Java Card Introduction
for Project Gemini

Ken Peterka, VP of Software Development
Cristian Toma, Director of Software Development
Sebastian Hans, Consulting Member of Technical Staff

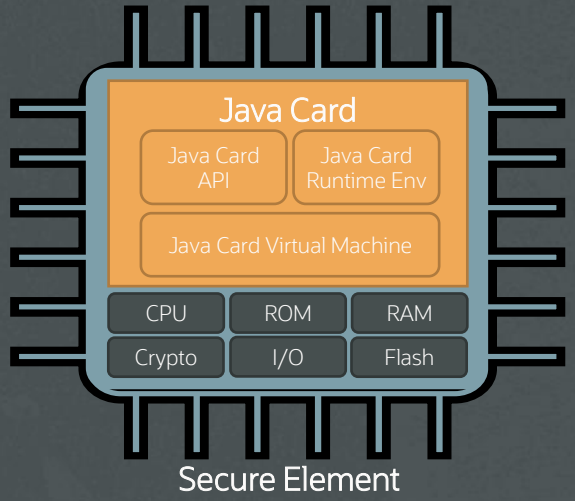
Oracle Java Platform Group | Java Card

July 26, 2024

What is Java Card?

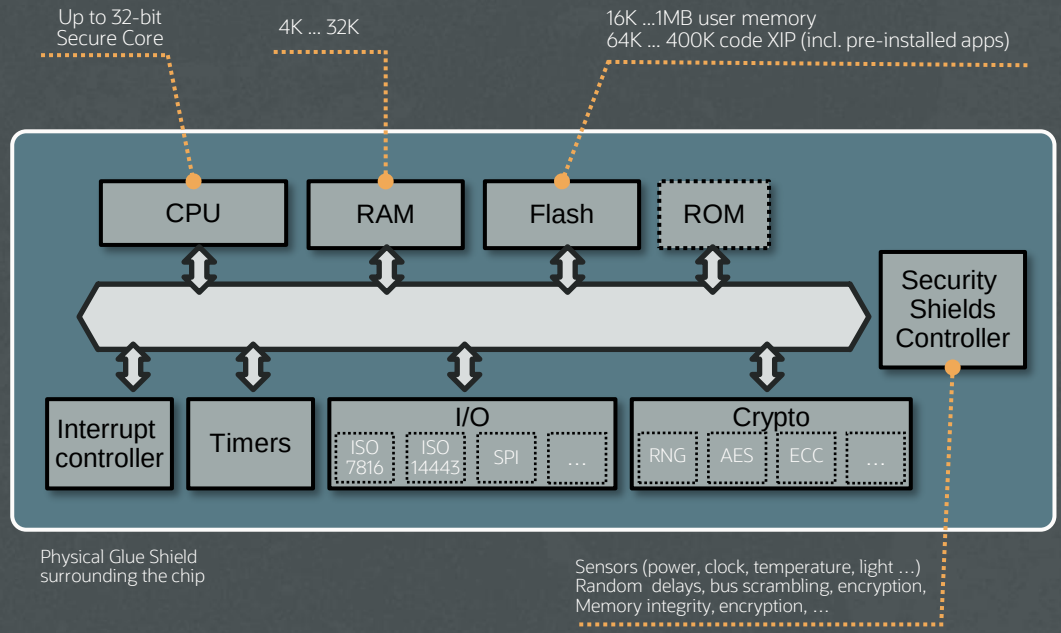
Provides a secure, interoperable, and portable execution environment for applications running on a Secure Element, which is an isolated, tamper-resistant compute resource for high security applications:

- Provides hardware abstraction for application execution and management
- Harnesses Java technology (‘write once; run anywhere’) to provide cross-platform support across chip manufacturers
- Facilitates a programmable secure element with multiple application support, application isolation, and secure channel communications
- Standardized Java Card API facilitates application portability for cryptography, communication, and data storage
- Proven ability to achieve highest levels of security certification from Common Criteria and FIPS



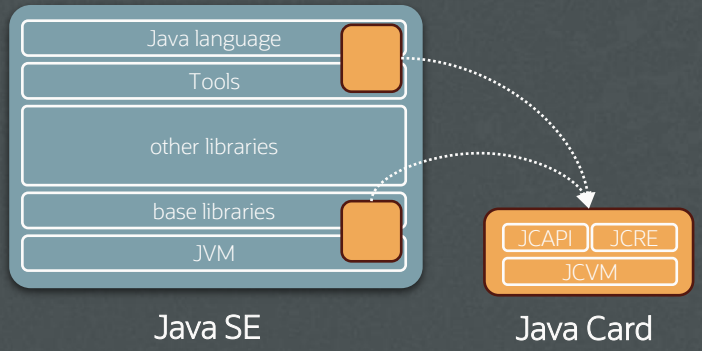
What is a Secure Element?

- Hardware Root of Trust
- Isolated security chip with tamper resistance technology protecting against hardware attacks to manage and execute sensitive data:
  - in unprotected environment
  - with non trusted users
- Support preloading of secure assets (crypto keys, certificates) during manufacturing process
- Security Certifications (e.g. FIPS, CC EAL4+ EAL7+ …)



Java Card DNA

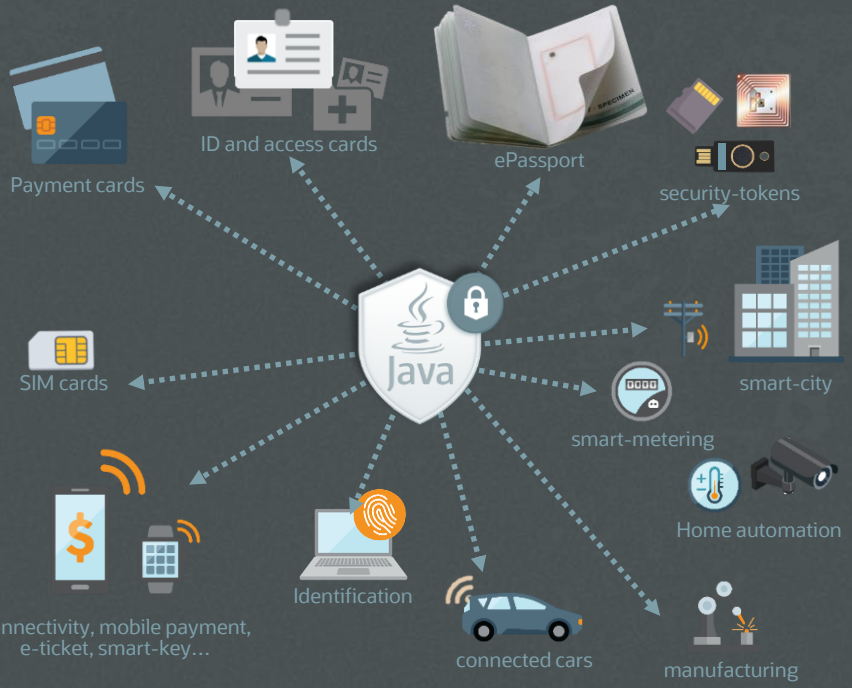
A tiny subset of Java, adapted and optimized for Secure Elements

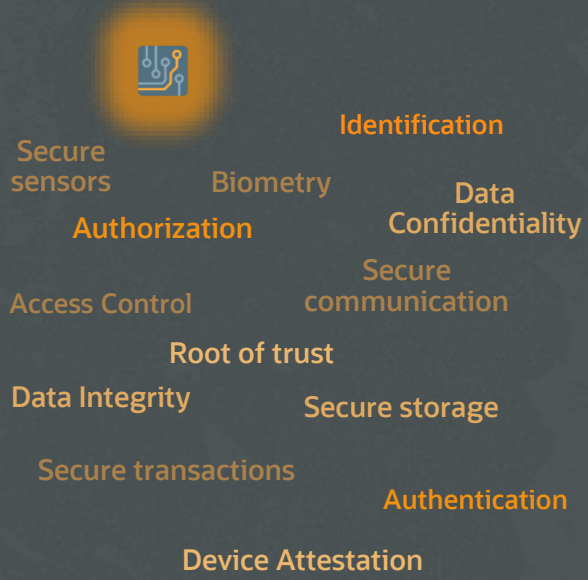


Key Characteristics:

- Uses Java language, compiler and essential core libraries
- Optimized runtime for secure elements with highly constrained resources
- Extended to support multiple applications with firewalling and controlled sharing
- Designed for the portability of secure services

Java Card Use Cases





Securing Medical Devices

Java Card can be used to secure all types of medical devices

- Point-of-Care
- Patient-Connected

Single Secure Element can be leveraged for multiple security use cases such as:

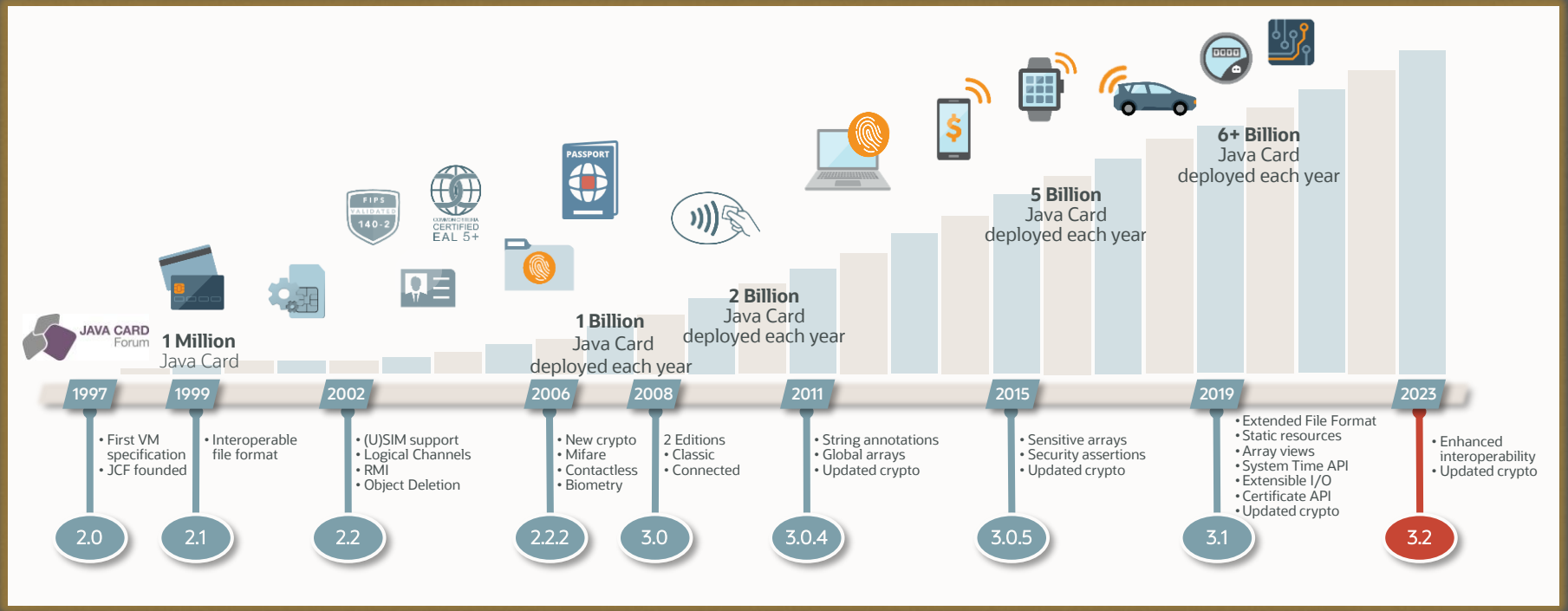
- Device integrity (tamper detection, secure boot)
- Secure data communications (internal and external)
- Secure storage of private cryptography keys
- Authorization using contact or contactless technology
- Data integrity through digital signatures

Long-term Vision

- Educate healthcare organizations on the multifaceted benefits of using Java Card to secure medical devices
- Secure Elements need to be designed into medical devices

Decades of Technology Leadership

6B+ Java Cards issued every year



Management Through Standards

Major open standards for Secure Element application management references Java Card for enabling application download, personalization, and lifecycle management through wired, contactless or Over-The-Air connectivity.

ETSI, GSMA and 3GPP Support

- References Java Card functionality and specific Java Card APIs
- Directly resulting in Telco Operator adoption of Java Card

GlobalPlatform

- Close cooperation with Java Card and references the Java Card specifications
- Extends Java Card functionality and defines domain specific Java Card APIs
- Java Card binding with GP for application deployment and management
- Most Government eIDs mandate GP support : 100% of all commercial deployed Java Cards support GP

ETSI | TCA TRUSTED CONNECTIVITY ALLIANCE Enabling a secure, connected future | 3GPP A GLOBAL INITIATIVE

- TCA eUICC Profile Package: Interoperable Format Test Specification Version 3.2.2
- ETSI TS 102 241 V16.0.0 (2019-11) Smart Cards; UICC Application Programming Interface (UICC API) for Java Card (TM)
- ETSI TS 102 705 V12.0.0 (2019-05) Smart Cards; UICC Application Programming Interface for Java Card™ for Contactless Applications (Release 12)
- ETSI TS 102 267 V15.0.0 (2019-02) Smart Cards; Connection Oriented Service API for the Java Card(TM) platform (Release 15)

GSMA

- SGP.21 V2.2 eSIM Architecture Specification - 01 September 2017 (JC mandatory)
- SGP.22 V2.2.1 eSIM Technical Specification - 18 December 2018 (JC mandatory)
- SGP.23 V1.5 eSIM Test Specification - 25 April 2019 (JC mandatory)

GLOBALPLATFORM®

- Confidential Card Content Management – Amendment A v1.2 | GPC_SPE_007
- Card Specification V2.3.1 | GPC_SPE_034Published Mar 2018
- GlobalPlatform Card API (org.globalplatform) v1.7Published Jul 2019
- Java Card Contactless API and Export File for Card Specification v2.2.1 (org.globalplatform.contactless) v1.1Published Feb 2012
- GlobalPlatform Card API – org.globalplatform.upgrade v1.1Published Mar 2018
- GlobalPlatform Card API – Secure Channels and Privacy APIs v1.1Published Jun 2017

Java Card Technology Platform

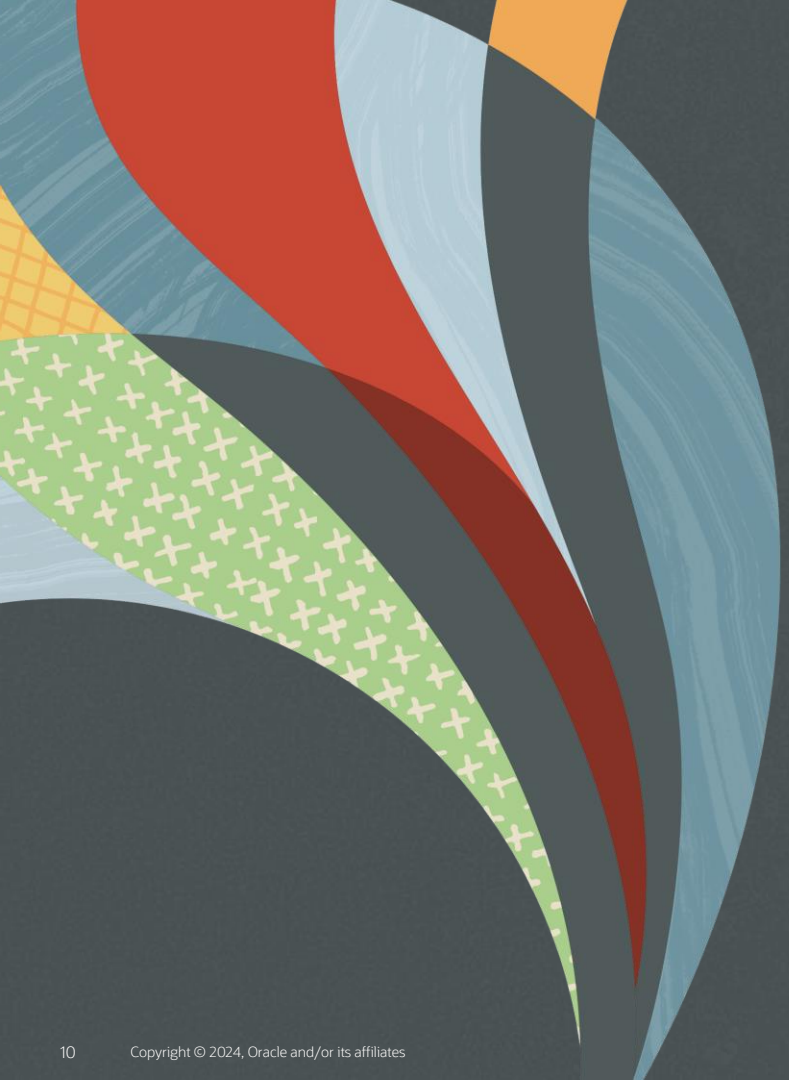
Proven **interoperability** for Secure Elements

Achieves highest levels of **security certification**

Programmable and Manageable **multi-application** framework

Continuously evolving, **26 years** of innovation

www.oracle.com/java/java-card



Thank you

https://www.oracle.com/java/java-card

https://javacardforum.com