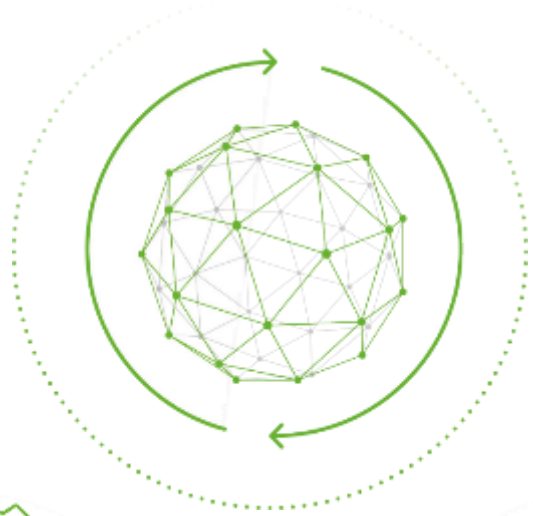
TCA Java Card Stepping Stones: Advancing eSIM Security

Amedeo Veneroso

Chair, TCA Interoperability Working Group

About Trusted Connectivity Alliance

Trusted Connectivity Alliance (TCA) is a global industry association, working to enable trust in a connected future.



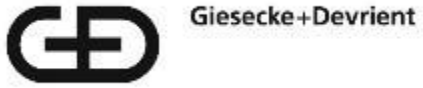
VISION:

To drive the sustained growth of a connected society through trusted connectivity which protects assets, end user privacy and networks.

Market Monitoring	Specifications and Interoperability	Industry Engagement and Strategy	Education

Our Members

Executive:



Full:

eSIM:

Ordinary:

Trusted Connectivity Alliance:
eSIM Industry Insights 2024

Trusted Connectivity Alliance (TCA) is the industry association estimated to represent approximately 98% of the global eSIM hardware market.

TCA is the only organisation to offer a quantitative global view of eSIM shipments, providing both actual and forecast data. This offers unparalleled and authoritative intelligence into the ongoing development of the eSIM ecosystem.

A Landmark Year of Growth for the Global eSIM Ecosystem

- **eSIM shipment volumes collectively reported by TCA members surpassed half a billion units increasing**

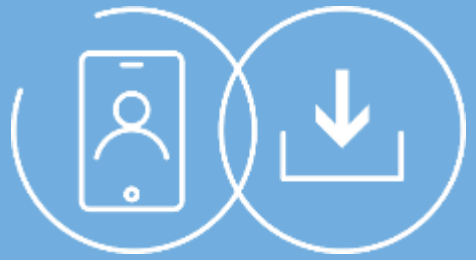
↑ **35%** year-on-year

to reach **503 million units**

TCA estimates that the total available market for eSIM was

514 million units

- **Growing availability of eSIM-enabled devices was matched by rising consumer adoption.**



Consumer eSIM profile downloads increased ↑ **56%** year-on-year

eSIM profile downloads - also known as eSIM profile transactions - refer to the number of times a mobile operator profile was downloaded to a device.

Improved Economic Conditions and Continued Innovation Drive eSIM Growth

The eSIM market was positively impacted by:

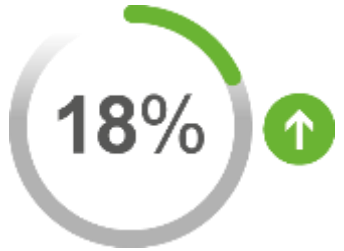
- Improving economic conditions that saw demand for smartphones and mobile subscriptions recover.
- The launch of new eSIM-only devices, eSIM-enabled mid-range models and 5G smartphones.

North America once again led in consumer eSIM adoption due to the prominence of eSIM-only devices and because operators continued to pursue 'digital-first' strategies.

Profile downloads more than doubled in Asia, while Europe also saw strong uptake.

Increased consumer uptake was supported by ongoing investment in the enabling infrastructure.

- Number of deployed consumer eSIM SM platforms rose by



eSIM Subscription Manager (SM) platforms enable the remote provisioning and lifecycle management of eSIMs.

TCA members also reported significant M2M eSIM adoption.

Looking ahead, the release of GSMA's eSIM IoT Specification (SGP.32) stands to accelerate the use of eSIM technology across IoT use-cases.

TRUSTED CONNECTIVITY ALLIANCE

Spotlight on Security

The Critical Importance of Applet Security

As momentum and adoption builds, there is increasing industry demand for the delivery of various services through eSIM technology.

These include highly sensitive applications where security is paramount, including payments, transport ticketing, identity management and secure IoT services.

The Critical Importance of Applet Security

To maintain the highest level of security – particularly for sensitive use-cases – it is important that applets are correctly developed.

This is even more important with the evolution to eSIM.

On a single eSIM, several profiles containing applets by third parties are downloaded. These must all securely share the resources of the eSIM and the mobile device.

This means that if one of these applets is vulnerable to malicious software, the security of the entire device and the data it stores could be compromised.

Applet Security in Focus

As part of GSMA's Coordinated Vulnerability Disclosure programme, security researchers highlighted an issue impacting eSIM technology.

The researchers described how Remote Application Management (RAM) keys could be misused to install malicious Java Card Applications within a profile on an eUICC supporting Java Card technology.

Although though no direct consequences of the attack have been identified for most eSIMs on the market, downloading malicious Java Card applications is a significant security concern.

A Collaborative Response

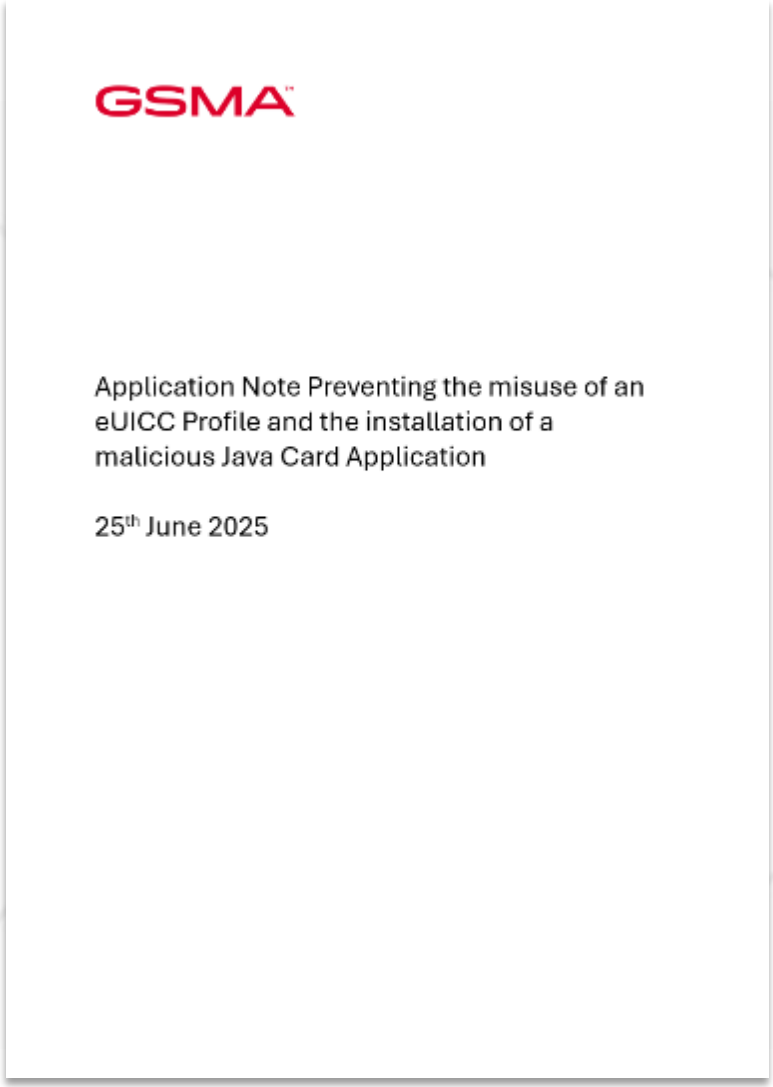
Following the disclosure, GSMA published an Application Note in June 2025 to prevent the misuse of an eUICC Profile and the installation of a malicious Java Card Application.

Other actions – including the update of the eSIM specifications and other GSMA-related documents – are now ongoing.

Longer-term, the industry is working collaboratively to further advance the security of the eSIM.

What Does This Mean for Application Developers?

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



TRUSTED CONNECTIVITY ALLIANCE

A Checklist for Secure Applet Development

What are the TCA Stepping Stones for Java Card Applet Developers?

Enables Java Card Applet Developers to maximise interoperability and security across eSIM deployments.

Provides:

- An analysis of key recent Java Card technology update.
- Guidance on the impact of broader ecosystem developments from 3GPP, ETSI and GSMA.
- A series of best practices and security recommendations.
- A comprehensive ‘interoperability checklist’ to help address common challenges and deliver high-quality applets.

It continues the success story of the Stepping Stones, born in 2003 with Java Card and continued with NFC, SCWS, Mobile Connect

Security Approach in the TCA Stepping Stones

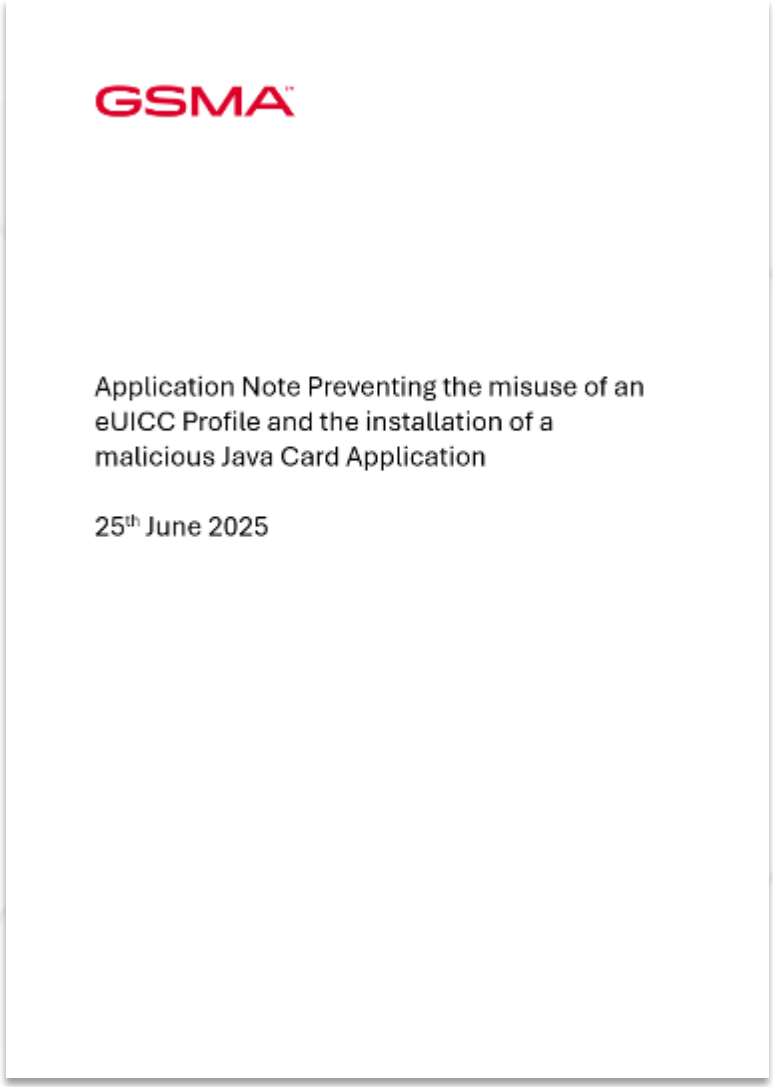
From SIM to eSIM

- In **SIM certified products,** typically the certification results in a series of security guidelines (like the “Operational procedure” of Common Criteria) for the Application developer
- Such guidelines, even with commonalities, differed from SIM provider to SIM provider due to different operating system implementation
- Applications targeting a specific certified SIM card had to verify its adherence with the related guidelines
- In eSIM, this is not possible: applet as part of interoperable profiles can be downloaded on potentially any GSMA certified eSIM

TCA with the Stepping Stones has made the effort of collecting the majority of security recommendations from the various guidelines, trying to harmonize them in a common set

Bytecode Verification

"Java Card Application developers should comply with "TCA Stepping Stones for Java Card Applet Developers" recommendations ***and in particular bytecode verification****"*



Off-card Bytecode Verification

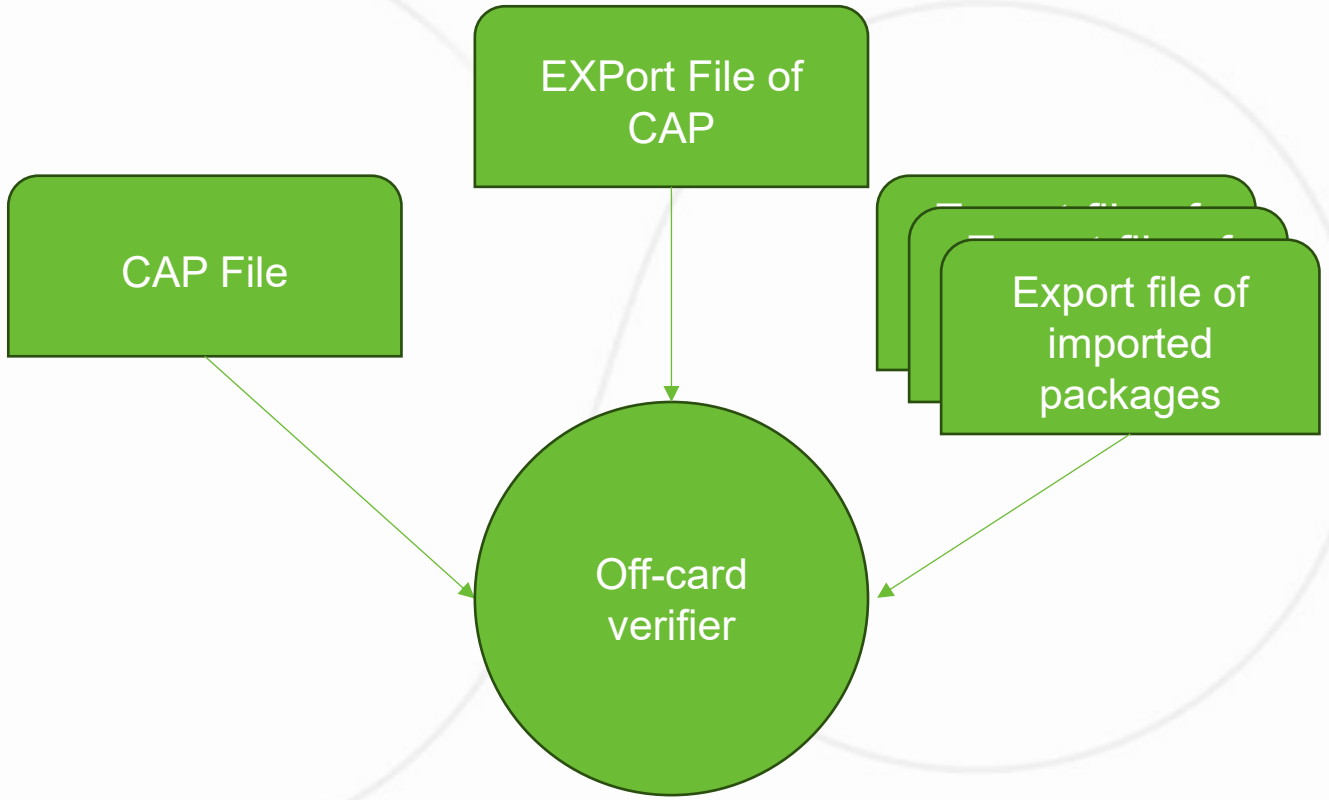
- Java Card applets must, at a minimum, follow the “GlobalPlatform Card Composition Model Security Guidelines for Basic Applications”.

- In particular, Java Card applets must successfully pass byte code verification using tools from Oracle. The tools used for byte code verifications shall be the latest versions available.

- Bytecode verification is a process that **statically analyses** the Java bytecode – the intermediate language into which Java source code is compiled – to ensure it adheres to the strict rules of the Java language and the JCVM specification
  - Enforce type safety and memory access restrictions
  - It is a cornerstone of correct API invocation and sandboxing

Off-card Bytecode Verification

- Off-Card Verifier accesses the CAP file, its export file and the imported export files to verify that no malicious manipulation has been performed
- The operation can be performed only when all those elements are present
- In particular, it requires that the CAP file contains the ***Descriptor component*** that is optional

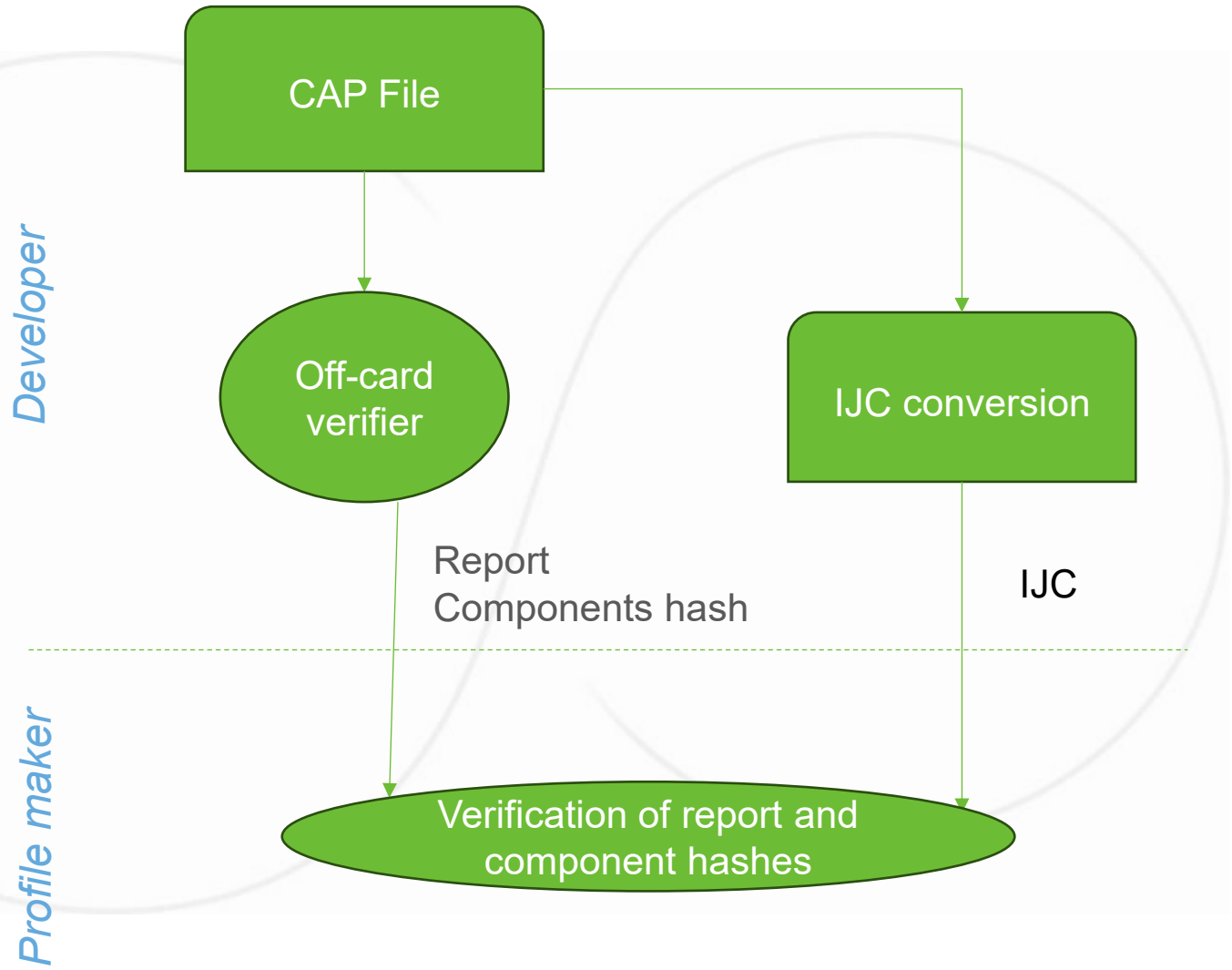


Off-card Bytecode Verification

- A popular format of applet exchange between developers and profile makers is the *Interoperable Java Card Format* (.ijc)

- IJC is an optimised format that does not contain the Descriptor

- It is advised that:
  - The developer executes the BCV and computes the SHA-256 (hash) of the components
  - The profile maker verifies the BCV report and the SHA-256 of the components



Application AID and Standard APIs

Java Card applet AID must be set as defined in ETSI TS 101 220. In particular, the applet developer shall use its own RID registered at ISO as defined in 7816-5.

The standard API should be used whenever possible, rather than rewriting methods.

This holds for:

- Java Card standard API
- GlobalPlatform API
- UICC API
- USIM API

The usage of the Java Card RMI mechanism is prohibited

Due to lack of security related features (e.g. authentication and secure channels).

For Sensitive Applets: Sensitive Data Management

- Sensitive data must be initialised at the beginning and cleared at the end of the session.
- Sensitive data should be stored in transient data.
- Always clear, with random data, (global) arrays used to store temporarily sensitive data. Confidential data must not be stored in plain (e.g. may be ciphered or masked and stored).
- Sensitive constant value: When a constant is used as reference value for a sensitive action, avoid choosing 0x00 or 0xFF for this constant.
- Sensitive data must be protected against rollback attacks.

For Sensitive Applets:
Flow Control

To protect against multiple perturbations, countermeasures should be implemented to detect any change to the normal execution flow.

If an inconsistent state is reached, an appropriate measure shall be applied according to applicable context (e.g. block the application, reset).

For Sensitive Applets:
Sensitive Standard API

When using a method of a standard API that needs absolutely to be executed, some consistency checking must be done to assume it has been correctly executed.

Since Java Card 3.0.5, the SensitiveResult class can be used for asserting results of sensitive functions.

For Sensitive Applets:
Random

Avoid using deprecated random (ALG_PSEUDO_RANDOM and ALG_SECURE_RANDOM).

Always use appropriate random depending on the usage. In particular, always use either ALG_KEYGENERATION or ALG_TRNG algorithms for sensitive use cases

For Sensitive Applets:
Programmatic Exceptions

Avoid the usage of programmatic exceptions to exit from a loop.

For example, do not parse table until catching an index out of bounds exception).

Application Checklist

The TCA Stepping Stones for Java Card Applet Developers contains a checklist to verify that best practices are followed.

The checklist can be used by:

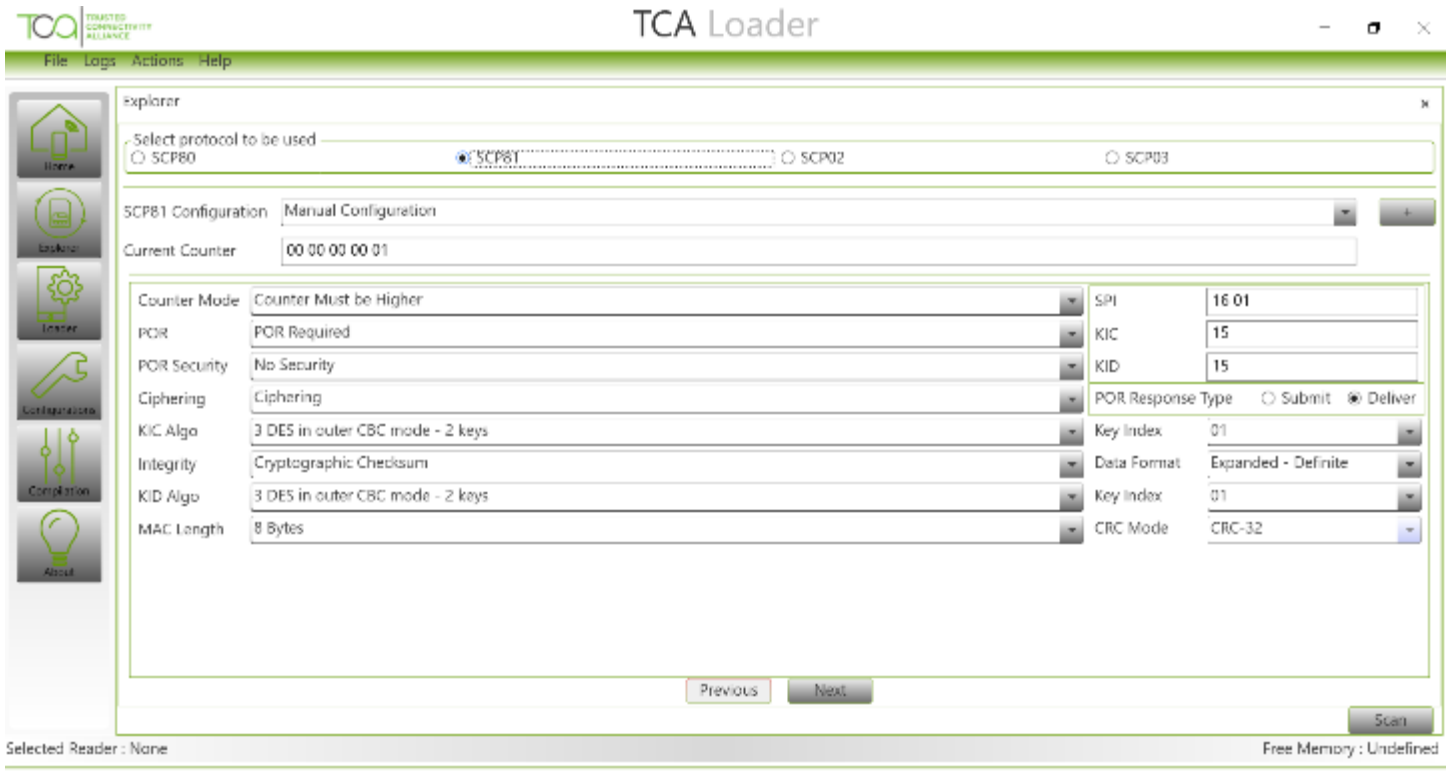
- Application developers, to take into account rules during applet design.
- Quality and test engineers, to verify proper implementation.
- Customers, as an evidence that application developers have respected the mentioned rules.

30. Rollback protection	Only applicable to sensitive applet - rollback protected	☐
31. Flow control	Only applicable to sensitive applet - flow control implemented	☐
32. Sensitive standard API	Only applicable to sensitive applet - Use `SensitiveResult` class when possible	☐
33. Random	Only applicable to sensitive applet - Use `ALG_KEYGENERATION` or `ALG_TRNG`	☐

TCALoader

- Enables mobile operators and application developers to download, install and manage applications on the UICC / eUICC to test interoperability across different deployments.

- Before loading applications, byte code verification shall be performed off card.



TCA's Interoperable Profile Package Specification

Used in every eSIM (eUICC) deployed in the field.

Enables mobile operators to load interoperable connectivity profiles in an eSIM, regardless of the SIM vendor.

Addresses the challenge of remotely managing 5G and network constrained IoT devices.

Latest version also includes updates and clarifications to promote security and interoperability.

Conclusions

The critical importance of applet security has been brought into sharp focus.

Applet developers should comply with the security recommendations within TCA's Java Card Stepping Stones document.

TCA continues to work collaboratively across the industry to maximise security and interoperability.

Audience Q&A

www.trustedconnectivityalliance.org

Trusted Connectivity Alliance

Thank You

For more information, please contact:
info@trustedconnectivityalliance.org

www.trustedconnectivityalliance.org