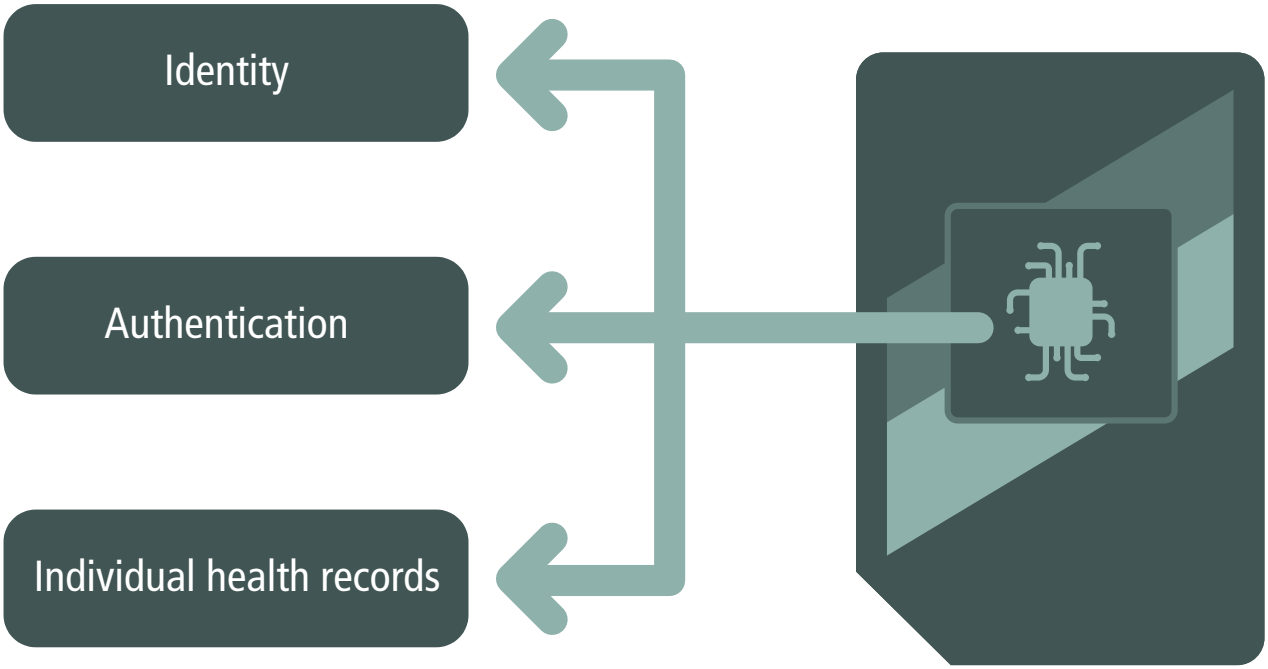
Mobile Health

Concept paper

The SIM: The Key to Better Healthcare?



Executive summary

More than five billion devices around the world are authenticated on mobile networks using an embedded SIM (an application running on a Universal Integrated Circuit Card or UICC), which stores and presents a unique identifier for each customer to their mobile operator.

SIM-style solutions could provide increased security for, and access to, healthcare providers' information and communications technology (ICT) systems, which can readily harness the strong identity management capabilities of a UICC. In most countries, healthcare ICT systems lack a widely-deployed identity management technology, so there is a clear opportunity to satisfy a critical market need.

This paper uses clear examples and case studies to explain how the UICC and other key components of the GSM ecosystem can enable the smooth and cost-effective deployment and enhancement of electronic healthcare solutions.

Secure application and transaction enablement – parallels with mobile money

Offering a high level of security and flexibility, the UICC underpins a growing number of services that enable people to complete transactions at point of sale or send and receive money using their mobile phone. To enable these services, the UICC is typically partitioned so that an individual's financial information is stored in a secure domain that can't be accessed by other applications running on the card. Partitioning can also be used to securely store healthcare information, such as a patient ID or National Insurance number, on a UICC.

Dual-factor authentication and security

The UICC can also enable dual-factor authentication: a combination of "something someone knows" and "something someone has". In this instance, the identity information stored on the UICC is 'something someone has', while the 'something someone knows' could be a PIN that is requested by an application that is running on the UICC.

The sensitive nature of data about individuals' health means information security is critically important. Applications running on the UICC can be integrated with almost any widely-used security system to provide a full end-to-end secure system.

Interoperable electronic health records

The majority of electronic health records today are locked inside proprietary systems and force patients to accept inefficient and, frequently insecure, data storage, retrieval, and billing. Moreover, only a tiny fraction of the systems today allow any direct control of that data by the patients themselves.

Using the UICC and related technology standards, mobile operators can provide a secure ubiquitous system that addresses these problems, while adding virtually no additional costs. The UICC could store an individual's summary care health record - a defined subset of the individual's total health record in a compact form that would include only basic information, such as blood type, allergies, current prescriptions, and important medical history information within a secure domain. The secure domain could also include the patient's insurance and billing information, enabling payment for healthcare via a simple swipe of a device or an authenticated SMS transaction.

In essence, the UICC is well-positioned to provide user identity management systems, health ICT user authentication, and individual health record storage, adding considerable value to both new and existing healthcare ICT systems.

Contents

1. Introduction

The overall environment in which health ICT systems must operate is one of the most complex in any field. Regulations vary widely from country to country and range from fully-regulated socialized medicine and health system implementations in parts of Europe and Asia, to the free-market environment in the United States where the quality of medicine is regulated, but no price controls are set on health services, drugs, or insurance. This diversity is further compounded by a lack of clear interoperability standards, creating a host of problems for integration efforts, aging legacy systems and an increasing awareness of security problems.

This paper describes a number of ways in which ubiquitous GSM technologies can solve some of the most complex problems in many health systems around the world. Clear examples and case studies explain how some key components of the GSM ecosystem, which are frequently taken for granted, already have more capabilities than most competitive technologies and are also being extended with even more powerful features.

Over the past decade, the global healthcare community has recognised that efficiency improvements and cost savings can be realised by implementing electronic health record and management systems. Mobile health technology, systems, and solutions can be a key enabler of this effort. Like financial systems, health information and communications technology (ICT) systems need the kind of authentication, identity management, security, and information controls provided by the GSM family of technologies. Health ICT systems can also benefit from the omnipresent capabilities available via GSM.

Figure 1.

The ubiquitous UICC

No device is better equipped to support ubiquitous healthcare than GSM-enabled mobile phones because no other digital device has been deployed to so many people in so many countries. There are more than 5.25 billion active[1] GSM accounts on more than 900 mobile network operators in more than 200 countries. At the core of GSM networks lies the Universal Integrated Circuit Card (UICC). The UICC is a class of smart cards engineered for the GSM phone. Years of use, and continuous improvements in the technology, have proven the UICC to be resilient to attack and therefore a suitable platform on which to host and execute sensitive applications.

Many mobile phone users frequently and incorrectly call the UICC a "SIM card." The Subscriber Identification Module (SIM) is actually an application that resides on the UICC along with multiple other applications. On 3G networks, the SIM has been replaced by (U)SIM and this technology is backwards and forwards compatible with most phones made in the past decade, including phones that lack 3G capabilities. In other words, even simple inexpensive phones can accept most new UICCs with the additional security capabilities and UICC memory this provides, even though the phone may not work on a 3G network.

The UICC stores and presents a unique identifier for each customer to their mobile operator. The UICC is the most universally-deployed application delivery, provisioning and deployment platform in the world, because it works with billions of 2G and 3G devices produced by the world's leading mobile device manufacturers.

1 Wireless Intelligence (https://www.wirelessintelligence.com/)

UICC-based solutions can be leveraged to provide increased security for, and access to, health ICT systems for customers of mobile operators that are also patients within the health ICT system. The strong identity management capabilities of the UICC can be easily and readily leveraged into larger systems. This level of widely-deployed identity management technology is lacking in most health ICT systems in most countries, so this is a clear opportunity to satisfy a critical market need.

Moreover, UICC technology can be paired with existing health ICT systems to create an inexpensive, common platform that enables multiple independent vendor solutions to easily integrate which each other via common interface standards.

Secure application and transaction enablement – parallels with mobile money

Mobile money, mobile banking and mobile financial technology have reshaped the financial services industry in many countries, providing new levels of access and security to people around the world. The most successful of these systems are built around the UICC. This white paper outlines and provides conceptual models which explain how UICC technology can also be leveraged to provide the basis for:

- Health ICT identity management
- Health ICT authentication systems
- Health data storage in the form of individual health records.

This paper highlights how similar systems are already in place and being used securely in many mobile money deployments, supported by a wide variety of security systems. The existing GSM security and authentication algorithms have fully developed reference models and it is a straightforward process to supplement these with almost any widely-used security system including:

- Public (aka asymmetric) key cryptography
- Shared secret key cryptography
- Certificate based authentication systems
- Two (dual), three or four factor authentication systems
- Smartcard-based authentication systems
- Secure storage.

Enabling interoperability

In this paper, the GSMA focuses on three areas of possible development and deployment of UICC technology in the health ICT space, including an examination of capabilities that can extend existing health ICT systems in new ways made possible by the UICC. These include health ICT user identity management, health ICT user authentication into systems, and individual health record storage on the UICC itself.

Perhaps the most innovative proposition is the concept of securely storing an individual's critical care health record on their own UICC. This record, combined with a simple application that gives the customer continuous control of its accessibility within mobile operators' networks, could fundamentally change the way health records are stored and distributed.

Mobile operators, in conjunction with the existing ETSI and 3GPP standards, can solve a complex problem that is facing most countries today in healthcare - a lack of interoperable e-health records. The majority of e-health records today are locked inside proprietary systems and force patients to accept inefficient and frequently insecure data storage, retrieval, and billing. Within the US alone, there are literally hundreds of electronic health record vendors. Each vendor's product offering has it's own unique implementation challenges and integration issues.

2. A Complex but solvable problem

The global health care community is seeking efficiency improvements and cost savings by implementing electronic health records. Unfortunately, these efforts are being hampered by integration problems, as few of these applications were ever designed to be part of larger nationwide health management and forecasting systems. The lack of clear policy and regulatory environments that would compel, or at least enable, systems integration further hampers even the best endeavours.

The majority of the application offerings in the health ICT space are proprietary in nature. Although some use underlying standards, such as HL7, most of these do not allow for simple or efficient integration between systems from different solution providers as the baseline architecture is so disjointed. A large number of countries have been struggling with this problem for well over a decade while overhead administrative costs have soared.

To date no organization has found an effective economic incentive that can be leveraged to encourage simplification of the overall health ICT solution in most countries. Yet there is a clear set of strategic drivers in healthcare that can be brought to bear and help define what such a system would look like and would need to accomplish in order to be successful. The table below lays out the three most critical common drivers across the global field of healthcare and matches them with specific use cases for mobile technology.

Table 1.

Use case for mobile	Strategic drivers for healthcare industry: Increase positive health outcomes	Increase efficiency of overall healthcare system	Reduce administrative costs
Deployed ID system	Easier secure sharing of data	Allows for better integration across previously disparate systems as single-sign on solution	Less expensive than dedicated smart card or token
Remote data access	Immediate access to critical data	Allows access to new locations and increase service to underserved populations	Increased speed and accuracy over paper reduces staffing costs
Remote data entry	More accurate data with reduced time for feedback	Increased speed and accuracy over paper reduces staffing costs	Increased speed and accuracy over paper reduces staffing costs
Patient education	More frequent access and access to underserved populations	Reduction in visits to health facilities = more patients served per facility	Reduction in visits to health facilities = more patients served per facility
Patient interaction	More frequent access and access to underserved populations	Reduction in visits to health facilities	Better feedback and billing process via the electronic audit trail
Geo-location	Better data collection and matching of resources to patient	Reduction in travel times and mismatched servers for needs	Reduces total staff in a given area by more efficient deployment

Mobile health is starting to gain traction, but much of the current focus is on simply extending existing health ICT systems to the mobile phone as a replacement or supplement to personal computers. New applications and solutions are being developed, but most are focused on single health problems and use standalone systems. While this approach is achieving successes, few of these mobile health solutions have leveraged the existing assets now widely used in mobile financial services. New innovative mobile health solutions could build on the years of development efforts in mobile finance, along with lessons of past failures and current successes.

Multiple established and proven existing solutions are available today that can be redeployed from mobile financial systems into mobile health solutions. Many of these underlying technologies can be adapted to support health ICT systems more easily, and at lower cost, than deploying new or custom solutions.

2.1. The advantages of the UICC

One of the most widely-deployed technologies in the world is the UICC smart card. All phones that use the dominant GSM family of mobile technologies require the use of a UICC for operation and no other technology has been manufactured in numbers that approach the scale of the UICC. Market data collected by Wireless Intelligence indicates that there are over five billion users of this technology in every corner of the globe.

Table 2.

	User experience		
Operator capability used (Bearer channel)	**Single command**	**Interactive network-based session**	**Interactive menu-based session**
Data	Typically not implemented	Any IP protocol including HTTP, HTTPS and WAP	Java applet, OS application
USSD	USSD to short code	USSD session	SIM toolkit
SMS	SMS to short code	System implemented on server-side	SIM toolkit
Voice	Dial-back	IVR via tones or recognition	IVR via tones or voice recognition

One of the advantages of the UICC is that it is a long-term sustainable business solution that leverages technologies unique to the GSM family of technologies that cannot be easily displaced or replicated by another technology. While the Internet may also have a massive number of hosts, it lacks a unified tracking and billing system and suffers from growing security concerns. According to the latest figures from security software supplier MacAfee, more than 66,000[2] new viruses and malware applications are created each and every day. In contrast, the UICC has proven itself to be robust against attack and is well-suited to hosting sensitive applications and data.

As the UICC is an integral part of every GSM subscription, it can access a range of bearer channels, including SMS and USSD, which are supported by all 2G and 3G devices. This means that even the most basic 2G devices can be part of a UICC -based system. Newer devices have the ability to access 3G bearer channels that provide substantially faster connection and data speeds.

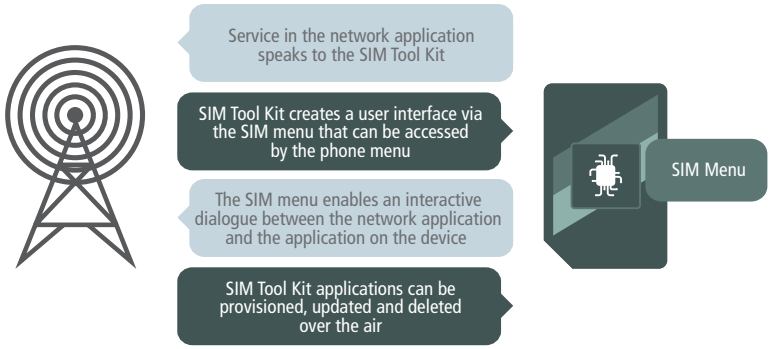
Since their introduction in the early 1990s, UICCs have become much more sophisticated with dedicated processing power, significantly-increased memory and extended security capabilities, including both physical and virtual tamper-resistance technologies. Most UICCs shipping today offer between 64K and 256K of on-board dedicated memory and UICCs with gigabytes of memory will be available in the near future. The UICC is therefore an ideal environment for use in mobile health systems deployment.

2 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf

Mobile operators and the GSMA have been recommending the UICC as the most appropriate host and enabler for key elements of the mobile financial services market, since early 2005, because it offers many unique advantages for the customer, including:

- **Ubiquitous deployment:** Universally-issued and deployed in mobile devices by local network operators as standard in every country of the world.
- **Individual usage:** Even in emerging markets UICC are rarely-shared between individuals and increasingly government require one UICC per individual, which is achievable due to the low cost of SIM card technology.
- **Security:** The UICC is a tamper-resistant secure element that conforms to industry standards including the latest ISO, ETSI, and Global Platform specifications.
- **Security:** The UICC supports the deployment of almost all widely-used global security standards.
- **Portability:** The UICC enables a customer to transfer their identity, key data, and service settings between mobile devices because they are configured on the UICC, which can be inserted in any compatible device.
- **Remote management:** Allows the applications and data on the UICC to be modified over the air easily and cost-effectively by mobile operators and trusted parties greatly simplifying service upgrades and configuration changes.
- **Device Agnostic:** Since the UICC is a standardised specification the functions it provides are independent of the mobile device operating system, which means solutions built on top of it do not have to be tailored to specific mobile platforms.
- **Long operational lifespan:** UICC technology is very rugged and is protected by the mobile device. Even in accidents that destroy the mobile device, the UICC itself typically survives. UICC are required to be manufactured to specifications that allow for operation in temperatures ranging from -25 °C to +85 °C (-13 °F to 185 °F) which is well outside the operating temperature of most mobile devices, laptops and netbooks.
- **Long operational lifecycle:** UICC designs change slowly, on a much longer timescale than mobile devices, but data stored on them is easier to access than data in proprietary mobile device operating systems due to the standardisation of the UICC specification. The UICC will therefore continue to be compatible with future devices, thus reducing operational and replacement costs.
- **Standards-based solution:** The UICC solution is based on internationally-agreed specifications, including those from 3GPP, the ETSI Smart Card Platform (ETSI-SCP), and the Global Platform standard, ensuring global interoperability and economy of scale.

The UICC and the SIM Tool Kit – A powerful combination

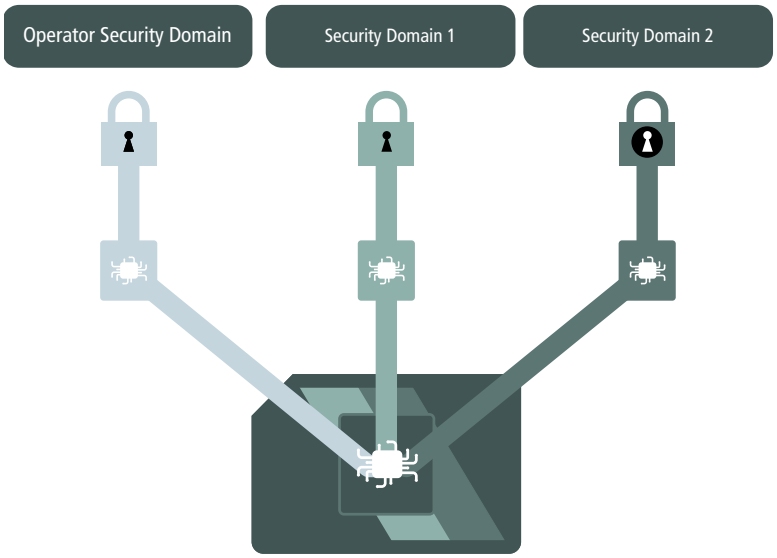


- The SIM Application Toolkit allows operators to add additional functions to the phone menu in order to provide new services for mobile banking or mobile health.
- The SIM Application Toolkit consists of a set of commands programmed into the SIM which define how the SIM should interact directly with the outside world and initiates commands independently of the handset and the network.
- The STK is replaced by the more powerful USAT in 3G, taking advantage of the multi-application environment of 3G devices including an advanced security model with integrated firewalls.

Most importantly, advancements in integrated chip (IC) technology permit the partitioning of the UICC into several security domains. The security domain structure as shown on the previous page provides a solution for a secure environment for hosting data and applications provided by multiple third parties.

Partitioning enables the UICC owner, the mobile operator, as well as third parties, such as card issuing banks, or in this concept, healthcare systems providers, to maintain the confidentiality of their data and applications and protect them from access by other third parties. This security domain concept allows the mobile operator's (U)SIM application to reside in parallel with different third party applications on one UICC. Each application is stored in its own security domain, and neither the mobile operator nor the third parties have access to each other's application and/or data. This is a critical advantage of this architecture for use in health ICT systems. Most existing electronic health record systems, particularly those hosted in the cloud, do not offer this level of security and reassurance.

Figure 3. UICC Security Domain logical model



- Each Security Domain is owned and managed by a separate Trusted Service Provider.
- Each memory partition on the UICC has a unique cryptographic key and can even use a unique cryptographic algorithm.
- Although the Operator issues the UICC and controls the root partition this does not give it access to any of the other partitions.
- Partition size is set by the Operator and is typically proportioned to the overall memory on the UICC.

2.2. Existing parallel solutions in mobile money

Although healthcare systems may not, at first glance, appear to be similar to financial systems, the underlying technologies in each solution space are driven by a critical need for security at all levels, which the UICC can satisfy. Within the broad landscape of mobile money, there are literally hundreds of technologies, deployments and implementations. Mobile health systems architects could benefit from careful study of mobile money technology and business models and examples that were successful, as well as the systems that were not. Such study would maximize the opportunities for success and avoid repeating the mistakes of the past.

In the mid-1990s, just a few short years after the introduction of mobile services based on the GSM family of technologies in Europe, it became clear that these could serve as a critical tool to securely access financial transactions and data, as well as provide a more secure replacement for some types of credit cards. Leveraging the UICC, the financial services sector has developed an array of related services and technologies that are variously referred to as: mobile banking, mobile money, mobile finance, mobile commerce, mobile payment systems, mobile wallets, and contactless Near Field Communication (NFC) payments. Part of the reason such a wide array of names exists is because of the crowded and rapidly growing and evolving field of technical solutions, often branded as unique products, but all using standardised and interoperable UICC capabilities.

Table 3.

Successful mobile banking solutions			
Technology implementation	**Single command**	**Interactive network-based session**	**Interactive menu-based session**
Data (2G, 3G, 4G)	**N/A**	**HSBC**	**Obopay**
USSD	**EKO/-**	**Wizzit**	**Vodafone M-PESA**
SMS	**Globe GCASH**	**Mgive Social Giving**	**M-PESA**
Voice	**EKO/-**	**HSBC**	**N/S**

Since 1999, when Fokus Bank became the first bank in the world to offer banking services via mobile phone, there has been an ever-increasing number of ways to conduct banking via mobile devices securely, inexpensively and safely. The glowing success story in this space is the M-PESA system in Kenya, which is a product of Safaricom. Current reports estimate that about 20% of Kenya's total GDP flows through the M-PESA system.[3] Although few other countries have seen a clear single winner, usage of mobile commerce and mobile financial services is growing rapidly. Within the United States alone, a study from Forresters recently found mobile commerce revenues are expected to hit $6 billion by the end of 2011, growing to $31 billion by the end of 2016[4] and a new study by Juniper Research reports that the total value of global mobile financial transactions will exceed half a trillion dollars in 2011.[5] Much of the future growth in this market is likely to come from Near Field Communication technologies which are discussed in the next section of this paper.

3 http://www.microfinancegateway.org/gm/document-1.9.43376/Mobile%20Payments%20Go%20Viral_M-PESA%20in%20Kenya.pdf
4 http://forrester.com/rb/Research/mobile_commerce_forecast,_2011_to_2016/q/id/58616/t/2
5 http://www.juniperresearch.com/viewpressrelease.php?id=320&pr=262

3. Health ICT system user identity management, authentication and access control systems

UICC technology is well-suited for building health ICT systems and integrating with existing systems in a number of areas. As previously discussed, the UICC has many design features that position it well to become a highly-secure and ubiquitous identity management and authentication platform. Portable and rugged, the UICC has the advantage of already being part of most people's daily lives.

One of the key advantages of making the UICC part of a health ICT system's backbone of core services is that it is an extremely flexible technology. While security standards and maintaining secure ICT systems requires constant vigilance, UICC technology benefits from decades of deployments and hundreds of millions of dollars of investment in fraud prevention technology. It is a versatile system which has evolved to stay ahead of known threats and one that is compatible with almost all widely-used global security standards.

It is important to note that there is no single universally-used UICC authentication scheme. This is an intentional design feature to increase the overall robustness of the five billion UICC in use today. The GSMA makes a number of highly-vetted security reference models available to mobile operators and other businesses interested in using UICC technology, while encouraging each to pursue its own standard. The interoperability standards for mobile operators are designed to permit this level of flexibility and yet allow for roaming across networks with no decrease in the overall security of any of the systems. In fact, this very flexibility increases the overall security of each and every network by using a non-homogeneous design.

This approach means that today there are mobile networks currently using all of the widely known security classes including public key (aka asymmetric) cryptography, shared secret key cryptography, certificate-based authentication systems, dual or triple factor authentication systems, and smartcard-based authentication systems.

The GSMA has published a wide range of detailed papers and reference models and examples to aid in the understanding of how these various models can be deployed. One of the most detailed papers, entitled *Identity Management Framework Document*,[6] provides clear descriptions of a wide range of possible types of deployment, including basic use cases. It is now available to the public on the GSMA web site.

It should be noted that the UICC is one class of smartcard so virtually any smartcard-based authentication system can also be deployed using the UICCs in a GSM phone. As the UICC is something that most people keep with them at all times, it is ideally-placed to form the backbone of highly secure multiple-factor authentication systems. Multiple factor authentication systems rely on a user having something in their possession (in this case the UICC) and something they know, which is typically a password. Since the UICC is already contained within a mobile device, the device's keypad can be used as the data entry mechanism for the password, making it much less expensive to deploy than other alternatives.

UICC technology cannot be defeated simply by stealing the user's phone or UICC without having knowledge of the user's confidential password. The addition of password protection at the UICC level as well as the possibility for an additional password for accessing a remote system via the mobile network offers critical extra protection. In other words, merely removing the UICC and inserting it into another device accomplishes nothing as UICCs are typically configured to require a PIN to allow access to them when they are inserted into a new device.

Because of this capability, the UICC has been at the heart of many advances in authentication system design and deployment within the field of mobile banking. In essence, the difficult work of designing, testing and proving the security of UICC identity management and authentications systems has already been accomplished. A large variety of systems are already in place, including "mobile wallet" technology, which was deployed in Japan in 2006. That implementation was based on the Sony FeliCa smartcard chipset and it rapidly became the de facto standard across Japan. It has replaced a number of smartcard based systems including the system used for public transportation. Similar successes are found in South Korea, Philippines, Malaysia, Thailand and Pakistan.

6 http://gsmworld.com/documents/identity_management_framework.pdf

3.1. The emerging abilities of Near Field Communication

A similar, but more advanced and flexible, system has been developed using Near Field Communication (NFC) technology. The system combines UICC technology with the NFC chips in new mobile devices, which enables them to securely exchange information with a nearby receiver. The original intention was for the mobile device to be used to quickly and easily complete transactions at point of sale, while providing more security. However, many other vertical industries have also jumped on-board this technology and there are already products shipping that allow for everything from keyless locks for homes to worker time-card and hour tracking systems. Not surprisingly, substantial work is underway to integrate NFC-based solutions into healthcare systems. A partial list of innovative ideas, concepts and deployments is listed in the table below.

Table 4.

Current or Near-term NFC uses in healthcare
Check-ins: NFC-enabled mobile phones could allow patients to check in at the doctor's office, hospital or even Emergency Room, rapidly and without errors or re-keying data. This is a significant improvement over sign-in sheets which require manual error-prone transcription of data or even kiosk sign-ins which can be confusing and time-consuming for many patients.
Staff location/management: Home care companies in the Netherlands and the U.K. are using the technology to determine when staff arrive and leave a patient's home, and to allow them to upload and download patient information in a hands-free manner. Another compelling business efficiency case is to use NFC technology to sign healthcare workers in and out of hospital units.
At-home diagnostics: One of the leading firms in the space is developing a testing platform that would combine NFC with immunoassay technology to allow at-home self-testing for pregnancy, fertility, drugs, allergens and even pathogens, according to company officials.
Fitness: NFC chips could enable phones to automatically upload (or download) an individual's exercise performance, rather than requiring them to upload or data-enter their information.
Emergency connectivity: Medical professionals could use the technology to identify injured patients without touching or moving or even talking to them.
Pharmacy: Patients could update and refill prescriptions and get information on side effects through NFC-enabled phones.

Although NFC is only just beginning to be deployed, the work that went into designing and architecting the back-end identity management and authentication systems can be used today even without the addition of NFC-enabled phones and readers/receivers. UICCs are capable of storing large cryptographic keys which are much better than passwords.

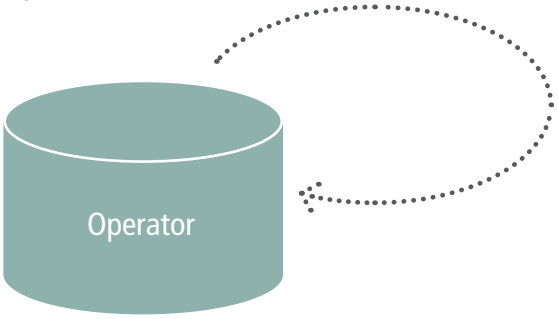
The GSMA has issued a number of white papers that detail the design and architecture of such systems including a paper entitled *Identity Management Requirements, Issues, and Directions for Mobile Industry.*[7]

In the final two sections of this whitepaper 4 generic use cases and their applications are discussed. These use cases are labelled A-D, and for consistence the labelling of these use cases has been continued into this paper. Within the following section the use cases will be laid out in the order of their complexity along with discussions of their real world applications. For more detailed technical information on each of the use case please refer back to the original paper.

7 http://www.gsm.org/documents/se4710.pdf

3.2. A mobile health insurance conceptual architecture based on M-PESA

Figure 4. Model D



Model D – This diagram represents simplest technical implementation and service model where a Mobile Operator provides all the identity management, authentication and access control of provisioned users to itself. Example: Health Insurance.

In the GSMA *Identity Management Framework Document* paper, the last model discussed is the simplest, but it has led to one of the most successful mobile money systems in the world – M-PESA. While the conceptual model is one where the mobile operator is providing identity management and authentication to itself, the key differentiator is that it is using UICC technology to provide those services to create a new service distinct from the mobile calling services that are the core business of the mobile operator. This is not a trivial deployment as it requires a completely new application, typically within a vertical market that is not a core expertise of the mobile operator. It, therefore, requires everything from additional market research and development, to application development and deployment plus marketing, all completed in a way that needs to be complementary to the existing business of the mobile operator.

Within the world of mobile money, the M-PESA solution is typically regarded as the most successful service. Just four years after the initial deployment it is used by more than 65% of Kenyan households. It has also served as a key market differentiator for Safaricom allowing it to attract an even greater share of Kenyan mobile phone users.

Why was M-PESA successful when many earlier mobile money implementations had failed? It is likely that two factors determined the success of M-PESA; first M-PESA uses a simple business model that was easy for users to understand and met a need within Kenyan society, and second, its technology design and architecture allowed for ubiquitous deployment on literally any mobile device. This was a direct result of relying solely on the UICC architecture of the mobile system for identity management, authentication, security, access and control for all aspects of the system. Kenyans had had good experiences with Safaricom and trusted its network to be safe and secure and to protect them from fraud.

The technical implementations of M-PESA using a SMS-based system allows the use of any mobile device manufactured by any vendor to be used. People receiving money do not need to be part of the system and do not require any software to be installed. M-PESA clients use a SIM Toolkit Application installed on the UICC to add basic menus to the user's phone. The transaction system is fully contained in the back-end functions within Safaricom's data centre.

One of the key lessons learned from M-PESA, which should be carried into mobile health system design, is that it also has a relatively simple technical implementation that is fully owned and controlled by a single mobile operator. Safaricom did not originally integrate with any other systems outside of Safaricom. This is not to say that it can't be integrated with other systems, but the choice was initially made not to do so in order to speed the deployment and limit the initial technical complexity. The M-PESA concept, as well as the business model of the system, was simple for consumers to grasp and it offered a critical service not otherwise available in Kenya.

Within the field of mobile health there are no close analogies available at the moment to the M-PESA system, but medical health insurance comes closest. Insurance is a much more complex business model than simple money transfers, but technically there is no reason why a mobile health insurance offering and system could not be implemented with the same back-end technology and SIM Toolkit interface used to create M-PESA.

3.3. Conceptual architecture – multiple operators, no external partners

Figure 5. Model C

Model C – This diagram represents a relatively simple and likely technical implementation and service deployment model where one operator provides identity management, authentication and access control of provisioned users to itself, against a data store or service operated by a second mobile operator. Example: Health Saving Account.

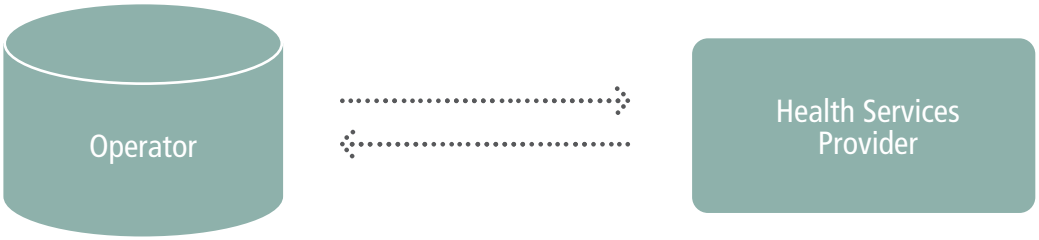
Many mobile money and mobile banking offerings allow third-party systems to integrate via application programming interfaces (APIs) directly into those systems and, in some markets, are required to do so by law or regulation. This model examines a use case where one product (mobile money) is provided by one mobile operator and another mobile operator provides a complementary service offering (mobile health insurance).

In a market where a single mobile operator controls a dominant mobile banking or mobile money offering, other mobile operators may not want to compete head-on with the established system and may seek to tackle other areas of innovation instead. In this model, the second operator may leverage the existing and established mobile money system and elect to extend that via a private health insurance system.

In such a case, mobile operator A would provide the identity and authentication system as well as the money management and cash transfer capabilities for users. These money transfers would be exchanged with mobile operator B, which would run the health insurance account system and make direct health care payments for their health insurance clients. As both companies are mobile operators, the integration work required to enable the UICC of all users to function as the identity management and authentication system for the total offering would be straightforward, since the back-end systems are already in place.

3.4. Health Record Access and Control Conceptual Architecture

Figure 6. Model B



Model B – This diagram represents a common but typically complex technical implementation and service deployment model where an operator provides identity management, authentication and access control of provisioned users to itself, against a data store operated by a health services provider (HSP). Example: Health ICT System Authentication.

One of the critical, yet time-consuming, processes in patient care is identifying an individual with their existing medical records, history, insurance and payment information. In most countries, this is still a manual paper-based system endured upon entry to any (new to the patient) health facility or pharmacy.

In this model, the mobile operator's UICC system would function as the identity management and authentication system to allow sharing of billing information and data upon clinic entry. This could be extended to allow the system to further function as the identity management and authentication system for the total health ICT system run by the health services provider. Such a system could be used both by healthcare specialists and administrators for access into health ICT systems and by patients wanting to access their own health, billing and insurance information.

A similar second model already being deployed in Kenya is the use of a health savings account. Again, the key to successful deployment of such a system is the ability to easily and inexpensively leverage and extend existing mobile operator assets. In this case, Safaricom deployed the M-PESA mobile money system. After an initial successful rollout, the system was opened via an API to allow for third-party direct use and this enabled the deployment of new complementary systems and businesses that extend M-PESA's capabilities into new areas.

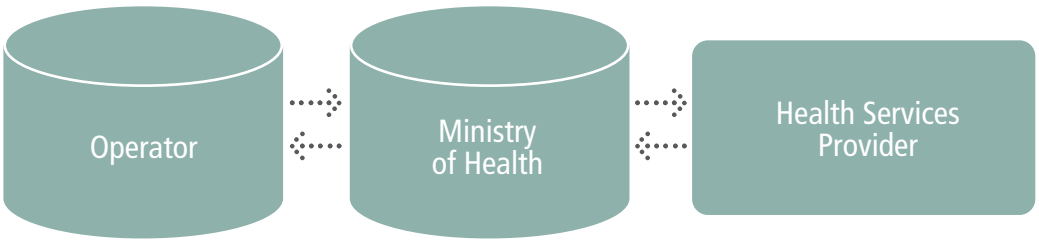
In wealthy countries, a common solution for paying for healthcare is via various insurance schemes. Unfortunately, the weakness of such plans is that they typically require regular payments which many citizens in marginal economic circumstances may not be able to consistently meet.

The health savings account seeks to bridge the gap between being completely without any insurance or financial cover and being a full member of an insurance scheme. Significantly for this target market, the health savings account concept allows for group pricing of various medical procedures, including drugs, as is typical in insurance schemes. It is particularly advantageous for medical procedures which might otherwise be ignored, but where some medical intervention can improve the likelihood of positive outcomes.

One clear case where this is true is the use of a medical savings account to cover birth delivery in a controlled environment particularly where an intervention, such as a caesarean, may be necessary. Nairobi's Pumwani Maternity Hospital enables just such a system. An independent NGO has issued a secure smartcard system which is integrated with the Safaricom M-PESA system and allows for direct transfer of micropayments into a health savings account. These smartcards use UICC technology, but in a form factor that was perceived as easier to support among the target market in Kenya.

3.5. Conceptual architecture – single operator, multiple external partners

Figure 7. Model A



Model A – This diagram represents one of the most complex but likely technical implementation and service deployment models where an mobile provider provides identity management, authentication and access control of provisioned users to itself, against a data store operated by a national agency with additional independent parties (HSPs) also providing their own identity management, authentication and access control into the same data store. Example: Health ICT System Provisioning.

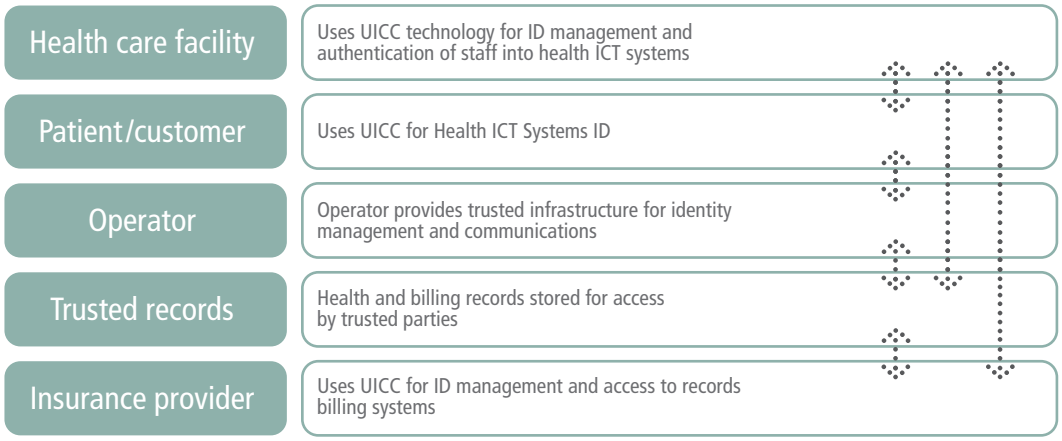
This model for deployment is the most complex, but best reflects the realities of the healthcare system in most countries, which have a mix of public and private players including Ministries of Health, health care facilities, pharmacies, insurance providers, and others.

In the referenced identity management papers, the GSMA defined this complex model as "Use case A" and it is represented here as the most likely deployment of UICC technology for identity management, authentication, and access control system for health ICT systems spread across many agencies, including private corporations and public health facilities. In this case, a single mobile operator would provide the back-office infrastructure to enable users of any mobile device to use their UICC as their primary identity. This would enable the deployment of strong multi-factor authentication systems via the mobile network using a combination of public-key cryptography and passwords.

3.6. Organisation relationships and structure

Many of these deployment models create a system where the mobile operator becomes a key stakeholder in the middle of healthcare delivery systems. This has the advantage of moving patient management out of the hands of typically under-resourced and expensive healthcare providers and into the realm of customer service, which is a core competence of mobile operators. Even if the operator is only providing identity management and authentication services, it would still be inserted into the middle of key business, customer and societal relationships, furthering its business opportunities, while increasing the overall security and efficiency of the total system. In other words, this model of the deployment allows the operator to provide and support the technical aspects of the healthcare information and management system and, therefore, leaves the healthcare to the healthcare providers. Each organisation is doing what it does best, creating a more efficient, better-run and lower-cost overall system.

Table 5.



As can be seen in the diagram above, the mobile operator would be in a position to access and maintain relationships with virtually all of the entities involved in the provision of healthcare services. This includes the customer, who is also a patient of the healthcare system, the healthcare providers and facilities, and the insurance providers, especially if the mobile operator elected to host records securely or operated a mobile money system for payment processing.

4. UICC-based individual health record system

Mobile operators, in conjunction with existing ETSI standards, can solve a vexing problem that is facing most countries today in healthcare - a lack of interoperable e-health records. The majority of e-health records today are locked inside proprietary systems and force patients the world over to accept inefficient and frequently insecure data storage, retrieval, and billing. Worse still, only a tiny fraction of the systems today allow any direct control of that data by the patients themselves.

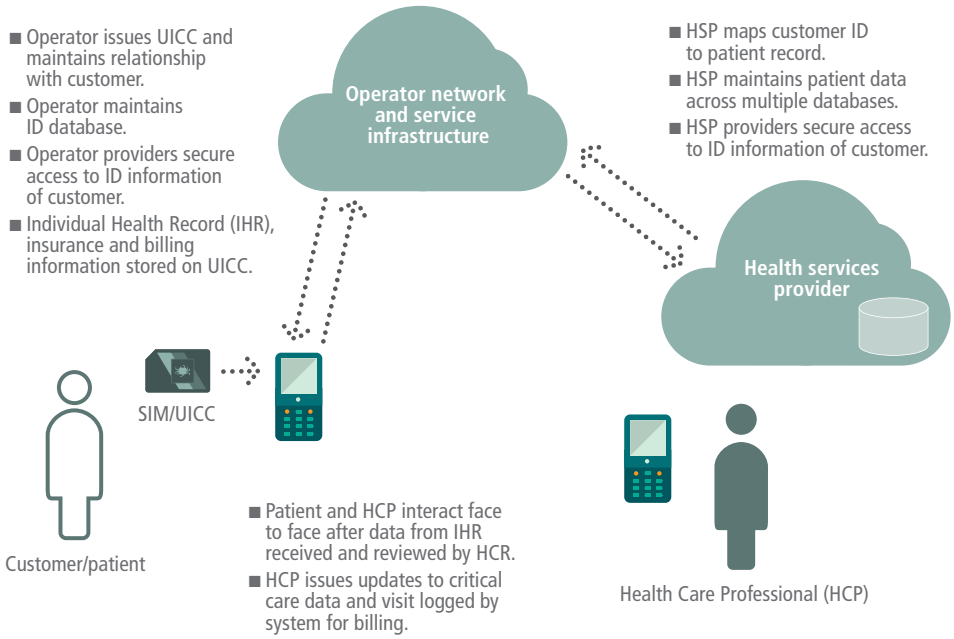
Using the UICC and mature standards, mobile operators can provide a secure ubiquitous system that addresses all of these problems while adding virtually no cost to future deployments. The low unit cost of this system is a powerful incentive to assist the creation of a more universal e-health record system.

The UICC is extremely rugged and resistant to both G-forces and temperature extremes and because it can be quickly backed up over the mobile network, it is an ideal location for the storage of an individual's summary care health record (IHR). For routine use this would allow the transfer of patient history, insurance and payment information quickly and easily and additionally allow for the easy transport of pharmacy prescriptions from a healthcare facility where they are issued, to a pharmacy where they are fulfilled. In an emergency, the data would likely be with the patient (and the UICC would be protected by the mobile device within which it is contained) and be able to provide both needed identity information and a summary care patient record, thus speeding and supporting accurate care of the individual.

The summary care record would be a defined subset of the individual's total health record in a compact form that would include only basic information, such as blood type, allergies, current prescriptions, and important medical history information. This data, along with insurance and billing information, would be stored in a separate UICC memory partition with its own defined security domain. Access control to this data would be via an independent trusted service provider and the information would be under the control of the patient who is also a customer of a mobile operator.

UICCs are available today that have a storage capacity of up to 256K and future UICCs will have even greater capacity. This memory capacity is not set by technological limits, but by economics – demand for larger memory UICCs is currently low. As early deployments of the IHR will likely require a tiny fraction of this limit, memory capacity is unlikely to be a roadblock to implementing this concept.

Figure 8.



By using an externally-defined data descriptor, and possibly a compression algorithm, it should be possible to keep the total size of the critical care record to less than 1K depending on the required volume of data stored. The advantage of keeping the data store small and efficient is that it allows for storage on the smallest and oldest of existing UICCs. It further allows for the transfer of the data from the UICC into applications on the phone and over the mobile network to external applications very quickly. Even transferring the data from a remote tower at the maximum operating distance of the mobile specifications via sequential SMS (which is the slowest GSM bearer) the total transfer time for 1K of data is less than 1 minute. This is significantly less time than most healthcare workers spend retrieving paper records.

Individual health records stored on a UICC, combined with a simple application that enables the customer to instantly share the information via mobile networks, could fundamentally change the way health records are stored and distributed.

In routine use, the healthcare facility would send a request to the user/patient similar to a software license agreement. Once the user/patient agrees to share his or her profile and medical records the data would be unlocked either on the UICC or remotely in a secure medical records storage facility. This would allow instant sharing of the data with the facility even for new patients. As the system and the user record the transaction, it creates a data audit trail.

This system would empower patients in a way rarely achieved but frequently requested. Most individuals view their mobile phone as an innate part of who they are and as an expression of their identity. It is a logical extension of this thinking to include medical information in a personal location and under the control of the individual.

5. Conclusion

No device is better equipped to support consumer-based and accessible healthcare than GSM-enabled mobile phones and no device has a larger installed base than the UICC with over five billion in current use today. As the UICC is something that most people keep with them at all times, it is ideally placed to form the backbone of highly secure multiple-factor authentication systems. The difficult work of designing, testing and proving the security of UICC identity management and authentications systems has already been accomplished. A large variety of systems are already in place including "mobile wallet" technology and the emerging Near Field Communication deployments.

Most UICCs deployed today have the ability and excess memory capacity to enable immediate use for the storage of individual health records. UICC systems will increase the speed by which electronic health records are deployed in the developing world and allow for immediate access of an individual's critical care record in an emergency.

In conclusion, the UICC, which already plays a pivotal role in mobile networks and mobile banking solutions, could be further exploited to take on a key role in mobile health, enabling modern healthcare information and communications systems in both the developed and developing world.

UICC technology can be easily paired with existing health ICT systems to create an inexpensive, common platform to enable multiple independent vendor solutions to easily integrate with each other via common interface standards. By providing user identity management systems, health ICT user authentication, and individual health record storage, the UICC is well-positioned to make a major value-added contribution to new and existing health ICT platforms.

6. Glossary and acronyms

3GPP

The 3rd Generation Partnership Project, a grouping of international standards bodies, operators and vendors with responsibility for standardising the WCDMA-based technologies in the IMT-2000 family.

Access Control

A discrimination process to determine whether an actor X (e.g. a person, program or device) is allowed to have access to data, functionality or service Y.

Attribute

A description of a characteristic of an identity. Examples include: hair colour, age, blood-type, or location. Note, an attribute may be uniquely identifying the identity, in which case it is an identifier.

Authentication

The overall process of establishing that the actor being authenticated is indeed the actor in whose name assertions are being made, with an implicit or explicit level of confidence and liability. The actor in question may be a human or any non-human system entity (client, server, application, etc.). The authentication authority may perform authentication for the benefit of another entity that resides in another domain.

Authentication Authority

An actor guaranteeing that an assertion is indeed correct, with an explicit or implicit level of confidence and liability.

Authentication Level

A hierarchical assignment of authentication methods reflecting increasing strength to resist violations and attacks.

Authentication Mechanism

Functions that validate claimed identities and that output a status that is either true (verified) or false (rejected). Also see: Mutual and Single-sided.

Authority

A data structure that can be validated and that contains one or more identifiers and various contexts.

Bearer

A telecommunications term that is short for "bearer service" that allows transmission of information signals between network interfaces or devices. EDGE, 3G and USSD are all GSM bearer channels available to application developers for transmitting data.

Certificate

A data structure that can be validated and that contains one or more identifiers and various contexts.

EDGE

The GSM Evolution (EDGE) technology, which provides up to three times the data capacity of GPRS.

EHR – Electronic Health Record

A term used to describe a health record stored electronically, often managed by a healthcare organisation or clinician.

ETSI – The European Telecommunications Standards Institute

An independent, non-profit, organisation based in Sophia Antipolis, France, ETSI is officially responsible for the standardisation of information and communication technologies within Europe. It has 740 members from 62 countries/provinces inside and outside Europe. These technologies include telecommunications, broadcasting and related areas such as intelligent transportation and medical electronics including the GSM specifications and standards. ETSI members include hardware and software manufacturers, network operators, administrations, service providers, research bodies and users.

GPRS

A very widely-deployed wireless data service, available now with most GSM networks.

GSM

An open, digital cellular technology used for transmitting mobile voice and data services.

GSMA
The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers, Internet companies, and media and entertainment organisations.

HL7 – Health Level 7
A standards body that defines interoperability and messaging standards for the health industry

HSPA – High Speed Packet Access
The set of technologies that defines the migration path for 3G/WCDMA operators worldwide. It is a combination of two technologies, one for download and one for upload.

ICT
Information and communication technologies.

Identity
The collective aspect of the set of characteristics by which an actor is uniquely-recognisable or known. The set of behavioural or personal characteristics by which an actor (e.g. individual or group) is recognisable. An identity is described by its attributes, some of which may be identifiers.

IDM – Identity Management
A set of processes, technologies and services in order to manage principals' identities (creation, maintenance and termination of principal accounts), to provide secure access to an operator's resources (data and services) and to protect principals' private data.

IdP - Identity Provider
A provider that manages identity information. On behalf of users, it may provide information and a statement of authentication to other actors.

Identity Token
A credential used in a specific context.

IHR – Individual Health Record
A term used to describe a single health record, sometimes called a Personal Health record, if managed directly by the patient.

ISO
International Standards Organisation.

LTE – Long Term Evolution
LTE is a 3GPP technology that is designed to be backwards-compatible with GSM and HSPA and forward-compatible with LTE Advanced. LTE incorporates MIMO in combination with OFDMA.

OTA – Over the Air
OTA is a technology that allows access to and updating of all data on a UICC virtually via various bearer channels, including 3G and other data standards. OTA allows mobile operators to update either a single subscribers' information or an entire class of users without the need to physically touch or service the phone.

SMS – Short Message Service
A short text based messaging system available within the GSM communication standards. SMS was first deployed in 1994.

SP – Service Provider
A provider of services and/or goods, which may require an actor authentication and/or transfer of actor information for the purposes of a particular transaction.

SIM – Subscriber Identity Module
An application on the UICC that stores and handles the Subscriber identities (IMSI) and authentication keys (Ki in GSM).

SIM Card
See UICC.

STK – SIM Toolkit
Provides a set of commands that allow applications existing in the UICC to interact and operate with a mobile client that supports the specific command(s) required by the application. The STK allows mobile operators to add additional functions to the phone menu in order to provide new services such as mobile banking or email. The SIM Toolkit allows applications to be downloaded to the SIM in a secure manner.

Subscriber (also known as a customer or bill payer)

Role carried out by a company (usually represented by an administrator) or a person (or a group), which pays for the services offered by the operator. These services are used by end users linked to the subscriber (i.e. the subscriber: end user relationship is 1:N; where N=1, 2,). A person (or a group) may play both roles, subscriber and end user, or only one of them.

TSM – Trusted Service Manager

This entity is primarily responsible for securely distributing, provisioning and managing the life-cycle of a Pay-Buy-Mobile application and other NFC-based services to a mobile operator's subscriber base on behalf of the service providers. The TSM will have business relationships with both the mobile operators and the service providers.

UICC – Universal Integrated Circuit Card

A physically secure device, an IC card (or 'smart card') that can be inserted and removed from terminal equipment, such as a mobile phone. A user's UICC card, which can be moved from phone to phone, contains all the key information required to activate the phone. It may contain one or more applications. The UICC is commonly, and incorrectly, called the SIM or SIM-card. SIM and USIM are actually applications on the UICC. Additional applications frequently found on the UICC are CSIM and ISIM which are used to manage the user's identity on CDMA networks and IP networks.

USAT – USIM Application Toolkit

The equivalent of the SIM Toolkit but for 3G networks. See also STK.

USSD – Unstructured Supplementary Service Data

A session-based protocol implemented on all GSM phones used typically by mobile operators to communicate between the mobile phone and the service provider's servers. USSD can be used for prepaid call-back services, mobile-money services, menu-based information services, and to configure the phone on the network. USSD messages are up to 182 alphanumeric characters in length and, unlike SMS messages, USSD messages create a real-time two-way data connection.

User Authentication

The process of authenticating a personal (physical) user. User authentication may consist of one, or combinations of the following (independent) three elements: something the user knows, has or is. If only one factor is used, UA is denoted as weak (like PIN or password only); 2-factor UA is denoted as strong.

User Authentication Methods

Commonly classified as being one-factor, two-factor, or three factor, whereas the said factors are normally: "something you have", i.e. a physical device (e.g. a smart card), something you know (e.g. a password), or something you are (e.g. a biometric factor, such as a fingerprint).

USIM

An application on the UICC that can register with, and access services provided by, mobile networks, with the appropriate security.

WCDMA

The air interface for one of the International Telecommunications Union's family of third-generation (3G) mobile communications systems.

Authors:
Bart Stridham
Richard Cockle

GSMA Head Office
Seventh Floor, 5 New Street Square, New Fetter Lane, London EC4A 3BF UK
Tel: +44 (0)207 356 0600
www.gsmaembeddedmobile.com
mobilehealth@gsm.org