

# Telecommunications

||||| The role of the UICC in Long Term Evolution  
all IP networks



FINANCIAL SERVICES & RETAIL

ENTERPRISE

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR

**TELECOMMUNICATIONS > PRODUCT**

TRANSPORT

# Telecommunications

## The role of the UICC in Long Term Evolution all IP networks

**Authors:**  
**Jean-Louis Carrara,**  
Marketing Director  
**Hervé Ganem,**  
Software Architect  
**Jean-François Rubon,**  
Director of Technology Development  
**Jacques Seif, Technical Marketing,**  
Standardization and Technology

January 2009

## Table of Contents

Executive Summary .....	5
The value the UICC can bring to Long Term Evolution (LTE) .....	5
Long Term Evolution – The role of UICC technology .....	6
A refresher course on the UICC - Enabling the magic .....	6
The value of the UICC in LTE networks .....	7
Application Delivery (operator and end-user facing) .....	7
Network Access Applications .....	9
A wider mobile eco-system .....	9
Addressing non-subsidized devices .....	9
Not to mention security .....	9
Personalization .....	10
A secure storage device .....	10
Business opportunities .....	10
Wireless PKI transactions .....	11
Different Form Factors .....	12
A vision of the future .....	12
Conclusion .....	13
About Gemalto .....	13

## Executive Summary

### The value the UICC can bring to Long Term Evolution (LTE)

The UICC (Universal Integrated Circuit Card) is the smart card used in mobile terminals for GSM and UMTS/3G networks. It authenticates the subscriber to the network while ensuring the integrity and security of their personal data. It also stores applications for both operator and end-user use for the correct deployment of mobile services. Now in the pipeline for LTE, the UICC brings a whole host of fundamental features, tried and tested within GSM and now perfected for LTE. This paper will talk about its role as a secure device for authentication and the storage of personal data, as well as the value it can bring in terms of revenue generation and new service deployment.

A few key points:

- Ready to deploy - LTE networks do not need a specific LTE USIM (Universal Subscriber Identity Module) function.
- Fully integrated into IP networks - The UICC, as per existing standards, has become an IP connected processor with its own IP layers and IP stack (USB IC). This means that it is ready for deployment in all IP networks such as LTE.
- Works with all 3G handsets - This means a wider park of cell phones to propose to your customer base.
- Compliant with all distribution models - The UICC's portability encourages the widest possible distribution model for the wireless business – UICC built in, subsidized handsets, or even generic, non subsidized phones.
- Makes personalization easy - Carriers can use the UICC for plug and play personalization of the handset, both pre and post issuance on the field, offering a more tailored service for their subscribers.
- Multi-device and convergence ready - The UICC comes in different form factors to suit your business model – standard USIM card, USB dongle, SIM in 3G laptops and Smart modem.
- Secure storage of personal content - The UICC now stores up to 2GB of personal content for your user's pleasure

All of the above has made the inclusion of the UICC mandatory for accessing Long Term Evolution core networks. So what does this mean for your business?

## Long Term Evolution - The role of UICC technology

3GPP LTE refers to the evolution of UMTS networks. This evolution towards a faster communications standard brings with it the promise of greater connectivity and a transfer speed equal to that expected from current internet connections. In this way, operators will be able to offer highly sophisticated quadruple play services, such as Internet access, Mobile TV, and VoIP, to name a few.

It is estimated that by 2012, LTE will dominate mobile broadband for 2 main reasons: It is backwards compatible with GPRS and UMTS and offers an enhanced data rate of 100Mbit/sec (compared to 70Mbit/Sec with WIMAX).

However speed is not the only advantage brought by LTE. The UICC brings to LTE networks a higher level of security and better equips carriers to cope with the security threats present in all digital networks.

LTE, the next generation mobile broadband network from the 3GPP, brings the promise of hyper-connectivity and true mobility wherever you are, whatever the device. With this comes the expectation of new services such as identity management, payment, content protection etc. So the real question of this paper is – what value can the UICC bring to LTE operators?

### A refresher course on the UICC - Enabling the magic



Since the beginning of GSM in the 1990's, the UICC, a 32bit processor housing the USIM (Universal Subscriber Identity Module) application, has had the fundamental role of **authenticating the subscriber** onto the wireless network. Delivered in billions of units worldwide, the UICC has proven its reliability and was instrumental in the success of GSM. This function is now extended to LTE networks, which brings with it the disassociation of the subscription from the mobile device.

Over time, the UICC's role has evolved and it has become known as the only operator owned part of the network residing in the hands of each subscriber.

Its inherent **portability** brings many advantages and encourages the **widest range of distribution models** – Signature versus vanilla devices, USIM built in, subsidized handsets, or even generic, non subsidized phones.

Regardless of the distribution model, all these subscriptions rely on the UICC to provide access to the network, to ensure continuity of all services and to bring operator services through device customization.

Over the Air platforms turned USIMs into **dynamic management platforms**, supporting remote updates to cards already in the field, **brand management** and the delivery of new services. OTA services are now used to update any area of the memory profile of the UICC for such activities as downloading information related to the latest roaming agreements, voice mail, and more generally, all updates to the subscriber profile.

Fast forward to 2008 and half of the USIM cards carry specific **operator service portals**. With these service portals, users access operator applications integrated to offer self care, billing information, prepaid reload, mobile banking, remittance, and information on demand, in as little as one click. Each operator designs its own portal, makes it available in every phone on its market with the USAT interface, and updates the services regularly according to the reported usage with the OTA.<sup>1</sup>

In order to make browsing for services easier and provide a multimedia service presentation, the Smart Card Web Server (SCWS) is an application execution environment to develop interoperable and portable operator applications that run on the USIM. Recently standardized by OMA (Open Mobile Alliance), the

---

<sup>1</sup> For more information on operator service portals from the USIM, visit our site on [mobile portal management](#)

SCWS leverages the handset browser to run offline applications as the cards host a real web server. The SCWS communicates with the handset using the USIM IP stack.<sup>2</sup>

The new generation of USIM cards can now store up to **2GB** of personal content and offer the requisite communication speeds to make the **end-user mobile experience richer**, personalized and adapted to user preferences.

With **USB IC technology** as the high speed protocol, the UICC has gained a high bandwidth communication channel between the handset and the network making it suitable to securely store large quantities of data, with the possibility of integrating flash memory on board.



The higher data bandwidth available means faster communication between the UICC and the handset. In turn this means that the card can secure access to the internet, while being an **enabler for rich, convergent services**.

### The value of the UICC in LTE networks

The UICC is the trusted operator anchor in the user domain in LTE/SAE. The SAE flat and open architecture brings high-security risks that must be mitigated by deploying highly secure and tamper proof devices in the user domain. All LTE/SAE services are based on the high level of security of the UICC card. Furthermore, it's a solution platform that secures applications residing not only in the handset but in any device used in an open access network.<sup>3</sup>

The standardized, removable cards bring many benefits to the carrier and the subscriber alike. Among the most important are **portability, security, trust**, and a **clear liability separation model**. The separation of the USIM card with the subscription on one side and the handset on the other creates an open distribution model that is both efficient and beneficial to end-users, operators and equipment vendors. All mobile services rely on the high level of security of the USIM card which offers the highest guarantee of security for businesses and mobile users alike. Last but not least, convenience and ease-of-use are crucial to customer satisfaction and for 95% of the mobile users worldwide, the USIM is part of their way of life.

### Application Delivery (operator and end-user facing)

For today's networks as well as tomorrows, carriers can rely on the UICC to protect themselves from becoming simple bit pipes. Each carrier can use the card as a network end point independently from the mobile phone.

The UICC is the port of call within each mobile device where mobile carriers can store the applications that bring their services to fruition, such as for roaming, branding, device tracking and browsers to name a few. Storing such applications in the UICC means that they benefit from the UICCs' security credentials, thus offering revenue protection for the operator. Being removable, it is easy to transfer them in the case of device renewal with no need to rewrite the application.

The UICC is the only operator-owned item that resides in the hands of the end-user. It connects into the operator system via Over The Air technology which is synonymous with secure remote management. To take roaming as an example, the combination of UICC and OTA technology means that carriers can update their roaming agreements, remotely, and with no visible impact for the end-user.

In a world where 3G connectivity is directly embedded into each user's laptop, the battle is on for ownership of services and the connection. A **USIM in a "mobile broadband" notebook**<sup>4</sup> solution means

<sup>2</sup> More on SCWS? Visit our [UpTeg site](#) for all multimedia related topics.

<sup>3</sup> More on the LTE/SAE network? Visit <http://www.3Gamericas.org>

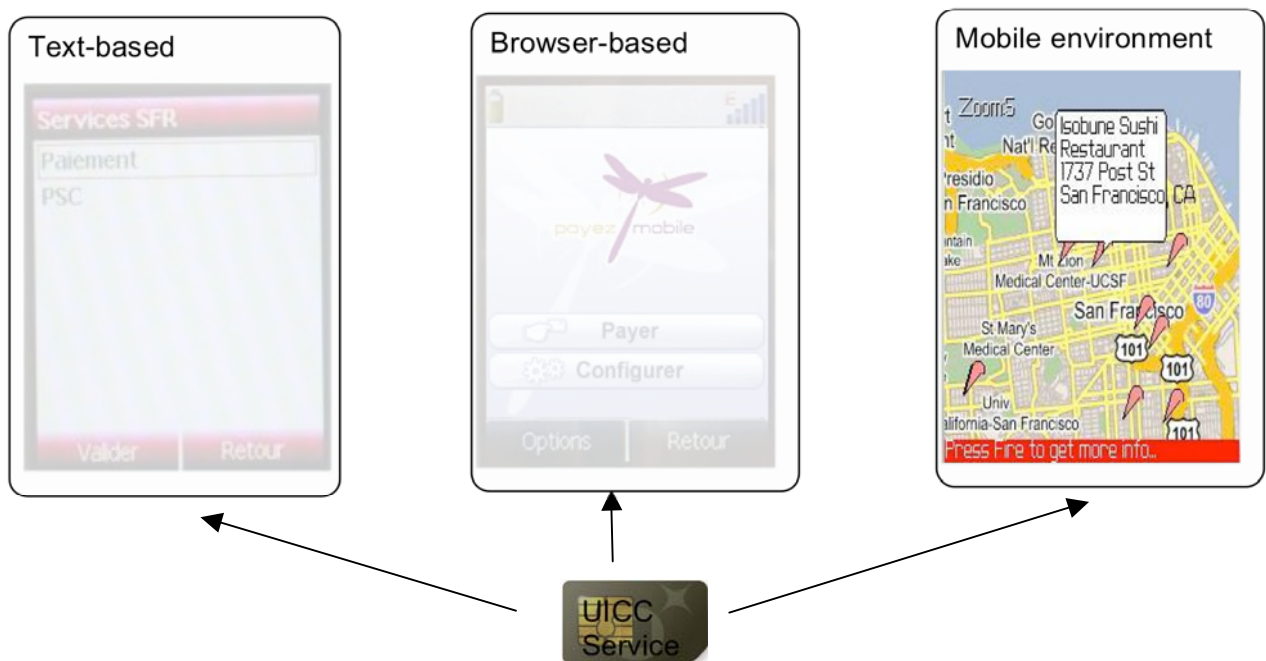
<sup>4</sup> The "[mobile broadband](#)" brand was launched by the GSMA on 30 September 2008.

that the carrier can manage personalization of the device (branding, service access, etc) post issuance. Over The Internet technology will also play a crucial role in the life cycle management of PC and UMPC applications.

### Examples of the types of applications that can be stored in the UICC

High level applications	<p>High-level applications based on standard APIs Java Card applets Example Device tracking</p>
Operator Service Portal	<p>Based on service engines using standard APIs S@T and Smart Card Web Server</p>
OS with add-	<p>Low-level applications Network access applications: USIM, CSIM (CDMA SIM), ISIM (IP Multimedia Services Identity Module) OS Add-ons loaded at personalization Cryptographic applications</p>
	<p>Requiring chips with optional features NFC applications USB-IC and mass storage</p>

As mentioned above, the UICC can store browsers which make the navigation of end-user centric applications easy and intuitive. This brings the end-user experience more in line with the use of the Internet while at the same time rendering the applications according to the capabilities of the mobile device.



## Network Access Applications

Co-existing on the same UICC platform with the USIM application is the ISIM - IP Multimedia Services Identity Module – which provides access to the IMS (IP Multimedia Subsystem) via any IP access network.

The ISIM enables each subscription to have multiple public identities. It enhances interoperability by reducing the options for implementation as there is no need to accommodate legacy USIM or CSIM (CDMA Subscriber Identity Module) applications. In addition, the ISIM facilitates the provisioning of important parameters across all mobile terminals.<sup>5</sup>

It works by providing a set of IMS security data and functions for IMS access: mutual authentication and key agreement, provisioning and GBA for IMS-based services.

## A wider mobile eco-system

Creating a more dynamic market

As part of the wider mobile eco-system, the UICC offers wireless carriers certain advantages. More handsets support SIM technology than don't, so its integration into LTE networks opens up the handset base offering more choice for subscribers and keeping the price down. Within the GSM market place, statistics show that handset renewal is on a two-yearly basis, compared with CDMA, which is every four years. Good news for handset manufacturers and wireless carriers as it makes for a more dynamic market. In addition, storing all user, network and service configuration data in the UICC **simplifies handset upgrades and reduces inventory costs.**

## Addressing non-subsidized devices

The world over, mobile carriers have to address the issue of mobile devices sold directly to the consumer. This means a lack of customization and the improper configuration of mobile handsets for operator services. In some countries this accounts for more than half the devices on the market, for example, in China, Belgium, and for some very large accounts such as Orange Group and Vodafone Group.

To tackle this, many operators have turned to device tracking solutions in order to reduce the costs of customer care and insurance fraud.

Automatic device provisioning services within the UICC make it possible to offer post-issuance customization and remote management of the device settings, while also sending service messages to the unsubsidized devices. They can also customize any device with a local service portal, which ties into the device tracking tool to provide device specific features.



## Not to mention security

The very core of the UICC is the notion of security. It checks that the right person has access to the network in the conditions agreed with the operator. It **securely stores personal information** and is instrumental in the **personalization** of mobile communications. Each subscription is unique and therefore each card is different.

The UICC stores algorithms and certificates that make it extremely tough for an external third party to access your communications. The semi-open environment means that it can house different applications,

<sup>5</sup> More on IMS? Visit [www.3Gamericas.org](http://www.3Gamericas.org) for their [white paper](#)

while offering the level of security necessary in the banking world for financial transactions. Everything you do with your credit card is now possible with your phone, thus opening up the possibilities of **revenue generation** through transaction fees, and **boosting data traffic** on your network.

## Personalization

Secure remote management

“Personalizing” a smart card means making it specific for each carrier’s network and unique for each and every subscriber with the contents and features chosen by that particular carrier. Once the card has been activated, it can also be managed remotely via an OTA (Over the Air) platform, whose functions include remotely updating card profiles and downloading/deleting application applets on the cards.

This also enables the **introduction of new services** during deployment or post-issuance.

The card issuer is also responsible for personalizing the cards using data provided by the wireless carrier, under the utmost **confidentiality**.

## A secure storage device

The extra storage capacity of the UICC brings it into the realm of a connected storage device. Coupled with the high speed USB interface between the card and the handset, carriers can open up mobile services to a host of new potential applications such as mobile TV and user generated content:

User generated content:  
Your digital life follows you

The new generation of multimedia-enabled USIMs offers protected storage of all user related content (emails, pictures, videos, PIMS data) and handset settings for portability. This means that the end-user can carry their whole user environment from one handset to another. Not to

mention personal data protection in case the handset is lost or stolen.

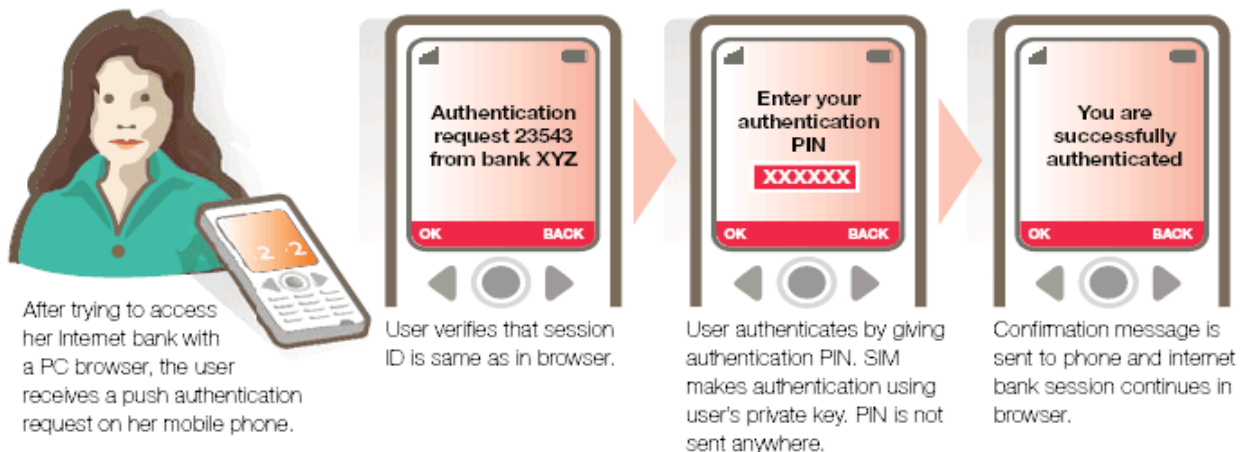
Within LTE networks, the USIM will continue to provide key additional value with roaming revenue enhancement and secure mobile transactions.

## Business opportunities

Wireless carriers are constantly updating their partnerships for roaming agreements in order to optimize [roaming](#) costs and revenues. The USIM combined with an OTA remote management platform means real-time updates with no headache, no re-issuing of the cards and no need to involve the end-user. A real-time, handset independent solution to roaming - What could be better? With LTE, the roaming is enhanced to include various network technologies, including CDMA 1X and EVDO, as well as WLAN systems.

Around the world, the USIM secures transactions within secure international remittance, mobile payment, and mobile banking. As a basis for trusted service infrastructures, the USIM helps operators generate new revenues with the generation and validation of [digital signatures](#) in compliance with global digital signature laws. The latest implementations rely on wireless PKI signing engines in the USIM to secure mobile but also online transactions for banking, investments, corporate, and government applications.

## Wireless PKI transactions



With [Near Field Communications](#), these transactions will also include proximity transactions. The world over, many countries are looking to deploy contactless solutions, convinced by the business case of seamless, fast and secure transactions. For the mobile world this comes in two guises: transport and retail.

In transportation, contactless infrastructures are already deployed in almost every major city. It is a natural move to offer this functionality over the mobile phone.

For retail, the use of contactless cards is growing rapidly. We saw a tremendous success of contactless payment in the US: more than 10 million users one year after the launch of the service, being comfortable with the use of a mobile phone to pay for transport and small transactions.

For this complicated system to work, wireless carriers, retailers, transport providers and banks have to work together. What is required is a central organization that works as a trusted service manager, organizing and housing each application independently and securely. The UICC acts as the ideal storage and management point for each member of the NFC value chain.

These are just some examples of areas where the UICC can add value. The list is not exhaustive and depends on each carrier's marketing strategy. One thing is sure: wherever there is a UICC, there is greater flexibility, security, portability and opportunity.

Within LTE all-IP networks, these applications will be enhanced and others will appear. The UICC is now fully integrated with IP layers and can even benefit from an IP stack. This brings a whole new range of use cases to which the UICC can bring added value:

**Identity management with secure devices:** Since the earliest days of the GSM standard, the UICC has been an omnipresent part of the mobile phone. This made it a key element in creating what has become the **biggest identity management infrastructure** to date, based on its primary focus on **user authentication**. With the addition of IP connectivity, the value of the UICC card now can be directly brought to internet applications, for example, in performing strong back-end user authentication with popular identity management protocols such as OpenID. In this way, carriers can position themselves as identity providers, protecting users against identity fraud— a major point in the battle for **customer retention**.

**Secure Voice over IP:** The UICC can be used to secure VoIP communications by securing the network or IMS access. The VoIP communication then benefits from this secure link. Already for specific secure implementation, the UICC is used to secure VoIP communications end to end, with a close integration to soft phones.

## Different Form Factors

One way of meeting the growing pressure from internet service providers entering the telecom world is to deploy offers which allow end users to access the carrier's own internet services, regardless of device. In this way, the PC becomes a powerful communication tool giving access to wireless services.

The standard form factor of the Universal Integrated Circuit Card has therefore had to evolve to meet this market need. In the first instance, the use of a **USB key** bundled with the UICC and flash memory offers access to any carrier's services from any PC. By inserting it into the PC's USB port, the subscriber gains access to carrier communication applications including Voice over IP and Instant Messaging, as well as the available range of web services, such as music download and on-line storage.

Taking this further, it is also possible to include a **modem** into the USB key which means access from any PC wherever the user and whatever the connection.

If deploying a [Mobile broadcast TV](#) service, the UICC has a strong role to play in the secure storage and administration of the keys and user rights of a Conditional Access System. This is the primary enabler for a TV operator to develop a variety of business models to maximize their revenues i.e. subscription, Pay-Per-View, Pay-Per-Time etc. However, not all devices to which mobile TV could be broadcast require the use of a USIM, for example, portable TV media players (PTMP), personal navigation devices (PND), gaming consoles. In this case, the **Micro SD™** card allows service providers to deploy their service on all portable terminals where the USIM is not present. The Mobile TV micro SD card is also available with high storage capacity to offer users the possibility to transport recorded video content or any other media content.

[Machine2Machine](#): The wireless M2M market represents a huge opportunity for mobile operators. Applications in remote management, industrial data collection, intrusion control and healthcare are expected to account for 10% of operator revenues in 2010. The benefits are substantial: M2M contracts are long-term: machines do not churn, nor ask for expensive voice support, and while the volume of data traffic generated by an individual device may be small, the total number of machines is huge. However, the market is calling for a solution that combines traditional smart card security with an altogether more rugged form factor that responds to the extreme, industrial demands of the M2M environment. It must be simple to deploy, able to reduce spiraling logistical costs and invulnerable to theft, while reinforcing the role of the wireless carrier in the value chain. This is why smart card manufacturers have developed a more **robust, dedicated M2M product range** which comes in the form of an electrical component integrated into the M2M module at the manufacturing stage.

## A vision of the future

Beyond high speed data in mobility situations, LTE will bring another benefit to end users: hyperconnectivity. This means that a large quantity of day to day objects that are currently not connected, or not connectable, will tomorrow be connected in an era known as the *Internet of things*. LTE is likely to be a first step toward this global vision of a world where everything is inter-connected at high speed regardless of the mobility of the individual. Such seamless connectivity will require objects to authenticate themselves to the network, which revises completely the business model for subscriber identity, as new value chains with new actors, customers and suppliers, will emerge. More than ever, the SIM will be a core aspect of this business, extending its expertise to **Consumer Electronic Devices**, such as digital cameras, mp3 players, and digital photo frames, in the first instance. The SIM will have a strong role to play in guaranteeing authentication of the owner of the device to the network.

## Conclusion

For a cellphone user, a UICC brings freedom from being tied into one phone, portability of personal data including contacts, video clips, photos, etc., not to mention the ability to customize the phone screen and services to their heart's delight.

For wireless carriers, the UICC protects them from the bitpipe status with added values beyond the basics of authentication. It is the only carrier-owned device in the hands of the subscriber and as such can be seriously exploited in order to improve the relationship between the two. It plays a major role in optimizing roaming traffic and offers substantial opportunities for greater personalization, new service deployment and brand reinforcement.

The development capabilities are huge: the card itself can now store up to 2GB, which represents a great deal of photos and music clips. The Smart Card Web Server makes it easy to browse for content and services while the USB-IC offers the communications speeds that each user is used to finding at home.

Gemalto is committed to help operators make the most of their trusted UICC identity infrastructure and to innovate together as we create the new generation of secure operator-branded services.

## About Gemalto

Gemalto, the world leader in digital security, helps make people's digital interactions with the digital world secure and easy. Our trusted tokens and state-of-the-art solutions are in the hands of telecom operators all over the world. In migrating to LTE, our customers, current and potential, can count on the stature of a leader committed to their success and to supporting them with new and innovative features that fit each particular market. Gemalto offers technical, marketing and sales support in order to make the move to a USIM-based network as smooth as possible, based on the following points of expertise:

- We work with over 400 mobile network operators worldwide, including almost all of the top 50.
- Leader in personalization services with over 30 personalization bureaus worldwide.
- Remote management and provisioning experience in managing USIMs and downloading accounts/applications with OTA, managing 700 million USIM subscriptions and applications – the world's largest OTA platform
- Experience in advanced telecom solutions – NFC, Mobile TV, Convergence and multimedia
- For NFC services, we are no. 1 market leader in each relevant market - USIM cards, managed OTA platform services, contactless cards for banking and transit and EMV bank cards.

||||| The world leader in digital security

[www.gemalto.com](http://www.gemalto.com)

**gemalto**   
security to be free