



Java™
ORACLE®

Landscape of Hardware Roots of Trust for Connectivity and Security

Sophia Security Camp 2020

Nicolas Ponsini
Security Solutions Architect at Oracle
Java Platform Group
Oct, 2020



Safe Harbor Statement

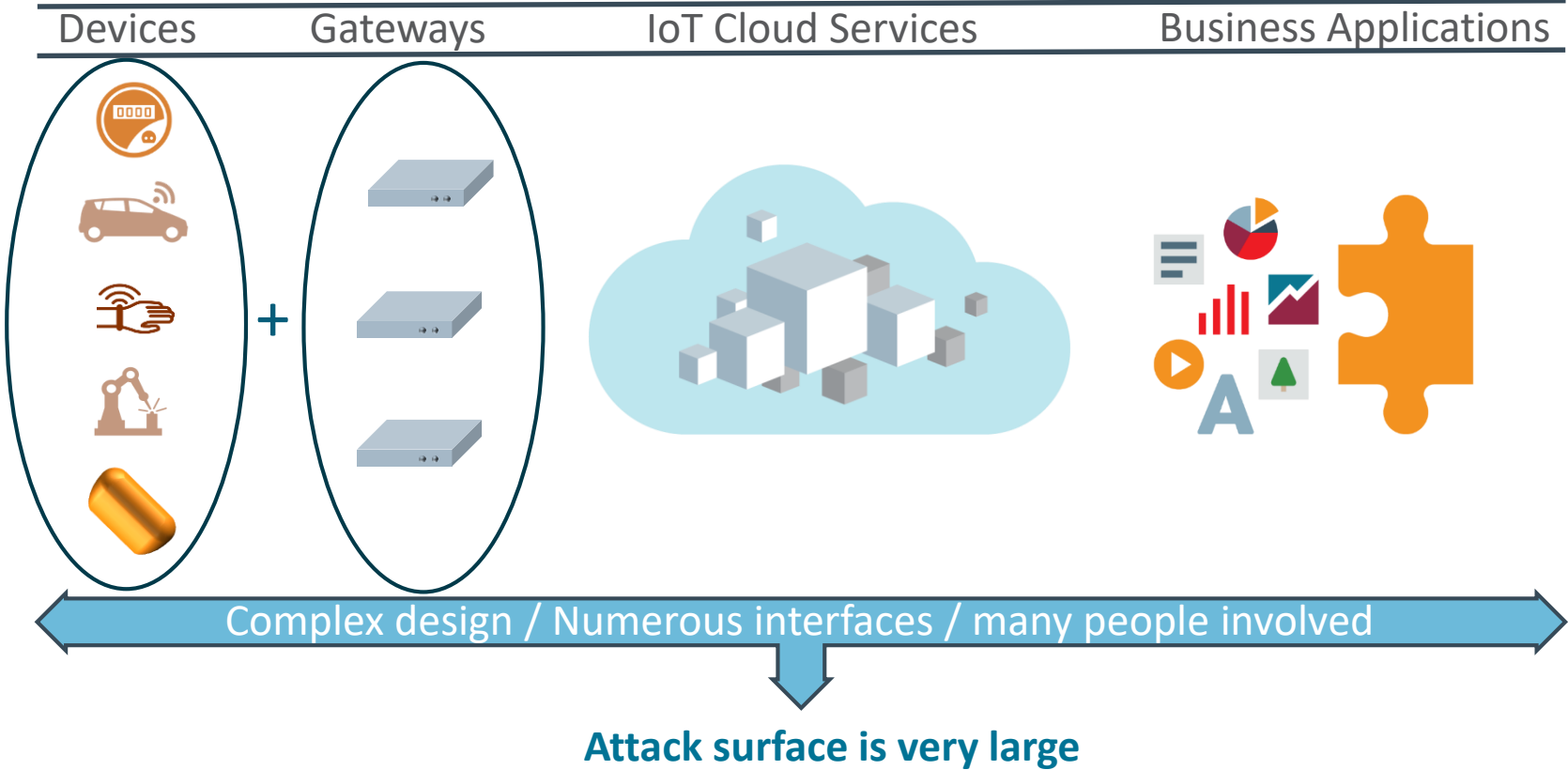
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Agenda


- 1 IoT Security at the device edge
- 2 Hardware Roots of Trust
- 2 Java Card & IoT

IoT Security at the device edge

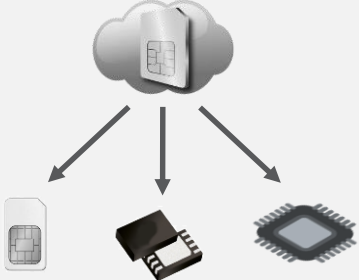
IoT Architecture




Use-cases in IoT security market

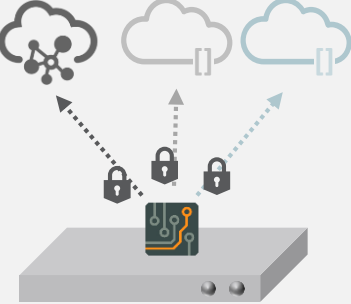
 **DIGITIZED SIM**

Abstract the underlying hardware for portability of the SIM applications across multiple hardware at lower cost.



 **MULTI-CLOUD AUTHENTICATION**


Provide device security across multiple IoT Solution Vendors and authentication schemes.




 **ADAPTABLE ATTESTATION**

Support multiple proprietary or standard Device Attestation schemes.



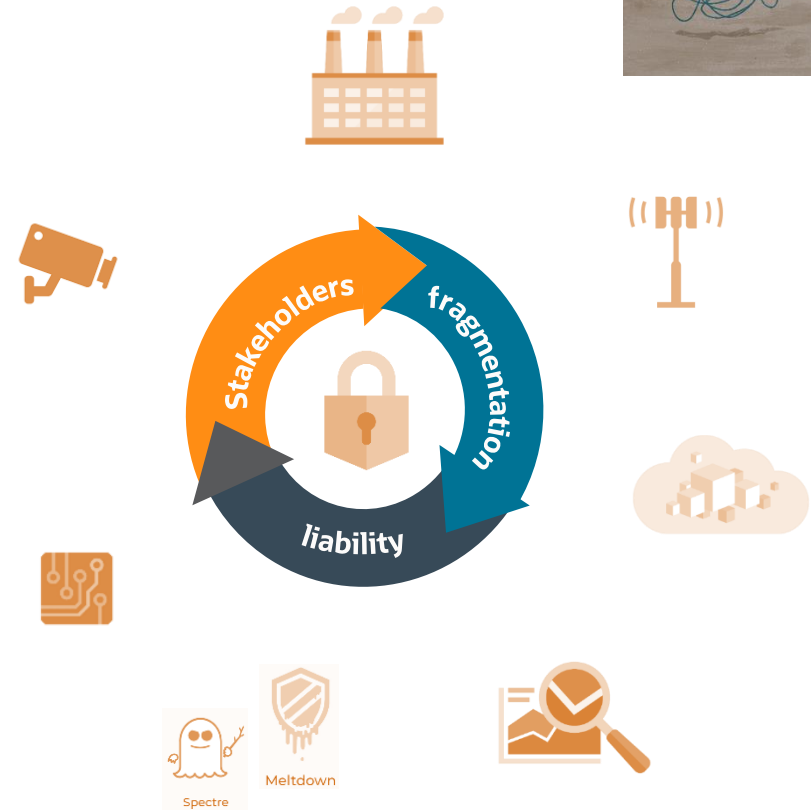
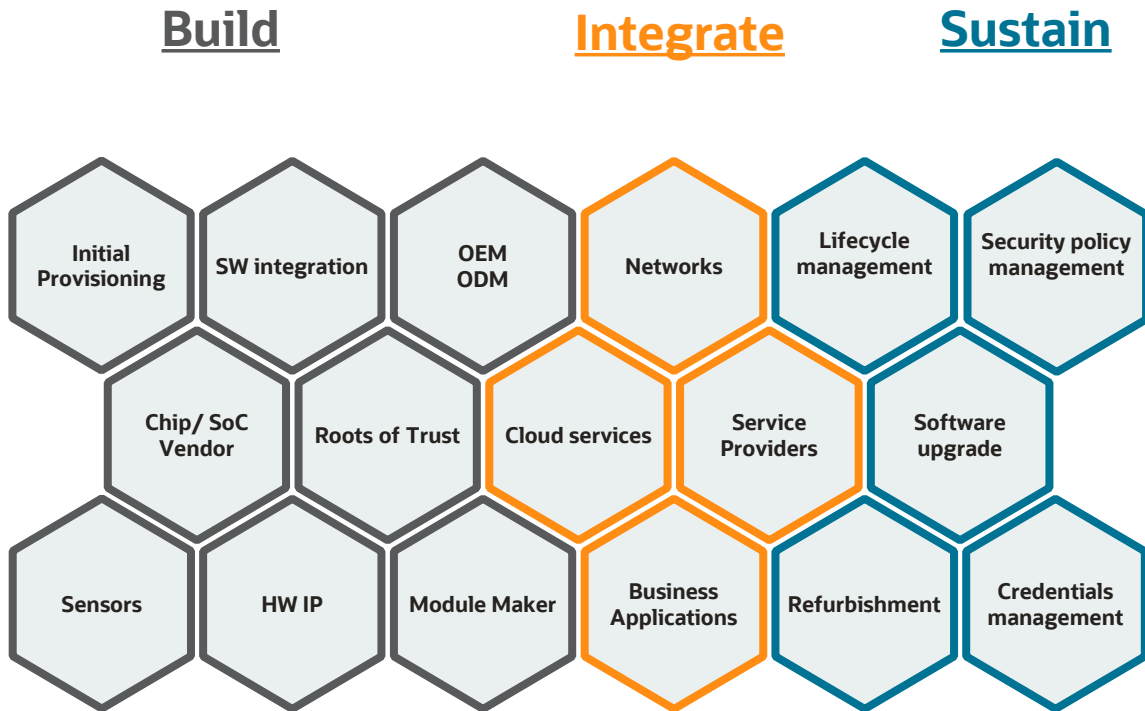
 **SECURE PERIPHERALS**

Securely access and control peripherals, enabling trust and exchange of sensitive data at the very edge.



Security at the device edge

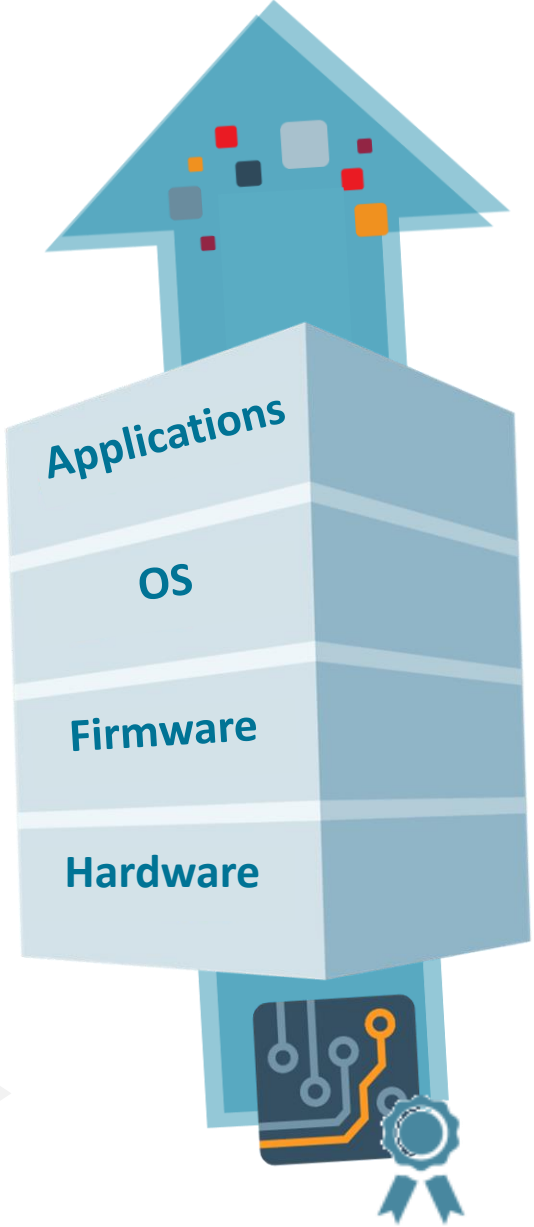
A Complex Ecosystem



Hardware Roots of Trust

Roots of Trust & Hardware Security

- Security relies on **Trust**
- Trust** implies secure design
- Roots of Trust** are Initial Sources of **Trust**
- Higher layers **Trust** lower layers



Hardware Roots of Trust

Trusted Execution Environment

Privileged mode of an Application processor

Removable Secure Element

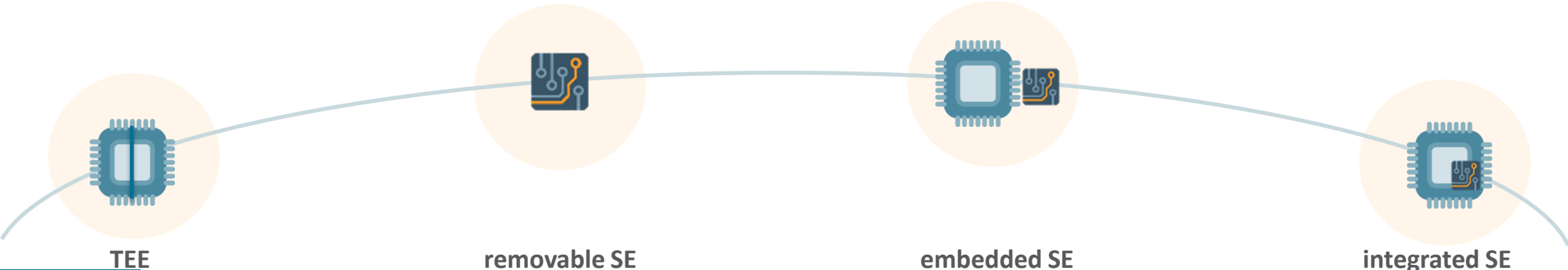
standalone secure microcontroller plugged into host device

Embedded Secure Element

separate chip soldered in host device

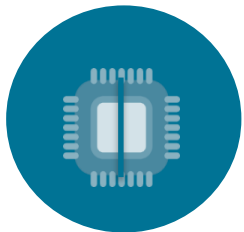
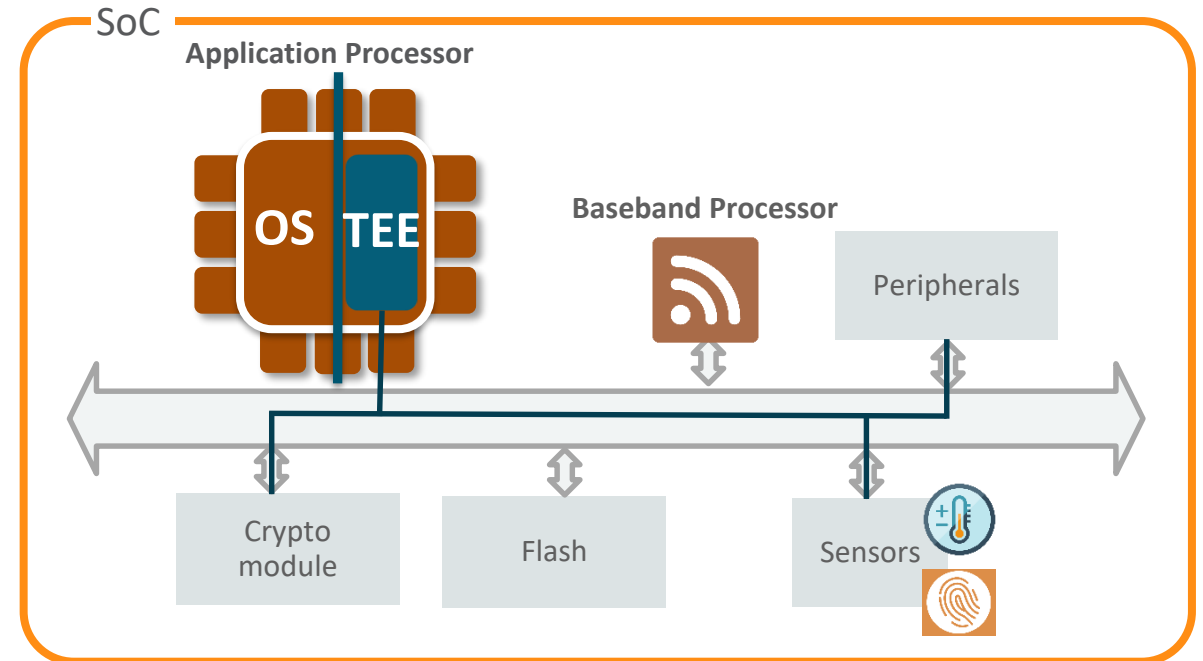
Integrated Secure Element

Dedicated secure core part of the design of a chip



Trusted Execution Environment (TEE)

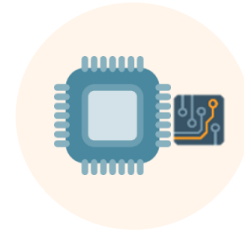
- Two execution modes of the application processor (e.g ARM TrustZone on Cortex)
 - Regular OS runs in the Normal World
 - TEE runs in the Secure World with more privileges
- Secure world can be extended to peripherals to build secure sub systems
 - e.g with cryptographic accelerators
- TEE is protected against software attacks
 - No or poor tamper resistance against hardware attacks
 - Complex and long to certify due to its large scope



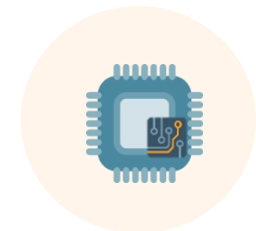
TEE



removable SE



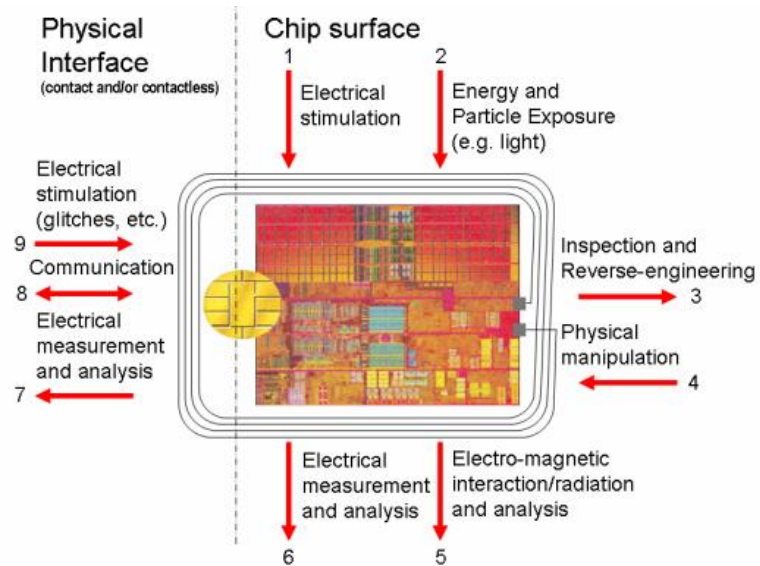
embedded SE



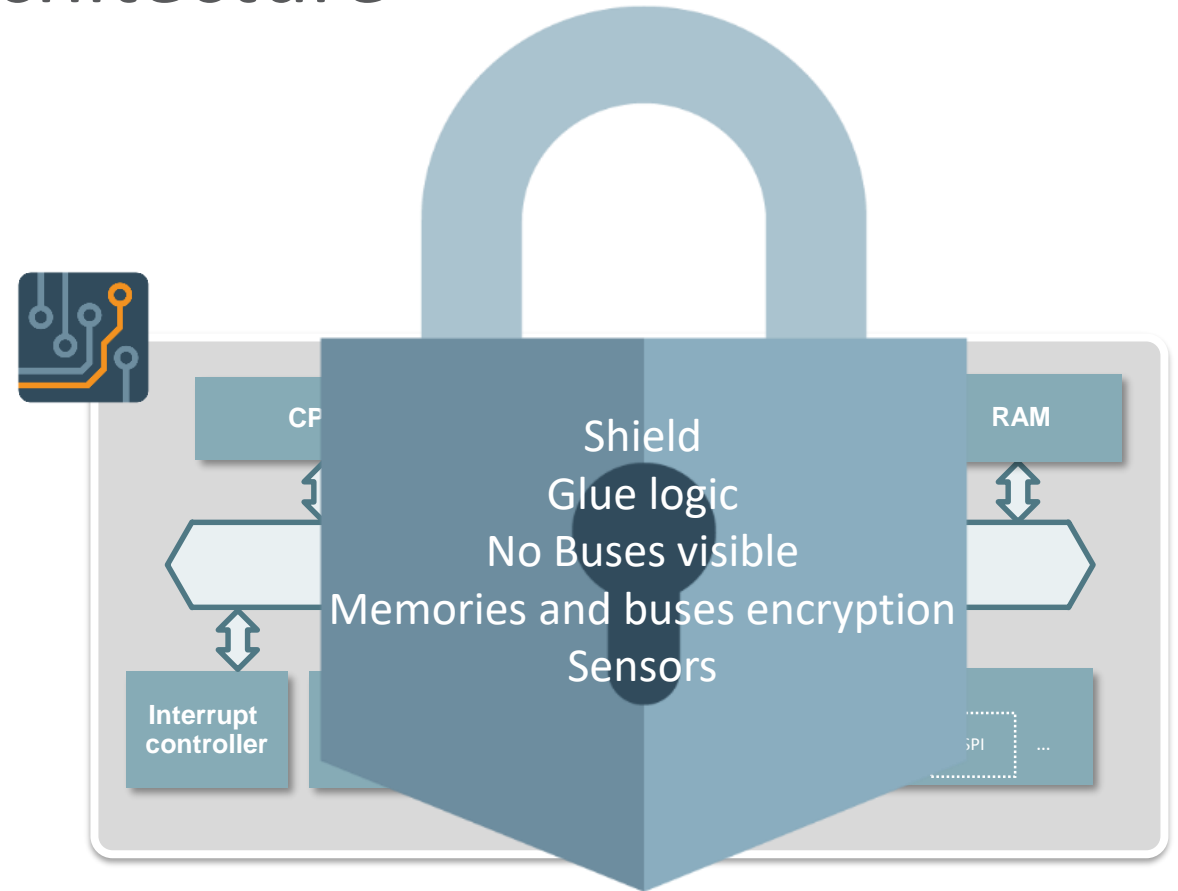
integrated SE

Typical Secure Element (SE) Architecture

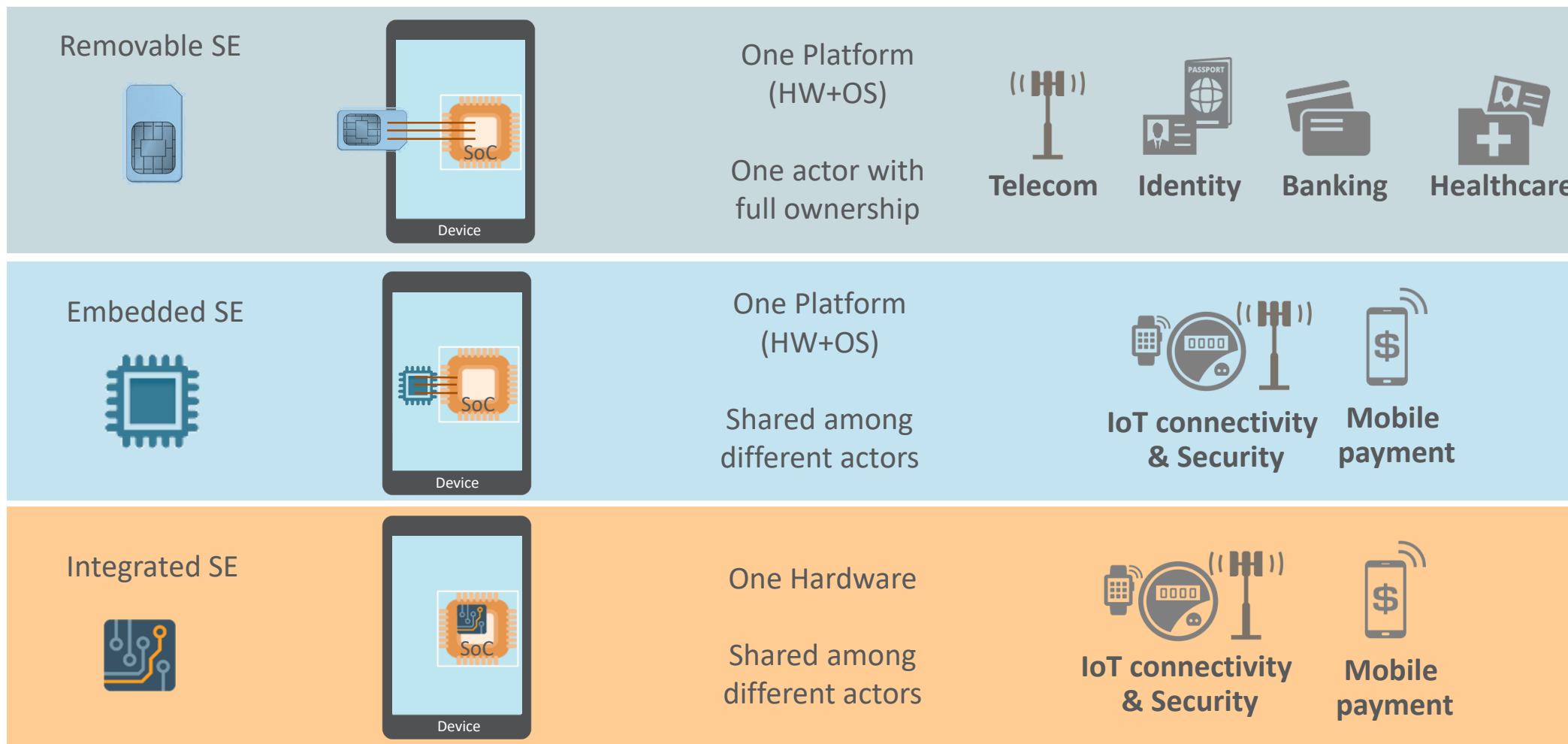
- Tamper Resistance to manage and execute sensitive data:
 - in unprotected environment
 - with non trusted users
- Certified EAL4+ EAL7+







Extract from Eurosmart Security IC Platform Protection Profile

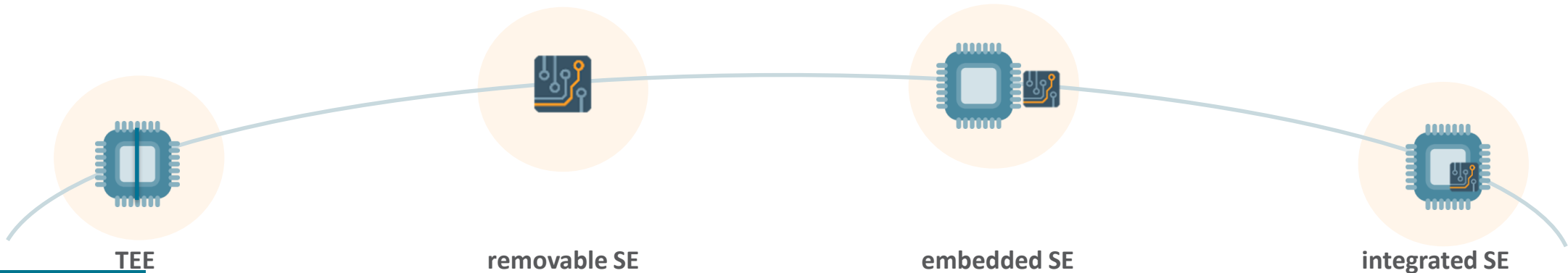


Secure Element Form Factors : Removable/Embedded/Integrated SE

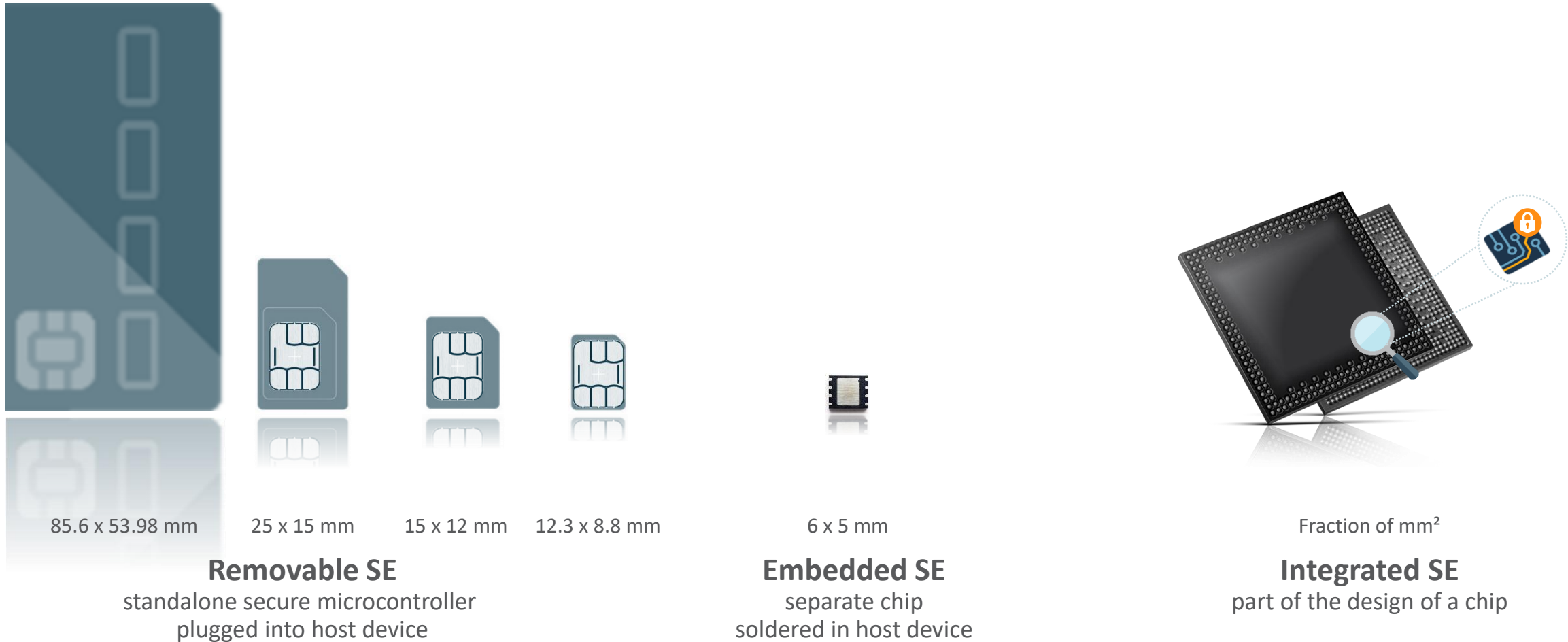


Comparative

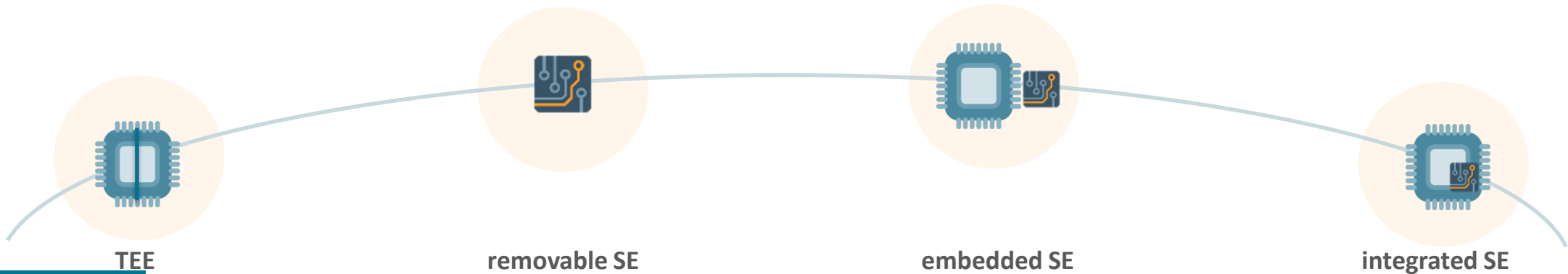
Certification 	+	+++	+++	++
Flash Memory 	~256Kb-2+Mb	~64-512Kb	~64-512Kb	~64-512+Kb
Processing	~128Kb - 2+Mb	~3-12Kb	~3-12Kb	~3-12+Kb
Platform Resources Access 	~200Mhz 1+Ghz	~50Mhz	~50Mhz	~200Mhz
Platform Resources Access	Access to peripherals	Confined to Microcontroller	Usually Confined to Microcontroller	Access to peripherals
Cost 	+	+++	+++	+



Integration trend

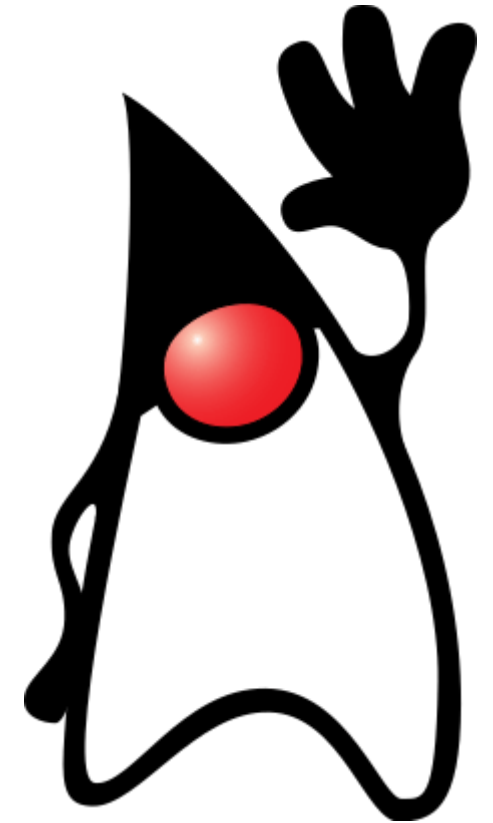


Standards coverage

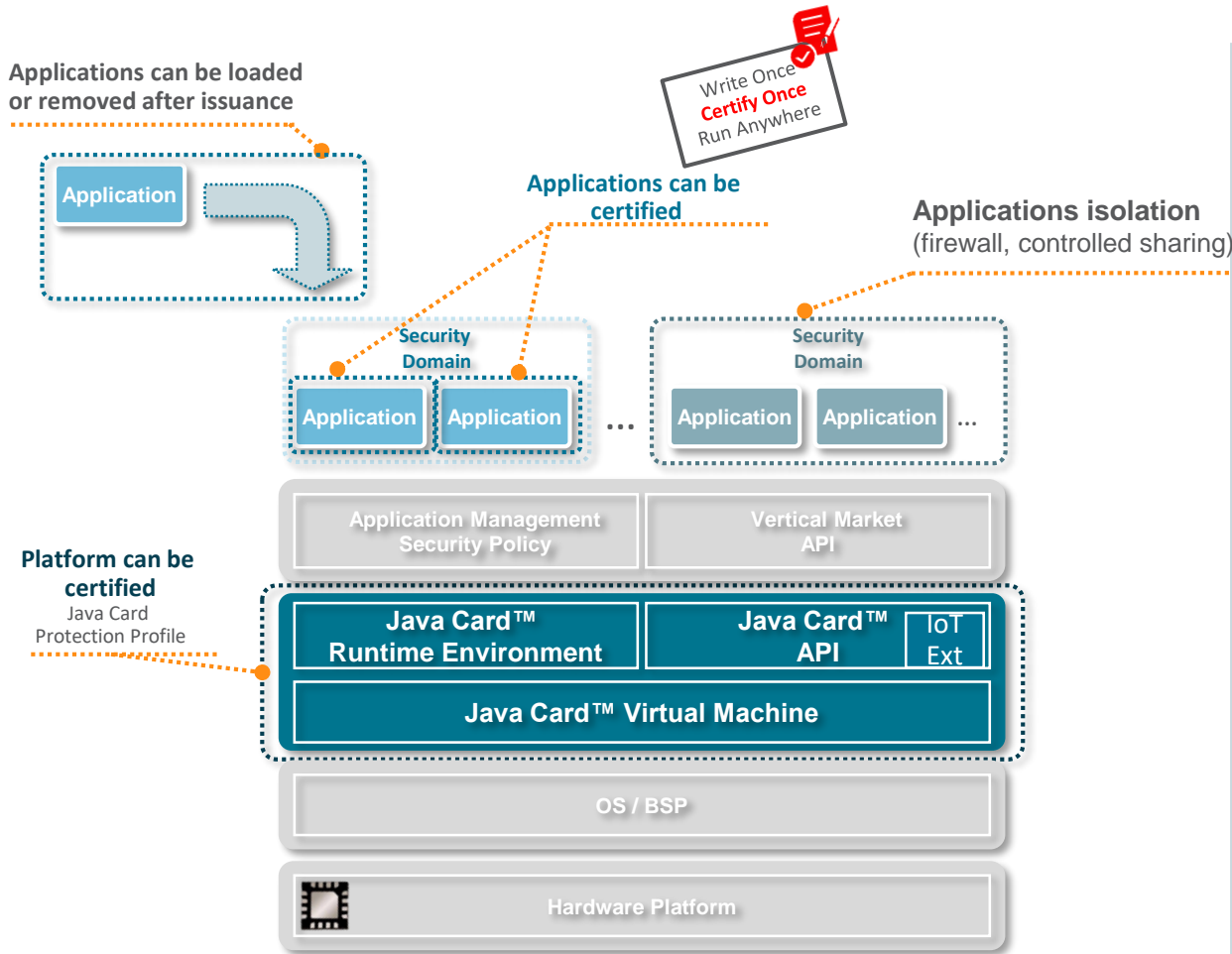


Java Card & IoT

Who already heard about
Java Card?



Java Card Platform



COMPACT VIRTUAL MACHINE

Low footprint Split VM.
Hardware-agnostic Content.

OPEN PLATFORM

Public specification & SDK
Community support through Oracle and Java Card forum
Multi applications

APPLICATION FIREWALL

Allowing Secure Multi-Application and Multi-Tenancy with low memory consumption.

CERTIFIABLE DESIGN

Products certified at Common Criteria EAL 5 and above.
Protection Profile available.

COMPLIANCE

TCK Enabling compatibility across products and implementations.
Align with standards (GlobalPlatform, ETSI, 3GPP, GSMA, ISO...)


IoT EXTENSIONS

Introduced in Version 3.1
Security Service APIs.
GPIO, SPI, ISO support.


Framework to take the Risk out of IoT Security

 **DIGITIZED SIM**
 **MULTI-CLOUD AUTHENTICATION**
 **ADAPTABLE ATTESTATION**
 **SECURE PERIPHERALS**

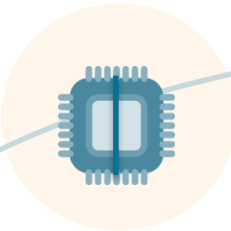



EDGE SECURITY ON ANY HARDWARE
 IoT Security Services with a choice of hardware options

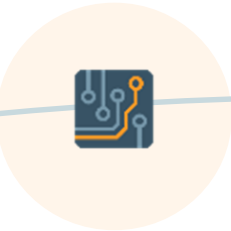

CONNECTIVITY + SECURITY
 Security and SIM applications into one security device


PROGRAMMABLE AND EXTENSIBLE
 New IoT services can be added

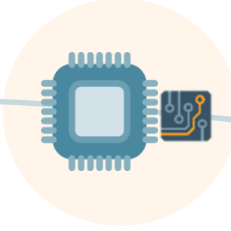

RENEWABLE SECURITY
 Updatability ensures always-current device security



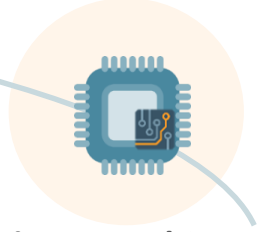
TEE



removable SE



embedded SE



integrated SE



More Information

<https://www.oracle.com/technetwork/java/javacard>



[Java Card Platform Specification 3.1](#)

Latest release of the Java Card specification and the reference for Java Card products.



[Java Card Development Kit Tools](#)

The Java Card Development Kit Tools are used to convert and verify Java Card applications. The Tools can be used with products based on version 3.1, 3.0.5 and 3.0.4 of the Java Card Specifications.

[Java Card Development Kit Simulator](#)

The Java Card Development Kit Simulator includes a simulation component and Eclipse plug-in. Combined with the Java Card Development Kit Tools, it provides a complete, stand-alone development environment.



[Java Card IoT and Security blog](#)

This Blog covers the latest Java technology for small devices and security in the IoT, mobile, ID and Payment.

[Webcast – Secure Business Runs Java Card](#)

[Webcast – How to secure IoT Edge with Java Card](#)

[Webcast – How to secure IoT Edge with Java Card](#)

Q&A



Java™
ORACLE®