White Paper

SIM – The basis for Mobile Value Added Services

Authors: Lars-Erik Sellin and Anna-Stina Strömbäck

Document number: CTO 02:001

Revision: A

Contents

Document number: CTO 02:001
Revision: A

1 Introduction

This paper gives an overview of technologies to implement value added services based on the mobile smart card, e.g., the SIM and the UICC platform.

An important aspect is also the positioning of the UICC/SIM as a platform for Value Added Services in current and future wireless technologies. The basis for a successful service offering is applications that can bring revenue today from the existing customer base, and at the same time ensures a reliable roadmap to the future wireless technologies. We focus also on applications where the wireless operator, or service provider, can have a central position today as well as tomorrow.

The UICC/SIM is changing to a multi-application platform where you can have several telecom applications in parallel with non- telecom applications. The UICC/SIM is also evolving to a JAVA based platform, allowing the development of interoperable UICC/SIM applications. This technology evolution of the SIM/UICC increases the value of the SIM/UICC as a basis for Mobile VAS.

For a more complete technical description of SMS, SIM Toolkit and SmartTrust WIB technologies please refer to the book “Developing Mobile Applications using SMS and SIM Toolkit” written by Scott Guthrey and Mary Cronin, McGraw-Hill, ISBN 0-07-137540-6.

1.1 The UICC/SIM as the basis for Mobile Value Added Services

The evolution during the last couple of years has been very favorable for the SIM technology. It is now clear that almost all of the future mobile telecommunications technologies will have a smart card based Subscriber Identity Module, whether it is called SIM, USIM or R-UIM. The Short Message Services is experiencing a similar evolution; all existing and future mobile telecommunications systems will have an SMS service that is backward compatible with the SMS service of the 2G systems.

This places the SIM Toolkit services in an excellent position as it can be implemented today for the entire existing subscriber base, as well as being future proof. The SIM Toolkit and SMS services will exist in 2G, 2.5G, 3G and 4G. It is a true “11.5 G” technology (2+2.5+3+4=11.5G). The SIM technology is the least common denominator in this multi technology environment of today and tomorrow.

Document number: CTO 02:001
Revision: A

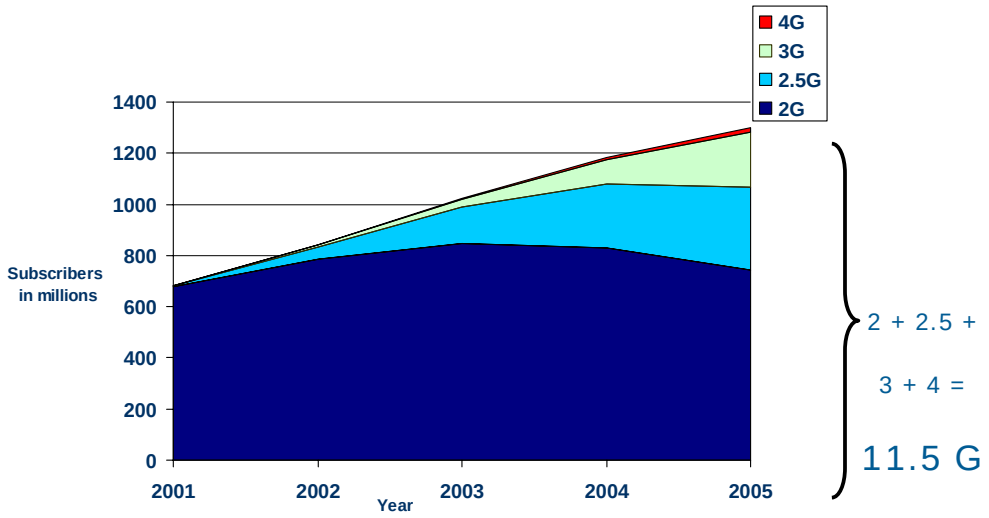

Figure 1. *The 11.5 G technology environment*

The SIM technology gives the Mobile Operator, or the Mobile Service Provider, a possibility to add something extra to their offering – something that is not possible for a party that does not control the issuing of the SIM. With the SIM technology the operator has the possibility to give the subscriber an always available and online set of services direct from the handset menu.

With WAP or standard web based services, the operator has very little extra to offer compared with any other service provider. Why would the subscriber set the WAP configuration for the operator's portal when she can just as well connect directly to Yahoo or AOL? With the SIM technology the operator can add new features to the service offering, e.g., location based services, digital signatures (for payment schemes) and advanced always online value added services, thus avoiding becoming 'just' a bit pipe.

Looking into the future - let's say four years from now - it is fair to say that the player to be in the best position to realize the business potential in the 11.5 G environment will be the one that can:

1. Enable the "mobile phone" to function as the "digital identity" of its owner.

   The "digital identity" will be a key enabler for services related to payments, secure access to services, and, maybe most importantly, to the secure distribution of software and digital media in future Internet based 3G and 4G networks.

2. Enable billing for services

   Billing is essential to allow distribution of meaningful and qualified

information and goods. The problem today with the content on internet is that it is very hard to find any qualified information or goods as there is no easy-to-use billing structure for real time distribution of content. The introduction and management of digital identities tied to the UICC/SIM will remove this problem.

3. Enable service management and portability in a multi technology environment

   If the services are not easy to provision and deploy they will never take off. There must be an easy to use service management system that works across the technology borders. The subscriber shall be able to access a basic set of services independent of the technology of the handset she chooses or if she is in the home network or roaming.

Through the UICC (the SIM card for the 3rd and 4th generation networks) and the SIM the operators, or anyone that issues the UICC/SIM, have a unique chance to take a central position in the emerging mobile economy. The UICC/SIM is the ideal platform for the digital ID in the 11.5G environment as it fulfills the above requirements as well as it has a set of other interesting capabilities:

1. The SIM has a global penetration soon exceeding the “Windows PC” reach
2. It is portable and almost always online
3. There is a complete service billing infrastructure already connected to the SIM as it already is the digital (network) ID for the subscriber
4. It has a global reach through roaming.
5. A remote service management infrastructure already in place and well proven on the market
6. The SIM/UICC is the least common denominator in the 11.5G

But the key to success is to start moving now! A rapid - and revenue generating - deployment of enhanced SMS services based UICC/SIM will have some interesting strategic “side effects” as:

1. Implicitly start the deployment of “digital id’s” in the user base
2. Make the users get used to the operator as the natural supplier of services “worth paying for”

2 Background to the SIM Application Toolkit

SIM Toolkit (STK) is today mainly used as a tool that enables an operator controlled menu for SMS and voice services. It is also used for more advanced services that require high security, where the SIM plays a natural role as a Smart Card.

The SIM Toolkit is, just as SMS, a well proven GSM standard (phase 2+, GSM 11.14) that has been out on the market since 1995. It has by now been incorporated into all major mobile telecommunications standards. Just as SMS it experienced a slow take off in the beginning, partly as the market has been in a wait state for new more 'hype' technologies. SIM Toolkit technologies enhance the ease of deployment of mobile services. As the Toolkit in practice is supported by all handsets (the phase 2+ compliant ones) on the market it is reasonable to believe that we will see a massive increase in services utilizing SIM Toolkit functionality. The fact that the operator controls the SIM makes it also an ideal platform for operator-provided services.

The major drivers for implementing services using SIM Toolkit are the combination of its maturity, and its network technology independence as it is now incorporated in 3G and TDMA standards (GAIT). An application developed using SIM Toolkit will work in the 3G networks as well as when roaming into a foreign 2G network.

SIM Toolkit (STK) should be used for user-oriented services based on short transactions of the type 'request – response' and for implementing advanced SIM based functionality as a complement to a service developed using another browsing channel, e.g., the web . Examples are advanced security functionality, telephony services, address book management, and location based functionality.

SIM Toolkit is also ideal for server-initiated transactions, as the main data bearer is SMS. This makes it perfect for Internet services where the handset is only one of the devices, e.g., using the handset and the SIM for authentication of users and confirmation of payments while using a PC as the browsing device.

STK services have had moderate take off due to interoperability issues between different SIM vendors. But maybe even more important there hasn't been any standardized application language for the communication between the SIM and the Server component. A dedicated Client and Server component had to be developed for each service, i.e., it was a traditional Client/Server technology. As such the STK has the same drawbacks as the Client/Server technology that was popular in the eighties before the introduction of HTTP and HTML. It generates a good business for the companies offering professional services to build the solutions while the customers, e.g., the operators and the content providers, get stuck with a static and proprietary solution.

3 The SmartTrust Wireless Internet Browser and the USAT Interpreter

SmartTrust developed the WIB (Wireless Internet Browser) technology to ease the development of SIM-based services using a generic SIM supplier independent interpreter on the card for any kind of application. The WIB optimizes the utilization of SIM memory in addition to offering a true interoperable execution environment on the SIM. It also solves the client/server problem since it uses standard web technologies.

The WIB operates together with a network component called Wireless Internet Gateway (WIG). The WIG opens up a secure channel (utilizing GSM 03.48 security) to the WIB on the SIM. The WIG enables the usage of an easy to use application language, e.g., WML, for implementing STK based mobile services as well as a secure operator controlled interface for mobile Value Added Services.

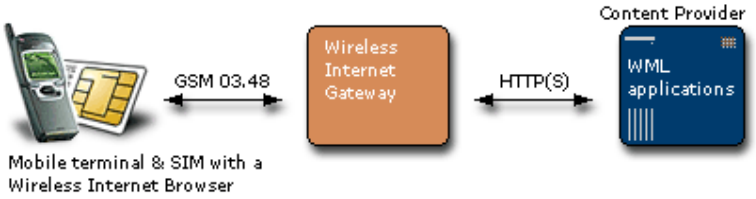

Figure 2. The WIB/WIG Architecture

The WIB is basically a specification, developed by SmartTrust, for a SIM Toolkit interpreter, or browser, that is licensed free of charge to companies developing software for SIM cards. It has been in commercial use since beginning of 1999 in various wireless applications, mostly in the m-commerce area. It is now in use at about 50 operators worldwide (Jan 2002) and is available from all major (and most minor) SIM vendors. There are also independent suppliers of SIM OS that license the OS with the WIB to SIM vendors. There are approximately 25 million SIM cards on the market with the WIB enabled (July 2001).
Since mid 2000 there is a standardization initiative, the USAT Interpreter, within 3GPP to standardize the concept. SmartTrust has been actively pushing for this standardization since 1996, and now it has finally been standardized in Release 5 of the GSM/3GPP specifications. SmartTrust development of the WIB is of course in line with these new specifications and the current WIB/WIG is compatible, on a service level, with the USAT Interpreter standard.

With the WIB/WIG it is possible to implement ease-of-use services to the operator's installed base of mobile phones, and still be compliant with future technologies. Operators that take this opportunity will be ahead of their

competitors in tightening their relationship with the subscribers and starting to make revenue on value added services.

With the WIB as a standard application in ROM from all SIM vendors all previous problems with STK are circumvented. SIM vendors have previously pushed for proprietary implementations with proprietary and difficult interfaces for service implementations. The WIB together with the corresponding Delivery Platform (WIG) drastically changes this as it provides one generic Internet based interface for service creation, independent of SIM suppliers.

3.1 WIB and WIG enabling Internet connectivity for 11.5G handsets

The WIG and WIB operate in two modes:

Request: Enables operator provided service menus on almost all handset on the market (phase 2+ and later). Service activation is done by the subscriber selecting an item in the service menu. The service typically includes a series of user interactions resulting in an action towards the network. The action could be a normal SMS, set up a call or more interactive Internet based services like prepaid top-up, horoscopes, banking, and so on. In the latter case the WIB sends ordinary URLs to the WIG server, which retrieves what the URL points to from the Internet, byte codes it, and sends the result back to the WIB. Using the WIG enables a range of capabilities such as location information and signing.

Push: The WIG offers access to advanced SIM based services (digital signing, location based information, call set-up and so on) to the Internet community using the push mode. The WIB acts very much like a WEB server in this case. The WIG receives a request from a web client (WML coded) over HTTP and converts the request to internal byte code format before the request is forwarded to the WIB. The request is responded to after execution in the SIM. An example is a notification that requires a user action, e.g., a certain stock has reached a threshold value and a notification is sent out with the option to sell or buy.

3.2 Extending the service spectrum with plug-ins

The WIB, as well as the USAT Interpreter, has an architecture that allows for the addition of so called plug-ins (as in the Internet world) to extend the service spectrum. Plug-ins are used to add functionality such as producing signatures, location information, file IO and other local SIM functionality. These plug-ins have until now been input into the SIM at personalization time as a static library with enhanced functionality.

3.3 WIB enabling dynamic menus in 11.5G

The efficient management of dynamic menus on the handset is maybe the most powerful feature of the WIB. It allows the operator to add an own menu structure on the mobile handset that follows with the subscription, e.g., if the user changes handset he will still get the same service offering in the new handset. With the WIB technology this menu can be easily managed by the operator or by the subscriber himself.

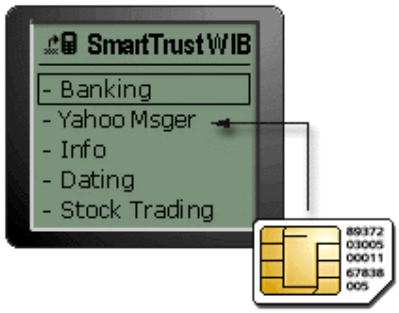

Figure 3. The WIB menu on a handset

Using the WIG it is also possible to optimize the split of the menu storage between the SIM in the mobile and Web servers in the network to achieve the best performance. By doing this you achieve:

1. A set of services that is not limited by the amount of space on the SIM card
2. Fast access to often used services as these menu entries are stored on the SIM
3. Easier re-configuration of services after loss of SIM card. Service configuration in the Web servers doesn't need to be downloaded
4. The architecture allows the operator, any third party or the user himself to add and delete services.

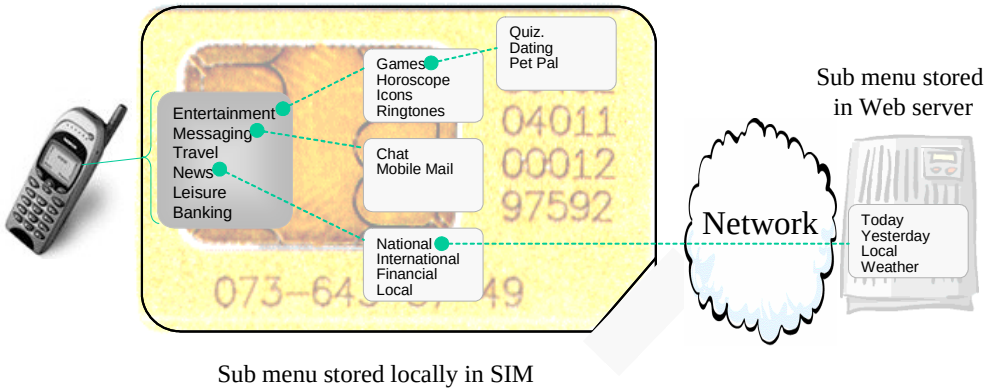

Figure 4. Storage of services both locally and remote on a web server

It is notable that this dynamic management of services is not only limited to WIG services, but it could also be any user services using SMS, voice call or even WAP (if handset supports the SIM Toolkit command LAUNCH BROWSER). It is a true dynamic menu and launch pad for operator provided services!

3.4 The WIB and security

The SIM is inherently secure as it is a smart card. It can perform secure atomic operations with access to a GUI, thanks to the SIM Toolkit. An example of such an operation is the signing of a text as one operation on the card. The card does not only sign the text; it also displays the text to the user and asks for the PIN before doing the actual signing.

STK together with a generic interpreter, like the WIB, adds a complete operator supplied crypto library for wireless applications. The SmartTrust Wireless Internet Browser already has the following security functionalities available and commercially implemented:

1. Symmetric 3DES based signatures (Message Authentication Codes)
2. Symmetric 3DES based field encryption
3. Derived Unique Key Per Transaction (DUKPT) for banking transactions
4. Master/Session key handling
5. WAP SignText based RSA signatures
6. RSA signing of hash values (used for signing material presented in other media)

7. RSA based decryption of public keys to be able to decrypt documents and contracts that are presented in another media.

The WIB security functionality complements the WAP application level security schemes. WAP only includes a simple signing operation of the type ‘What You See Is What You Sign’ equivalent to item 5 in the list above.

It should also be noted that the security plug-in functionality for the WIB has been accepted as one of the standard plug-ins to the USAT Interpreter by 3GPP T3.

4 UICC and Java for Smart Cards

The UICC is a platform allowing for multiple smart card applications running on the same card. This makes it possible to have parallel telecommunications applications as well as other smart card applications on the same card.

Java is emerging as the interoperable environment on the UICC. Java environment on the UICC opens the possibility to download interoperable applications on all SIM cards that are compliant with Java Card 2.1 and the UICC/SIM API specification from ETSI. Applications not compliant with the UICC/SIM API require a corresponding application component in the terminal. The WIM is one example of such a non UICC/SIM API application.

The UICC is specified by Smart Card Platform (SCP) standardization project. SCP is administrated by ETSI and supported by 3GPP, 3GPP2, GAIT, T1P1 and TR45. The UICC is used as the common smart card platform for CDMA, UMTS, CDMA 2000 and other mobile telecommunications systems.

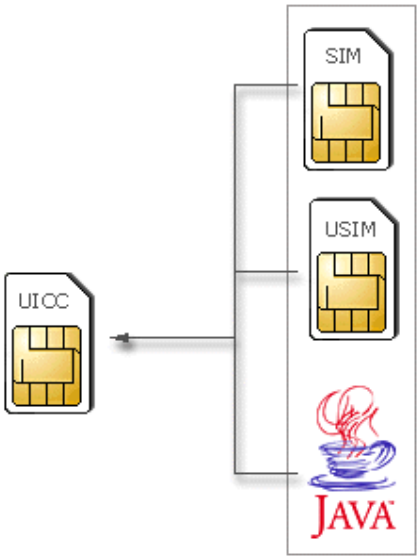

Figure 5. The UICC – a true multi application smart card

4.1 Java as the platform to develop SIM Toolkit applications

Java could be used as a generic way to develop STK applications (using the SIM API). STK applications are typically associated with a menu entry and some sort of communication with the outside world using the telecommunications network, e.g., voice, SMS, GPRS or USSD. The most common STK application is just a menu entry for sending a short message (SMS).

Although it is perfectly possible to use Java to develop STK services it has some drawbacks, compared with developing the same services using the WIB. Some of the drawbacks are:

1. Service development is much more complex than using a mark up language, such as WML.
2. STK applications developed using Java technologies require much more space than corresponding applications developed using the WIB technology.
3. Java does not include any application language for the communication between the SIM and the Server component. Again we face the same client/server issues as with traditional dedicated STK applications for each service.

What's positive with the Java technology, compared with the SIM vendor specific application environment, is that the operator will not depend on only one card vendor since Java, at least in theory, is interoperable between different SIM vendor platforms.

4.2 Remote Application Management

As we see more and more UICC/SIM based on Java technology on the market the need for interoperable remote management of applications is obvious.

The Java applet management follows the same trend as the remote file management on the SIMs. The first cards had no possibility of OTA management, followed by SIM vendor proprietary implementations and finally the standardized procedures as described in GSM 03.48.

Remote Java applet management is specified in the ETSI/3GPP specification GSM 03.48. The command set used is based on the Open Platform specifications from Visa International. The Open Platform Specifications are now being moved to the Global Platform multi industrial initiative.

5 The WIB and Java

How do these technologies compare?

By listing the differentiating characteristics we see that they complement each other.

The WIB offers:

1. An easy to use mark-up language to develop compact and efficient mobile services, hiding the complexity of the SIM and telecommunications environments for the service creator.
2. A generic application protocol for the communication between the client, the SIM, and a server component.
3. Libraries extending the basic command set with enhanced functionality such as signing, encryption, location information and call control, making advanced SIM functionality accessible to any service creator
4. Dynamic menu handling allowing storage of sub-menus locally on the SIM and/or remote on a web server, thus extending the service spectrum.

Java offers:

1. A unified programming environment, for native UICC applications (applets). The applets could be based on the SIM/USIM API as well as non SIM/USIM applets, e.g., a WIM applet.
2. A standard procedure, using GSM 03.48, for remote management of the applets on the card

There is basically no overlap between the two technologies. On the contrary they complement each other to form a complete technology platform for developing solutions using SIM Toolkit technology and Java technology. Using the WIB/WIG for driving the user interface and for the communication with external servers in a telecommunications environment and Java for development, and dynamic management, of plug-ins for the WIB makes a perfect match.

5.1 Using Java technology for dynamic management of WIB plug-ins

The WIB and the USAT Interpreter have the possibility to add a library with additional functionality using plug-ins. These plug-ins have so far been developed using the SIM vendors' proprietary development environment and stored into the card during personalization.

With Java and GSM 03.48 remote management the following can be achieved:

1. A plug-in can be developed in one language for all SIM vendors platforms. This enables third parties to developed add-on functionality that could be added to the WIB/USAT Interpreter basic functionality on any Java Card 2.1 compliant SIM.
2. The plug-ins can be managed dynamically during the life cycle of the SIM. A set of plug-ins is installed at personalization, another set could be installed at Point Of Sales (POS), and the operator could also allow the subscriber to add new plug-ins OTA using the GSM 03.48 mechanism when subscribing to new services.

6 The WIB and Internet technologies

GPRS, 3G or 4G all effectively provide an IP connection to the handset. We will actually have real Internet to our handset without the need to set up a data connection over the voice channel. All the standard Internet based applications can be delivered to wireless devices. The mobile device becomes an Internet terminal with a smart card reader and a SIM card.

These Internet technologies do however lack one essential feature that already exists in the mobile environment – namely the secure subscriber identification. It is in this cross-section we can see a lot of interesting use-cases for the mobile operator as the operator controls the means for the subscriber identification, i.e., the SIM and it is derivates USIM and RUIM. The SIM is the bearer of personalization data as well as a tool for advanced services like security and other telecom-related services such as call set-up, location based services and roaming management. A SIM with a WIB is an excellent complement for adding mobility and security features to the mobile Internet, e.g.:

1. It is a container for the subscriber's personal data;
2. It is the perfect tool for transaction based services that works wherever you are and whatever network you are roaming into;
3. It is ideal for secure call control. One example is the set-up of a telephone call initiated from a web browser, e.g., after a look-up in the yellow pages;
4. It adds the authentication that is needed to connect to VPN, or use e-mail, anywhere at anytime;
5. The WIB push service adds the possibility for notification services and remote launch of applications on the mobile device.

7 Glossary

11..5G	2G + 2.5G + 3G + 4G, the multi technology environment
3DES	Triple DES (Data Encryption Standard)
3G	Third Generation, meaning the third mobile generation
3GPP	Third Generation Partner Project , a 3G standardization body
ETSI	European Telecommunications Standardization Institute
GAIT	GSM/ANSI-136 Interoperability Team
GPRS	General Packet Radio Services
GSM	Global System for Mobile communications
HTTP(S)	Hypertext Transfer Protocol (s) over Secure Socket Layer
IP	Internet Protocol
OTA	Over The Air
PKI	Public Key Infrastructure
ROM	Read Only Memory
RSA	Algorithm named after its inventors: Rivest, Shamir and Adleman
RUIM	Removable User Identity Module (3GPP2 equivalent to SIM)
STK	SIM application ToolKit
SIM	Subscriber Identity Module
SMS	Short Message Service
URL	Uniform Resource Locator
UICC	Universal Integrated Circuit Card
USAT	Universal SIM Application Toolkit
USAT Interpreter	ETSI Standardized version of the WIB
USIM	Universal Subscriber Identity Module
UMTS	Universal Mobile Telecommunications System
WAP	Wireless Application Protocol
WIB	Wireless Internet Browser
WIG	Wireless Internet Gateway
WIM	WAP Identity Module
WML	Wireless Markup Language

Document number: CTO 02:001
Revision: A