ETSI
The Standards People

Improving security and privacy in Smart ICT

Presented by: **S. Compans** For: **ILNAS workshop**

28.06.2019

Agenda

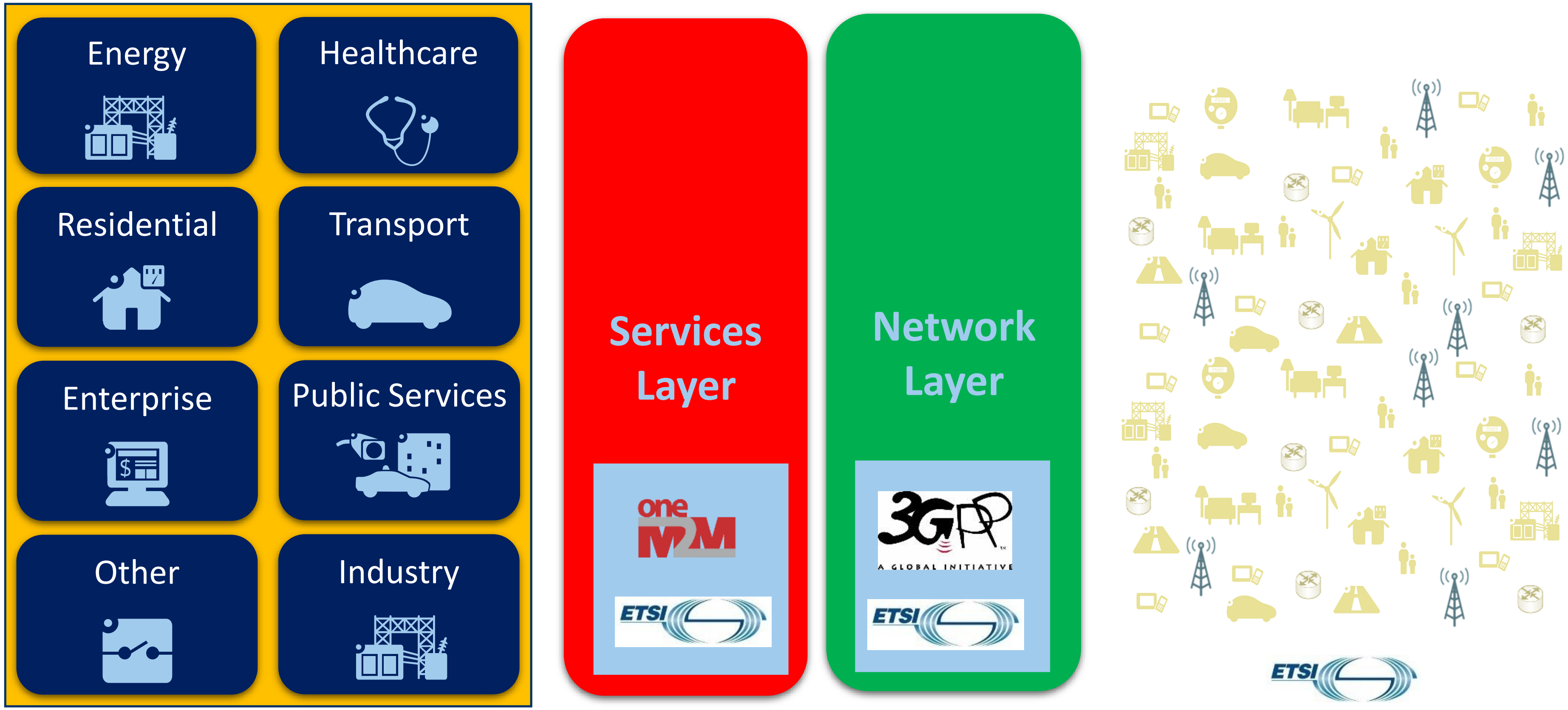
IoT

5G

AI

IoT

IoT - Connecting everything



Energy

Healthcare

Residential

Transport

Enterprise

Public Services

Other

Industry

Services Layer

Network Layer

TC SmartM2M: IoT security & privacy specific work

TR 103 591	Privacy; Standards Landscape and best practices
TR 103 533	Security; Standards Landscape and best practices
TR 103 534	Teaching Material

- Part 1 Security: allows readers, identified by role, to gain knowledge of the fundamentals of IoT security.
- Part 2 Privacy: helps readers acquire basic knowledge to apply IoT privacy in their area of engagement or at least know where to obtain that information

Security in oneM2M Release 2- Release 3

oneM2M Secure Environment and security levels

« Secure Environment » concept abstracts the security implementation

- Expose common services to applications, depending on implementation
- Provide common interface for remote security administration, if needed

oneM2M supported implementations distinguish 4 security levels

- No additional security
  - devices otherwise protected from attackers, i.e. on trusted networks
- Software only security (obfuscation, White box crypto etc.)
  - Always vulnerable to sufficiently motivated attacker
  - Acceptable when compromise is not critical
- « Trusted Execution Environment » (TEE) relying on main CPU hardware features
  - Good barrier against software based attacks
  - Sufficient for remotely accessible, but not physically exposed devices
- Tamper resistant hardware embedded Secure Element (eSE)
  - Required to protect secrets within devices physically exposed to attackers (SPA / DPA etc.)
  - E.g. to protect unattended devices against cloning

Security in oneM2M Release 2&3

Device Configuration
TS-0022

Security Solutions
TS-0003

MEF & MAF interfaces
TS-0032

Enrolment services (RSPF / MEF)

Credentials Provisioning/Security Configuration of the M2M System

Secure communications services (SAEF / MAF)

Methods for Securing Information (PSK/PKI/Trusted Party)

Point-to-point and end-to-end solutions (TLS / DTLS)

Access Control & Authorization services

Requester Authentication

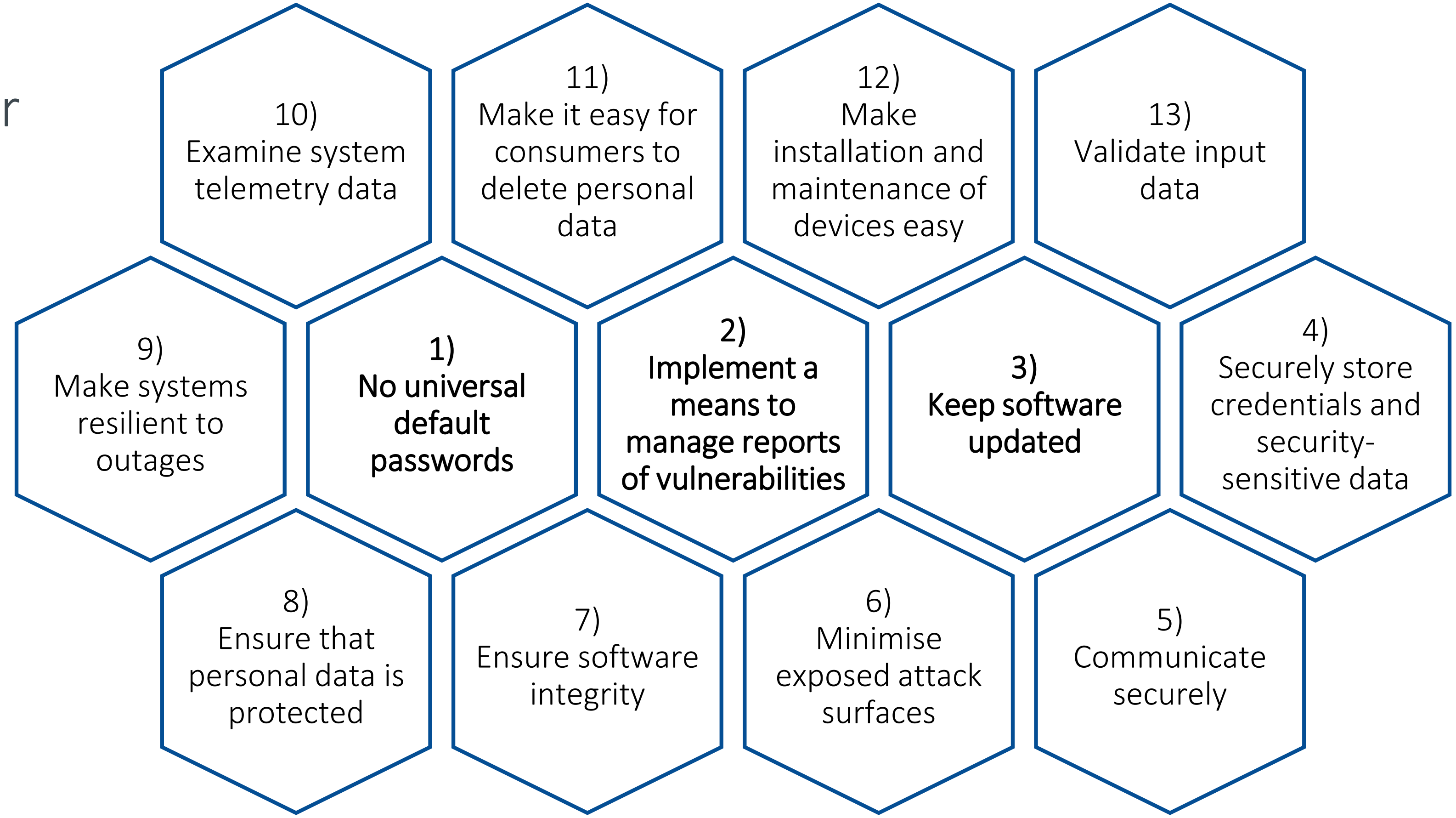
Information access Authorization(ACL based)

Static and Dynamic solutions

Privacy Policy Management

TC CYBER: Developing a consumer IoT security standard

- TC CYBER's approach:
  - Defined scope of 'consumer IoT'
  - High-level to be flexible as tech moves on
  - Focused on provisions that matter most
  - Pragmatic and manageable



10) Examine system telemetry data

11) Make it easy for consumers to delete personal data

12) Make installation and maintenance of devices easy

13) Validate input data

9) Make systems resilient to outages

1) No universal default passwords

2) Implement a means to manage reports of vulnerabilities

3) Keep software updated

4) Securely store credentials and security-sensitive data

8) Ensure that personal data is protected

7) Ensure software integrity

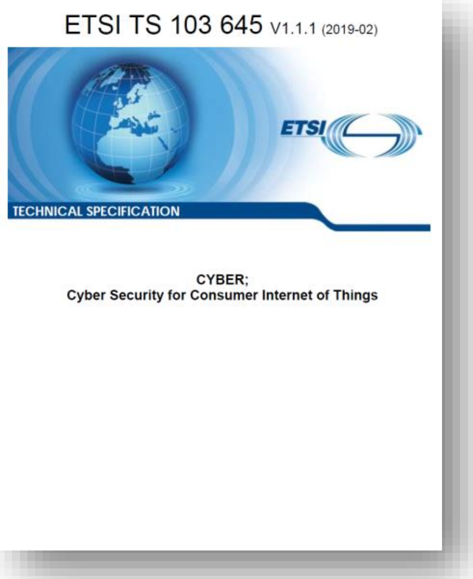
6) Minimise exposed attack surfaces

5) Communicate securely

TC CYBER: TS 103 645’s reception

- First globally-applicable industry standard on consumer IoT security.
- TECH ACCORD

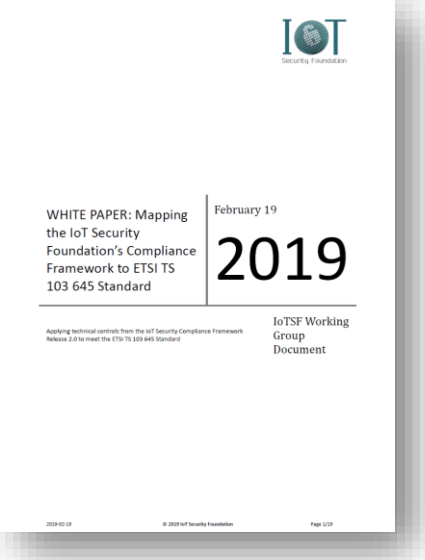
  “Cybersecurity Tech Accord Signatories Endorse ETSI Technical Specification for IoT Security”
- Mapped to IoT Security Foundation’s Compliance Framework
- BSI / PETRAS: “the ETSI standard [addresses] major security failings in IoT devices and propose[s] design principles that are deeply pragmatic…”



ETSI TS 103 645 V1.1.1 (2019-02)

TECHNICAL SPECIFICATION

CYBER;
Cyber Security for Consumer Internet of Things



IOT Security Foundation

WHITE PAPER: Mapping the IoT Security Foundation’s Compliance Framework to ETSI TS 103 645 Standard

February 19

2019

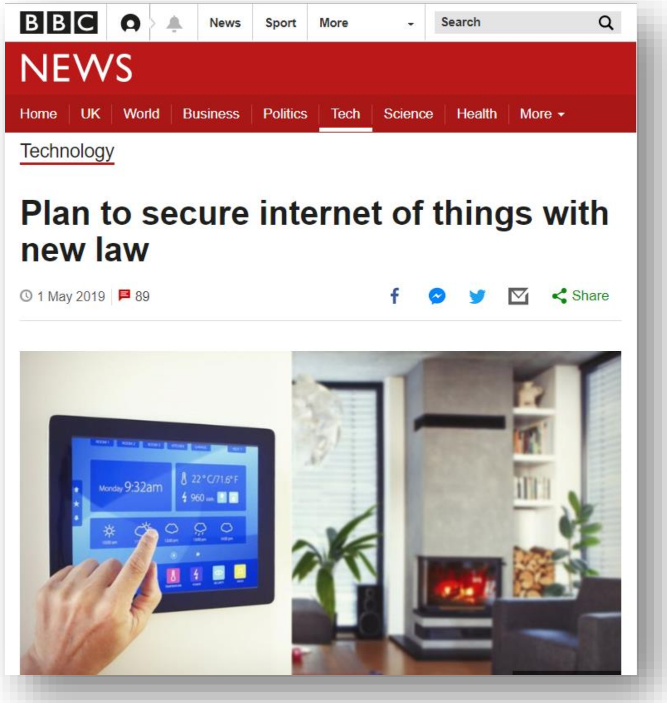
Applying technical controls from the IoT Security Compliance Framework Release 2.0 to meet the ETSI TS 103 645 Standard

IoTSF Working Group Document

2019-02-19 © 2019 IoT Security Foundation Page 1/19

TC CYBER: Next steps for TS 103 645

- To inform future certification schemes under the EU Cybersecurity Act and national regulatory initiatives.
- TC CYBER's May meeting:
  - Agreed to transpose TS 103 645 into a European Standard (EN)
  - Considering a test specification to sit alongside TS 103 645
- Opportunity to contribute



Technology

Plan to secure internet of things with new law

1 May 2019 | 89

TC SCP: The Challenge

The new generation of connected mobile devices and IoT devices pose new challenges concerning security and integration

- A system of sensors in an IoT application may not require a fully fledged UICC in very sensor

Can the “traditional” UICC be the solution for the new requirements ?

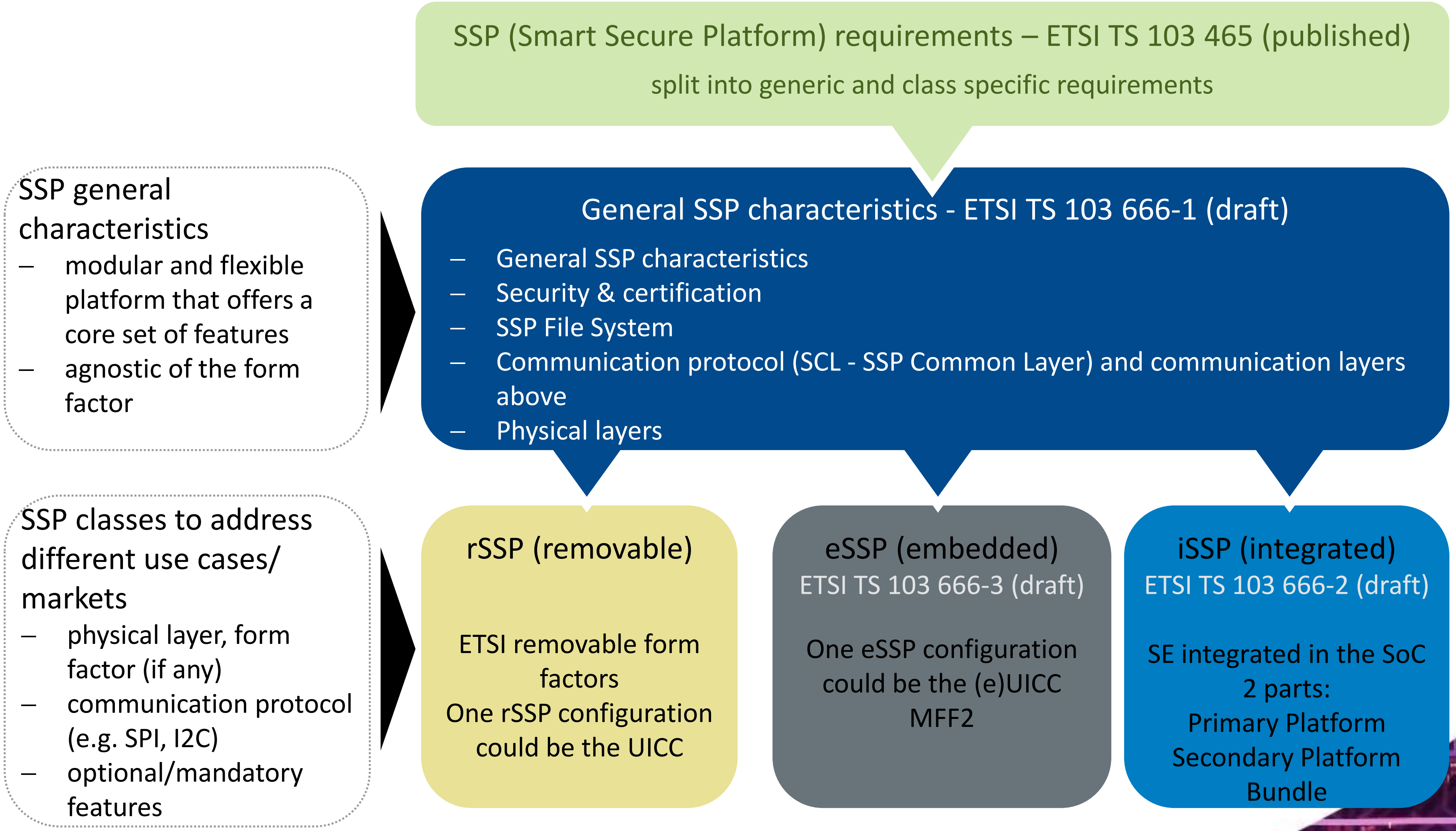
There are issues related to …

- Specific smart card protocol from the eighties
- Limitation of data structures
- Limitation of parallel execution of applications
- Size of the hardware
- Complexity and cost of the product

TC SCP Answer:
The Next Generation **Smart Secure Platform** (SSP)

- Objective: better integration of the UICC into the specific use case while retaining its characteristics
- The SSP is designed to be a modular platform offering a core set of features as well as a number of options that need to be selected at the time of implementation based on the intended application
    - An open platform for multiple applications (multiple issuers can share the same hardware)
    - Choice of interfaces and protocols (SPI, I2C, I3C, …)
    - Faster and more flexible
    - Choice of hardware
    - New filesystem
    - Support of existing features: Contactless, Toolkit, …
- Still supports UICC applications ensuring smooth migration

TC SCP: The SSP Specifications



SSP general characteristics

- modular and flexible platform that offers a core set of features
- agnostic of the form factor

SSP classes to address different use cases/ markets

- physical layer, form factor (if any)
- communication protocol (e.g. SPI, I2C)
- optional/mandatory features

SSP (Smart Secure Platform) requirements – ETSI TS 103 465 (published)

split into generic and class specific requirements

General SSP characteristics - ETSI TS 103 666-1 (draft)

- General SSP characteristics
- Security & certification
- SSP File System
- Communication protocol (SCL - SSP Common Layer) and communication layers above
- Physical layers

rSSP (removable)

ETSI removable form factors
One rSSP configuration could be the UICC

eSSP (embedded)
ETSI TS 103 666-3 (draft)

One eSSP configuration could be the (e)UICC MFF2

iSSP (integrated)
ETSI TS 103 666-2 (draft)

SE integrated in the SoC
2 parts:
Primary Platform
Secondary Platform Bundle

5G

5G new security features

Better privacy protection

- Encrypted IMSI

Stronger air interface protection

- User plane integrity protection (encryption only in 4G)

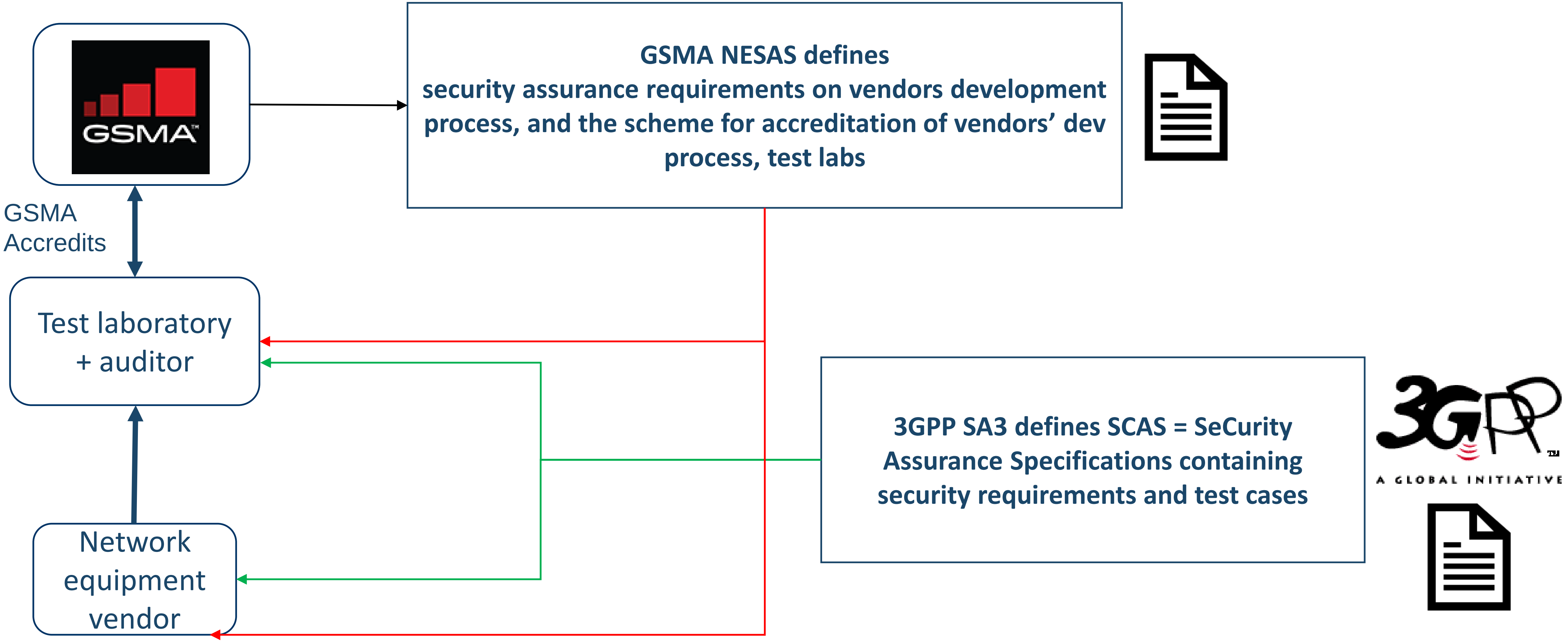
Enhanced interconnect security

- E2E security between PLMNs

Post quantum security algorithm

- 256-bit algorithm under consideration

Mobile Network Equipment Security Assurance Scheme (NESAS)



GSMA NESAS defines security assurance requirements on vendors development process, and the scheme for accreditation of vendors' dev process, test labs

GSMA Accredits

Test laboratory + auditor

Network equipment vendor

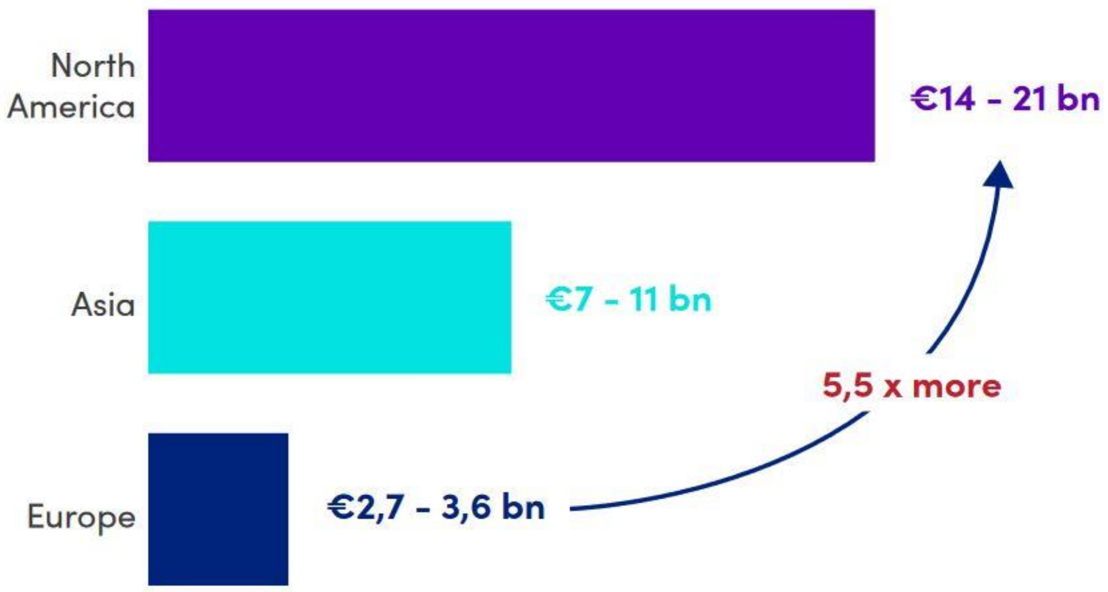
3GPP SA3 defines SCAS = SeCurity Assurance Specifications containing security requirements and test cases

AI

Investing in key technologies

"A general feeling that AI/ML will be crucial to many ETSI activities" *(ETSI Board #123 Strategy Workshop)*

Private investments in AI, 2016



Source: McKinsey, Artificial intelligence: The next digital frontier?, 2016

Artificial Intelligence will be a defining technology throughout society

Not only networks but, also, Industry4.0, eHealth, Caring, nextGen IoT, Energy,… will be shaped by AI/ML

Europe cannot afford to fall behind other regions (US & China)

One organization cannot do it alone – partnering is key to accelerate

ETSI is more and more engaged in AI

Summary

CROSS-DOMAIN CYBERSECURITY

- Ecosystem
- Protection of personal data & coms
- **IoT security and privacy**
- Critical infrastructures
- Enterprise and individual cybersecurity
- Forensics
- Information Security Indicators

SECURING TECHNOLOGIES & SYSTEMS

- Mobile / wireless systems (**5G**, TETRA, DECT, RRS,RFID...)
- **IoT**
- Network functions virtualization
- Intelligent Transports
- Broadcasting
- **Artificial Intelligence**

Security

SECURITY TOOLS & TECHNIQUES

- Lawful interception & retained data
- Digital signatures & trust services
- Permissioned distributed ledgers
- **Smart cards / secure elements**
- Security algorithms
- Quantum key distribution
- Quantum safe cryptography

Contact:
Sonia COMPANS
Technical Officer
sonia.compans@etsi.org

ETSI

The Standards People