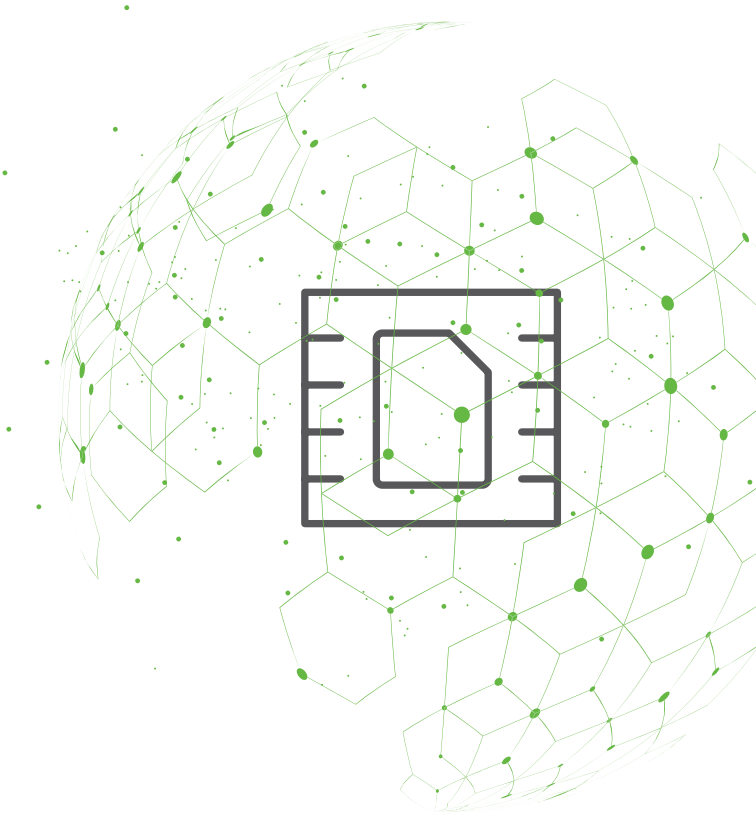
TRUSTED CONNECTIVITY ALLIANCE

Stepping Stones for Java Card Developers: Advancing eSIM Security



As eSIM adoption continues to build, so too does industry demand for using the technology's proven security capabilities to host the applets that enable various value-added mobile services.

These include use-cases where security is paramount:

Payments | Transport ticketing | Identity management | IoT services

The Critical Importance of Applet Security

- To maintain the highest level of security, it is critical that applets are correctly developed.
- **This is even more important with the evolution to eSIM.** A single eSIM can host several profiles, each containing third-party applets that must securely share the resources of the eSIM and the mobile device.
- If one of these applets is vulnerable to malicious software or can be used as a backdoor by hackers, other applets could be compromised and the security and privacy of the communication with that device could be at risk.
- This is why Trusted Connectivity Alliance released clear, industry-recognised guidance to support the development of secure, high-quality applets.

Stepping Stones for Java Card Applet Developers

- *Stepping Stones for Java Card Developers* provides harmonised best practices and security recommendations to maximise interoperability and ensure eSIM applet assets are sufficiently protected.

> Java Card Application developers should comply with *TCA Stepping Stones for Java Card Applet Developers* recommendations.
>
> GSMA™

A Checklist for Secure Applet Development

To offer practical guidance and promote compliance, *Stepping Stones for Java Card Developers* provides a comprehensive checklist that summarises all best-practices and recommendations within the paper. This can be used by application developers, quality and test engineers, and end-customers to verify implementations.

The checklist includes specific recommendations to support secure applet development:

Off-Card Bytecode Verification	• At minimum, follow the "GlobalPlatform Card Composition Model Security Guidelines for Basic Applications". • Verify that the applet passes bytecode verification using latest tools from Oracle.	○
Standard APIs	• Use standard APIs where possible, rather than rewriting methods.	○
Sensitive Data Management	• Implement all rules on sensitive data.	○
Rollback Protection	• Protect sensitive data against rollback attacks.	○
Flow Control	• Implement countermeasures to detect changes to the normal execution flow.	○
Sensitive Standard API	• Use SensitiveResult class when possible.	○
Random	• Do not use deprecated random (ALG_PSEUDO_RANDOM and ALG_SECURE_RANDOM). • Use ALG_KEYGENERATION or ALG_TRNG.	○
Programmatic Exceptions	• Do not use programmatic exceptions to exit from a loop.	○
Java Card RMI	• Do not use Java Card RMI.	○

To view the complete checklist detailing all the recommendations, download the 'Stepping Stones for Java Card Applet Developers' paper in full.

About Trusted Connectivity Alliance

Trusted Connectivity Alliance (TCA) is a global industry association working to enable trust in a connected future. The organisation evolved from the SIMalliance, reflecting the continued expansion of the global SIM industry and the need for broader collaboration.

Its members are leading providers of secure connectivity solutions for consumer, IoT and M2M devices. This spans Tamper Resistant Element (TRE) technologies including SIM, eSIM, integrated SIM, embedded Secure Element (eSE) and integrated Secure Element (iSE), as well as hardware and software provisioning and other personalisation services.