



## **Integrating the SIM Card into J2ME as a Security Element**

A smarter approach to secure Java™ mobile  
applications: JSR177

A Gemplus White Paper - April 2005

## Table of Contents

<b>EXECUTIVE SUMMARY</b>	<b>3</b>
<b>INTRODUCTION</b>	<b>4</b>
<b>1 A QUICK OVERVIEW OF THE JSR#177 FOR J2ME</b>	<b>5</b>
<b>2 USE CASES</b>	<b>6</b>
2.1 MANAGE USERS' RIGHTS & FIGHT PIRACY (SIM SENTRY INITIATIVE)	6
2.2 MOBILE BANKING	7
2.3 CORPORATE SIGN-IN PROCESS AND OTP (ONE TIME PASSWORD)	7
<b>3 CONCLUSION</b>	<b>7</b>
<b>4 CONTACTS</b>	<b>7</b>

## Executive Summary

While the use of an Open Operating System (OS) platform is not necessary for low-end devices such as those handling voice-only services or supporting simple data applications, this platform is crucial for managing intensively data-enabled phones. In a market where mobile phones increasingly support data communications and wireless networks promise more flexible mobility solutions, higher bandwidth and network interoperability, Open OS will be required to enable mobile devices to efficiently host and manage different applications and services enabled by wireless networks.

There are so many OS competing in the market for handheld devices. Some are derived from desktop OS and progressively downgraded to fit different handheld devices. This is the case of products such as Windows Mobile and Linux. On the other hand, Palm Source was specifically designed to work on handheld devices (PDAs) but now increasingly runs on connected handhelds. Symbian designed its OS specifically for the smartphone market. Additionally, SUN Microsystems' Java technology based SavaJe™ OS provides wireless developers with an optimized Java platform for application development at the hardware level. Other thin applicative runtimes such as BREW, which can be considered as an Open OS, are also fighting to gain market share in the handset market but will be restricted to application specific devices.

On top of the OS, a growing number of mobile phones support now the Sun's programming language (J2ME: Java 2 Micro Edition) that is improperly considered an open OS. Java is in fact an open, extensible programming framework. It enables developers, mobile operators and third-party solution providers to create applications.

From their origins, the mobile open OS environments have been designed independently of Smart Card capability; as a consequence, mobile handset applications can not take advantage of the (U)SIM execution platform. However both technologies offer, by nature, many bridges available for Content Providers and Operators through standard APIs.

Today, the *Security And Trust Services API* (aka JSR#177) allows J2ME applications to benefit from Smart Card services. This specification became public in mid October 2003 and supporting devices are expected in 2005.

This white paper addresses the JSR177 Smart Card communication API and set of cryptographic high level APIs useful to benefit from (U)SIM card services such as safe runtime execution, safe storage and cryptographic operation handling in order to perform user authentication, non-repudiation mechanism, signature generation and verification, certificate management, etc.

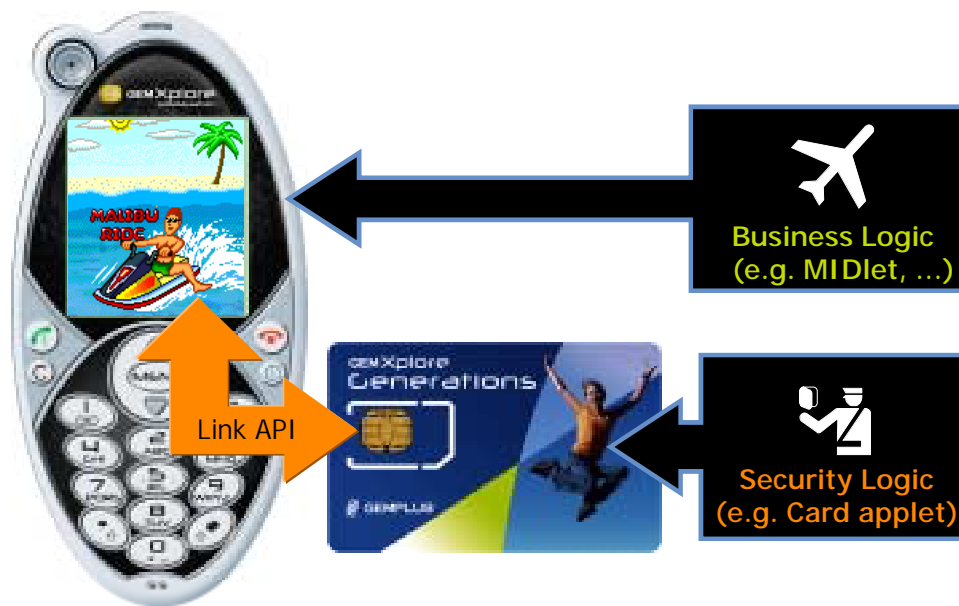
## Introduction

A Smart Card communication API on top of J2ME enables a mobile J2ME application (i.e. MIDlet) running on the handset to access to certain services, data or applications running into the (U)SIM card.

In order to ease signature and low level cryptographic services provided by the (U)SIM, a second high level API helps the J2ME application leverage the card cryptography capabilities without handling low level functions.

By using both APIs, the J2ME application designer applies the most appropriate design pattern to best fit this client/server architecture: *The distributed application!*

As shown in Figure 1, the mobile application consists of the client (The MIDlet) and a server (Smart Card applet). To benefit most from this architecture only the sensitive part of the mobile application must reside in the Smart Card rather than the handset.

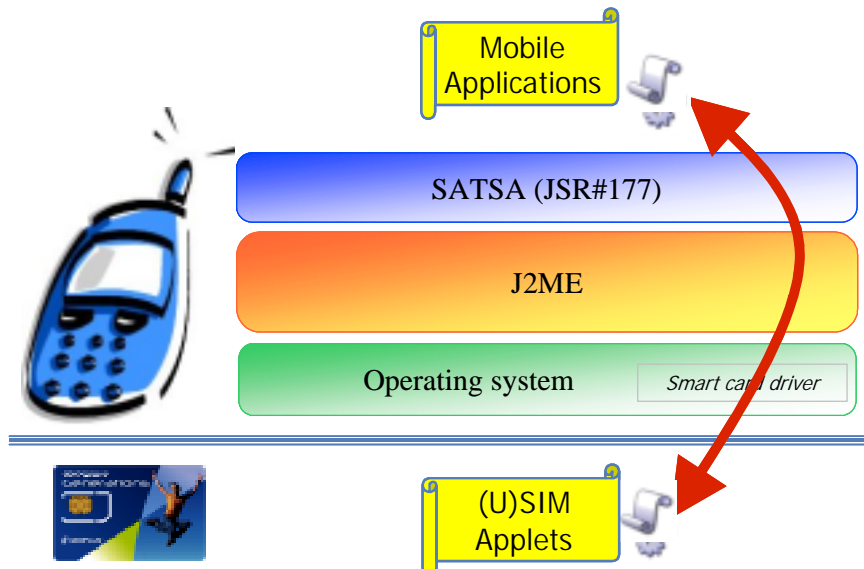


- Figure 1: Distributed application scheme (MIDlet + Smart Card applet) -

Before introducing the JSR177 use cases, it is interesting to start with a quick overview of the JSR 177 API (Security And Trusted Services API for J2ME).

# 1 A quick overview of the JSR#177 for J2ME

A new J2ME specification called JSR#177 (aka SATSA: Security And Trust Services API) opens an important and strategic communication channel from MIDlets to Smart Card applications. In this way, the Smart Card becomes the “Security Element” of the distributed application and is available for each J2ME application running on the mobile phone to perform signature operation, user authentication and secure processing in general.



The JSR#177 specification consists of 4 independent “building blocks” and 1 recommended practice:

- **APDU**: Defines an API to support communication with smart card applications using the ISO7816 APDU protocol on each logical channel except the default one (channel 0). As a reminder, this default channel is dedicated to the Telecom application for (U)SIM cards. It is still possible, through a specific mode, to use the logical channel 0 by sending SIM Toolkit envelopes.
- **JCRMI**: Defines a Java Card RMI client API that allows a J2ME application to invoke a method on a remote Java object running in the Smart Card.
- **PKI**: Defines an API to support application level digital signatures and basic user credential management (X509 and CSR). To provide broader use, this API is independent of the type of Security Elements that are utilized by the J2ME device but is mapped on WIM functionality.
- **CRYPTO**: Defines a generic low-level cryptographic library for J2ME as a subset of the Java Cryptography Extension (JCE) defined for J2SE. This subset addresses the basic cryptographic primitives that are required to implement encryption, decryption and signature validation. It is important to mention here that the (U)SIM card is not involved into this module, then we strongly advise the developers to use the APDU/JCRMI modules instead if they need to handle sensitive and/or valuable data.
- **Access control policy engine** (Recommended practice): The access control model is applied to the API of the SATSA-APDU and SATSA-JCRMI packages to control access to smart card applications. This model is designed to protect Smart Card applications from malicious J2ME applications, to allow a J2ME application to select a Smart Card object for temporary exclusive usage and to safeguard PINs from improper usage by the J2ME application.

The Smart Card communication API is composed of the 2 following building blocks: **APDU** and **JCRMI**.

To allow MIDlets to communicate with the Smart Card, the Generic Connection Framework (GCF defined in CLDC) is extended by adding 2 new protocols: **APDU** and **JCRMI**.

## 2 Use cases

JSR177 enables new applications and services to emerge in which the business logic (MIDlet) is split up from the security logic (Smart Card application). This will strengthen securing mobile application execution, and will offer mobile device value added features thanks to the (U)SIM card. As an example, it will allow secured distributed applications between the mobile device and the smart card.

Hereafter are some use cases illustrating the need to have a distributed applications between the handset and the (U)SIM.

### 2.1 Manage users' rights & fight piracy (SIM Sentry initiative)

A telecom operator offers J2ME services on its portal. He provides application providers with a "piracy and copy protection" service compliant with the SIM Sentry specification endorsed by the SIM Alliance according to GSM Association requirements.

In order to purchase and application, the user connects to a WAP site and downloads a trusted J2ME game (certified by a trusted domain: cf JSR118). The game is deliberately split in two parts: A MIDlet and its corresponding smart card application that are respectively downloaded on the handset and on the (U)SIM card. To run the game, the MIDlet accesses its corresponding card application (aka dongle agent) thanks to SATSA Smart Card Communication APIs (APDU or Java Card RMI).

#### Hacking protection

In the case of a "man in the middle attack" a hacker intercepts the game and then attempts to modify it to make it free of charge and break-down dependencies with the content provider. The hacked MIDlet is installed. When the MIDlet is run, the user is prompted that the application is untrusted and as a consequence, does not have access to the required Smart Card application (aka dongle agent). The game no longer works because the (U)SIM does not provide the needed information to the MIDlet necessary for execution.

By using SATSA APIs along with MIDP platform security mechanism ("A J2ME application must be granted a permission to use the SATSA API"), we can build a copy protection mechanism.

If the (U)SIM card contains a part of the application logic of the MIDlet, a hacker who tries to remove the copy protection of the MIDlet would turn it into an untrusted MIDlet which can no longer access the (U)SIM card and needed information.

#### Copy protection

If user A forwards the MIDlet to user B using IRDa/Bluetooth/MMC/SDcard connection, the cloned MIDlet will use SATSA Smart Card communication APIs to try to access its corresponding needed application on the Smart Card. The application on the Smart Card and the corresponding license are not available, so the game will not work on the destination device.

As a conclusion, cloning of J2ME application by a user from one handset to another is impossible because of the control and secure management of SIM Card applications by the operator.

Beyond copy protection and hacking, the (U)SIM does not only store the certificate but also information related to the game such as how many lives they have, special powers won, credits, etc. These will be carried over to the next level ensuring a smooth transition from one game version to another.

## 2.2 Mobile Banking

Banks are willing to deploy mobile banking solutions on the latest J2ME handsets, but are worried that this technology is not secure enough. The banks require high levels of security to handle user credentials, manage authentication and non-repudiation services, and perform low level cryptographic operations in order to build the necessary levels of trust between the customer, bank and mobile operator. This is where the inherent security of the SIM plays a vital role.

Java Card™ (U)SIMs are already in use in financial applications, with notable success in countries such as Belgium & South Korea. The (U)SIM, present in every GSM and 3G handsets, and well known for its tamper resistance, is used to store the part of the software containing the strong authentication and user credentials.

This is linked to the application on the handset, which ensures the "look and feel" for the end-user experience. The (U)SIM is able to generate digital signatures as it interacts directly with the handset.

Financial data, such as account status, stored in their mobile device, can even be viewed off-line when there is no network coverage. Banks and their customers will therefore have differentiating services and peace of mind when using the mobile channel to distribute them.

## 2.3 Corporate Sign-In process and OTP (One Time Password)

The (U)SIM application manages employee's profile and rights like a corporate badge does currently. The (U)SIM card can be also used to generate an **OTP**.

Then, the couple handset/USIM acts as a badge and a reader that you can store in your pocket.

By using a bluetooth connection, the user can use this "e-badge" to ensure the corporate security required by classic IT systems on his/her PC (VPN authentication, password management, etc.).

This e-badge can also be used to manage mechanical access into secured and sensitive areas.

## 3 Conclusion

The use cases discussed in this paper show only a portion of the possibilities the JSR177 provides to enable mobile applications. User rights and content protection are critical to mobile application distribution in a wireless environment. Mobile banking and corporate sign-in/OTP open new opportunities to Mobile Network Operators to offer services that bridge the gap between the USIM and other traditional smart card applications.

The standards are in place now, and the terminals to support the interface will be available in the near future. JSR177 will allow Mobile Network Operators to realize the full advantages of the secure tokenization that the USIM provides, while maintaining control of that token and the potential revenue streams that it generates.

## 4 Contacts

Remy CRICCO - [remy.cricco@gemplus.com](mailto:remy.cricco@gemplus.com)

Yale VINSON (North America) - [yale.vinson@gemplus.com](mailto:yale.vinson@gemplus.com)

**Gemplus - Telecom Business Unit**



## About Gemplus

Gemplus International S.A. (Euronext: LU0121706294 - GEM and NASDAQ: GEMP) is the world's leading player in the smart card industry in both revenue and total shipments (source: Gartner-Dataquest (2004), Frost & Sullivan, Datamonitor.). It has sold over 5 billion smart cards.

With security at its core, and 2400 patents and patent applications produced by its innovative R&D team, Gemplus delivers a wide range of portable, personalized solutions in areas including Identity, Mobile Telecommunications, Public Telephony, Banking, Retail, Transport, Healthcare, WLAN, Pay-TV, e-government, and access control. Gemplus' revenue in 2004 was 865 million Euros.

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