RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **SAT-R01**

How Tamper Resistant Elements Can Secure the IoT

Jean-Louis Carrara

Trusted Connectivity Alliance / Kigen
Twitter: @_TCAlliance

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

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.
- **MISSION:** To collectively define requirements and provide deliverables of a strategic, technical and marketing nature that enable all stakeholders in our connected society to benefit from the most stringent secure connectivity solutions that leverage our members' expertise in tamper proof end-to-end security.

Specifications and Interoperability	Market Monitoring	Industry Engagement and Strategy	Education

Our Membership

Founding:

Giesecke+Devrient Creating Confidence · IDEMIA · 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:

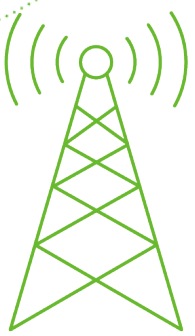
COMPRION

Security in an increasingly connected world

The number of IoT connections is forecast to reach **24 billion by 2025** (Source: GSMA)*

The global IoT market could be **worth $900 billion** in revenue by 2025**.

- As more and more user data and critical information is shared by connected objects, security becomes vital to protect assets, IP, privacy, users, businesses and brands.
- However, innovation has outpaced security and privacy across the IoT landscape.
- Many manufacturers have adopted a ‘connect first, think later’ strategy, where security has been an afterthought.



TRUSTED CONNECTIVITY ALLIANCE

*https://data.gsmaintelligence.com/research/research/research-2020/iot-connections-forecast-the-impact-of-covid-19

**https://www.gsma.com/iot/resources/gsmai-iot-revenue-2020.

Understanding IoT security

The challenge

Insecure objects are an easy target for:

Physical or proximity attacks on a SINGLE device

Remote attacks from the cloud to MANY devices

- Manufacturers of traditionally offline products have not previously had to consider the digital security and privacy implications of their products.
- This has resulted in a significant knowledge and capability gap.
- When security and privacy 'by-design' is neglected, end-users and actors in the connected value chain are left vulnerable.

Increasing IoT regulations, frameworks and guidance

NIST

ETSI

enisa

National Cyber Security Centre
a part of GCHQ

GDPR

California LEGISLATIVE INFORMATION

Interventions from regulators tend to focus on recommendations across several key areas:

Trusted connectivity

Device security

Protection of assets

TRUSTED CONNECTIVITY ALLIANCE

RSAConference2022

How does Tamper Resistant Element (TRE) technology address these challenges?

Tamper Resistant Element (TRE) form factors

Include SIM, eSIM, integrated SIM and eSE

SIM | eSIM | Integrated-eSIM | eSE

There are numerous advantages to leveraging TRE-based SIM products to protect mobile and IoT devices

- An established security platform already present in billions of devices
- The ability to protect data at rest and in transit
- Future-proof security through remote management
- Certification fast-track

RSAConference2022

eSIM for flexible security

Momentum for eSIM continues to build

TCA members report

337 million

eSIM shipments for 2021.

9% Year-on-Year increase (YoY)

TCA members reported 38% growth in **M2M** **eSIM** shipments, driven by uptake across **automotive** and **IoT** verticals.

Increasing uptake enabled by a global, well-established infrastructure

eSIM: The key to connect & secure objects

All SIM

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

eSIM additions

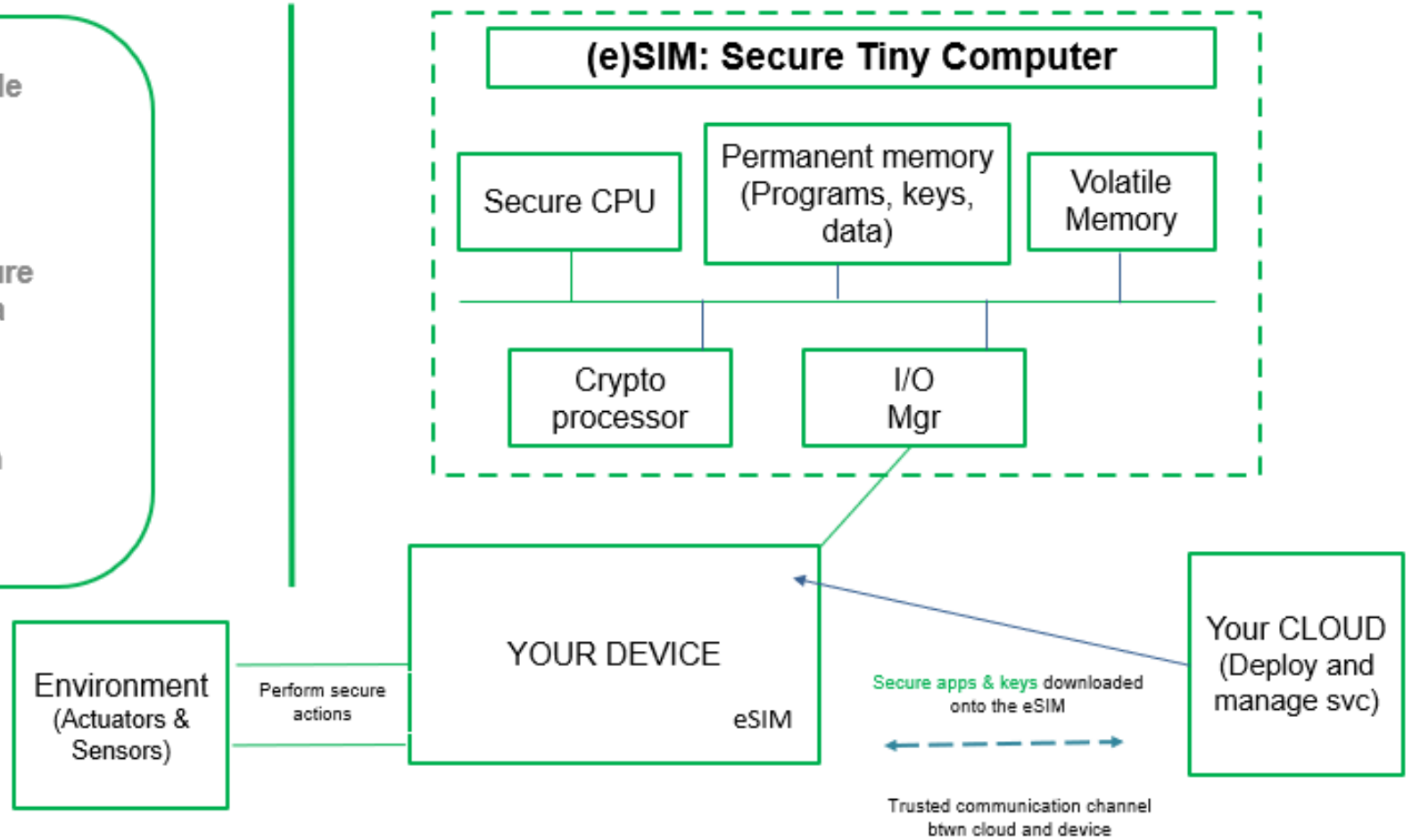
- Execute sensitive operations as mandated by certified schemes (e.g. payment, ID, cybersecurity)
- **Multiple** MNOs / carriers (Remote connectivity profile mgt)
- **Dynamic mitigation capability:** Immediate security updates and upgrades; responsive to emerging threats and attacks

eSIM: A key enabler for device security

eSIM

Well adopted to enable authenticated and flexible connectivity to cellular networks, BUT not only this…

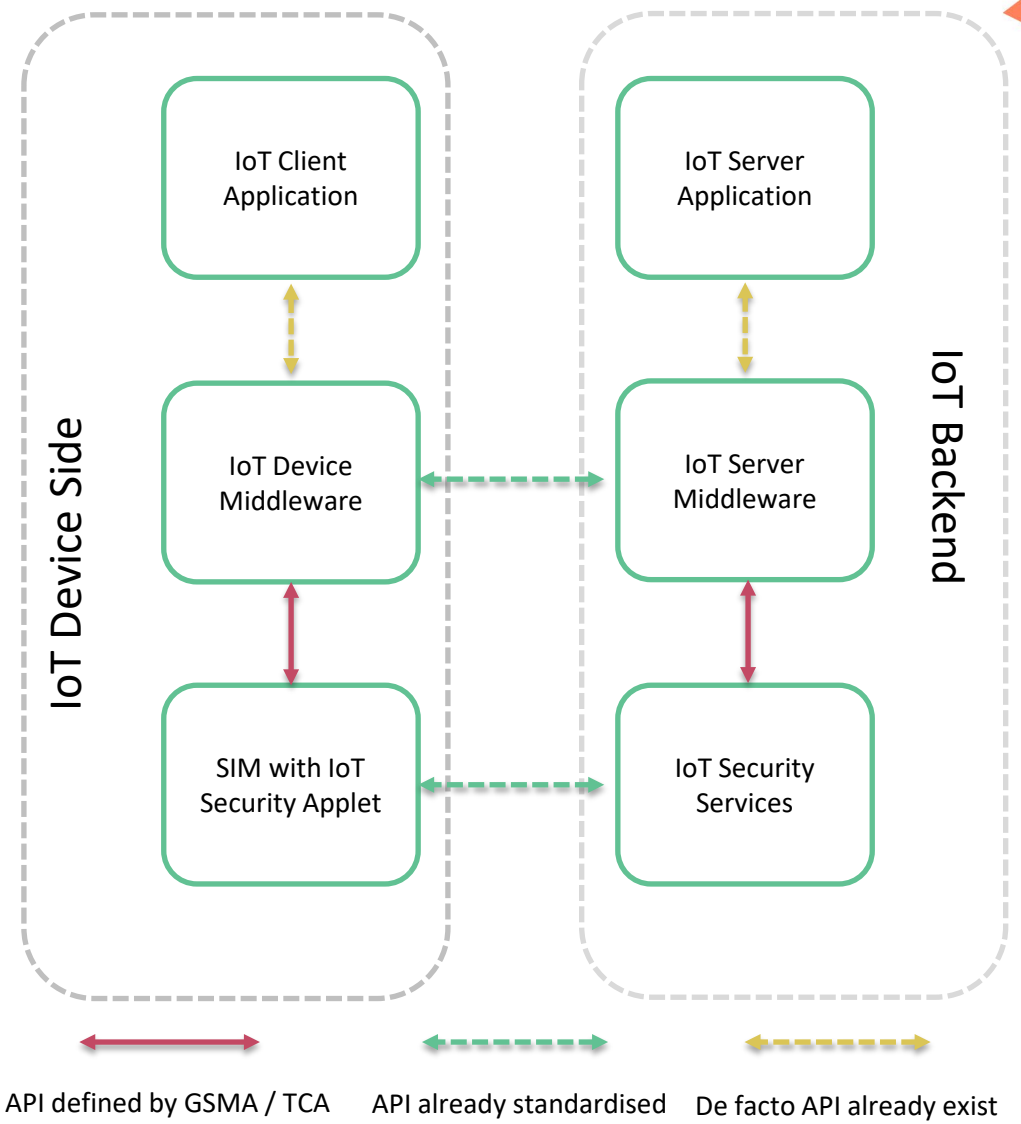
A tiny safe box and secure computer (eSIM is also a Secure Element (eSE)) delivering advanced security and crypto services to prevent from attacks



IoT SAFE

To further extend the capability of the SIM, GSMA and TCA have partnered on IoT SAFE (**IoT SIM Applet For Secure End-2-End Communication**).

- Specifies a common API and defining a standardised way to leverage the SIM 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 being executed in the SIM.
- Removes the IoT device and SIM applet fragmentation barrier by specifying a common “IoT device to IoT security applet” API.



Expanding the benefits of eSIM

Ensuring eSIM interoperability and expanding the benefits of the technology to emerging IoT market segments are key objectives for TCA.

TCA has various working groups that work in close collaboration with GSMA, and are dedicated to optimising the eSIM for use in IoT and to also position it as a Root of Trust for protection of IoT data:

eSIM Working Group

Develops and manages the eSIM Profile Package Specification.

IoT Security Application

Works to extend the security capabilities of the SIM to overcome IoT market fragmentation.

RSP for IoT

Guides and supports the development of eSIM-related specifications, to address eSIM market evolution and the needs of the IoT.

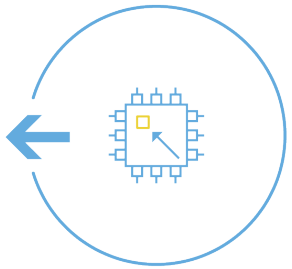
SAM

Guides development of GSMA SAM-related specifications, addressing TRE market convergence.

Market forces driving the integration trend

In recent years, market forces have promoted the integration of SIM functionality on a System on a Chip (SoC).

This has created increasing demand for **the integrated SIM.**



- **Device miniaturisation**
- **Digitalisation**
- **5G**
- **Sustainability**

Integrated SIM

What?

SIM functionality implemented on a hardware TRE integrated within a host SoC.

Delivers equal levels of security assurance already associated with other SIM form factors.

Self-contained from a security perspective and does not rely on any protection mechanisms of the host SoC.

Why?

Need for global interoperability and security assurance levels.

Avoid market fragmentation risk, reduce product development costs and potential for premature obsolescence.

Technical advantages – e.g. optimised power consumption to increase battery life.

How?

Global efforts to standardise nascent integrated SIM technology.

Specifications and definitions for the TREs enabling SIM functionality.

Integrated SIM solutions which align with open standards can now be recognised for their high levels of security assurance and global interoperability.

Leveraging integrated SIM for device security

Enhanced subscriber privacy in 5G

IMSI encryption to protect subscriber identity

Protection for device and digital identities

Secure storage capabilities for security sensitive digital ID

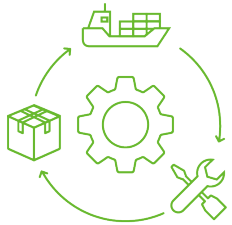
Harnessing the potential of integrated SIM

Utilities

Connectivity for smart meters requires reliable, robust security and long battery life.

An integrated SIM offers significant power-saving benefits over its predecessors.

Integrated SIM also provides further assurances to utility companies that it cannot be removed or swapped to misreport the amount of utility consumed.



Logistics

Increasing requirement for real-time information to support logistics at all levels.

Devices enabled with integrated SIM functionality can be leveraged for near real-time monitoring, using Low Power Wide-Area Network (LPWAN) connectivity.

Allows suppliers to track large and take immediate corrective action if needed.

Consumer Devices

Fitness and health wearables have become hugely popular.

However limited battery life is a pain point for wearable users, and many have to charge daily.

Integrated SIM technology helps to optimise the device real-estate and reduces the power budget of wearable significantly.

Key takeaways

Understand that IoT security is becoming mandatory.

- Growing consensus on the urgency of the IoT security challenge is driving new legislation, regulations and baseline security recommendations from authorities worldwide.

Recognise the potential of TRE technology to immediately address security vulnerabilities.

- TREs offer the most stringent secure end-to-end connectivity solutions for connected consumer and industrial devices.

Realise the advantages of leveraging TRE-based SIM products to protect mobile and IoT devices.

- SIM, eSIM and, increasingly, integrated SIM form factors are already deployed across billions of devices and can deliver unsurpassed security features and services.

Learn More and Get Involved

For more information, **all technical and educational resources are available for free download** from the TCA website: www.trustedconnectivityalliance.org

TCA also encourages organisations to actively participate to **help develop, define and influence the future technologies, standards and services that will impact our industries and sectors**. To find out more about joining TCA, contact: info@trusteconnectivityalliance.org

Stay up to date by following TCA:

@_TCAlliance

Trusted Connectivity Alliance

Trusted Connectivity Alliance

TRUSTED CONNECTIVITY ALLIANCE