Java Card

The Open Application Platform for Secure Elements.

Java Card™ enables secure elements, such as smart cards and other tamper-resistant security chips, to host applications, called applets, which employ Java technology.

Java Card technology offers a secure and interoperable execution platform that can store and update multiple applications on a single resource constrained device, while retaining the highest certification levels and compatibility with standards. Java Card developers can build, test, and deploy applications and services rapidly and securely. This accelerated process reduces development costs, increases product differentiation, and enhances value to customers.

A COMPACT, SECURE JAVA RUNTIME

The Java Card platform is specified by Oracle, through a close collaboration with its customers and industry groups such as the Java Card Forum. It is at its core a very minimal subset of Java, enriched with unique features catering to the needs of secure elements implementers and developers, specifically:

- **Interoperable**: Applets developed with Java Card technology will run on any Java Card technology-enabled product, independently of the software vendor and underlying hardware. Java Card is available on a wide range of silicon form factors : smart cards, embedded chips, secure enclaves within CPUs and MCUs, removable SIMs... Applications can be reused across those form factors, enabling customers to maximize their security / cost ratio, and supporting seamless migration if security requirements evolve.
- **Secure**: Java Card technology relies on the inherent security of the Java programming language to provide a secure execution environment. An open design process, proven industry deployments and high-level security evaluations guarantee that the Java Card platform is the most capable and secure technology available today. Java Card also supports the latest security standards and is regularly updated with state of the art cryptography algorithms, modes and protocols.
- **Multi-Application multi-tenant**: Java Card technology enables multiple applications from multiple vendors to coexist securely on a single secure element. For example, several payment schemes can be included in the same chip, or a SIM application can be loaded alongside device security services in an embedded Secure Element.
- **Extensible and Updatable** : new services are developed using standard-based Java tools, and can be created and deployed at any time during the life of a Java Card product. Remote management and upgrade of applications allows service providers to constantly adapt to security threats. Applets are updatable in the field, ensuring always-current device security to end-users.

Java Card technology is the leading open, interoperable platform for secure elements.

- The Java Card Platform Specification provides the basis for cross-platform and cross-vendor applet interoperability
- The Java Card Development Kit offers a complete, standalone development environment in which applets written for the Java Card platform can be developed and tested

Key Benefits

- Tens of Billions deployed
- Open Java Platform
- Certifiable Security
- Standards based
- Dedicated IoT APIs

Disclaimer: This document is for informational purposes. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

- **Compatible with standards**: The Java Card API is compatible with international standards for secure elements such as ISO 7816 or mobile communication standards issued by ETSI/3GPP. Major industry-specific standards such as EMVCo, GlobalPlatform refer to it.

TENS OF BILLIONS DEPLOYED ACROSS INDUSTRIES

Java Card is licensed on an OEM basis to security specialists and chip vendors worldwide. Since its introduction, Java Card has evolved from a smart card-focused technology to a versatile security platform used in billions of devices. In 2018 alone, close to 6 billion Java Card-based chips were deployed by Java Card licensees, providing trust and security services across vertical markets :

- **Telecom**. Billions of SIM cards have been issued including Java Card technology. Mobile operators use Java Card to provide network authentication according to telecom standards, to manage subscriptions and to optimise network utilisation. They can also offer value-added services to their customers such as home security, or NFC based services. Java Card is also a key enabler to the “virtualization” of the SIM, as the SIM application becomes hosted in new silicon types such as the embedded SIM or the integrated SIM.
- **Mobile phone and wearables**. Mobile OEMs and Wearables device vendors use Java Card embedded and integrated secure element to offer contactless and online payment services, NFC services and to offer a root of trust for device software integrity.
- **Finance.** Java Card technology is often at the base of payment transactions, using payment cards or using NFC transactions in cards or mobile phones. Leading payment institutions trust Java Card to host their payment applications and accelerate vendor certifications. Java Card also allows banks and other financial operators to differentiate by offering new modes of authentication such as biometry, or additional services such as loyalty.

- **Government and Identity**. Many governments are including Java Card technology in their requirements for electronic identity documents such as ID cards and Passports. Java Card provides strong guarantees of interoperability and security, as required by these sensitive deployments. Applications include PKI, Digital Signature, Encryption and more
- **Automotive**. In addition to subscription management and connectivity services, Automotive OEMs offer secure remote services using the embedded secure elements for authentication.
- **IoT Security**. Smart meter and Gateway OEMs leverage Java Card-based secure element to ensure device attestation and integrity, and device credential protection. IoT device makers can utilise security chips running Java Card technology to deliver secure authentication to IoT solutions.
- Other Java Card applications include Pay TV subscription management, Digital Rights Management, transportation ticketing, and much more.

Edge Security at IoT Speed

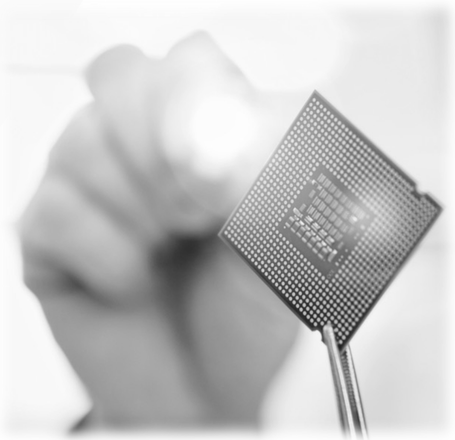
- Java Card products deployed in automotive, wearables, smart meter, gateways…
- Connectivity & security services can coexist on same chip
- New dedicated IoT functionality introduced in Java Card 3.1
- Unlocks new IoT Security use cases: Trusted peripherals, multi-cloud authentication, Attestation…

Lower Certification Costs

- Product have been certified at the highest security levels: CC EAL5+ to EAL7+, FIPS 140-3
- Java Card supports composite certification schemes
- Application reuse streamlines industry certifications: Visa, MasterCard, China UnionPay
- Strong Evaluation and certification community

BRIDGING IOT AND EDGE SECURITY

To support the growing security needs of connected devices, Java Card now includes dedicated features for the development of Internet of Things (IoT) Security applications at the edge of the network:



- Java Card Platform version 3.1 introduced a new I/O model that can be extended to support a variety of physical layers and application protocols, allowing the logical access to device peripherals by secure element applications.
- Certificate APIs, Extended Cryptography support and anti-replay mechanisms facilitate the implementation of Cloud Authentication protocols using secure hardware, the support for device to cloud communication security and the deployment of device attestation mechanisms.
- Continuous improvement in compatibility testing and standardisation of Java APIs ensure that Java Card applications can be quickly ported and work across a fragmented IoT Silicon landscape.

In addition to existing applications of Java Card in smart metering, automotive, and wearables, this dedicated IoT functionality unlocks a wealth of new use cases for IoT devices, for example :

- **Virtualized SIM** : the latest ETSI, 3GPP and GMSA standards allow for the SIM application to be abstracted from the underlying tamper-resistant hardware, and offer a choice of form factor and supplier. Java Card facilitates porting of the SIM application and operator services onto a wide range of chip architectures, at lower cost.
- **Device attestation** : a Java Card secure element in an IoT device can support multiple proprietary or standard secure boot and device attestation mechanisms without a requiring dedicated security chip. This allows a single secure chip to be used in multiple attestation ecosystem, and ensures compatibility with future standards.
- **Cloud security** : Java Card can provide hardware-based device security services across multiple IoT solution vendors, with low switching costs. Authentication schemes from multiple IoT solution or cloud providers can be consolidated on a single chip.
- **Trusted Peripherals** : Java Card can secure the “last yard” between devices, gateways and attached peripherals, enabling trust and exchange of sensitive data at the very edge. A secure channel can be established between peripherals and security chips, to allow out of band communication for sensitive data (for example biometric information, or provisioning of root of trust credentials).

Many more use cases are being designed, as implementers and developers of Java Card technology are driving Java Card based products into IoT solutions.

MARKET PROVEN SPECIFICATION

At the heart of the Java Card platform is the Java Card Platform Specification published by Oracle, and providing the basis for cross-platform and cross-vendor applet interoperability.

- **The Java Card Virtual Machine**
  Specification defines the features, services, and behavior that an implementation of Java Card technology must support. It includes the instruction set of a Java Card Virtual Machine (VM), the supported subset of the Java language, and the file formats used to install applets and libraries into smart cards and other devices that host Java Card technology.
- **The Java Card Runtime Environment**
  Specification defines the necessary behavior of the runtime environment (RE) in any implementation of the Java Card technology. The RE includes implementations of the Java Card Virtual Machine, the Java Card API classes, and runtime support services such as the selection and deselection of applets.
- **API for the Java Card Platform** complements the Java Card Runtime Environment Specification and describes the application programming interface (API) of the Java Card technology. The API is compatible with formal international standards and industry-specific standards, and contains the class definitions required to support the Java Card VM and the Java Card RE.

In addition to the Java Card Platform Specification, Oracle publishes **the Java Card Protection Profile**: a modular set of security requirements designed specifically for the characteristics of the Java Card platform. It reduces the time and cost for developers of Java Card-based products to complete security evaluations under the Common Criteria for IT Security Evaluation. It can be used to reach certification levels of 4+ and above for Java Card products.

The Java Card Platform specification and Java Card Protection Profile are freely available to Java Card application developers.

REFERENCE IMPLEMENTATION AND COMPATIBILITY TOOLS FOR IMPLEMENTERS

Java Card technology is licensed on OEM basis to companies that now represent a large majority of the world’s secure element manufacturing capacity. Java Card licensees can implement the Java Card Platform specification and distribute Java Card - based commercial products. To its licensees Oracle provides the Java Card Reference Implementation, an implementation of the Java Card Runtime Environment written in the C programming language, which provides an illustration of the correct semantic behaviour of the Java Card Platform specifications. It also includes the Java Card Virtual Machine interpreter, and related tools.

Java Card technology licensees can also acquire a license to the Java Card Technology Compatibility Kit (TCK), which can be used to certify a Java Card implementation on a particular platform, ensuring the applet interoperability at the core of the Java Card value proposition.

JAVA CARD DEVELOPMENT KIT FOR SECURITY SERVICES DESIGNERS

Developers creating applications using Java Card technology enjoy all the advantages of working in the Java programming language:

- Object-oriented programming yields greater code modularity and reusability, leading to higher programmer productivity.
- Protection features characteristic of the Java programming language apply to Java Card applets, enforcing strong typing and protection attributes.
- Powerful off-the-shelf development tools are readily available.

The Java Card Development Kit is a free suite of tools for designing implementations of Java Card technology and developing applets based on the Java Card API Specification:

- The Java Card Simulator offers a testing and debugging reference for Java Card applications
- Off-card platform components such as the Java Card Converter and the Java Card Verifier complement the Java Card simulator to provide a complete development chain.
- Additional design and testing tools enable developers to prototype and test applications, including integration with commercial IDEs such as Eclipse

A variety of Third party tools and testing products are also available to help developers design and test applications on secure element hardware.

FOR MORE INFORMATION

To learn more about Java Card technology, please visit https://www.oracle.com/technetwork/java/embedded/javacard/overview/index.html.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/oracle   facebook.com/oracle   twitter.com/oracle

Integra