RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: MBS2-F03

SIMs, eSIMs and Secure Elements: Dynamic Security for Connected Devices

Mike Strock

Operations Secretariat
Trusted Connectivity Alliance
Twitter: @TCAlliance_

Trusted Connectivity Alliance: Who we are

Our Membership

Executive:

gemalto a Thales company

G+D Mobile Security

IDEMIA augmented identity

life.augmented

VALID

Full:

CARD CENTRIC SOLUTIONS LTD. CARD CENTRIC

kona i KONA international

Linxens crafting the future of connections

Watchdata

TIANYU

WORKZ

Ordinary:

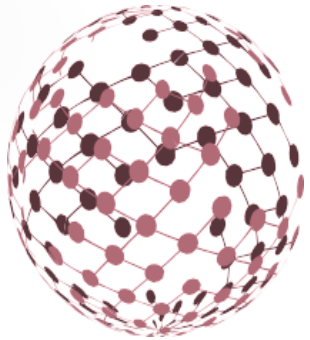
arm

COMPRION

TCA TRUSTED CONNECTIVITY ALLIANCE

Enabling a secure, connected future

About Trusted Connectivity Alliance



Our members are participants within the SIM ecosystem, which is the most widely distributed, secure application delivery platform in the world.

The organisation's vision is to facilitate the sustained growth of connected objects through trusted connectivity which offers protection for service provider assets, application and device data and end user privacy.

Our members represent over 80% of the global SIM market and include organisations with an interest in SIM, embedded SIM (eSIM), embedded Secure Element (eSE), integrated SE and SIM (iSE, iSIM), hardware and software IP provisioning or related personalisation services.

Key achievements

IoT SAFE (GSMA collaboration)
Specifies a common API and defines a standardised way for the SIM to be leveraged to securely perform mutual authentication between IoT devices applications and the cloud

eUICC Profile Package Technical and Test Specification (GSMA collaboration)
Enables mobile network operators to load standardised, interoperable connectivity profiles in an eSIM, regardless of the SIM vendor

5G Security
Played a significant role in supporting the maintenance of the hardware SIM in 5G

Open Mobile API (GlobalPlatform collaboration)
Established the first API for Android apps to communicate with the SIM or Secure Element and execute security services

Standardisation support
Including 5G for 3GPP, SSP for ETSI

Annual Shipments Monitoring
The definitive source for global shipments

Helping developers use SIM products
(CAT Loader)

Best practices for developing apps on a Secure Element
(Interoperability Stepping Stones)

Recommended connectivity profiles for each new network release (e.g. LTE)

Dynamic SIM Service: facilitated deployment of MNO services
(SAT)

Establishing interop tests and device recommendations for NFC services

Marketplace education

An increasingly connected world: The vital components

75 billion connected devices by 2025*

New digital services continue to ease our personal and professional lives

Connected objects are here to stay….

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.

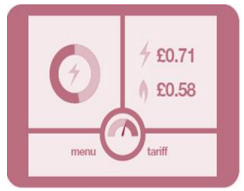
**https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/*

There are still many security challenges to address…

Connected cars

- Privacy breaches
- Hijacking
- Losing car control / safety
- Liability mgt & asset traceability in case of issues
- In-car entertainment piracy

Smart meters



- Threat to critical infrastructure
- Energy theft / tampering
- Privacy breaches
- Unauthorised network access

Mobile devices & wearables

- Privacy breaches
- Data tampering
- Lost and stolen devices

Insecure objects: An easy target….

There are two main ways to attack devices….

- Remote attacks from the cloud to **MANY** devices by hackers, criminal organisations, etc
- Aim: steal and change data of one organisation resulting in financial loss or personal injury. Or perform silent DDoS attacks to several targets

- Physical or proximity (e.g. BLE) attack on **ONE** device by an individual (device owner or hacker)
- Aim: extract credentials to produce clones and attack infrastructures

Why secure-by-design matters

- Many connected devices have no inbuilt security.
- Many device manufacturers are starting to develop security expertise.
- End users are not educated well enough on risks / precautions (e.g. change default password, certificates).

- **Secure-by-design is mandatory**
- **Penetration testing is key before go-to-market**

RSAConference2020

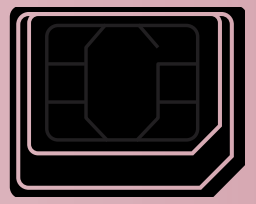
How does the (e)SIM address these challenges?

(e)SIM: The key to connect & secure objects

Service execution platform

Authenticated connectivity

All SIM



Enable carriers' value added services
(e.g. QoS, smart roaming…)

Single connectivity profile
Connect devices to cellular networks

Most widely distributed secure application delivery platform in the world

eSIM and eSE Additions

Dynamic security proposition:
immediate security updates and upgrades; responsive to emerging threats and attacks

Execute sensitive operations as mandated by certified schemes (e.g. payment, ID, cybersecurity)

eSIM only

Multiple MNOs / carriers

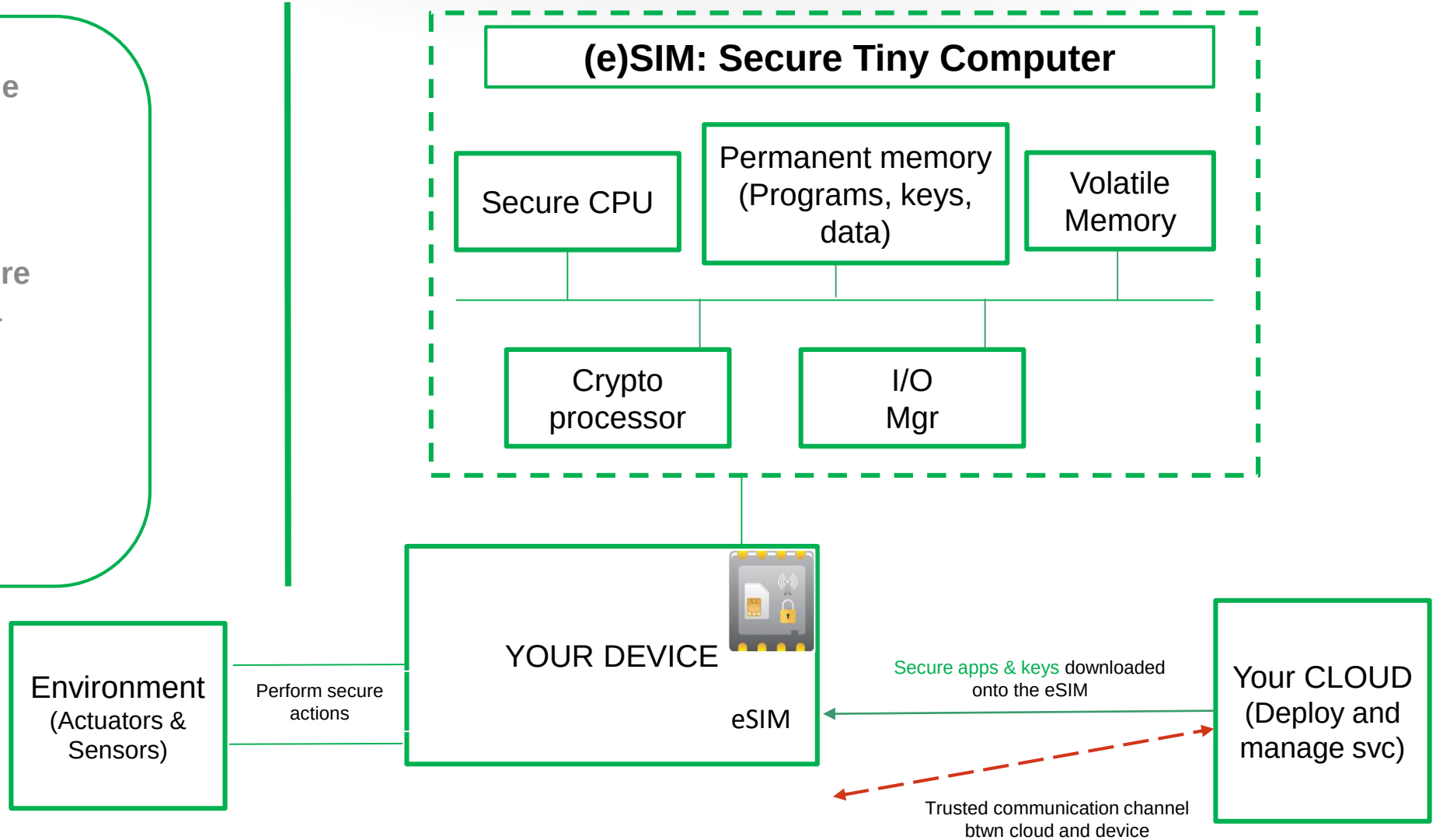
Remote connectivity profile mgt

(e)SIM: 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



Security in IoT: Regulation is helping

- Many organisations are addressing the IoT security challenge; many are dramatically increasing the recommended level of security, which is encouraging the use of secure hardware:

Industry initiatives

GSMA

See CLP.13

Regional / regulatory frameworks

National Cyber Security Centre
a part of GCHQ

General Data Protection Regulation

enisa

ETSI

California LEGISLATIVE INFORMATION

GSMA IoT Security Guidelines & Assessment

GSMA: GLOBAL MOBILE OPERATORS COMMIT TO COMMON APPROACH TO IOT SECURITY

June 27, 2018 | Press Release

Tweet Share Share 1

AT&T, China Mobile, China Telecom, China Unicom, Deutsche Telekom, Etisalat, KDDI, LG Uplus, Orange, Telefónica, Telenor Group, Telia, Turkcell, Vodafone Group and Zain Agree to Adopt GSMA IoT Security Guidelines

Shanghai: The GSMA today announced that global mobile operators including AT&T, China Mobile, China Telecom, China Unicom, Deutsche Telekom, Etisalat, KDDI, LG Uplus, Orange, Telefónica, Telenor Group, Telia, Turkcell, Vodafone Group and Zainhave committed to adopt and implement the GSMA IoT Security Guidelines. The guidelines outline best practice and recommendations for Internet of Things (IoT) security for the entire IoT ecosystem and set out a comprehensive security assessment scheme to help ensure IoT services are protected against IoT security risks. There will be reach 3.1 billion IoT connections by 2025, according to GSMA Intelligence.

"For the IoT to flourish, the industry needs an aligned and consistent approach to IoT security. Our guidelines encourage the industry to adopt a robust set of best practices that will help create a more secure IoT market with trusted, reliable services that can scale as the market grows," commented Alex Sinclair, Chief Technology Officer, GSMA.

GSMA press release – 27 June 2018

Security Principles

Security by design
Privacy by design
End to end
Across the lifetime
Evaluate technical model

Review security model
Assign security tasks
Review component risk
Implementation
Ongoing lifecycle

IoT Security Guidelines

IoT Security Guidelines for Service Ecosystems

Detailed Control Statements

IoT Security Assessment

Referenced by:

TCA TRUSTED CONNECTIVITY ALLIANCE Enabling a secure, connected future

enisa

WORLD ECONOMIC FORUM

ETSI

ECS EUROPEAN CYBER SECURITY ORGANISATION

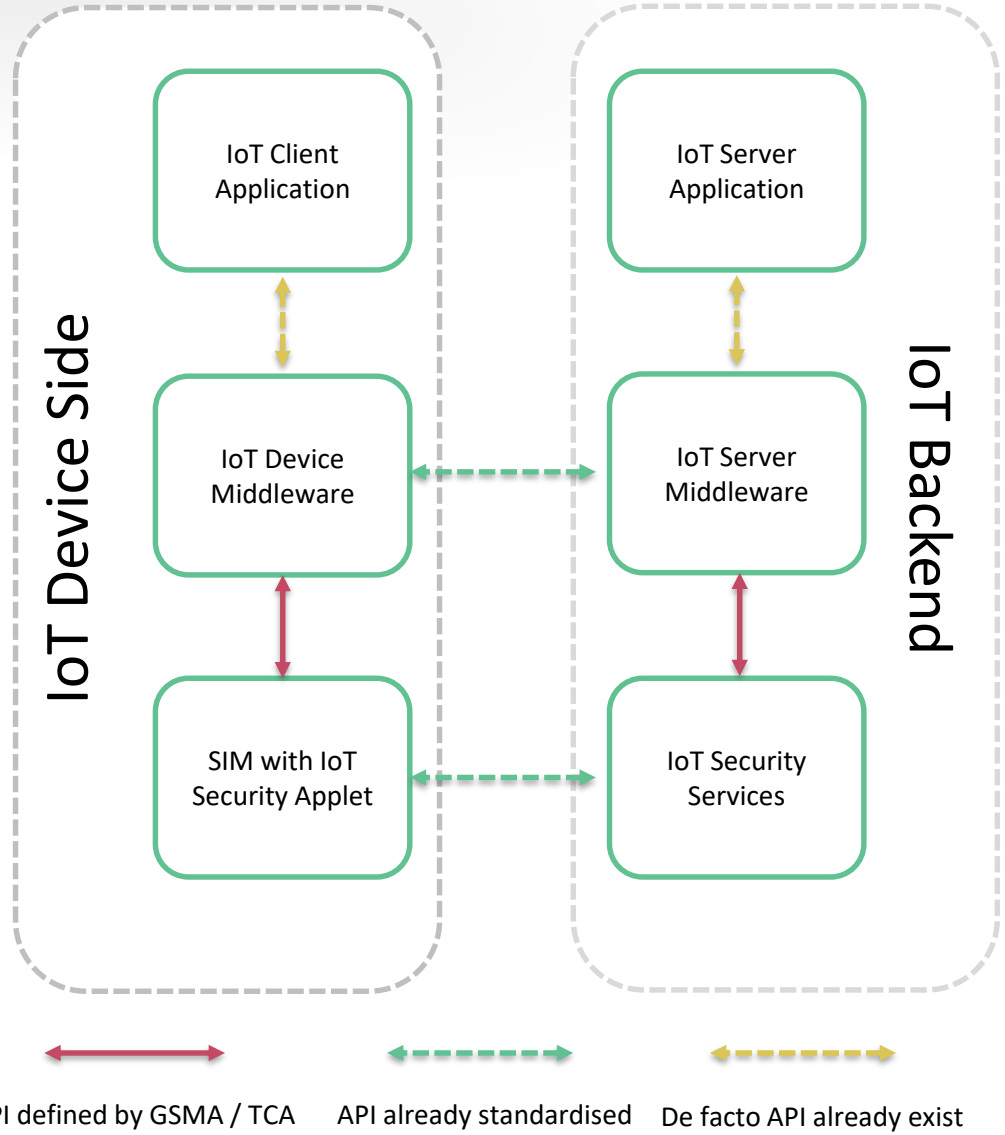
Department for Digital, Culture Media & Sport

Source: GSMA
www.gsma.com/iotsecurity/

IoT SAFE

To further extend the capability of the SIM, GSMA and SIMalliance 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 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



Benefits of IoT SAFE

- **Immediate scalability** – by defining a common way to leverage the SIM to securely perform mutual authentication between IoT device applications and the cloud, it is easier for IoT device makers to execute security services and manage credentials across billions of devices.

- **Flexibility** – by enabling security functions to be delegated to the secure IoT applet, IoT device makers are not solely dependent on cloud provider services for securing their IoT devices.

- **Increase security** – through the ability to perform secure mutual authentication.

- **Maximise investments** – SIMs are already deployed to provide secure cellular connectivity and can be leveraged to deliver enhanced security for IoT devices with minimal additional investment.

- **Proven expertise** – mobile operators and their ecosystem partners are experienced, trusted providers of secure IoT solutions and have the necessary infrastructure and processes in place to deliver SIM-based security services promptly and reliably.

RSAConference2020

Apply

Apply

- **Recognise that IoT security is becoming mandatory.**
  - Increasingly, global authorities and industry bodies are working towards defined IoT security guidelines / mandates.
- **Adopt a ‘secure-by-design’ mindset.**
  - Security and privacy must be considered from the outset and penetration testing for all devices before launch.
- **See the SIM as a tiny secure computer.**
  - The SIM and eSIM are already being used for connectivity, but can also be leveraged to deliver advanced security and cryptographic services.