The Future of the Embedded Secure Element

The next generation of Secure Enclaves for IoT and Digital Applications

21/03/2024

David Kerr-Munslow
Product Manager

“In today’s connected world, there are many facets of technology that we do not directly see, but these still play a very important role in our digital safety.

Among the ranks of encryption algorithms and authentication mechanisms, we have a contender for the hidden watchdog of the digital world, it’s called:

“Secure Element”

PUBLISHED ON DECEMBER 22, 2022

Secure Enclaves are one of the most overlooked facets of digital security
BY ANIRUDH VK

A Few Key Points about Secure Elements

Definition

Secure Element
Secure Enclave
Root of Trust
Secure Vault

Tamper Resistant
Isolated Execution Environment
Protects Secrets
Executes Secure S/W

High Level Security

Smartcards for EMV Payment
Transit / Ticketing
Access Control / Credentials
ID & Government Documents

Protection against
- Software attacks
- Physical attacks
- Side-channel attacks (DPA)

Certification

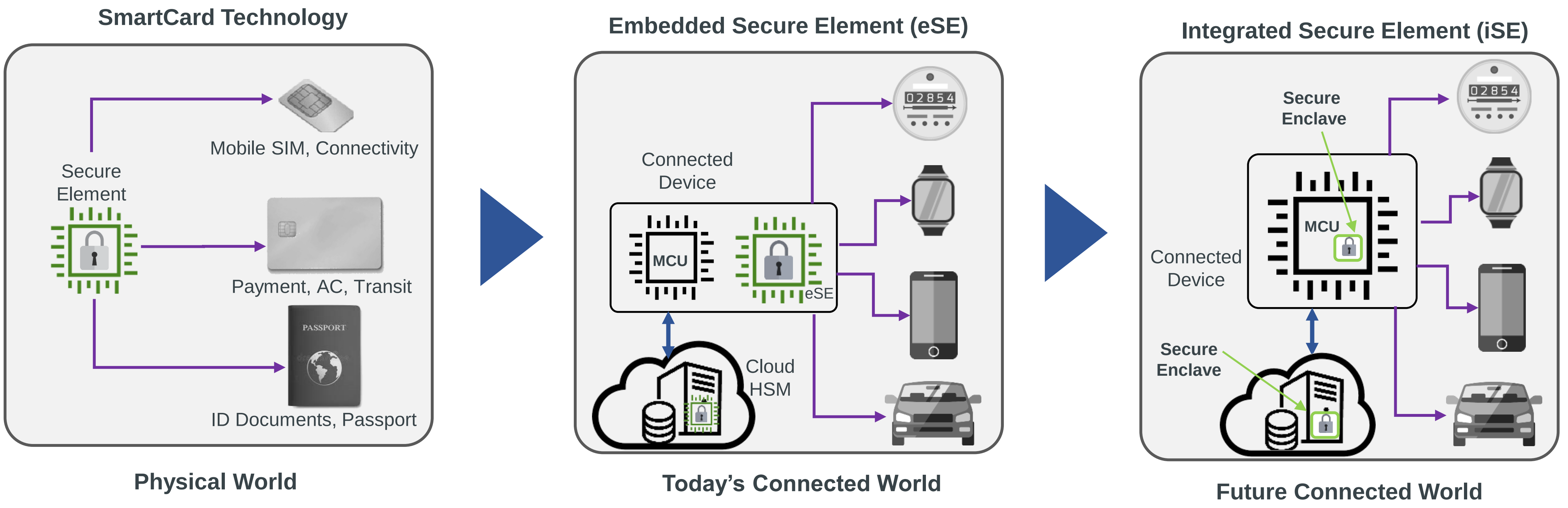
Common Criteria (EAL4+ and above), EMVCo, FIPS 140.3

Multiple Applications

Security Evolution and Transformation

Through closer software and hardware integration

Security needs to be tightly embedded at the heart of any system



SmartCard Technology

Secure Element

Mobile SIM, Connectivity

Payment, AC, Transit

ID Documents, Passport

Physical World

Embedded Secure Element (eSE)

Connected Device

MCU

eSE

Cloud HSM

Today's Connected World

Integrated Secure Element (iSE)

Secure Enclave

MCU

Connected Device

Secure Enclave

Future Connected World

Integrated Secure Element – Advantages

1 Better Integration

- Smaller form factors for addressing low footprint devices (e.g wearables)
- Lower power consumption → longer battery life and better user experience
- Easy interaction between functions of a device

2 Flexibility

- Late personalization of a device already in the field
- Can be activated wirelessly using industry standard secure protocols
- Security integration is more streamlined

3 Higher Security

- Fast update/loading of secure services and operating systems
- Crypto agility
- Tighter integration reduces the attack surface

4 Cost Effective

- Reduced Engineering Cost
- Reduced Bill of Materials (BoM)
- Cost effective support of multiple certification schemes (GSMA, EMVCo, CC EAL5+, CC EAL6+…)

5 Update/Upgrade

- Tighter integration and connectivity facilitates security updates and adding features

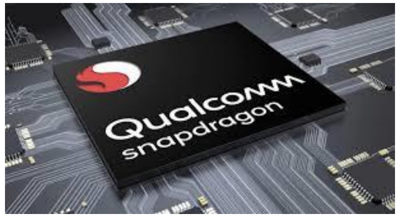
Integrated Secure Element is coming (already here)!

Through fast-growing adoption & demand

Apple A16 Bionic Specs – 4nm Process, 6-Core CPU

To maintain user privacy and security, **the Secure Enclave** protects personal information such as Face ID, contacts and more.

Qualcomm introducing Integrated SIM - The next generation of SIM technology



AUG 11, 2021

The first mobile solution to support eUICC is the Snapdragon 888 5G Mobile Platform. The built-in Qualcomm Secure Processing Unit (SPU) in Snapdragon 888 features an integrated Secure Element (iSE), enabling new security-critical use cases and applications.

A Secure Vault System for Internet of Things Devices

April 10, 2020

Silicon Labs said **the Secure Vault subsystem (iSE)** can be used to store and manage secret keys, which are needed to authenticate that interconnected devices can be trusted. It is also designed to stop attackers from stealing data by tampering with the hardware.

Quectel powers global connectivity and flexible deployment models with new iSIM-enabled module

June 21, 2022

NUREMBERG, Germany--(BUSINESS WIRE)--Quectel Wireless Solutions has launched the new BG773A-GL ultra-compact LTE Cat M1, NB1 and NB2 module which offers integrated SIM (iSIM) support. The iSIM capability of this new module provides huge flexibility and simplicity for integrators and IoT service providers

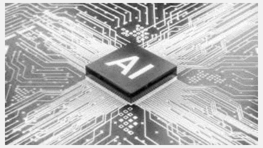
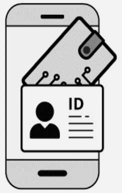
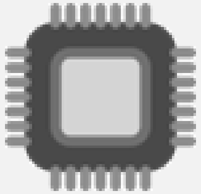
Samsung Introduces Game Changing Exynos 2200 Processor With Xclipse GPU Powered by AMD RDNA 2 Architecture

Korea on January 18, 2022

For safekeeping, the Exynos 2200 comes with **Integrated Secure Element (iSE)** to store private cryptographic keys as well as to play a role as RoT (Root of Trust). Also, an inline encryption HW for UFS and DRAM has been reinforced to have user data encryption safely shared only within the secure domain.

Typical Markets

Vertical Markets

Today				Emerging Verticals			
IoT/Mobile Cellular Connectivity	Secure Transaction	IoT Platform/ Device	Automotive	Data Center/ Cloud / AI	Digital Identity	Digital Currency	Aeronautic/ Defense
iSIM / eSIM	NFC / UWB	MPU /MCU	SE/ MCU	HSM	ID Wallet	HW Wallet	Strategic Application
 GSMA	 • Secure payment • Access control • Transportation	zigbee csa connectivity standards alliance matter	 • Secure Access • Secure Processing • Secure Network, • Secure Garteway Secure Interface (V2X..	 	 	 • Secure Digital currency > Mobile HW Wallet	 • Strategic applications for military equipment, Cloud….

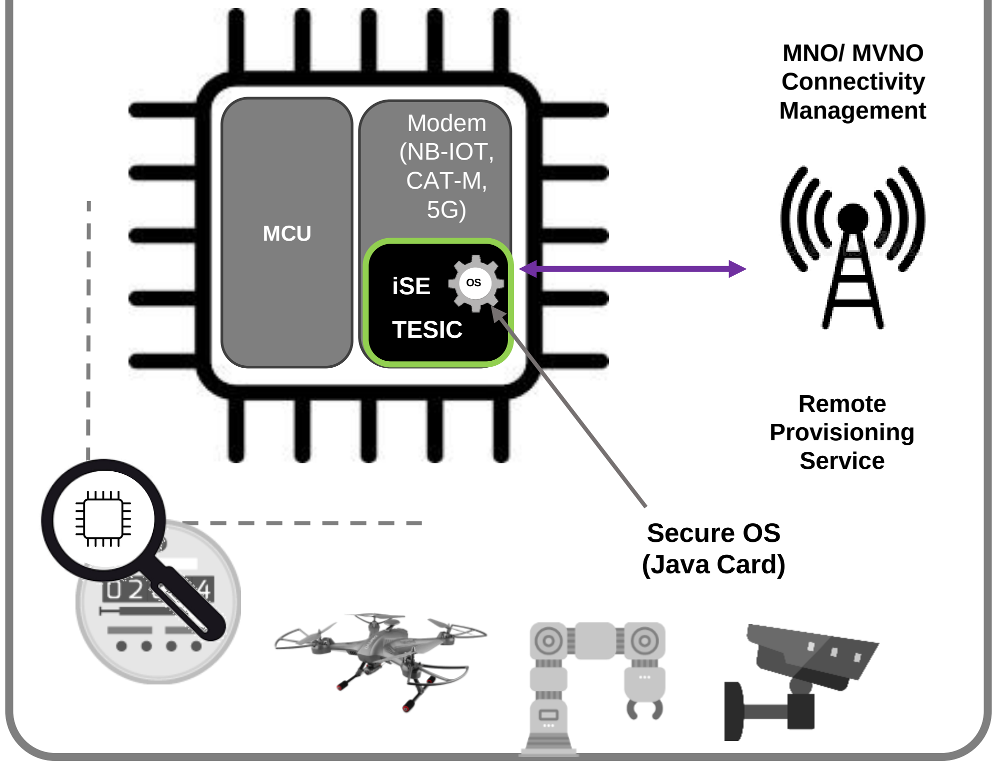
IP SE

Customer References in IoT

Qualcomm

Renesas

iSIM IoT Connectivity Chipset



MCU

Modem (NB-IOT, CAT-M, 5G)

iSE OS TESIC

MNO/ MVNO Connectivity Management

Remote Provisioning Service

Secure OS (Java Card)

Current secure OS partners

THALES

IDEMIA

Kigen

RedteaMobile

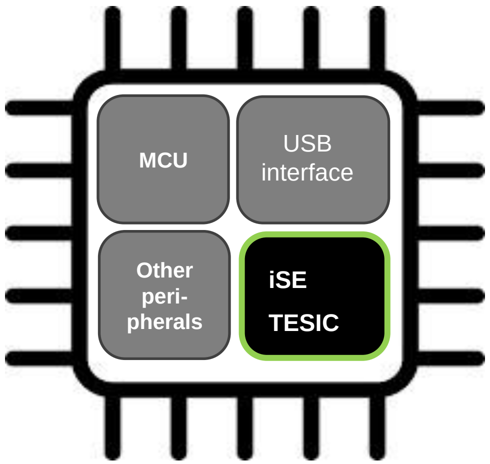
jNet ThingX HELPING YOU FIT JAVA EVERYWHERE

Coming soon

Giesecke & Devrient

intel.

Web authentication (FIDO 2) chip product



MCU

USB interface

Other peri-pherals

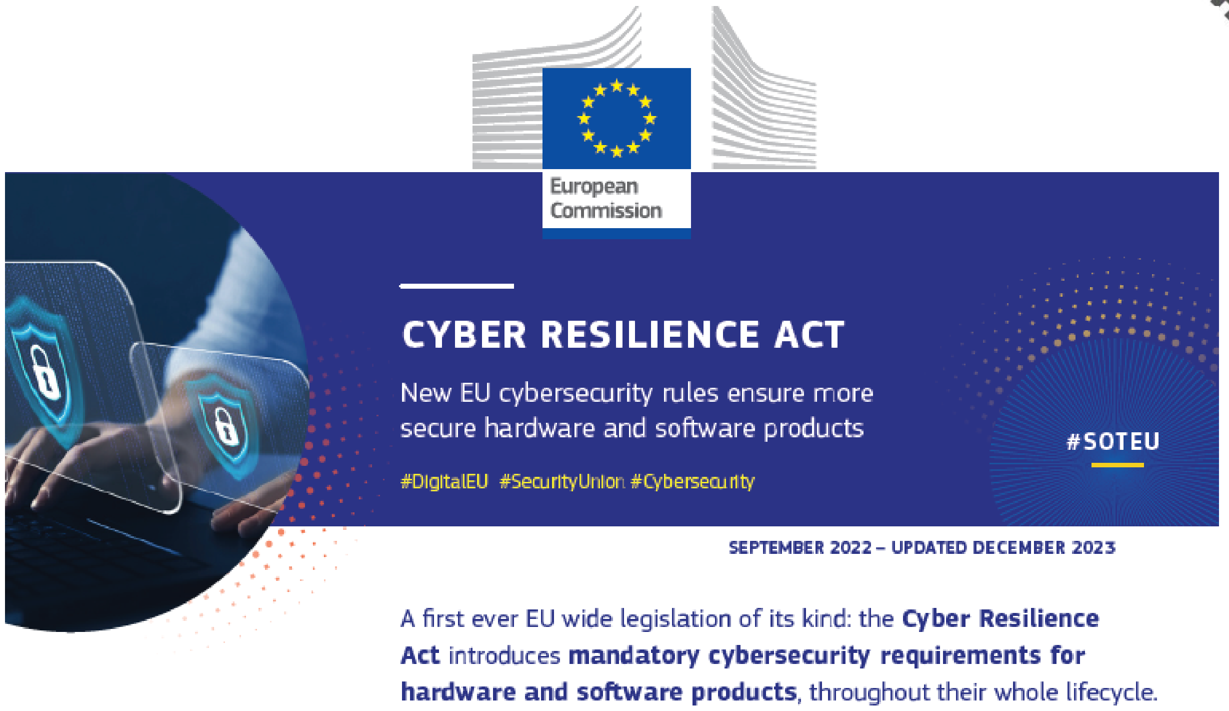
iSE TESIC

Factors Encouraging Adoption

- European Cyber Resilience Act
  - CE marking will require consideration of connected security
- Enters into force early 2024
  - 36 months to meet requirements

- Increase Consumer Confidence and Protection
- Increases Manufacturers Obligations

- Other organisations are creating standards:
  - GSMA: SGP 32
  - NIST
  - CSA



European Commission

CYBER RESILIENCE ACT

New EU cybersecurity rules ensure more secure hardware and software products

#DigitalEU #SecurityUnion #Cybersecurity

#SOTEU

SEPTEMBER 2022 – UPDATED DECEMBER 2023

A first ever EU wide legislation of its kind: the **Cyber Resilience Act** introduces **mandatory cybersecurity requirements for hardware and software products**, throughout their whole lifecycle.

GSMA
Official Document SGP.32 – eSIM IoT Technical Specification v1.0.1

GSMA™

eSIM IoT Technical Specification
Version 1.0.1
04 July 2023

Play in a Challenging Ecosystem

Developing IoT landscape with silicon, s/w and solutions integrated for best-in-class security

CISA Cybersecurity & Infrastructure Security Agency

ANSSI Agence nationale de la sécurité des systèmes d'information

Prävention Detektion Reaktion

LEGISLATION

What is required legally?

NIST

ETSI

enisa European Union Agency for Cybersecurity

STANDARDS DEFINITION

What is required functionally per market?

csa connectivity standards alliance

Global Platform™

EUROSMART

GSMA™

psacertified™

DEVICE PROTECTION PROFILE

What is required functionally?

Common Criteria

FIPS 140-2 Cryptography

SESIP™

psacertified™

CERTIFICATION SCHEMES

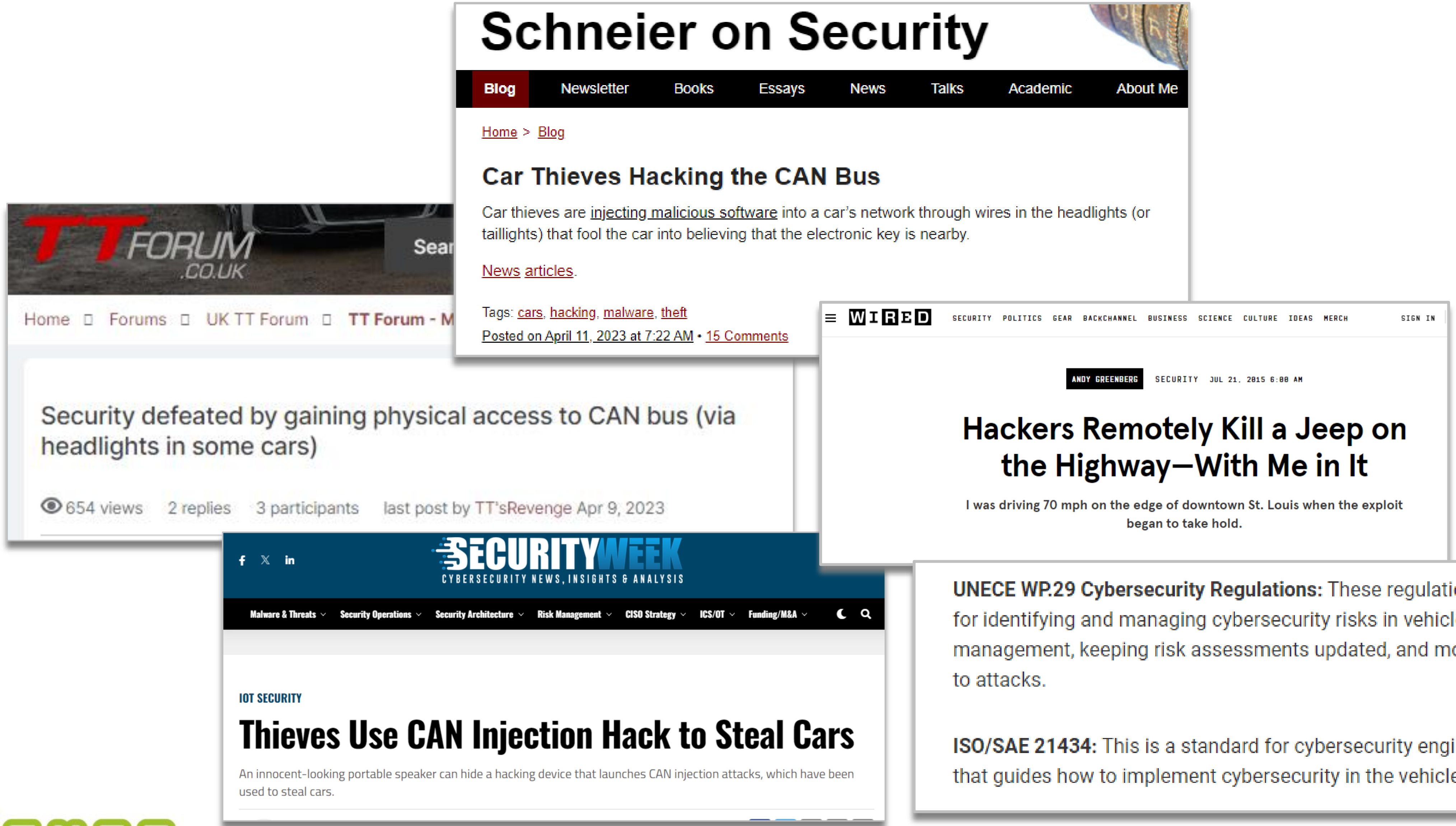
How to standardize Silicon Platform?

Tiempo SECURE

Use Case & Application

March 25, 2024

Real Security Problems Also Become Safety Risks



Schneier on Security

Car Thieves Hacking the CAN Bus

Car thieves are injecting malicious software into a car's network through wires in the headlights (or taillights) that fool the car into believing that the electronic key is nearby.

News articles.

Tags: cars, hacking, malware, theft

Posted on April 11, 2023 at 7:22 AM • 15 Comments

Security defeated by gaining physical access to CAN bus (via headlights in some cars)

654 views 2 replies 3 participants last post by TT'sRevenge Apr 9, 2023

WIRED

ANDY GREENBERG SECURITY JUL 21, 2015 6:00 AM

Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

SECURITYWEEK

IOT SECURITY

Thieves Use CAN Injection Hack to Steal Cars

An innocent-looking portable speaker can hide a hacking device that launches CAN injection attacks, which have been used to steal cars.

UNECE WP.29 Cybersecurity Regulations: These regulations define a framework for identifying and managing cybersecurity risks in vehicle design, verifying risk management, keeping risk assessments updated, and monitoring and responding to attacks.

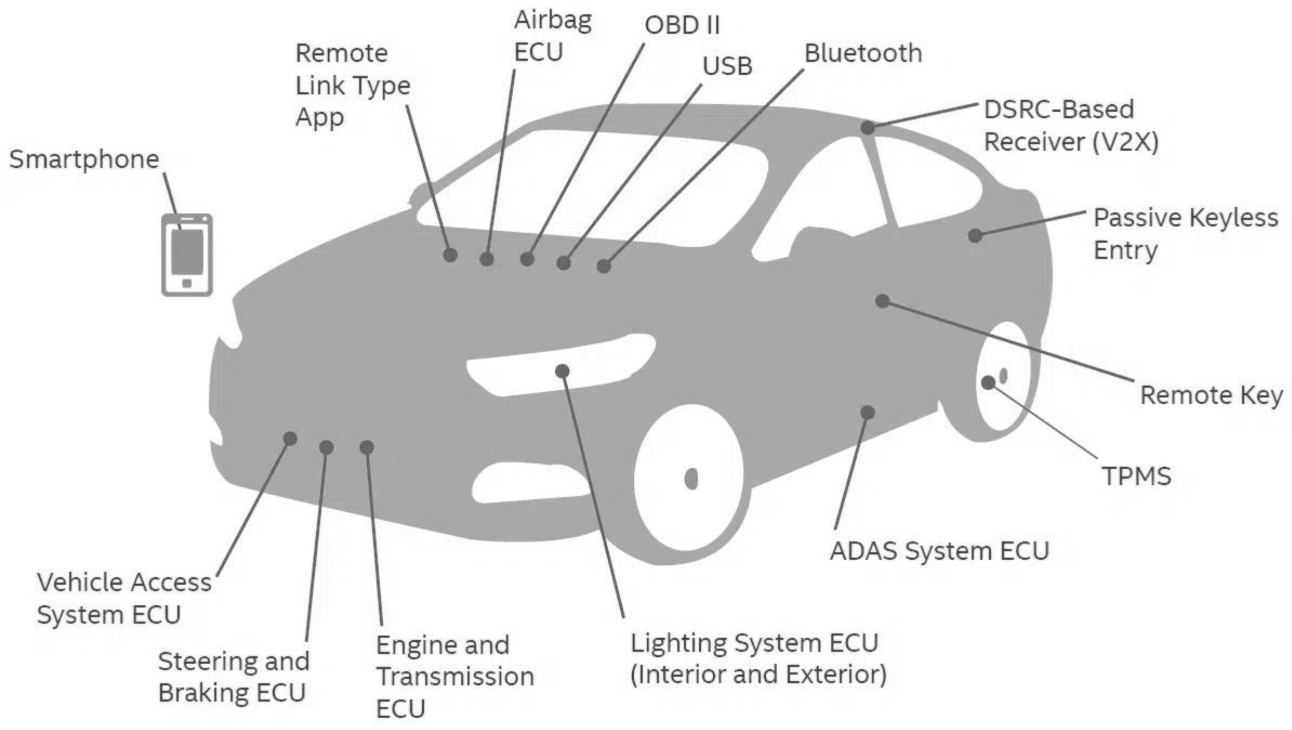
ISO/SAE 21434: This is a standard for cybersecurity engineering of road vehicles that guides how to implement cybersecurity in the vehicle development process.

Automotive – Cybersecurity

Multiple Use Cases requiring high-level "Safety → ISO 26262 " and "Security → HSM"

Electronic systems will account for 50% of a new vehicle's total cost by 2030. source: Deloitte

Demanding different Safety & Security requirements for:



- Multiple electronic control units (ECUs),
- Advanced driver-assistance systems (ADAS)
- Machine learning CPUs
- 5G and vehicle-to-everything (V2X) connections
- Multiple sensors
- Infotainment systems
- In-cabin artificial intelligence
- Remote engine starting
- Key Car Access / Secure Driver Authentication

Automotive Standards Driving HW Security Requirements

Security HW Requirements & Certification

EVITA

European project documentation describing recommendations in terms of architecture, features and API for vehicle security. Three levels (low, medium, full) corresponding to different types of ECU.

CC V2X PP

Protection Profile V2X Hardware Security Module based on Common Criteria EAL4+, AVA_VAN.4 and ALC_FLR.1. Sets up the requirements for connected communication modules in the vehicle that must be met to achieve proper security level

SAE J3101

Common set of Requirements to be applied to hardware assisted functions in order to ensure the security of cars and other vehicles against cyber security threats.

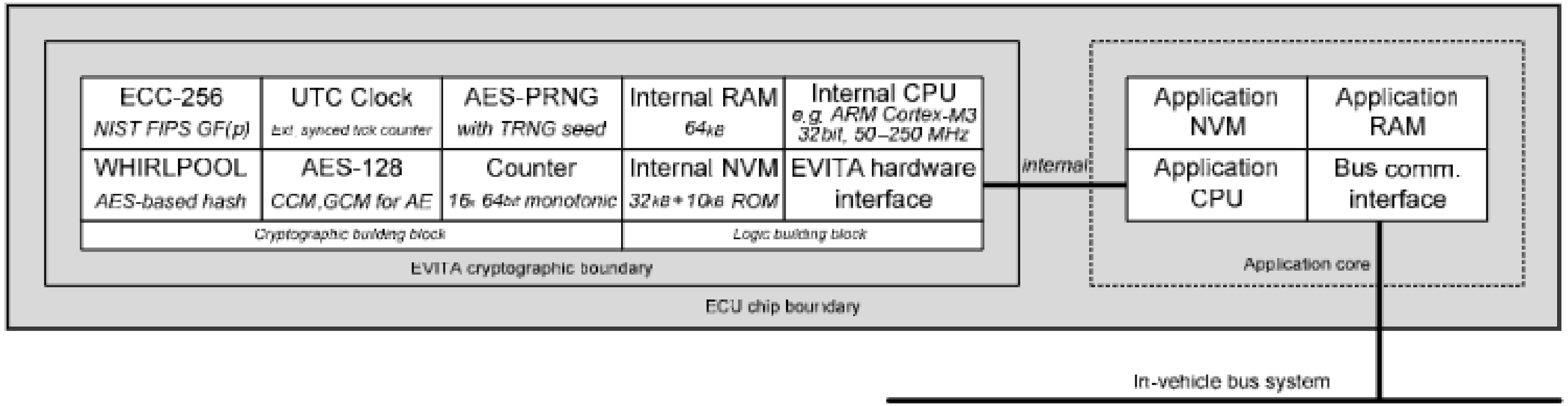


Figure 7: EVITA full hardware security module (V2X level)

AUTOSAR Secure Onboard Communication (SecOC)

Security HW Requirements & Certification

SecOC Secure Enclave Provides

- Message Authentication Code (MAC) based on AES
- Monotonic Message Freshness Counter
  - To prevent replay attacks

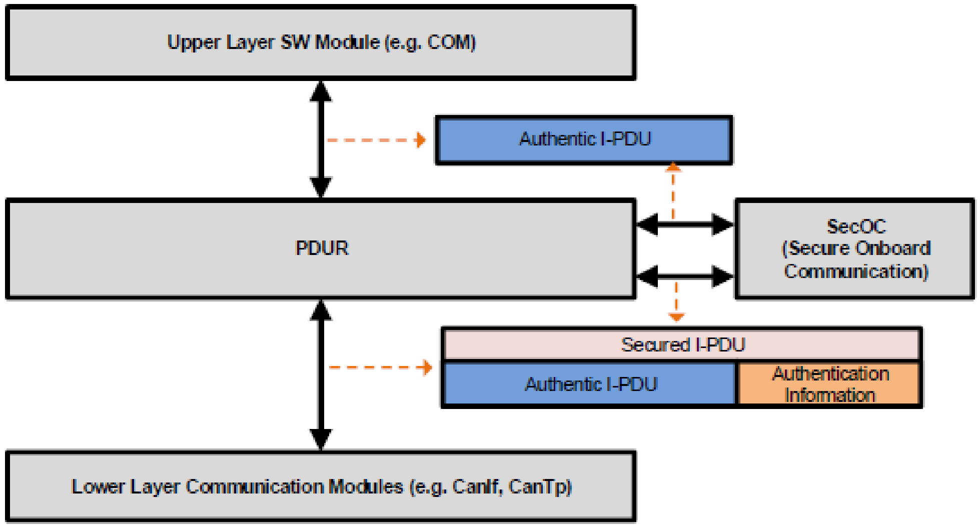


Figure 7:Transformation of an Authentic I-PDU in a Secured I-PDU by SecOC

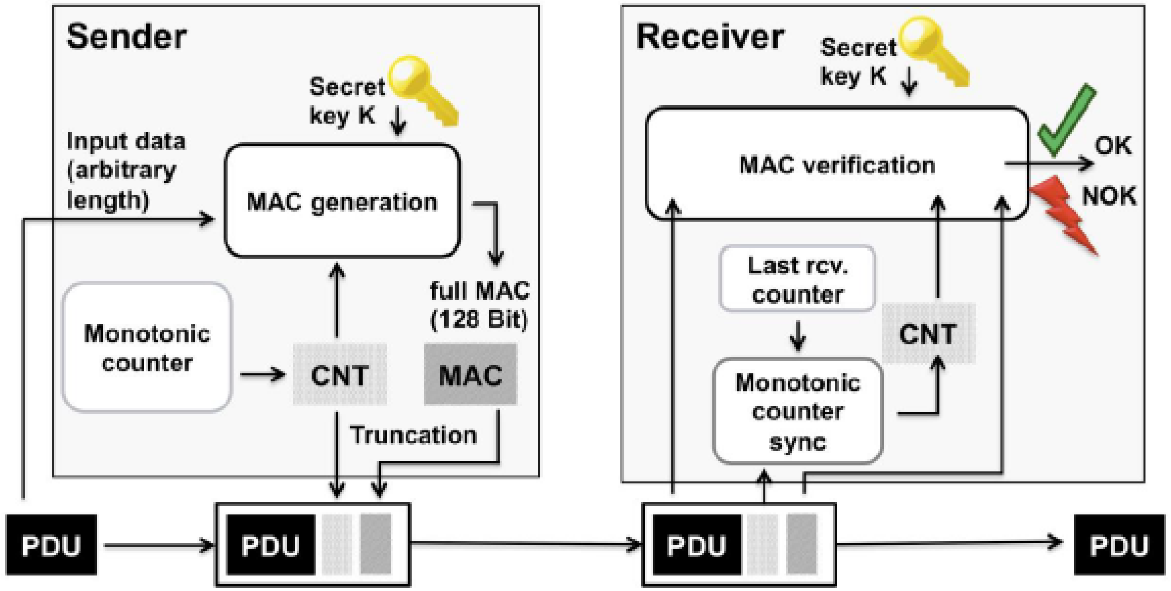


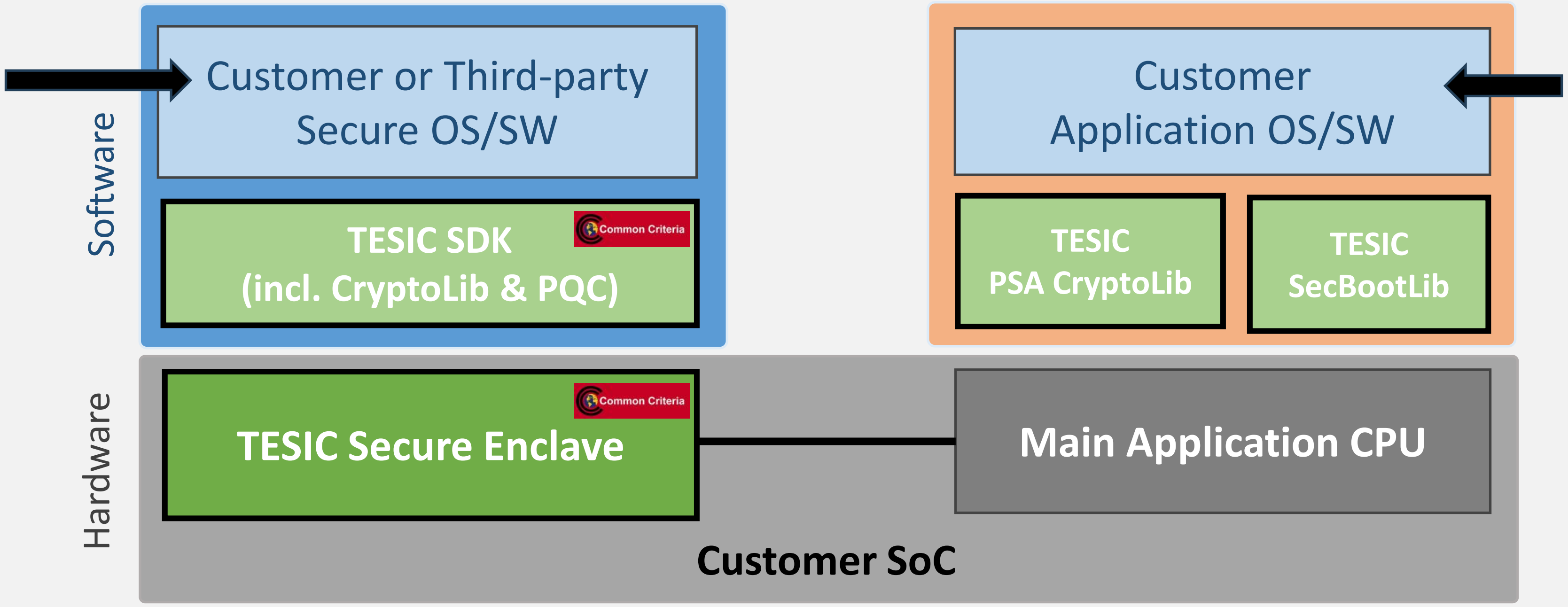
Figure 2: Message Authentication and Freshness Verification

Secure Enclave IP Overview

Timepo’s TESIC solution is adapted to cover security needs for many use cases

TESIC enables secure software to be executed in certified secure enclave TESIC…

Typical usage: secure and certified OS/SW (e.g. JavaCard OS and applets) developed by third-parties for standard secure applications such as GSMA iSIM and FIDO authentication



…and exports security services to application software executed by application CPU

Typical usage: secure boot for application CPU or integration of cryptographic function calls inside non-secure/non-certified application software

Compliant ISO 26262 – ASIL B & D (*)

(*) Currently collaborating with TÜV NORD Mobilität GmbH on safety compliance assessment

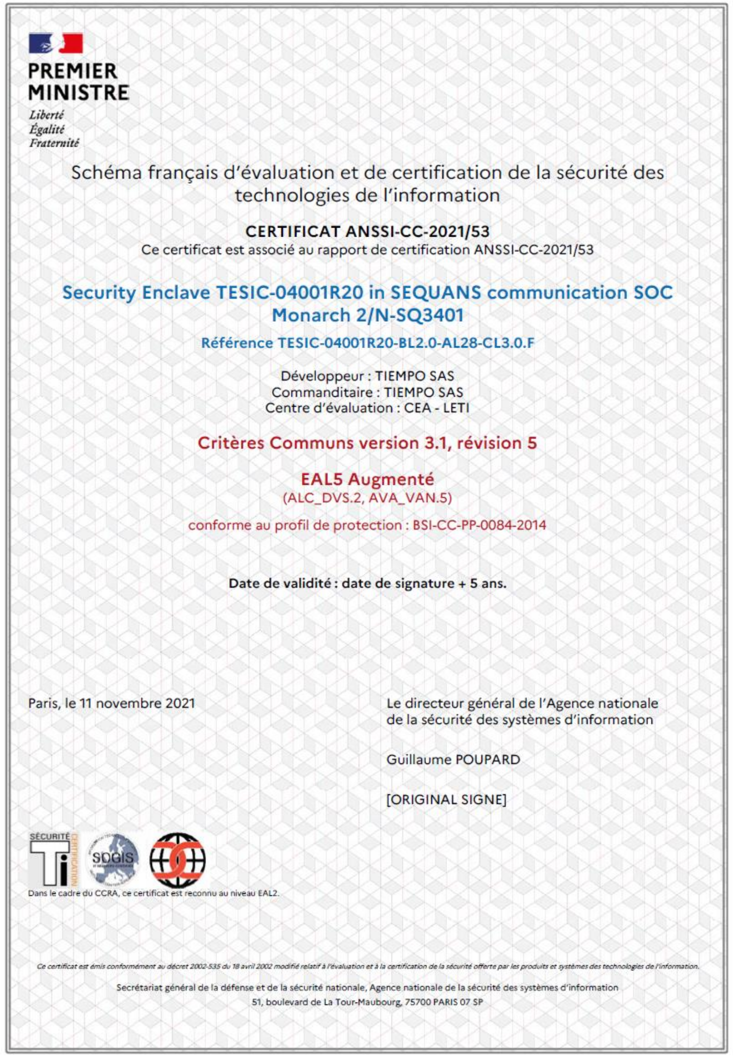
Common Criteria = CC EAL5+ AVA_VAN.5 compliant/pre-certified

□ = TESIC deliverable

World’s First CC EAL5+ Certified iSIM Module

Thanks to Tiempo Secure’s TESIC secure element IP that is pre-qualified for CC EAL5+ certification

- https://www.sequans.com/press-release/sequans-delivers-industrys-first-common-criteria-eal5-certified-cellular-iot-platform/
- https://www.tiempo-secure.com/first-soc-ever-to-pass-cc-eal5-certification-thanks-to-tiempo-secure-tesic-secure-element-ip/



PREMIER
MINISTRE

Liberté
Égalité
Fraternité

Schéma français d’évaluation et de certification de la sécurité des technologies de l’information

CERTIFICAT ANSSI-CC-2021/53

Ce certificat est associé au rapport de certification ANSSI-CC-2021/53

Security Enclave TESIC-04001R20 in SEQUANS communication SOC Monarch 2/N-SQ3401

Référence TESIC-04001R20-BL2.0-AL28-CL3.0.F

Développeur : TIEMPO SAS
Commanditaire : TIEMPO SAS
Centre d’évaluation : CEA - LETI

Critères Communs version 3.1, révision 5

EAL5 Augmenté
(ALC_DVS.2, AVA_VAN.5)

conforme au profil de protection : BSI-CC-PP-0084-2014

Date de validité : date de signature + 5 ans.

Paris, le 11 novembre 2021

Le directeur général de l’Agence nationale
de la sécurité des systèmes d’information

Guillaume POUPARD

[ORIGINAL SIGNE]

Dans le cadre du CCRA, ce certificat est reconnu au niveau EAL2.

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 modifié relatif à l’évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l’information.

Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d’information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Tiempo SECURE

THANK YOU

&

Any Questions?