

Java Card™ & J2ME Integration

A smarter approach
to Wireless Java™

"The JSR177 ecosystem"

A Gemplus White Paper
February 2005

1. Introduction

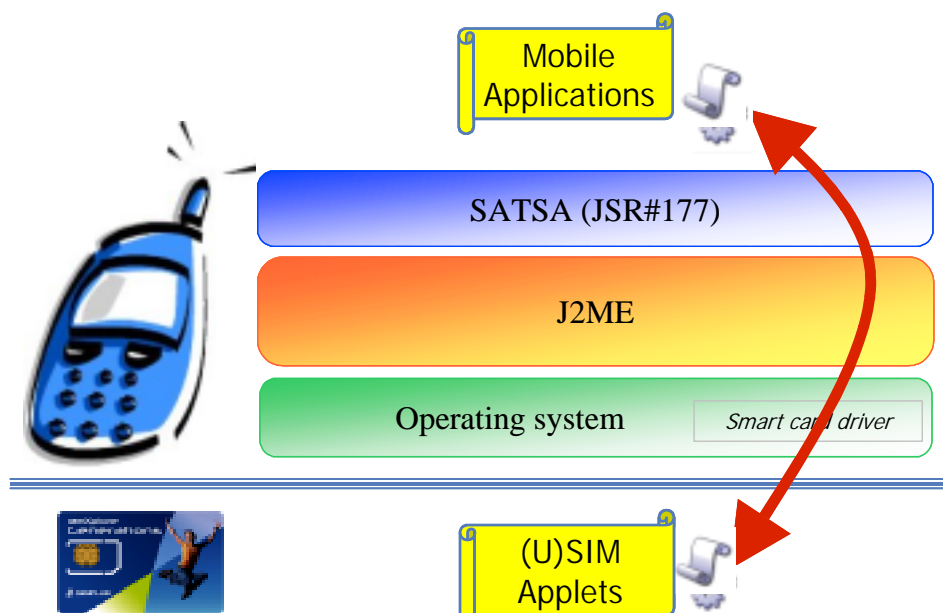
Java applications now represent a major technology and service trend in the wireless industry. In tune with Operators' 3G service strategy, the deployment of Java powered handsets and Java Card (U)SIMs is growing fast. Java enables them to design and deliver more responsive, interactive and dynamic applications for their subscribers. The roll-out of two open execution platforms (J2ME & Java Card) within the subscribers' device means that every end-user will soon be able to discover and enjoy new kinds of interactive, graphical and secure applications.

In 2006 data services are set to make up around a third of total operator revenues, while total voice revenues should only increase slightly (source: Frost & Sullivan). Java appears to be the language of choice. Millions of subscribers are already taking advantage of the creativity and flexibility of Java-based mobile services. The direct impact of such downloadable Java applications has had a tremendous increase on data traffic.

Java downloads can only grow as deployment of Java handsets reaches critical mass with over 438 million in the field as of June 2004 (OVUM). 85 operators worldwide have deployed Java services, supported by 200 models from 27 device vendors representing a combined 80% market share (sources: NOKIA and SUN Microsystems). To take advantage of the opportunities offered mobile network operators are in the process of defining their provisioning strategy, exactly how they will provide access to these applications and how the security & payment for these applications will be handled.

Gemplus, the world's number one provider of solutions enabled by smart cards, bring its lengthy experience providing security, trust & customer proximity for the mobile telecom market to the established field of Wireless Java.

This white paper explains how a J2ME specification called JSR#177 (aka SATSA: Security And Trust Services API) will definitely open an important and strategic communication channel from Java Mobile Phone applications (i.e. MIDlets) to Smart Card applications. By this way, the Smart Card becomes the "Security Element" of the whole system and is available for each MIDlet application running on the mobile phone to perform signature operations, user authentications, and secure processing in general.



2. Creating new applications markets

By opening and specifying the right level of communication between the Java execution environment in the mobile phone and the Java execution environment in the (U)SIM Card, new markets and business models for applications are emerging. This should benefit Operators, content providers and subscribers alike.

The (U)SIM card brings added value to the Java Wireless World through administrative or application-based roles.

Off-line communication between the mobile phone and the smart card is also extending the potential interactions between such distributed applications even with no network coverage. An end-user could play a game in the subway and store the game score on the card for future transmission as soon as the network becomes available.

The (U)SIM card can also store the profile of a game player such as the extra lives acquired, different weapons gained, the sequence of episodes purchased which all contribute to making the application dynamic, secure and personalized. This helps smooth the transition from one game version to another by ensuring continuity of the player's profile.

Java applications in the mobile phones will be able to take advantage of the secure Java applications stored on the (U)SIM card. With the convergence between wireless and financial markets, Java MIDlets in the phone will be able to benefit from the payment/transaction capabilities of the smart card. For example, it could be possible to develop and launch an airline ticketing Java application combining a payment, loyalty and ticket storage function in the card with a graphical flight schedule Java application on the phone.

For mobile commerce Java applications, the end-user will be able to automatically transmit pre-formatted forms for retailers via the (U)SIM card profiling capabilities. In term of profiling management, end-users will be able to store shipping and billing information, payment methods, receipts management, user interface preferences, etc.

Today, operators use SIM Toolkit (STK) as a technology to build menus and personalize handsets with their services. However, this technology is strongly dependent on standards implementation by handset manufacturers and it can sometimes take a long time for new MMI (i.e. user interface) oriented commands (such as icons, color text etc.) to be supported by handsets.

An alternative to STK technology for operators could be a standard MIDlet provisioned on every JSR 177 handset to build attractive menus which can be personalized by the (U)SIM. This MIDlet would interpret information on the card to build menus with icons, animations and sound. This means that take advantage of the J2ME world can be triggered (downloading of data/synchronization, interaction with remote hosts, etc.)

This would enable the operator to build attractive menus on their handset while limiting the cost of handset personalization.

A further benefit would be increased flexibility to the existing Sandbox and function sharing between MIDlets. The idea here is not to break such a well-designed mechanism but to offer the possibility for different MIDlets to access the same Java Card applet therefore creating a secure communication channel. For example, it would be possible to have a single card-based e-purse function that could talk and interact with various MIDlets.

The main benefits of this new vision are two-fold:

1. Enlarge the wireless Java application market by:

- Speeding-up end-user adoption of services
- Take advantage of the push capabilities of the (U)SIM card to launch communication with subscribers
- Integrating two worlds of Java developers to allow content providers to seamlessly deploy applications across 2 mobile execution platforms

2. Build a smarter wireless Java application market:

- Proposing a secure and dynamic framework to enable distributed applications between a server, handset and card.
- Leveraging the unique security capabilities of the (U)SIM Card environment to extend Java MIDlet existing value proposition.

3. Viral marketing controlled by the (U)SIM

Once applications have been downloaded from the Operators' server or that of a trusted 3rd party, there is nothing to stop the subscriber from sharing these applications with their friends and family. In fact, in order to create the necessary critical mass for Wireless data services, Operators want to empower their subscribers to share, buy or trial new services while keeping control over their distribution.

In order to successfully deploy new Java services, and control their access once in the field, Operators need a way of tracking the applications & identifying end-users.

By distributing the application between (U)SIM card, handset and server, the owner of the application can allow execution and sharing of applications on their terms.

For example, if the original subscriber sends their latest Java game to a friend during a free trial, the Smart Card will allow access for a limited time before prompting the new user to buy the application and blocking execution until payment is received.

The benefits of this distributed architecture are two-fold; firstly, the Operator will be able to employ viral marketing for their new services and secondly by allocating space for each subscriber on a remote server they create a network-based personal repository and thus increasing their application storage capacity.

The Java Card applet identifies the owner of the mobile content through its "watermark" and can therefore monitor remote applications and manage access to the content.

Finally, (U)SIM cards, by enabling m-payment schemes (prepaid, e-purse, m-banking, credit card, etc.), will be able to support a range of robust yet flexible billing mechanisms tailored to a defined market segment and the Operators' needs.

4. End-to-end security

Current wireless devices are becoming more like personal computers. They have open Operating Systems, are well documented and have freely available software development kits. They can store a lot of confidential and personal information. Mimicking the PC world this means they are open to attack. Several malicious codes programs and Trojan incidents have proven that it is possible to create viruses that run on both a PDA and a mobile phone. It is therefore crucial for mobile operators to provide a secure infrastructure in order to build consumer confidence in their network.

With the increasing amount of data that accompany GPRS and 3G, there is a need for enhanced security. In order for mobile business to really take off it needs to come with the right level of security to create an environment of confidence between suppliers and customers. In such an environment end-users and handset manufacturers can rest assured that they are not downloading malicious applications onto the phone while operators and content providers can identify users and manage copyright issues. The network operators' top priority is to maintain the integrity and security of their delivery chain.

Smart cards provide a portable, secure way for operators and mobile service providers to offer trust and identity proofing. The smart card is the best way to ensure privacy of data, security of transactions and non-repudiation.

Beyond this, it is also the most appropriate platform for securing data applications while providing a certain level of control to the carrier within the new eco-system. (U)SIM cards can guarantee the integrity of the downloaded MIDlet with an authentication of such MIDlets by the (U)SIM through the operator's certificate. (U)SIM cards ensure a secure execution environment and manage the MIDlets' digital rights.

The card plays a fundamental role in enabling service provisioning and offering a secure payment platform. Its unique value is in managing network and content access, privacy and profiling, trust and payment.

The arrival of the extended on-line relationship to the wireless market requires a higher level of identification and authentication. The (U)SIM enables identity proofing for Internet-based services and security (network access control, anti-viral systems, etc.). It is also able to identify the end-user rather than just the wireless device in order to guarantee payment for transactions, reduce fraud and provide digital receipts for purchased goods

5. The current standardization situation

Until JSR 177 was definitely approved in June 2004, there was no standardized integration of Java Card into the J2ME specifications. By looking at the strong points of each of the Java standards, Java Card and J2ME can now be used in tandem to create the "open" and "secure" infrastructure that operators and content providers need in order to increase their ARPU and diminish costs. At present, the specifications of this infrastructure just exist as leading operators, handset manufacturers, content providers and (U)SIM suppliers have been working together to make it a reality.

The specifications were first published in November 2003 and their implementation has been supported by the relevant test suites since July 2004. As the standardization process has received strong support from many different actors in the wireless sphere it looks set for implementation in wireless Java phones in late 2005. Nokia and Vodafone have launched a new initiative (MSA) to lead the roadmap for mobile Java standards. This aims at creating a mobile service architecture and platform definition for high volume wireless handsets (CLDC configuration) and for advanced mobile handsets (CDC configuration) continuing the work started in JSR 185 and enhancing the definition with new technologies such as JSR 177. The anticipated schedule for delivering this architecture is September 2005.

Gemplus was the first smart card supplier to join the standardization process. As part of the working group, Gemplus provides its expertise to ensure that the resulting standard is quickly achieved and meets market needs.

6. Conclusion

Value and attractiveness of applications are the keys to ensuring consistent revenue streams for operators. The (U)SIM card is the only interoperable, trusted device in the wireless ecosystem and can be used to help operators consolidate their position in the mobile application value chain.

Along with the perpetually quickening pace of development in every technology field, the right Java application strategy needs to be developed now. With the right strategy, operators can be first to market and start gaining valuable field experience.

In addition to its current products and applications, Gemplus has placed special emphasis on bringing creativity to your future wireless applications world.

In other words, we are ready to show you how distributed Java can become a reality for your business through the use of the JSR177 API. Gemplus is fully committed to our customers in the creation of their next wave of high-value and attractive applications.

Glossary

- GSM Association: a global trade association serving the world's GSM mobile operator member community by promoting, protecting and enhancing their interests and investments.
- JCP - Java Community Process: an open organization that holds the responsibility for the development of Java technology.
- SIMalliance: a non-profit organization created to promote the benefits of (U)SIM Cards and (U)SIM-based services.
- Sandbox: The original security model provided by the Java platform
- J2ME : Java 2 Micro Edition
- CLDC: Connected Limited Devices Configuration
- MIDP: Mobile Information Devices Profile
- MIDlet : A Java application running on MIDP handset

Legal notes

Java & Java Card & J2ME are registered trademarks or registered trademark of Sun Microsystems, Inc. in the U.S.A. and other countries.

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 4 billion smart cards.

With security at its core, and 2400 patents 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 2003 was 749 million Euros.

www.gemplus.com