IoT Week 2022

Evolving cellular connectivity for the IoT

Saïd Gharout, PhD
Chair of the TCA IoT RSP Working Group
Head of Standards at Kigen

14/10/2022

About Trusted Connectivity Alliance

Trusted Connectivity Alliance (TCA) is a global, non-profit 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 Membership

TRUSTED CONNECTIVITY ALLIANCE

Founding:

Giesecke+Devrient Creating Confidence

IDEMIA augmented identity

life.augmented

THALES

Valid

Executive:

Kigen

NXP

Full:

CARD CENTRIC SOLUTIONS LTD. CARD CENTRIC

东信和平 EASTCOMPEACE

Linxens crafting the future of connections

OASIS smart sim Embed. Connect. Activate

Qualcomm

TIANYU

WORKZ

Ordinary:

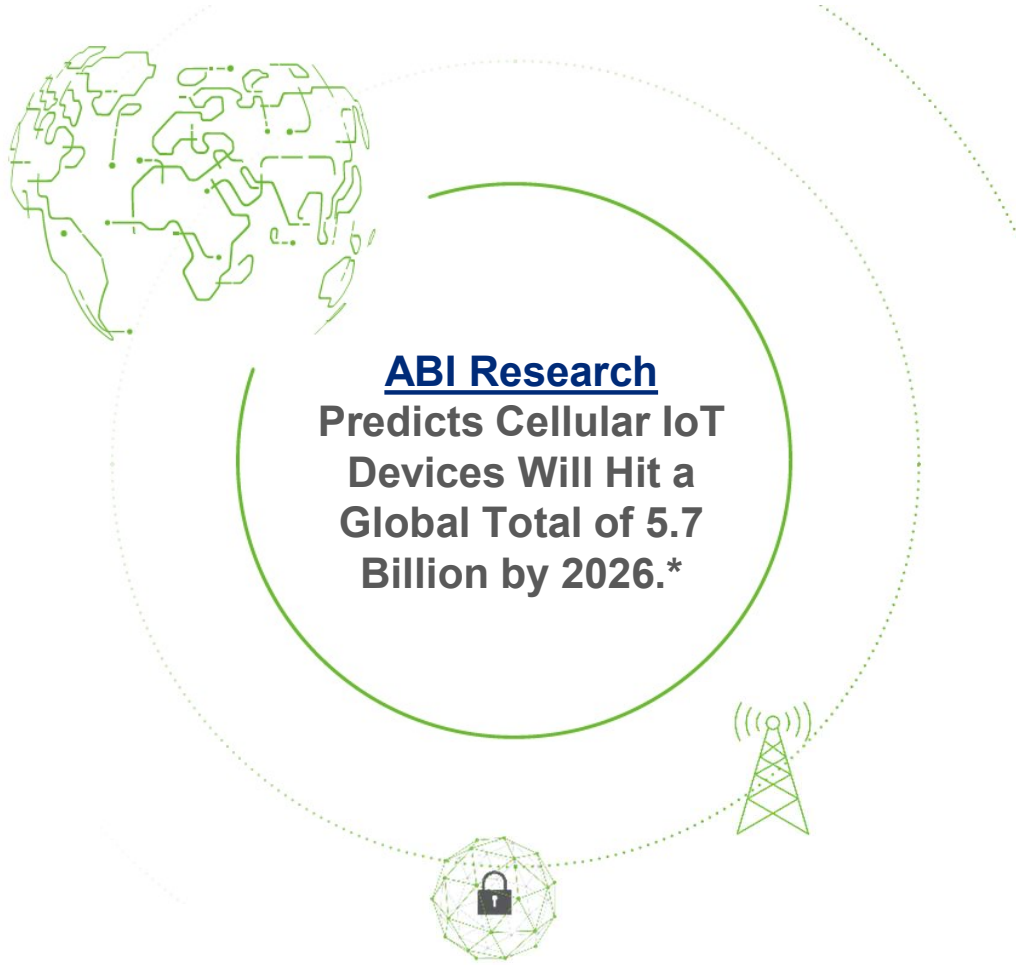
COMPRION

An increasingly connected world

A rapidly growing array of devices, low-cost sensors and systems are combining to form a vast IoT ecosystem.

More and more industries are harnessing the power of the IoT to enhance services, transform operations and maximise efficiencies.

It's crucial that the industry can overcome fragmentation, vulnerabilities and complexity that could hamper IoT deployments.



RR1

Potential of eSIM

- eSIM provides **flexible, trusted connectivity** to meet complex logistical needs across various industry verticals.
- Multiple connectivity profiles, post-issuance personalization and remote management capabilities **simplify supply chains and ease deployment challenges.**
- Based on the most widely distributed **secure application delivery platform** in the world.
- **Advanced security and cryptographic features** for operating system programmes, keys and certificate data.

Slide 5

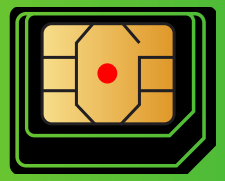
RR0 Updated icons
Rebecca Richardson; 2022-10-06T15:54:42.852

RR1 Propose having this as a separate slide and have added some additional points on the advantages / benefits of eSIM
Rebecca Richardson; 2022-10-06T15:54:58.156

eSIM: The key to connect & secure objects

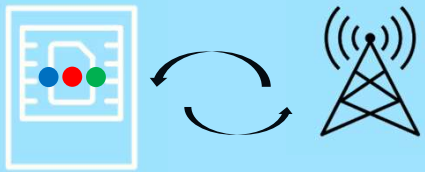
TRUSTED CONNECTIVITY ALLIANCE

All SIM



- Enables a device to connect to one cellular network
- Most widely distributed secure platform in the world

eSIM additions

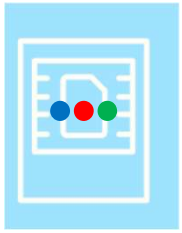


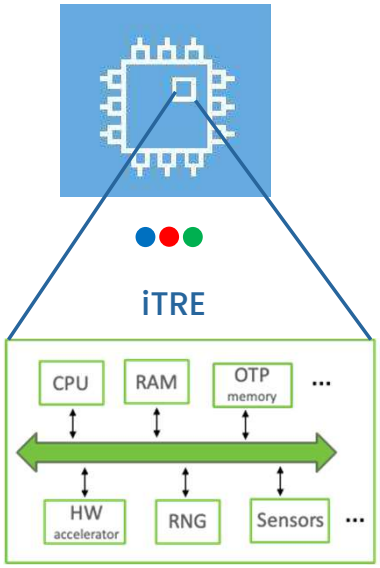
- Execute sensitive operations as mandated by certified schemes (e.g. payment, ID, cybersecurity)
- Multiple Mobile Network Operators (Remote provisioning of connectivity profile)
- **Dynamic mitigation capability:** Immediate security updates and upgrades; responsive to emerging threats and attacks

Potential of iSIM

- Integrated SIM technologies can provide interoperability and security levels **that match eSIM and removable SIM**.
- All cellular devices can **directly benefit from the technical advantages** offered by integrated SIM solution: **utilities, logistics, consumer devices.**
- Performance advantages include **low energy consumption**, **accessible memory**, **computing power** and **performance**.

eSIM / iSIM solutions





Discrete eUICC: An eUICC implemented on separate standalone hardware, including its own dedicated volatile and non-volatile memory. A Discrete eUICC can be removable or non-removable.

- **eSIM:** eSIM is the generic term applied to devices and eUICCs that support Remote SIM Provisioning as defined by GSMA.

Integrated eUICC: An eUICC implemented on an integrated TRE (Tamper Resistant Element).

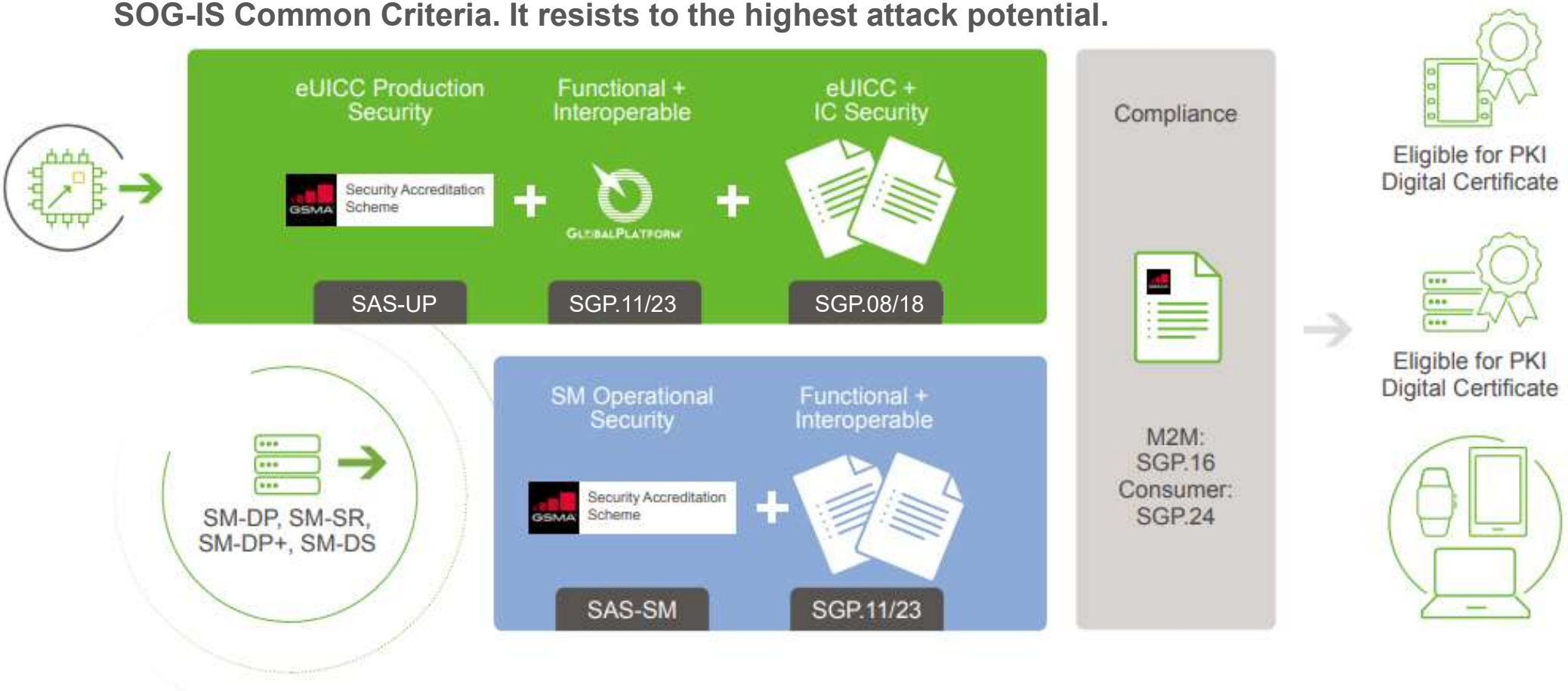
Integrated TRE: A TRE integrated inside a System-on-Chip (SoC), optionally making use of remote volatile and/or non-volatile memory.

- **Integrated SIM:** Either an integrated eUICC or an integrated UICC.

Source TCA: https://trustedconnectivityalliance.org/wp-content/uploads/2022/04/TCA_INTEGRATED-SIM_WHITEPAPER_FINAL.pdf

eSIM / iSIM Certification Programme

- Production environment certification: covered by GSMA SAS (Security Accredited Scheme).
- Functional and security certifications of the eUICC.
  - **The eUICC is security certified using either GSMA eUICC Security Assurance scheme or SOG-IS Common Criteria. It resists to the highest attack potential.**



Leveraging eSIM and iSIM for the IoT

TRUSTED CONNECTIVITY ALLIANCE

Simple and resilient remote activation and management, alongside robust, dynamic security for devices and data.

Most enterprises want their data to be end-to-end protected: from the IoT device to the backend Server/Cloud.

(D)TLS security, together with the secure storage of the credentials used for the connection, enables this.

To ensure the integrity and authentic provenance of information received from a device and to approve a transaction, a signature is required.

GSMA

TRUSTED CONNECTIVITY ALLIANCE

IoT SAFE

IoT SIM Applet For Secure End-to-End Communication

98% of Enterprises want end-to-end solutions that protect data from place of collection, to cloud

Secure Element as a root of trust

Protecting data using the credentials inside the secure element

Inter-operable, advanced cryptographic features of an eSIM/iSIM/SIM

IoT SAFE protects IoT data from chip to cloud(s)

Source: GSMA Intelligence, Dec 2020

IoT SAFE – a TCA and GSMA initiative

TRUSTED CONNECTIVITY ALLIANCE

To further extend the capability of the SIM, GSMA and TCA have partnered on IoT SAFE (**IoT S**IM **A**pplet **F**or Secure **E**nd-2-End Communication).

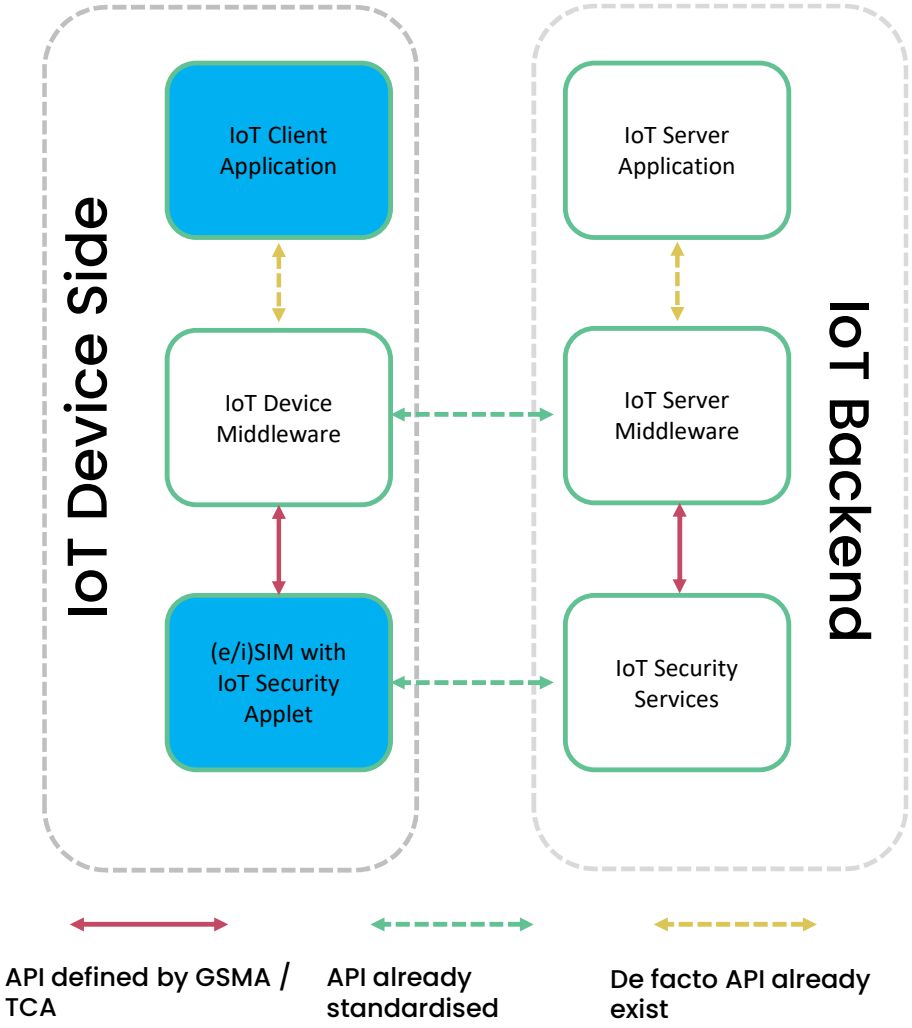
Specifies a common API and defining a standardised way to leverage the SIM/eSIM/iSIM to securely perform **mutual authentication** between IoT Device applications and the cloud.

Ensures maximum robustness of the mutual authentication, due to all critical security functions and long term keys being processed by IoT SAFE in the SIM/eSIM/iSIM. The long term keys never leave the (e/i)SIM.

Generate at SIM/eSIM/iSIM the session keys that are used to protect the IoT data in terms of confidentiality, integrity and authenticity.

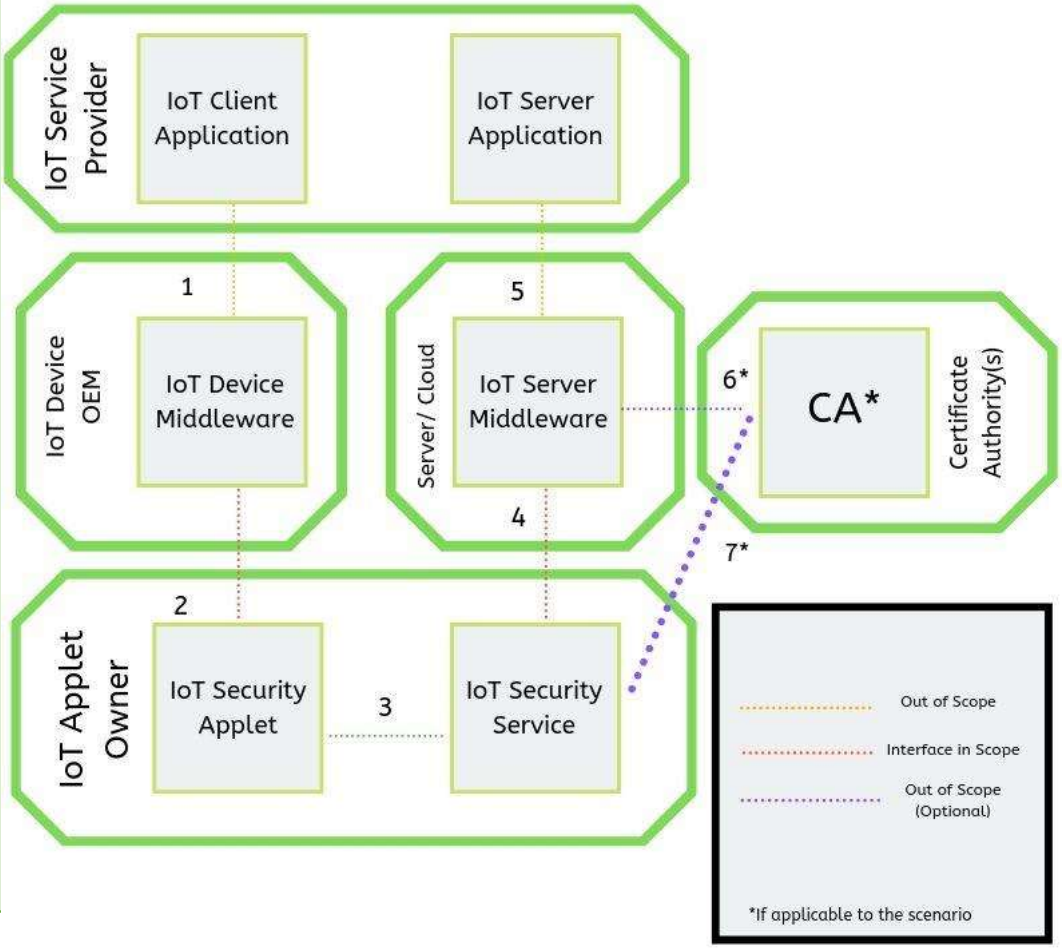
On-board -at SIM/eSIM/iSIM- generation of keys (symmetric and asymmetric).

Removes the IoT Device and SIM applet fragmentation barrier by specifying a common “IoT Device to IoT security applet” API.

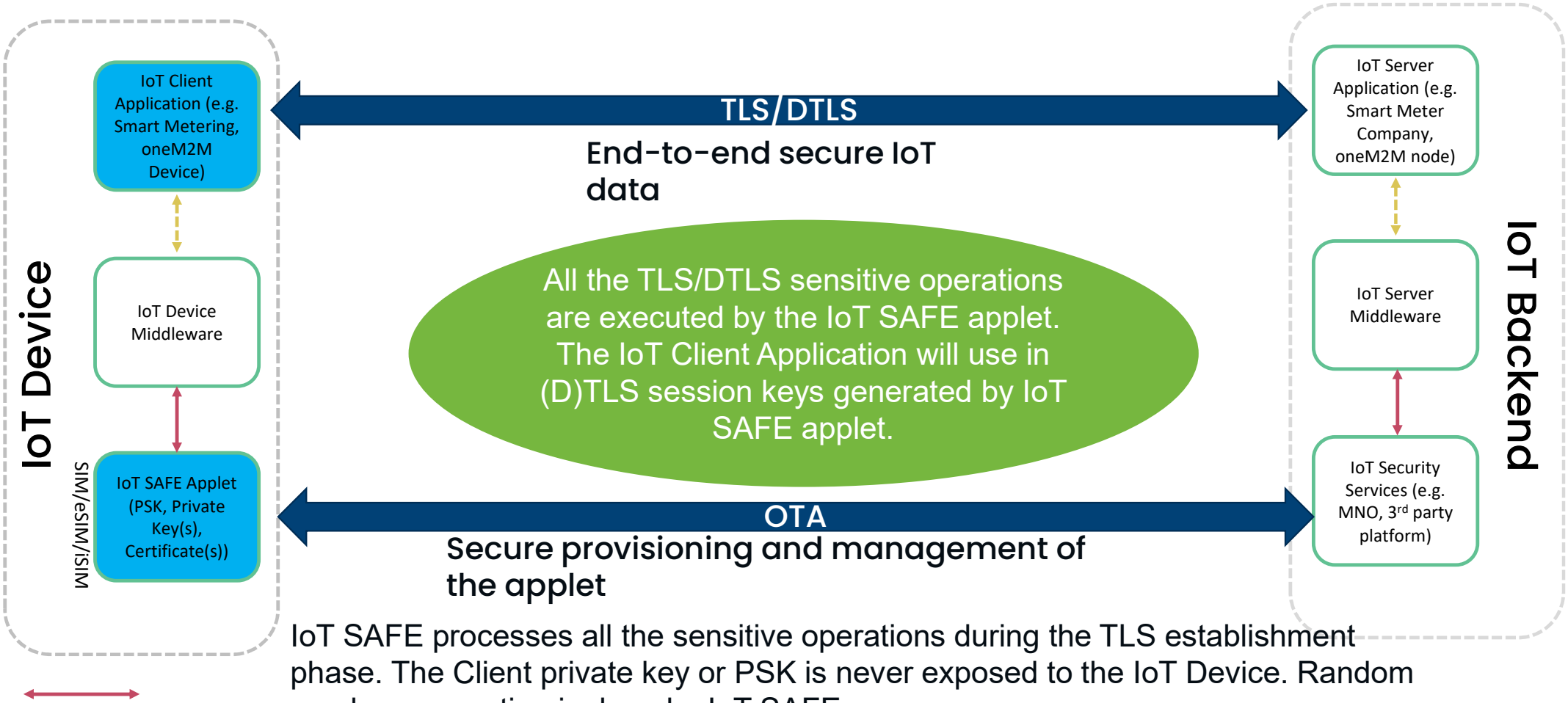


eSIM as RooT of Trust for the IoT data

- Applet specification (GSMA IoT.05) developed by the TCA IoT Working Group:
  - IoT Security Applet; Device-to-Applet Interface of the Asymmetric Cryptography Applet (ACA)'
- Compliant with GSMA requirements defined in GSMA IoT.04 'Common Implementation Guide to Using the SIM as a 'Root of Trust' to Secure IoT Applications'
- Two types of IoT SAFE Applet
  - IoT SAFE #1 uses digital certificates for authentication of server and devices.
  - IoT SAFE #2 uses pre-shared keys for authentication for more constrained devices.



IoT SAFE in practice



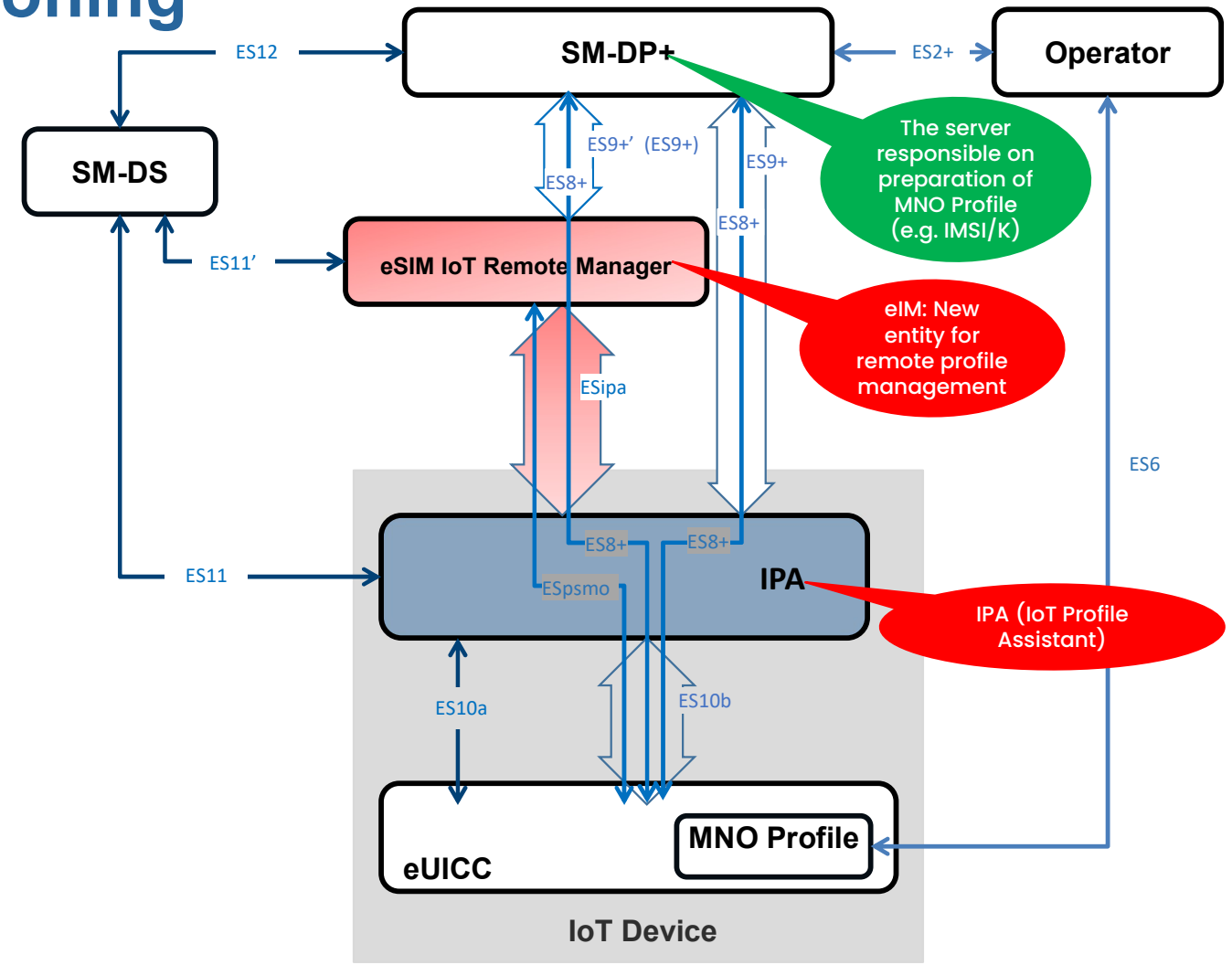
IoT SAFE processes all the sensitive operations during the TLS establishment phase. The Client private key or PSK is never exposed to the IoT Device. Random number generation is done by IoT SAFE.

IoT Remote SIM Provisioning

- Ongoing work at GSMA eSIM to create a new technical specification to cover:
  - UI Constrained Devices
  - Network Constrained Devices (e.g. LPWAN)

- Ongoing discussion on how the eSIM messages can be transported to the IoT Device.
  - There will be a need to use transport protocols where TCP could not be supported due for example to LPWAN bandwidth constraints. E.g. CoAP/UDP.

- TCA is working on a template for MNO Profile for IoT.



What is next?

TRUSTED CONNECTIVITY ALLIANCE

TCA is driving eSIM interoperability and expanding eSIM benefits to emerging IoT market segments.

TCA published v3.2 of its eUICC Profile Package Technical Specification in May 2022, to include support for GlobalPlatform's Secure Channel Protocol (SCP) '11' and Domain Name Server (DNS) Configuration to ensure proper onboarding.

Version 3.3 of the eUICC Profile Package Technical Specification is planned for later this year, to define a minimum 'lightweight' profile to address the challenge of provisioning profiles for network-constrained devices.

Download TCA's technical and educational 5G resources at:
www.trustedconnectivityalliance.org

Q&A

TRUSTED CONNECTIVITY ALLIANCE

www.trustedconnectivityalliance.org

Trusted Connectivity Alliance

@_TCAlliance