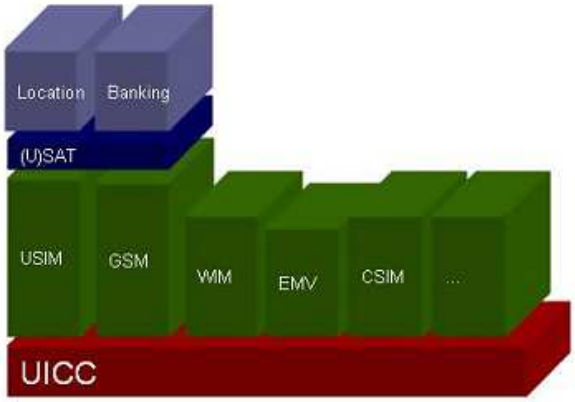
Critically, the SIM is the only network element in the hands of the subscriber and offers mobile operators the ability to deploy new functions and features, and manage permissions, new services and configurations Over-The-Air (OTA).

This central role made the SIM the most logical platform for deploying new value-added applications for mobile network operators and since the turn of the century operators have been using the SIM toolkit to do just that – adding new features such as the Smart Card Web Server (**SCWS**), USB IC, IP support and greater memory along the way.

With over 18 billion cards shipped since its inception, including more than 3 billion in 2009 alone, the SIM card is the most widely distributed application platform in the world.

With the introduction of 3G the SIM changed. Previously a single application smart card designed to work in GSM networks, today we have the UICC, an IP-connected cryptographic multi-application platform, containing amongst other applications:

- USIM (Universal Subscriber Identity Module); the network access application for 3G/UMTS
- ISIM (IP-multimedia subsystem Subscriber Identity Module) for accessing the IMS system
- CSIM (CDMA2000 Subscriber Identity Module), the network access application for CDMA2000



With the deployment of always-on LTE networks, the UICC is transformed into an IP-connected multi-application platform, allowing consumers to securely access a host of IP- and cloud-based services and applications - from banking through to presence-based instant messaging. But more than this, with storage now in excess of 2 GB, the card is also a secure applications store for a host of services including roaming and secure web browsing. These applications benefits from the inherent security of the UICC as well as its portability and interoperability…meaning write-once application become a reality for the first time in the mobile world.

Like the conventional SIM card before, the UICC is the only operator-owned part of the network in the hands of the subscriber, and as such is an incredibly valuable tool for seamlessly distributing new services and applications Over-The-Air (OTA). This allows operators to, for example, update their roaming agreements remotely with no visible impact for the end-user, and facilitate device personalization or activation in CDMA networks.

Remote File Management (RFM) is an enhancement of the over-the-air capabilities of the SIM card. It allows for content management (remove, add, update) within the UICC in a standardized and secure way.

Remote Application Management (RAM) also provides the capability to manage complete applications in a similarly standardized and secure manner to ensure the operator's UICC estate is fully up-to-date and able to respond to changing consumer tastes and demand. Utilizing the Bearer Independent Protocol (BIP) and LTE's high bandwidth provides a fast and efficient way to offer new services including dynamic application management, phonebook synchronization and preferred roaming solutions.

.

Similarly, its portability and interoperability with multiple mobile devices allows the provision of network specific services and customization irrespective of end-user device and that can increase operator value to the subscriber and encourage greater loyalty.

In addition to a standardized removable card offering the very highest levels of security and portability, the UICC underpins an open and distributed model with the subscription on one side and the handset on the other. This protects the operator from becoming the bit-pipe by using the card as a network end-point rather than the mobile device - a point that could become more significant over the next few years as handset brands consider turning this model on its head.

LTE + UICC = Security, Identity, Mobility

As we have already touched on in the paper, if the operator community is to minimize the risks and maximize the potential of LTE, then it must do so alongside the UICC - but not any UICC.

The UICC is a mandatory element in LTE as specified by 3GPP. However SIMalliance is recommending operators to adopt a UICC integrating specific features (See SIMalliance UICC Profile for LTE) to maximize their benefits in LTE migration.

MOBILITY: Intelligent Network Services

Global authentication and intelligent roaming in Radio Access Networks (RAN)

The delivery of intelligent network services is one of the central tenants of the UICC / LTE proposition. The key element of this is, of course, secure access.

Featuring a multi-application and authentication structure, the UICC in the LTE environment offers strong authentication to the different radio access network technologies from GSM and CDMA, through UMTS to WiFi and LTE via different applications.

This is critical to ensure the mobile operator is protected against the threats of the IP world, while the user can be assured of seamless connectivity across different networks. While there's a temptation to look forward, backwards compatibility is a must in today's diverse world where service delivery across legacy networks remains important to operator strategies to maximize previous investments.

Building on authentication and access, the ability to intelligently switch between networks is critical, for both operator and consumer. For the operator it allows intelligent traffic management and prioritization; the ability to offload video traffic onto other networks such as a WIFI hotspot for example thanks to advanced roaming control. Such flexibility allows capacity issues to be managed more effectively while reducing cost and assuring the highest quality of experience for the end consumer.

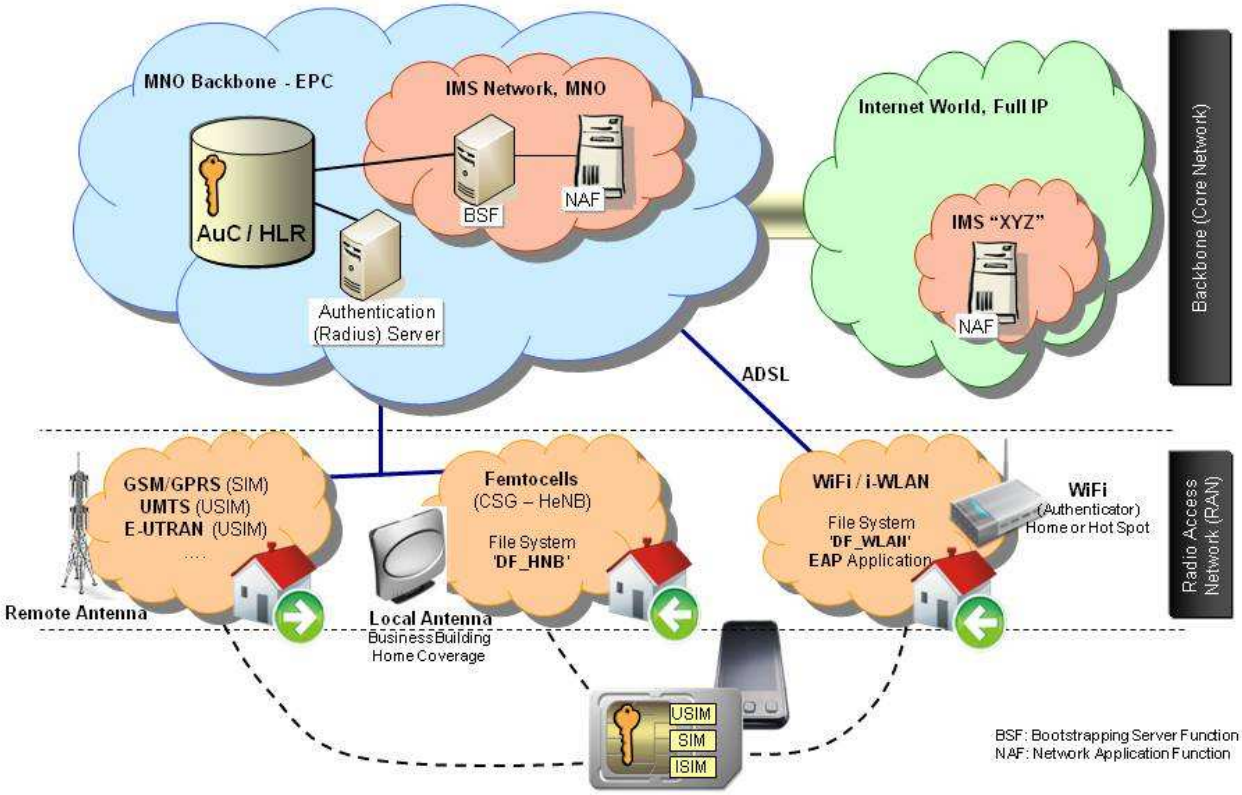
The UICC can also open a channel to download services to the card and 'intelligently choose' which network technology to use.

Authentication to the IP Multimedia System (IMS)

Immune to viruses and malware, the operator network has never been under permanent threat of malicious attack. By contrast, the number of attacks in the online world is huge.

This is where the Universal Integrated Circuit Card (UICC), integrating ISIM features for authentication to IMS, comes into play. This is a critical point because the flexibility of the Internet world brings with it security threats never seen before in the mobile environment.

IMS is the key to a converged wireless and fixed network world. Subscribers can use the same services across devices (mobile phones, PCs, office or home networks) and through a number of different channels (WiFi, DSL, LAN, 3G, Femtocell, etc). This is significant as subscribers have the potential to associate multiple devices to the same account, increasing the potential for a multiple penetration rates within an operator's existing subscriber base.

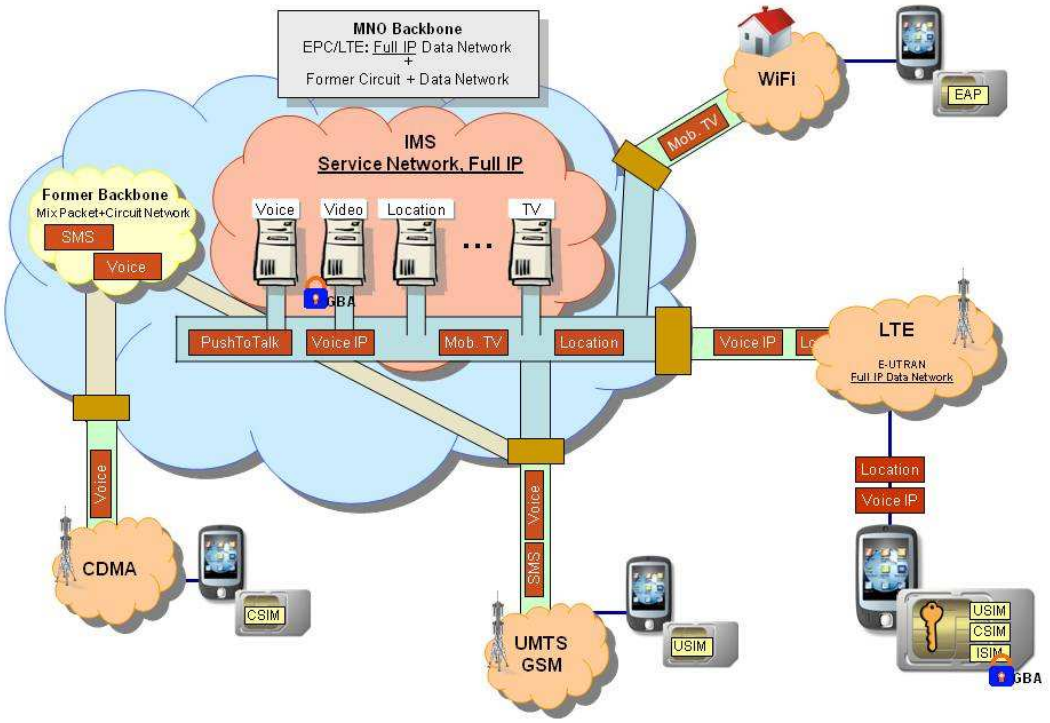


SECURITY: Secure Value Added Services

Access and secure exchange of data for value-added services

The ISIM offers a level of secure access similar to a desktop VPN connection, giving both user and service provider a secure connection unprecedented in consumer mobile communications. This VPN-style connection is achieved by opening a secure IP tunnel that doesn't endanger the MNO's core network.

This secure 'access tunnel' ensures users are securely authenticated to a defined series of services held on operator servers (Voice, SMS, Video etc.). Users could potentially sign up for embedded services and applications that require high levels of security and lightning-fast access.



Adding a Generic Bootstrapping Architecture (GBA) to ISIM makes the tunneling process for application execution more robust than with ISIM only, as well as being easier to deploy and manage. Similar to the mechanism used in Mobile TV to secure broadcast, the operator has the possibility to re-issue keys on demand via GBA encryption.

Using the ISIM in IMS is key for operators to offer a whole set of value added services where security is key ie. video, IM, presence, payment etc., while retaining revenue levels from traditional services like voice and SMS.

Standard & secure web interface for rich NFC services

Near Field Communications (NFC) moves the game on yet further. By integrating NFC and Smart Card Web Server (SCWS) technologies in the UICC, the operator is able to offer its subscriber a seamless experience between the virtual and real worlds.

NFC technology transforms the mobile phone into a universal and secure remote control to access multiple localized and contextualized services. Without doubt, NFC will revolutionize the way we interact with our environment. And with LTE migration and NFC roll-outs coinciding in many markets, it makes business sense to examine the possibilities of the technologies together!

The Smart Card Web Server technology allows the instant display of web look & feel, secure and standard NFC value-added services. It provides enhanced security between the local web site (located in the UICC) and the device, and critical network offloading made necessary by the greater bandwidth and corresponding increase in rich multimedia delivery we'll see over LTE.

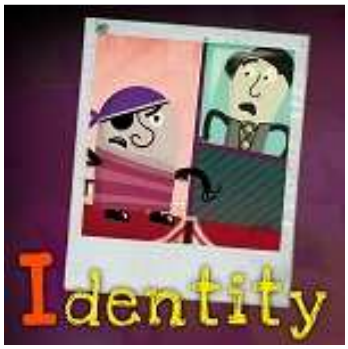
The secure standardized web interface delivered by the SCWS is especially important in NFC for operators as web technologies not only reduce the costs of cross-domain development across mobile, tablets, desktops, cars and consumer electronics - from toys to TVs, but also facilitate customer services' work having to deal with all the NFC services across all these different devices.

Secure and live management of services

OTA management has been optimized by combining TCP/IP reliability with pull mode from the UICC; allowing the card to be updated and provisioned, and new features added. The card is able to request the device to open a channel specifying the quality of services needed.

End user usage & quality experience monitoring: mobile marketing enabler

Finally, in the same way that loyalty cards provide supermarkets with important information on each shopper's purchasing choices, UICC over LTE could potentially return feedback to MNOs and service providers on usage. Naturally, the fine line between privacy and fair use of user data needs to be established, but it heralds exciting possibilities for further improving the service to end users.



IDENTITY: the SIM as a true secure Internet innovation platform

Identity management and Identity Provider services

With the addition of IP connectivity, the value of the UICC card now can be directly brought to the online world. In this way, operators can position themselves as identity providers, protecting users against identity fraud. There is also the potential to create new business models by offering third party access to an ISIM in the UICC which would allow that provider to build and deliver its own identity service.

Mobile wallet and cloud services

This identity provider role enabled by the UICC allows the operator to offer a whole set of new value-added services such as mobile wallet, ID, payment, health or any one of a host of online services where security either converges on the mobile - or in the cloud (such as online storage, software/ widget downloads or rich communication suites including social networks).

At a point in time where identity theft is part of every security discussion, it is logical that the mobile device will become the key for online authentication – for the simple reason that while consumers may leave their homes without their wallets or identity cards, they rarely forget their mobile phone!

And with NFC on the horizon it could be that identification rather than payment brings the technology into the mass market.

Using the mobile device for identification would be less expensive than any other type of card or token. There wouldn't be any issuance cost because most people already have a mobile device, and users would simply download the application onto the UICC and use it from there.

Operators have a great opportunity here to position themselves in this domain providing they can agree on the right business model with governments and other ecosystem partners.

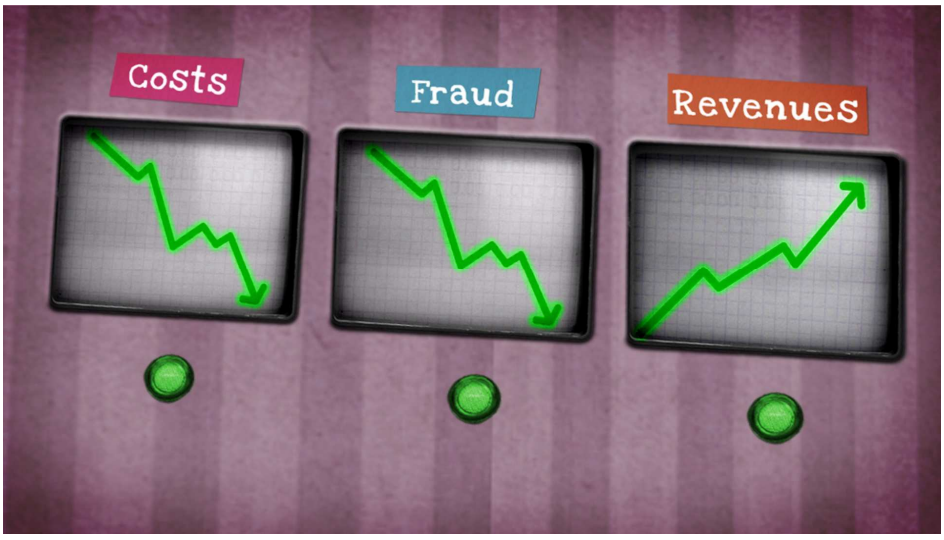
SIMalliance's Position

The SIMalliance believes, without a doubt, that LTE heralds the next major step in the development and delivery of a host of rich new multimedia services and applications. But more than this, by delivering a true broadband experience on the mobile, and through the integration of NFC, LTE will fundamentally change the way consumers communicate and transact, offering a seamless connection between the virtual and contextual worlds for the very first time.

SIMalliance believes LTE offers opportunities for mobile operators to retain control of their subscribers (and revenues) against stiff opposition from over-the-top players, and to extend their influence outside of conventional mobile boundaries and into the wider online world.

But LTE is also a disruptive force; it will enable greater competition from non-mobile players and increase the commoditization of voice services. Also, by opening the core network to a potentially unsecure IP layer, security will become an increasing issue.

The UICC is a mandatory element in LTE as specified by 3GPP. However SIMalliance is recommending operators to adopt a UICC integrating specific features (See SIMalliance UICC Profile for LTE) to reduce the disruptive impact of LTE and to support the creation of a secure, open and interoperable environment where mobile services, and mobile operator revenues, thrive.



SIMalliance: Security, Identity, Mobility

SIMalliance is (the non-profit trade association) dedicated to supporting the creation, deployment and management of secure mobile services across the globe. Working in partnership with members and the wider mobile community,
SIMalliance anticipates and addresses the security, identity and mobility challenges of an increasingly converged internet. Through its working groups the alliance seeks to offer the blueprint to create a secure, open and interoperable environment where mobile services thrive.

Each year SIMalliance brings the mobile industry together at its SIMposium series of events; showcasing new technologies, discussing emerging models and tackling key market challenges and also hosts the annual SIMagine competition, recognising the very best in secure mobile application and service creation.

Its membership is responsible for delivering the most widely distributed application platform in the world (SIM/USIM).

SIMalliance members are Datang, Eastcompeace, Gemalto, Giesecke & Devrient, Incard, Inkript, Kebt, Oberthur Technologies, Prism, Morpho, Valid, Watchdata & Wuhan Tianyu.

SIMalliance Strategic Partners are Comprion, FCI and Movenda.