Java Card™ Platform Security

Technical White Paper

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
1 (800) 786.7638
1.512.434.1511

http://java.sun.com/products/javacard

Table of Contents

CHAPTER 1

Executive Summary

Smart cards are small computing devices that act as tokens to enable services that require security. The Java Card platform was designed and developed from the beginning specifically to enhance the security of smart cards. As a neutral platform, Java Card technology is implemented on a wide variety of smart card solutions with security levels ranging from modest to extremely secure. The modern features of the Java programming language provide a rich array of tools to develop reliable and secure applications. The Java Card virtual machine separates applications from the underlying hardware and operating system. The Java Card platform's standardized API provides a uniform interface to disparate smart cards. This unique approach uses the widely-understood benefits of object-oriented programming to enable security at both the application and platform level.

Security is not a black and white "one size fits all" subject. This white paper summarizes the wide variety of developments and real world experience that have led to the current position of Java Card technology as a highly secure and market-proven open platform architecture available for smart cards. More than a hundred million Java Card products have been deployed. This installed base has demonstrated that the Java Card technology provides a secure platform for the rapid development and deployment of smart card applications that meet the real-world security requirements of secure system operators. These operators range from major wireless operators, to government agencies, to financial service providers, and others.

Smart Card Security

Smart card security is a complex multi-dimensional problem. There are different costs associated with different levels of security. Different cryptographic algorithms require chips at various costs, just as different security evaluations and certifications can vary costs in time and money. However, products at any level of security can benefit from Java Card technology.

The Java Card platform provides a secure execution environment with a firewall between different applications in the same card. This allows different applications on the same card to function separately and independently from each other as if they were on separate cards. The Java programming language and the Java Card API allow development using modern object-oriented programming to create secure applications quickly and easily. By contrast, traditional smart card application programming has used assembly language or the C programming language, which forces the security evaluation to look at the entire application as a unit to verify behavior. Java Card applications can encapsulate sensitive data and algorithms within objects, which have provable behavior and increased security. The result is code that is simpler and easier to develop and maintain. Thus, benefits including lower cost, faster time to market and higher security are realized.

One of the most important security benefits of the Java Card platform is the link it provides between smart cards and the larger world of Java technology. The Java platform has taken a leading role in the academic and developer community, creating a strong base of technical knowledge and shared understanding. Many of the issues surrounding security and "correctness" of operation using the Java programming language and Java Card technology have been widely researched and implemented in multiple contexts. Experts familiar with these issues can be found around the world. Smart card application developers and issuers benefit from all of this research on the Java Card platform, other Java platforms and the general principles underlying all Java technology.

An Open Architecture Designed with Industry Experts

The Java Card platform was developed from Standard Edition Java technology in consultation with a large community of smart card experts. Sun Microsystems, Inc. worked in collaboration with a global community of experts from all facets of the smart card community. For the past five years, there have been regular meetings with specialists from major financial institutions, telecommunications operators, smart card manufacturers, silicon manufacturers, software experts and other industry players. All this shared experience went into the Java Card 2.1 platform being shipped in high volume today.

Security Evaluation of Java Card Products

In the last five years, products incorporating the Java Card platform have passed real-world security evaluations for major industries around the world. The Java Card platform is the leading platform for multi-application cards in mobile telephony. It is also the only platform that has passed security evaluations for issuance by all major financial payment associations. In addition, it has passed security assessments by leading government authorities, including the US Department of Defense and the US National Security Agency. Java Card platforms have achieved compliance with FIPS 140-1.

In Conclusion …

The Java Card platform is the platform of choice for smart card deployments. This is based on the inherent security of the Java programming language and the Java Card technology, the open process for design and development of this platform, and the platform's proven deployments and security evaluations. Any smart card issuer considering an open standard smart card today can choose a Java Card product with the confidence, knowing that it contains the most capable and secure technology available today.

CHAPTER 2

Overview

The remainder of this White Paper discusses in greater details the topics discussed in the Executive Summary. We will demonstrate the Java Card platform's advantage in the market place by exploring the security related aspects of Java Card technology and the application of the Java Card platform in the real world today. The next chapter is a discussion of how Java Card technology was designed from the beginning with security in mind. The Java programming language itself has a number of advantages over other application programming languages in the area of security. And the Java Card platform provides further security enhancements, such as the applet firewall. (In Java Card terminology, an application is known as an applet.) Standard Java platform development practices allow for the secure distribution of compiled Java classes with Jar files and cryptographic signatures. And analogously, CAP files (converted applet files) and cryptographic signatures are part of installation procedures to load Java Card applets into the smart card.

Chapter 4 details how the Java Card platform has proven itself in practice. Beginning as an open standard that was developed with industry participation, it has proven itself in a multitude of deployments. The convenience of developing applets using standard Java programming language development tools is unmatched by any competing technology. This platform also passes the test of interoperability. Applets developed according to the Java Card specifications will function correctly on any Java Card technology-compliant smart card. And leading smart card issuers have demonstrated that Java Card applets can be securely managed: that is, downloaded, installed and deleted.

In Chapter 5, the topic of security certification is addressed. Formalized security evaluations, as specified by ITSEC or the Common Criteria, helps to build trust in very complex IT systems. But, it is generally accepted that, as a practical matter, the security of an IT system as a whole cannot be certified without a significant cost in time and money. Therefore, it is customary to focus on key components in a system, like the smart card. This section of the paper discusses the practical means of approaching security evaluation and certification of Java Card platform deployments.

Finally, in Chapter 6, we present some of our ideas on the future evolution of the security features of the Java Card platform.

CHAPTER 3

Designed for Security

Java Card technology was developed specifically to enhance the security of smart cards. Important security safeguards are built into the Java programming language itself. The Java Card platform provides further security enhancements, such as transaction atomicity, cryptographic classes and the applet firewall. Additional security is provided by the "split virtual machine" architecture of the Java Card platform on both the workstation side and the card side. The Java Card technology also embraces techniques using compressed archive files with cryptographic signatures to provide tamper-proof distribution and installation procedures for Java class files and Java Card applets.

Security Derived From the Java Programming Language

The Java programming language is used to develop a Java Card applet, which provides several inherent features that protect the integrity of the platform:

- This is an object-oriented language, which provides programmers with the means to encapsulate data with the very procedures that have exclusive access to it for processing.
- The language provides name space management for type and procedure names to control access to functionality provided by the objects, through the programmer's qualification of type members as "public," "protected," "private" and "package-private."
- Object encapsulation supports "programming by contract," which enables programmers to reuse code that has already been tested.
- The Java language is a strongly typed language. Type mismatches in the source language are detected at compile-time. Run-time security enforcement can be based on the compiler generating logically consistent data type information.

- The Java byte code language (generated by a Java compiler) is strictly defined by the Java specifications. This is a strongly typed language that contains all programmer specified type information, which is used for run-time access control.
- The Java language does not support pointers, preventing security risks known from the C and C++ languages.
- Array indices can't be used to access memory beyond the allocated array boundaries.
- The Java language provides transparent storage allocation, preventing programming errors by unintended reuse of memory.

Over the last few years the research community has investigated the formal aspects of the Java language, including formal models of security aspects of the strong type system, and has come to strong conclusions about the security advantages of the language. A wide body of scientific publications is available for use in formal evaluation of systems, like the Java Card run-time environment and the applets loaded in the card. Smart card products built using different, proprietary OS designs cannot provide the level of code reusability and data integrity guaranteed by the Java programming language. By relying on the Java programming language, Java Card technology is able to provide a level of security assurance unmatched in the market.

Java Card Platform Security Enhancements

Complementing features inherited from the Java language, the Java Card platform provides several specific enhancements to security. The Java Card framework and run-time environment provide these essential security features: transaction atomicity, the applet firewall, and classes to support cryptographic signing and authentication of CAP files.

Transaction Atomicity

Transaction atomicity is enforced by the Java Card runtime environment. This means that either all updates to persistent memory in a marked transaction will be performed if the transaction is completed normally, or none of updates will persist if the transaction is aborted (if, for example, the card is prematurely removed from a card reader). Atomicity contributes greatly to the security of the smart card. For example, if the card is prematurely removed during a transaction between reader and card that is supposed to update a secret cryptographic key, the card will be returned to its prior state and the application in the reader will know that the update has not occurred.

Applet Firewall

The Java Card platform provides a secure execution environment with an applet firewall between different applets in the same card. A Java Card applet resides in the card isolated from other applets by the firewall. The firewall is a feature of the Java Card runtime environment to provide detailed control over the use of data stored in objects that have a shared implementation. The firewall mechanism transparently gives an applet a private partition of the card memory. As a result, a malfunctioning or even hostile applet cannot affect the functioning of the card or any another applet loaded on the card.

Security and Cryptographic Classes

The Java Card security and cryptography packages allow an approach to application management that is analogous to the secure class loader of Java 2 Standard Edition. The cryptography and security classes support:

- symmetric encryption and decryption algorithms;
- asymmetric encryption and decryption algorithms;
- key interfaces;
- signature generation and verification;
- message digests;
- random data generation; and
- PIN management.

This cryptography and security support can be used to provide a secure mechanism for downloading and authenticating Java Card applets.

Split Virtual Machine Architecture

The Java Card platform has been developed and evolved in order to ensure security throughout the application development chain. Java Card technology uses the "split virtual machine" architecture: one part of the Java Virtual machine executes off-card, on a workstation, preparing the executable code that is executed in the other part of the virtual machine, on the card. The split VM design is a unique Java Card technology innovation, intended to reduce the size of the applet image downloaded to the card and to minimize run-time memory requirements.

The off-card part of the Java virtual machine does all the work for linking classes and resolving references and consists of a converter and a verifier. The on-card part consists of the Java Card virtual machine, the Java Card runtime environment, and the Java Card APIs. From reading in all Java executable code files for a Java Card applet the off-card components produce a file in the Java Card virtual machine loading format, the CAP file. The CAP file may be loaded on a Java Card product, and the code will then be executed by the on-card part of the Java Card virtual machine.

The off-card components consist of the converter and verifier. The converter accepts as input all of the Java executable code (class files) for a Java Card applet, and produces a file in the Java Card virtual machine loading format: the CAP file. The CAP file is loaded onto a Java Card product, and the code is then executed by the on-card part of the Java virtual machine. The Java Card technology also includes off-card development tools such as the Verifier, whose role it is to verify CAP files. That is, the Verifier provides a means to assert that the content of the smart card conforms to the Java Card specifications, providing additional assurance that the executable code in the files will not compromise the integrity of a Java Card virtual machine.

Once the applet has been verified, cryptographic authentication of the Java Card applet may be used to ensure that the applet is not modified prior to installation on the card. A code loading mechanism can be implemented on a Java Card product to check the authenticity of the loaded applet.

Applet Development on the Workstation

The use of Java 2 Standard Edition Development tools is a great convenience to Java Card applet developers. But there is a security advantage as well: compiled Java class files can be distributed within workgroups or between third party developers and smart card operators using Jar files with cryptographic signatures to ensure secure and untampered distribution.

CHAPTER 4

Proven Platform

The Java Card platform has proven itself in actual use. An installed base of more than a hundred million Java Card products that meet the real-world security requirements of secure system operators, such as major wireless operators, government agencies and financial service providers, have been deployed.

The Java Card platform began as an open standard that was developed with industry participation. The convenience of developing applets using standard Java programming language development tools is unmatched by any competing technology. The Java Card platform also passes the test of interoperability. And application management of Java Card applets is also a proven technology.

An Open Architecture Designed with Industry Experts

The Java Card platform has been evolved in collaboration with the experts from the smart card industry. From its infancy, since it is an open standard, Java Card technology has been exposed to the scrutiny of security experts around the world. With the deployment and wide acceptance of the Java Card platform, a smart card has for the first time become an easily programmable device. This has drawn the attention of many researchers to study the Java Card technology and its security, adding to research by hundreds of academic institutions on the Java programming language.

The advantage of having numerous qualified individuals voluntarily analyzing a technology (instead of a few engineers paid by private institutions) cannot be underestimated. It increases the quality and security of the Java Card platform, and is a key factor to help the platform keep its competitive edge compared to competing closed or proprietary solutions.

The result of the open specification process is that numerous implementations of the Java Card platform are available in the market today, all of which adhere to the same Java Card specifications. They are produced by well-established companies in the smart card and security arena, such as G&D, Gemplus, Orga, Schlumberger, Oberthur, and others. These companies have developed refined, well-honed engineering processes, and have implemented very strict security policies and procedures. They know what it takes to develop smart card products with a secure Java Card runtime environment. It is their interest to ensure that their products remain highly secure. Their reputation is at stake on every single smart card they ship.

No other technology can claim such widespread support from the smart card industry. The Java Card platform is the only smart card technology to have been developed in collaboration with the experts from such a wide spectrum of industry players.

Standard Java Development Tools

In the area of application development, the Java Card platform has a tremendous advantage. There is a wealth of Java development tools available on the market, for all kind of platforms where the Java programming language is the norm. This means that a developer can use many of the same development tools to develop a Java Card technology-compliant applet, and to support the other Java programming language development in his company. The result is reduced complexity and increased confidence for the Java Card programmer. Developing software for smart card products based on a different execution environment forces the developer to use proprietary tools and learn a programming language either totally new, or not adapted to industrial strength applications.

The Java programming language, on the contrary, is so popular that one continually finds new and better tools: for example, tools to support the integration of formal methods into the Java development environment. This is a dynamic, living environment in which many large corporations are investing.

Finally, to complement the generic Java development tools, the Java Card applet programmer can also find a variety of software components from many of the Java Card technology-licensed chip card vendors. The tools are state-of-the-art for smart card application development, which makes it very easy to develop applications, and lowers the bar for new developers.

All these elements account for the fact that the developer community for the Java Card platform is far larger than for any other smart card platform. The accumulated experience resulting from the resources already working on this platform is a guarantee of reliability, and makes it the most proven smart card development platform on the market.

Interoperability

In order to ensure the interoperability of the various products implementing the Java Card specifications, Sun Microsystems, Inc. provides the "Java Card Technology Certification Kit" (TCK). The Java Card TCK includes a collection of tests designed specifically for compatibility testing of a Java Card technology implementation. These tests are used to verify compliance of a Java Card implementation to the related Java Card technology specifications, ensuring that all Java Card products behave the same way. This minimizes any security risks due to variation in implementations.

Application Management

There are two major aspects to application management systems for smart cards: open issuing and support for secure post-issuance applet installation and deletion.

Open Issuing

The open architecture gives an issuer of smart cards implementing the Java Card platform discretion in management of all the issued cards. The issuer controls the implementation of the on-card loading mechanism as required by the security environment of the card scheme. It may be further configured to meet requirements of the commercial partners that provide applications for the card. For example, VISA International initiated the Global Platform specifications, which are an example of the flexible loading mechanisms that may be deployed with the Java Card technology. (See Chapter 8, "References.")

The commercial relation between card issuer and application provider is independent of the platform technology, providing a truly open market space. Centralized application models used by proprietary technologies often require the issuer to reveal its relationship with content provider to a centralized entity. This implies a single point of failure as well as potential bottlenecks limiting scalability, whereas with Java Card technology, the card issuer has the freedom to choose an appropriate cryptographic protection for card management, either with public or distributed cryptographic keys.

The use of a trusted third party, for example as a certification authority for public keys, is a matter between card issuer and application provider. With the open issuing architecture of the Java Card technology, the business arrangements are between the issuer and the application provider where the issuer can specify the extent of its responsibility for the overall card security. The application provider can assume its own responsibility for the secure operation of its in-card business logic implemented in the loaded applet.

Support for Secure Applet Loading and Deletion

The freedom to develop various card based applications for deployment on an existing card base or on newly issued cards is backed by well protected loading and deletion mechanism and an open architecture that asserts that: "***one size does not fit all***." For example, the Global Platform provides specifications to define security policies and cryptographic mechanisms to protect download and delete of applications focusing on the needs of the financial market. In that model, each applet can be securely loaded and removed using either Public Key or Symmetric key cryptography. In addition, the Java Card applet file format (CAP file) encapsulation using the jar file format can accommodate the application executable code cryptographic hash value and keys. This open architecture supports addressing different threat models as may be applicable to different market segments, e.g. to protect against known attacks.

Card products based on proprietary implementations are much more static: in general the card product has to be redesigned if a new security threat arises. This may mean a tremendous amount of work and delays to market.

CHAPTER 5

Security Certification

The use of formalized security evaluations, as specified by ITSEC or the Common Criteria, helps to build trust in very complex IT systems. In the smart card industry, security evaluation has taken a significant importance, as higher levels of compliance have been requested by the banking industry in some world markets.

But, it is generally accepted that the security of an IT system as a whole cannot be certified without significant costs in time and money. Therefore, it is customary to focus on key components in a system, like the smart card. Manufacturers of smart cards have obtained formal security evaluation for some of their products.

However, focusing on certification of only a single component may only bring a false feeling of safety. A practical security evaluation should include, apart from formal certification of key components, assessments of the procedures of other technical aspects of a system, including the way these might interact with each other. It is important to assess to what extent a formally certified key component really contributes to making the complete system secure.

In today's fast moving market, where new technologies are introduced on an accelerated rhythm, the commercial justification of submitting the card as a key component in a system for certification may seem questionable. Typically, a security evaluation certificate applies to a single "target of evaluation" specified for the system at the time of submission: The Target of Evaluation (TOE), which defines the scope of the security certificate, is a snapshot of the product and the environment of its intended use. As a result, without special preparation, by the time a security certification may be obtained for a multi-application card implementation, new products and advanced technologies may become available, along with the competitive pressure to adopt them.

At this moment, investing time, resources and money in a certification effort only makes sense to the extent that obtaining the certificate is seen as crucial for the growth of the business in a specific market segment. And in most cases, this currently means that an evaluation at a moderate level of strictness is sufficient.

Security Evaluation for Java Card Technology, an Open Platform

Until recently, the scope of security evaluation for smart cards has been limited to proprietary, mono-vendor smart card solutions. Experience has taught us that it can take several years at a considerable cost to obtain high-level security certification for smart card software.

At first glance, a multi-application, "open platform" architecture like the Java Card platform might seem a difficult target for security evaluation. In a typical system based on such a card several actors are involved:

- a silicon provider
- a card manufacturer
- a smart card OS provider
- the Java Card platform implementation
- application providers
- application development tools
- card issuers
- cryptographic certificate authorities
- manufacturer of the card-reader
- back office systems with implementations supporting various hardware security components for card issuers and application providers
- system support services

This typical real-world system, in which the Java Card platform implementation is only one of the commercially independent parties, could benefit from a comprehensive security evaluation. Such an evaluation might provide a basis for the legal arrangements needed to operate the system.

Security Evaluation of the Smart Card

Faced with such a complex system, the pragmatic solution has been to focus on the security of the smart card part of the system. Java Card technology was conceived with formal security certification in mind, directly supporting the all important divide-and-conquer approach to successful security evaluation. A strong foundation for security evaluation is provided by the object oriented nature of the Java programming language and the security support built into the language, complemented with Java Card technology-specific security enhancements.

The Java Card platform's applet firewall completely separates applets from other applets. Furthermore, applets interact with the runtime environment only in narrowly specified ways. This greatly reduces the security evaluation problem.

The publicly accessible specifications and reference implementations of the Java Card platform provide yet another, different approach to obtain trust in implementations. The open system model allows experts all over the world to scrutinize the security features of the components. Thus, trust in the system is supported by the consensus of unbiased experts.

The Appropriate Level of Security Evaluation

Certification is increasingly important to support consumer trust as dynamic multi-application card systems are being deployed more widely with more valuable personal data being stored and processed.

Java Card technology has experienced tremendous success in the market today. For instance, in the banking industry, where there are clear security demands, there are large deployments of Java Card technology-based products. In particular world markets where a certain security level is a prerequisite, Java Card product vendors are focusing on an attainable security evaluation: the Common Criteria EAL4. Toward this purpose, Protection Profiles for the Java Card platform have recently been defined.

Whether it is appropriate for a potential card issuer to apply for a high level of Common Criteria certification is more a business decision than a technical one. From the business perspective, when contemplating this, one should consider whether one might miss a moving target of market opportunity. High level certifications can lead to the scenario of deploying a generation of smart card technology that is already obsolete by the time the certification process is complete. Exactly what level of security to certify is a business risk management issue. In other words, one has to make a decision that a certain level of certification is critical to one's business to justify the investment in time and dollars.

A more pragmatic solution might have a card issuer working toward the highest level required by the target industry (for example, Common Criteria level 4+) while at the same time attempting to gain support in that industry for incremental security evaluation. As an alternative, an organization may choose to run their own certification process, as was done, for example, by Visa International.

In practice, Java Card implementations have achieved appropriate levels of security certification where needed. The intrinsic security features of this platform have made the certification process easier. In addition, protection profiles are being defined by specific industries to expedite the certification process of the Java Card platform.

CHAPTER 6

Future Directions

Security is not a static concern, but an evolving one. Those in the business of security must anticipate potential attacks on secure systems, and continue to innovate. This section discusses approaches that are being discussed by the Java Card community as the Java Card platform continues to evolve. Sun Microsystems, Inc. and its partners are investigating the possibility of speeding future security certification by a technique of incremental certification. And research has the community thinking about possible extensions of the Java Card platform.

The following discussion should not be taken as a commitment to add particular features to the platform, or as a prediction about the time frame when features might be added.

Incremental Certification

In the current state of certification technology, security evaluation is inherently a one-time operation, in which a single monolithic system is evaluated, including everything from back-end hosts to on-card OS to applications. Then, when the any part of the system moved to a new revision, it would require the vendor to apply again for certification of the whole system. Such a costly procedure would have led to a result that might quickly become obsolete. This has been an obstacle to higher levels of security certification of Java Card technology products. The impracticality of the current process, and the emerging need in the market place for higher levels of evaluation may accelerate the advent of more incremental methods of formal security evaluation.

Sun Microsystems, Inc. is engaged with its partners to promote the development and adoption of such procedures. They have discussed proposals with certification authorities to certify blocks of a system rather than only fully integrated final product; and to re-certify the product as a whole based on the certifications of the previously certified components. When, over time, these improved evaluation methods are available, more Java Card products will be evaluated for security certification at higher levels. As the technology and procedures mature, Java Card product families will become available with certification at the highest level of assurance.

In parallel to this long-term outlook at security evaluation for the Java Card platform, smart card industry players are looking for a short-term way to find the balance between market demands for enhanced products, and the need for a security evaluation of the products. Chipmakers and card manufacturers have undertaken formal evaluation at lower levels of assurance. This approach is a viable way for certification in specific application domains, especially banking.

Java Card Platform Enhancements

Possible enhancements to the Java Card platform might include:

- A framework component to specify the security mechanisms required to protect authenticity and confidentiality of data exchanged between a card and terminal.
- Support for on-card verification of downloaded applets
- Support for object checksums on objects containing sensitive data.
- Distributed object access mechanisms that enhance object encapsulation and reduce error-prone message parsing within applications.

CHAPTER 7

Summary

In this white paper we have addressed many aspects of security in the Java Card platform. Here are some of the key points we have explored:

- The Java Card platform was designed from the beginning with security in mind.
- Java Card technology leverages security benefits of the Java programming language, and adds important security features such as the applet firewall.
- The Java Card platform is the only really "open" smart card technology platform, since it has been developed in collaboration with the smart card industry, and has always been available for review to security experts.
- The Java Card platform is today the most widely deployed open architecture, with more than 100 million cards used around the world in 2001.
- The Java Card-enabled smart card is only one piece in a chain of trust in which every link must be strong to ensure security.
- Security is never more challenged than by real-life usage: Java Card technology, while the most exposed technology on the market, has received security validation in more deployments than all competing platforms together.

CHAPTER 8

References

Java Card™ 2.1.1 Application Programming Interface (Sun Microsystems, Inc., 2000)

Java Card™ 2.1.1 Virtual Machine Specification (Sun Microsystems, Inc., 2000)

Java Card™ 2.1.1 Runtime Environment (JCRE) Specification (Sun Microsystems, Inc., 2000)

Java Card Specifications are available online at:
`http://java.sun.com/products/javacard/javacard21.html`

Zhiqun Chen, *Java Card™ Technology for Smart Cards (Java Series)* (Addison-Wesley, 2000)

Other relevant industry standards available online:

`www.globalplatform.org`

`www.itsec.gov.uk`

Common Criteria for IT security evaluation:

`http://csrc.nist.gov/cc/sc/sclist.htm#SCSUG-PP`

Information on FIPS Security Requirements for Cryptographic Modules can be found at:

`http://www.itl.nist.gov/fipspubs/fip140-1.htm`

The FIPS certification for one Java Card product deployment can be found at:

`http://csrc.nist.gov/cryptval/140-1/1401val2001.htm`

(See certificate number 165.)

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303

1 (800) 786.7638
1.512.434.1511

http://java.sun.com/products/javacard

October 2001