A Java Card Forum White Paper

November 2013

Java Card Platform vs. Native Cards

Executive Overview

Java Card technology is widely used in high-end card markets, in which it helps increasing the value of cards through the deployment of value-added services. In these markets, issuers benefit from Java Card technology, and from the experience built over the past 15 years by vendors, in particular around quality and security.

In low-end markets, on the other hand, such value-added services are not as common. We show in this paper that Java Card can be present in such markets, simply by removing the ability to add applications after the issuance of the card. By doing that, issuers can keep most advantages of the Java Card platform, including in particular better time-to-market, as well as the ability to design a range of card platforms in their offers, ranging from a closed platform for mass deployment to a fully open platform for premium customers.

Introduction

Java Card provides two main features: a standard development interface, and an open and secure runtime environment. These features result in three main advantages, described in this white paper:

- Standardized services. With Java Card, service developers can write applications that are guaranteed to run on products from several card vendors, limiting testing requirements.

- Deployment flexibility. With Java Card, issuers can securely deploy new services throughout the lifecycle of their cards, and not only before issuing the cards.

- Economies of scale and scope. With Java Card, smart card issuers can maximize the reuse of value-added services across various markets.

These advantages apply to all markets, including those where Java Card is in direct competition with low-end products. We will specifically focus on the advantages brought by a Java Card platform to these markets.

Native Cards

Single-Application Cards

Before 1995, all cards contained a single application, which usually managed a simple file system, while allowing some security-related operations to be performed using the content of this file system, such as data encryption or signature, or PIN-based user authentication.

So-called multi-application cards simply divided the file system into several directories, allowing different services to be hosted on the same card. But ultimately, every card ran a single piece of software, mixing the application code with the operating system code in a highly optimized way.

Every vendor had its own implementation of each application. An issuer who wanted to source from multiple providers had the obligation to perform extensive tests on each product at the application level, which led to additional costs and delays, in particular when launching a new application.

Card Application Frameworks

With the apparition of the SIM Toolkit framework, the number of applications exploded, and vendors started to develop proprietary application frameworks to speed up the development of applications. However, application testing on non-interoperable platforms became a significant issue for network operators.

Java Card appeared in 1997, and rapidly became the reference card application framework. Within a few years, the SIM community had produced a complete framework to develop interoperable applets on top of this core framework, and Java Card-based SIM cards started to be deployed soon after 2000.

The Java Card Platform

The Foundation of Smart Card Ecosystems

Interoperability

With Java Card, card vendors started to provide interoperable SIM Toolkit implementations, allowing network operators and application developers to benefit from this interoperability in many ways:

- A single platform to develop, based on the Java Card specifications and on the vertical specifications issued by ETSI and later by 3GPP,
- A single set of acceptance criteria, such as the *Interoperability Stepping Stones for SIM Toolkit Applications* developed by the SIMalliance, and
- A single set of applications portable across several Java Card platforms.

With this standardization, issuers have the ability to select a SIM card on well-defined and measurable criteria, and they can also easily develop and test new applications. Over the years, the development of standardized test suites, complementing Oracle's Compatibility Kits, has further enhanced the level of interoperability between the different Java Card implementations.

Vendor independence

The competition shifted to the quality of the platform and of the services implemented on top of the platform, greatly increasing the value of the SIM Toolkit platform for network operators, and allowing card vendors to sell more sophisticated cards in large numbers. As a result, over one billion SIM cards are issued every year with a Java Card platform and applications.

Reuse of services

More recently, the NFC ecosystem has emerged. Secure NFC services, which offer smart card-like services in mobile phones, can be implemented on many types of secure elements, from SIM cards to embedded secure elements and SD cards. Java Card makes the link between these platforms, allowing them to run the same services, and to be certified using the same security criteria, defined globally by the industry.

A striking example is mobile payment. With NFC, the payment provider is usually not the card issuer, and moreover, several payment providers are represented on the same card. This is only possible because the level of interoperability between the different cards is

sufficient to allow a single application to run on different cards. And this interoperability goes further than simple functional behavior, as these applications also have stringent performance and security requirements, which must be met by all implementations.

Simplified security certification

In the payment card industry, security certification has been a growing concern since 2000 with the appearance of power analysis attacks, later amplified by recent advances in fault attacks. Card vendors spend more time and money on complex security certification schemes.

Java Card is very useful in this context, first by separating the certification of the Java Card platform and of the applications running on it. The complex platform code is certified once, and the certification of individual applications it simplified. More recently, some payment actors have developed generic Java Card applications, making it even easier to certify these applications on Java Card platforms that met their security requirements.

Making Cards More Valuable

A smart card is an asset for its issuer, whose interest is to maximize the value of the cards it issues. The basic value of a card is associated with its main application, such as a debit/credit application in the banking area, or a network access application in SIM cards. This initial value is typically linked to risk management considerations, where the use of a tamper-resistant smart card strengthens the security around a business model.

Innovative card services

With Java Card, issuers are given the possibility to make this asset more valuable. They can provide additional services to their customers, for instance by adding an application that generates one-time passwords on payment cards. They can also allow third parties to deploy services on their cards, in exchange for a fee, as operators in many countries are doing for NFC services. With SIM cards, network operators can also use SIM Toolkit applications that optimize their core services, for instance to offer roaming options to prepaid customers.

New business models

The Java Card platform also enables innovative business models. For instance, the mobile wallets that are used on NFC phones contain code from several payment networks on the same secure element. This is made possible by the Java Card platform, which provides a complete model for running several applications on the same card, guaranteeing their

isolation if their providers don't trust each other. The Java Card security model has allowed payment networks and other actors to agree on a common set of security requirements and security certification procedures.

Time to market

For an issuer, deploying a new product based on a Java Card platform can be very fast, especially if the product uses applications that have been previously deployed. The issuer simply needs to select the most appropriate Java Card platform for its deployment, and define the applications to be used on it. Testing time is reduced by first running acceptance tests on platforms.

If a security certification is required, the gain can be even greater, as the issuer can start from an already certified platform, and simply certify the applications that he added to it. This process, known as composition of certifications, is widely known by accredited laboratories and consultants, and can be very efficient.

Improving Quality, Security, and Stability

The Java Card specifications are available to the community, including academics as well as developers. The availability of Java Card has made it possible to include smart cards in computer security curricula, allowing students to get hands-on experience with smart card application development.

Quality through openness

Beyond teaching, the availability of Java Card specifications has triggered academic work around the topic. Because the Java Card platform is so small, it has been possible to formally prove results on the platform, identifying possible improvements on the way, and ultimately making the platform better.

Security through openness

The most interesting academic results have been obtained on security topics. Several laboratories around the world have performed some of the strongest possible attacks on a variety of Java Card products, and suggested countermeasures to be included in future products.

For instance, attacks on virtual machines and application frameworks have mostly been performed on Java Card products, allowing vendors to gradually increase the security of their offer over the years. This openness has also benefitted the testing and certification community. Several laboratories and test tool providers have developed security test suites

and frameworks for Java Card, allowing issuers to get a high level of assurance regarding the interoperability and security of the Java Card platforms they deploy.

Ready for security certification

The impact of the Java Card platform has been even greater in the evolution of the Common Criteria security certification process for smart cards. In addition to the Java Card Protection Profile maintained by Oracle, several organizations, including SIMalliance and EMVCo, have developed material that helps in the certification of Java Card platform implementations and applications.

Furthermore, as more Java Card products are certified, national certification authorities in many countries have acquired a strong expertise in the technology, which helps in the certification of new products and the emergence of innovative certification schemes. Java Card products have often been used in “first” evaluations, ranging from the first Common Criteria evaluation in 2000 of a card with distinct operating system and application developers, to the first EAL7 evaluation performed on a smart card (the highest possible assurance level) in 2007.

Java Card Platforms and Low-end Cards

High-end vs. Low-end

The first smart card markets were rather uniform, with all cards providing similar basic services. Over the years, there has been a more distinct split between high-end cards and low-end cards.

In high-end markets, the focus of issuers is to deploy value-added services in addition to their core application, in order to maximize the value of their cards. Such markets are typically entirely converted to Java Card. For instance, for SIM cards, Europe, North and South America, Japan and Korea, all have very high penetration rates of Java Card SIMs, over 95% in most countries. Today, beyond traditional SIM-based services, the availability of Java Card on SIMs eases the introduction of new technologies such as NFC.

In low-end markets, issuers are often faced with limited revenue, so their main focus is the cost. For instance, mobile operators face a low ARPU and a high churn rate. In order to reduce their costs, mobile operators turn to the simplest possible SIMs, focused solely on network authentication. Because these markets are also very large, like India and China, the resulting SIM volumes are enormous, with billions of SIM cards issued every year. These

high volumes also dilute the price of software development. In a basic analysis, this naturally leads to a dominance of native cards.

By moving in this direction, though, the issuers are caught in a spiral of low cost and low revenue, neglecting opportunities to improve their business models. In low-end markets, mobile phones often are the most widely available communication tool, which makes it an ideal tool for the deployment of additional services. Some programs have been very successful, like Kenya's m-Pesa in mobile payment.

Closed Java Card cards as a low-end alternative

Java Card technology is often associated solely with high-end cards, but the technology can also be leveraged in low-end markets, bringing additional services at a very attractive cost.

The payment market is moving in this direction. With the emergence of NFC, major payment institutions have developed portable payment applications that can run on a wide selection of Java Card secure elements (SIMs, embedded secure elements, SD cards, *etc*.). In order to reduce certification costs, they are now encouraging card vendors to reuse these well-known applications into traditional payment products, including low-end closed payment cards.

In order for these products to be competitive, the overheads associated with Java Card must be minimized. This overhead is in fact the consequence of one specific feature: post-issuance downloading. A sizable part of any Java Card implementation is the GlobalPlatform software required to dynamically manage applications.

In a closed Java Card product, this overhead can be removed. Oracle's Java Card S program even allows card vendors to remove the Java Card features that are not used by the included applications. Closed cards also do not require the deployment of any specific infrastructure for managing applications.

However, even on closed cards, there are many advantages of relying on a Java Card platform. First, the services deployed on the card are developed on the Java Card API, and they can run on platforms from several vendors without porting costs and delays. This allows issuers to improve time-to-market when they develop new services. In addition, with Java Card, issuers benefit from the quality and security of a Java Card platform, providing a safe foundation for their services.

Toward a Tiered Java Card Offer

One of the main interests of using closed Java Card platforms for low-end cards is the ability to implement a tiered offer, relying on different card platforms. Most consumers get a low-end closed card with a fixed set of services, with a short expected lifetime. Premium consumers, on the other hand, get an open card, on which services can be upgraded, with a longer expected lifetime.

With a Java Card platform, such an offer is easy to define, maximizing reuse between the offers through the portability of applications. It is even possible to deploy the same applications on very different platforms, including security-certified platforms used for NFC, as long as the Java Card applications that are developed follow the appropriate principles.

Conclusion

Java Card is mostly known for its ability to provide platform interoperability and post-issuance application management. These advantages are real, but it is wrong to reduce Java Card to only those, as the platform offers much more.

Many actors in the financial sector rely on Java Card to improve the time-to-market of new applications and releases, and to increase the level of assurance provided by smart card platforms, even if they don't use post-issuance management of applications.

Even in the highly competitive SIM market in Asia, the Java Card platform presents many advantages by allowing network operators to build a range effect, in which different SIM types can be offered, matching the needs of all customer types, while keeping costs in control.

The Java Card Form is a collaboration of companies from the smart card, secure operating system, and secure silicon industry, working together to promote and develop Java as the preferred programming language for multi-application smart cards and secure devices.

For more information about the Java Card Forum please visit http://www.javacardforum.org