



Scalable Security for Connected Devices

JAIF
Centre Inria - Université de Rennes

Serge Maginot
CEO - Tiempo Secure

October 1st, 2024



Tiempo Secure: Who we are

A dedicated team with 17 years of Expertise in Embedded Security Design and Certification.

An **independent European provider** with more than 17 years of experience in developing Secure IP and Embedded software.



The R&D Center is located in France, **certified CC/MSSR, audited/certified by the ANSSI** (French national cybersecurity agency)



European Technology Provider

Strong IP Portfolio & Services



Unique Expertise in IP security design and services, from design security hardening to customer chip certification and **HSM server set up for key management** to maintain trust throughout the entire product life cycle

Patented Technology and Innovation with design capabilities for any Secure IC Design: **IoT & Mobile Connectivity, AI, Automotive, Secure Transactions, Digital Currency & Identity, and Aeronautic/Defense**



Security Innovation DNA



Unique Certification Expertise



The only security IP provider that **contractually commits to the CC, FIPs, PSA, SESIP certification** of customers' chips integrating TESIS or TESIS RISC-V hard macro iSE/Secure Enclave

Long-term collaboration with ITSEF CEA-LETI and SERMA and certification bodies (ANSSI)

Member of



Member of

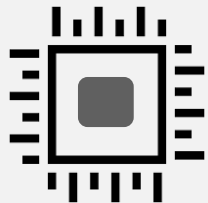


High-End Certified IP & Services for Secure IC Design and Production

Certified HW & SW Compliant Solutions

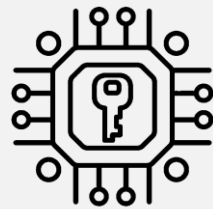
Design & Security Services

Secure Enclave IP



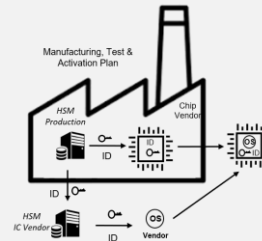
TESIC
Secure Enclave (certified)

Security & Crypto IP



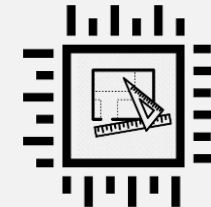
State-of-the-art secure HW & SW, certified cryptography IP

Secure Provisioning



Root of Trust Provisioning

Consultancy



SE design, System configuration and Application-Level needs

Certification



Full EAL5+/EAL6+/FIPs / SESIP for MCU/SE Certification

3 CPU Core Options

Legacy
Tiempo



Custom
e.g ARM

TRNG, LMS, AES, ECC, RSA, TDES, SHA2, SHA3, PQC...

API-First Approach

HSM Setup and Key Management Operations

Complete chip delivery and industrialization in strategic partnership With IC'ALPS:
Smartcard / SIM/eSIM, ID Gov, SE (CC) EAL5+ and IoT applications.

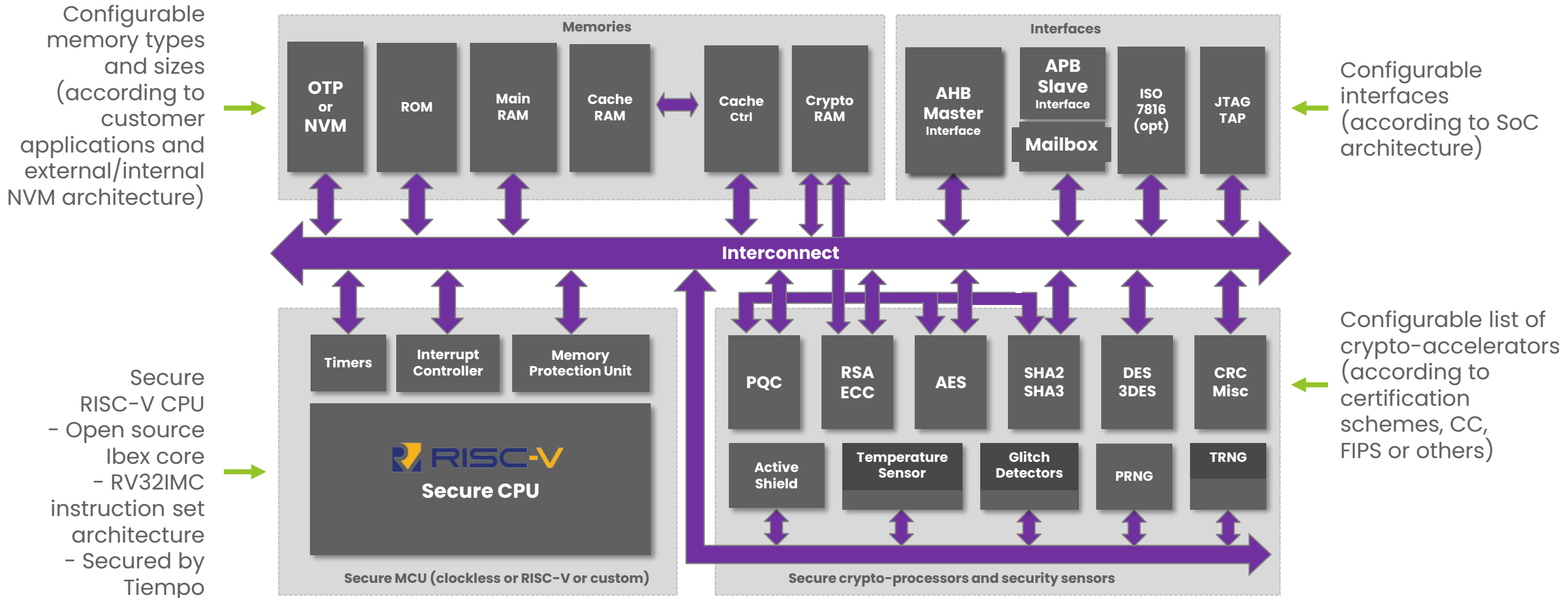


- Preparation of the full documentation set of the Authorized Product.
- Technical Support with Administrative work with gov cybersecurity authority.

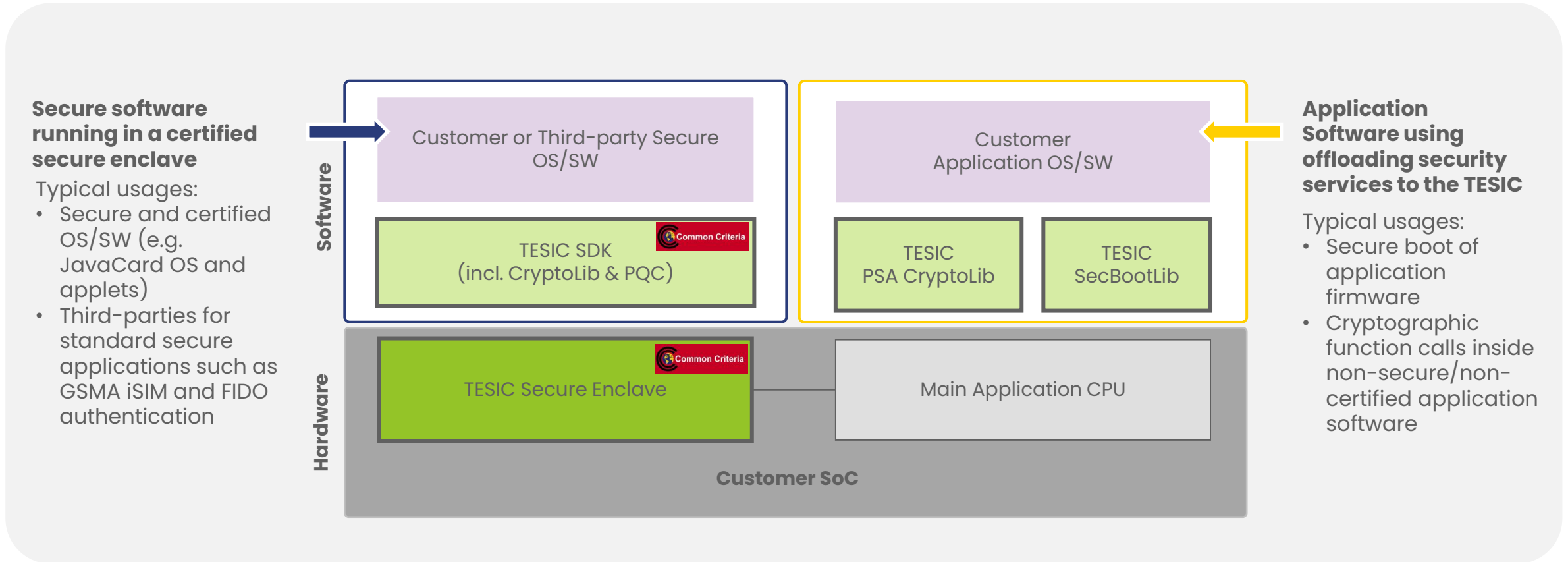


Trusted Devices provide a Trusted Environment for Data and Applications

TESIC Secure Enclave Flexible Architecture




TESIC – a Secure Enclave for multiple use cases



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

Ecosystem of Standards and Certifications

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



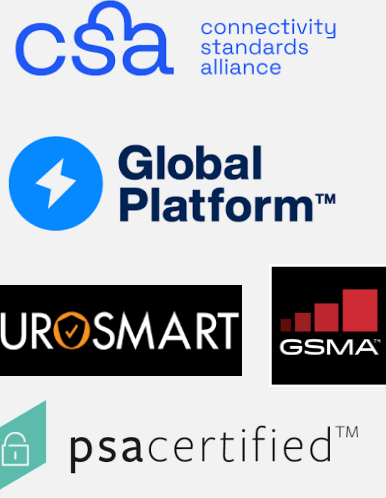
LEGISLATION

What is required legally?



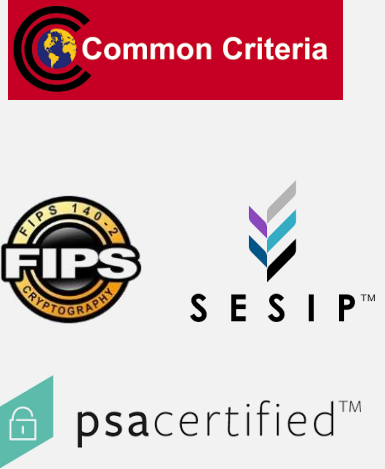
STANDARDS DEFINITION

What is required functionally per market?



DEVICE PROTECTION PROFILE

What is required functionally per usage?



CERTIFICATION SCHEMES

How to standardize Silicon Platform?

Security Certification Schemes

Common Criteria (CC)

- Common Criteria (CC) is an international set of specifications and guidelines designed to evaluate information security products and systems, to certify that products and systems meet a pre-defined security standard.
- EUCC** : adoption by EU of CC Certification Scheme (January 2024)



GlobalPlatform SESIP

- SESIP for “**Security Evaluation Standard for IoT Platforms**”
- Focus on the ‘thing’ side of IoT, on the security of connected devices based on connected platforms, and on services for connected objects
- IoT Platform parts can be developed and evaluated separately, with reuse of evaluation results for composition evaluations



FIPS 140-3

- The Federal Information Processing Standard Publication 140-3 (FIPS PUB 140-3) is a US government computer security standard used to approve **cryptographic modules**.
- FIPS 140-3 is based on ISO/IEC 19790, an international standard.



What certification standard/level for what usage ?

■ **Common Criteria (CC)** Certification Scheme

- Long proven for the most security demanding applications : governmental/ID documents, banking cards
- CC EAL5+ AVA_VAN.5 assurance level is an ideal target for devices needing resistance against side-channel and perturbation/fault injection attacks

■ **CC Protections Profiles**

- A protection profile defines a set of security objectives and requirements for a category of products that covers the security requirements common to several users
- **PP-0084** = smartcard chips, **PP-0117** = SoCs with secure enclave and external flash

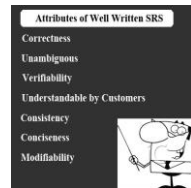
■ **Assurance level for connected devices**

- CC EAL5+ AVA_VAN.5 adapted for/required by standardized applications, e.g., eSIM/iSIM standardized by GSMA
- Naturally suited for digital ID, payment and potentially for other security sensitive domains like automotive (e.g., V2X HSM)
- What about other IoT applications ?

Difficulties with Common Criteria certifications

- Reusability of highest levels of certification : limits of *"qui peut le plus peut le moins"*
 - Specialized features to reach **AVA_VAN.5**, such as security sensors, requiring specific analog parts and physical designs, adding design and characterization costs on newly supported silicon processes
 - Strong constraints/limitations imposed on design deployments within large organizations (CC/MSSR compliant sites)
 - Impacts on area, power, performance
- Problems with CC evaluation/certification process
 - Not enough labs, not enough resources/planning slots among available labs
 - Too expensive, too long, too complicated (e.g., CC documentation, CC life-cycle)
 - Totally incompatible (or perceived so) with time-to-market constraints of many IoT products
 - Need for mentality and organizational evolutions: smartcards => IoT, regulatory => market

Common Criteria Assurance Families



TOE : Target Of Evaluation
 ST : Security Target
 TSF : TOE Security Functionality
 CM : Configuration Management

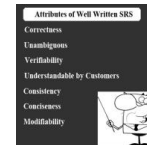
Assurance Class	Assurance Family	Subject
Development	ADV_ARC	Security Architecture
	ADV_FSP	Functional specification
	ADV_IMP	Implementation representation
	ADV_INT	TSF internals
	ADV_SPM	Security policy modelling
	ADV_TDS	TOE design
Guidance Documents	AGD_OPE	Operational user guidance
	AGD_PRE	Preparative procedures
Life-cycle Support	ALC_CMC	CM capabilities
	ALC_CMS	CM scope
	ALC_DEL	Delivery
	ALC_DVS	Development security
	ALC_FLR	Flaw remediation
	ALC_LCD	Life-cycle definition
Security Target Evaluation	ASE_CCL	Conformance claims
	ASE_ECD	Extended components definition
	ASE_INT	ST introduction
	ASE_OBJ	Security objectives
	ASE_REQ	Security requirements
	ASE_SPD	Security problem definition
	ASE_TSS	TOE summary specification
	Tests	ATE_COV
ATE_DPT		Depth
ATE_FUN		Functional tests
ATE_IND		Independent testing
Vulnerability Assessment	AVA_VAN	Vulnerability analysis

Common Criteria Evaluation Assurance Levels (EAL)

- Common Criteria has 7 levels
 - EAL1 Functionally tested
 - EAL2 Structurally tested
 - EAL3 Methodically tested and checked
 - EAL4 Methodically designed, tested and reviewed
 - EAL5 Semi formally designed and tested
 - EAL6 Semi formally verified design and tested
 - EAL7 Formally verified design and tested

- Augmented EAL (or EAL...+)
 - Example used by Tiempo: EAL5+ = EAL5 and AVA_VAN.5 and ALC_DVS.2 and ALC_FLR.2

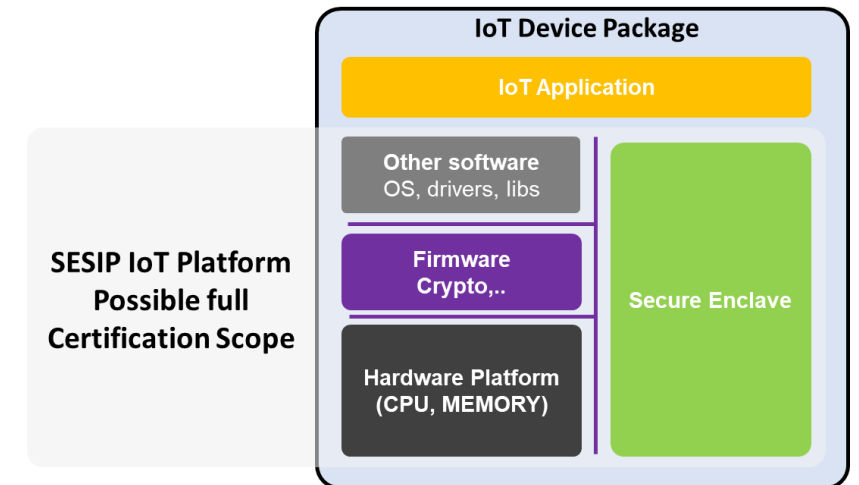
- MSSR = Minimum site security requirements
 - Example used by Tiempo: EAL6 = ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1, ALC_TAT.3 and ALC_FLR.2



Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Alternative to CC : GLObalPlatform™ SESIP

- Apparition of other security evaluation standards: **GLObalPlatform™ SESIP**
- According to GlobalPlatform™ Web site: “The Security Evaluation Standard for **IoT Platforms** (SESIP) is a methodology that reduces the cost, complexity and effort of security evaluation and certification.”
 - Perception shared by many of our customers/prospects
- Assurance levels SESIP 1 to SESIP 5, roughly:
 - SESIP 3 = “substantial” = AVA_VAN.3
 - SESIP 5 = “high” = AVA_VAN.5
- SESIP scope covers all needs of certification for the IoT devices: not only the secure enclave and low-level firmware, but also, the full IoT device, including its application



SESIP Assurance Levels

- Level 1 : Self-assessment - Utilizing public tools to discover publicized potential vulnerabilities (Common Criteria AVA_VAN.1)
- Level 2 : Black-Grey box penetration testing - Adding vulnerability analysis and penetration testing (Common Criteria AVA_VAN.2)
- Level 3 : White-box vulnerability analysis and penetration testing - Adding source code review (Common Criteria AVA_VAN.3)
- Level 4 : Adding source code review - More evidences and higher attack potential (Common Criteria AVA_VAN.4)
- Level 5 : Reuse of SOG-IS/EUCC CC evaluation - More evidences and higher attack potential (Common Criteria AVA_VAN.5)

Assurance class	Assurance Family	EAL3	SESIP3
Development	ADV_ARC	1	
	ADV_FSP	3	4
	ADV_IMP		3
	ADV_INT		
	ADV_SPM		
	ADV_TDS	2	
Guidance documents	AGD_OPE	1	1
	AGD_PRE	1	1
Life-cycle support	ALC_CMC	3	1
	ALC_CMS	3	1
	ALC_DEL	1	
	ALC_DVS	1	
	ALC_FLR		2
	ALC_LCD	1	
Security Target evaluation	ALC_TAT		
	ASE_CCL	1	
	ASE_ECD	1	
	ASE_INT	1	1
	ASE_OBJ	2	1
	ASE_REQ	2	3
	ASE_SPD	1	
ASE_TSS	1	1	
Tests	ATE_COV	2	
	ATE_DPT	1	
	ATE_FUN	1	
	ATE_IND	2	1
Vulnerability assessment	AVA_VAN	2	3

FIPS 140-3 Assurance Levels



- FIPS 140-3 is a US government computer security standard used to approve cryptographic modules and based on ISO/IEC 19790
- FIPS comes with four assurance levels. For each level, a greater amount of evidence and engineering is required from the product manufacturer in order to show compliance with the standard.
 - Level 1 : Validation of at least one approved algorithm or security function and requires production-grade equipment and externally tested algorithms.
 - Level 2 : Adds requirements for physical tamper-evidence and role-based authentication.
 - Level 3 : Adds requirements for physical tamper-resistance, environmental conditions for temperature and voltage. Must use a trusted channel for the transmission of unprotected key.
 - Level 4 : This level makes the physical security requirements more stringent, requiring the ability to be tamper-active, erasing the contents of the device if it detects various forms of environmental attack. EFP and protection against fault injection is required as well as multi-factor authentication.

About EUCC




- EUCC : adoption by EU of Common Criteria Certification Scheme (January 2024), including two assurance levels:
 - “Substantial” mapped to AVA_VAN.1 and AVA_VAN.2
 - “High” mapped to AVA_VAN.3 to AVA_VAN.5
- Main expected advantage: it might unify the adoption and interpretation of the Common Criteria Certification Scheme among the EU countries
- To be considered/evaluated : the so-called “substantial” assurance level



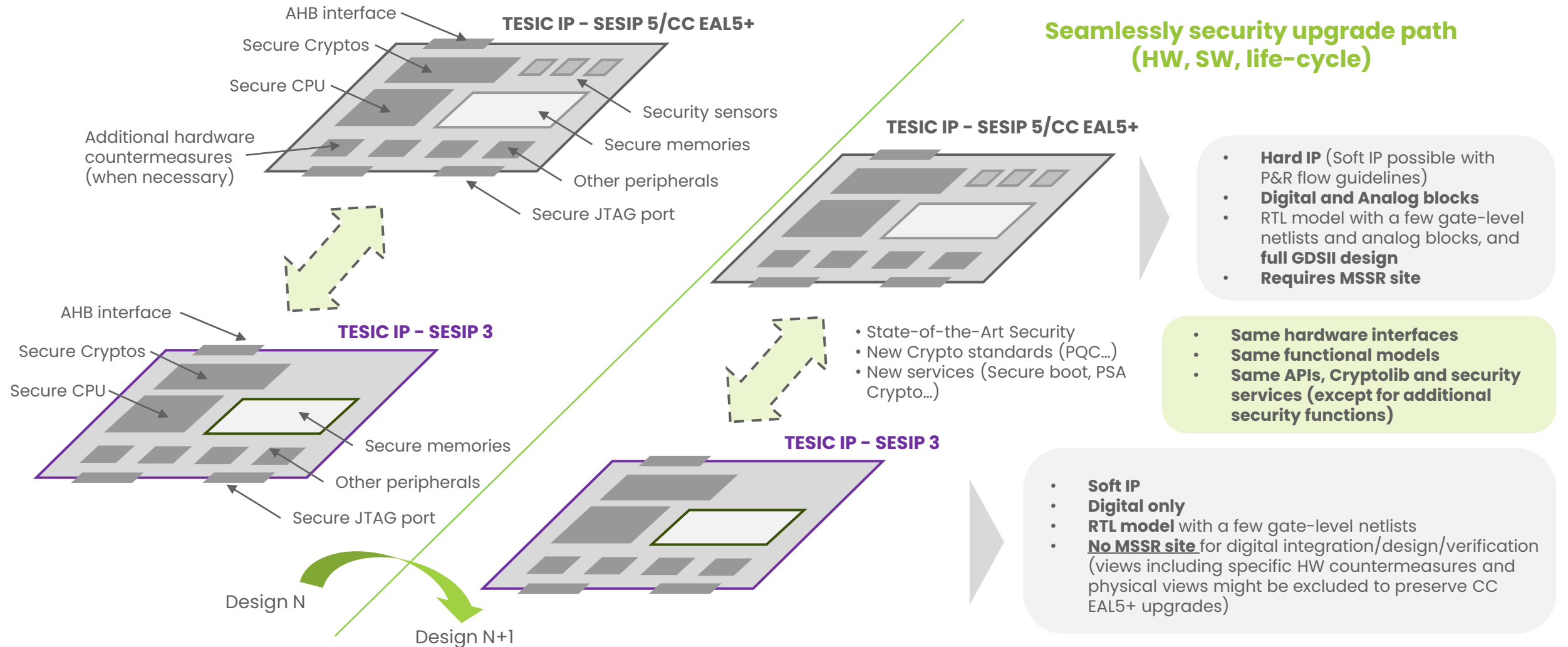
Tiempo extends its security solution portfolio with « lower » certification grades

- “Lower” grade does not necessarily mean less counter-measures
 - Assurance levels not defined by type of attacks, but by the efforts spent by the attacker during the evaluation
- Tiempo Secure choices:
 - Two general assurance levels: AVA_VAN.5/CC EAL5+/"high" and AVA_VAN.3/SESIP 3/"substantial"
 - Keep comparable hardware security ("comparable" secured RISC-V CPU, but no security sensors for SESIP 3)
 - Let SESIP 3 customers benefit from easier design/software deployment : Soft IP, (almost) full digital IP
 - Unfortunately, at the cost for Tiempo of maintaining two branches (spec/work in progress)
- Offer a complete security solution allowing upgrade from “substantial” to “high” assurance level
 - Family from TESIC 300 (SESIP 3 AVA_VAN.3) to TESIC 500 (CC EAL5+ AVA_VAN.5)
 - TESIC 300 family also includes hardware customized for specific security feature (e.g., secure boot)
 - TESIC 500 includes generic full-featured secure enclave hardware

TESIC Secure Enclave IP Family

TESIC IP Family	Key Features	Provisioning	Certification	Delivery	Process node (for hard macro)
<div style="border: 1px solid black; padding: 5px; display: inline-block;">TESIC – 500</div> 	RISC-V 32 Bits / 64 Bits (TBC) <ul style="list-style-type: none"> •Physically isolated Secure Element able to execute applets in a secured and certified environment •Runs SE applets on standard Java Card OS •Secure storage of sensitive data and key materials (e.g. private keys, encryption keys) 	Provisioning function supported by TIEMPO HSM Solution for Key Management / Key Ceremony and Image Generation	Meets government requirements with CC EAL5+ / EAL6+, SESIP 4 & 5 and FIPS 140.3 certifications	Delivered as a hard macro to meet certification requirements Targets RTL delivery +backend guidelines	55nm GF 40nm TSMC 22nm GF FDX 22nm TSMC 16nm TSMC
<div style="border: 1px solid black; padding: 5px; display: inline-block;">TESIC – 400</div> Proprietary Tiempo 	Tiempo Proprietary CPU <ul style="list-style-type: none"> •Physically isolated Secure Element able to execute applets in a secured and certified environment •Runs SE applets on standard Java Card OS •Secure storage of sensitive data and key materials (e.g. private keys, encryption keys) 	Provisioning function supported by TIEMPO HSM Solution for Key Management / Key Ceremony and Image Generation	Meets government requirements with CC EAL5+ / EAL6+, SESIP 4 & 5 and FIPS 140.3 certifications	Delivered as a hard macro to meet certification requirements	55nm GF 40nm TSMC 22nm GF FDX 22nm TSMC 16nm TSMC
<div style="border: 1px solid black; padding: 5px; display: inline-block;">TESIC – 300</div> 	<ul style="list-style-type: none"> •Off-loading of crypto functions from main CPU in an isolated environment with dedicated 32-bit RISC-V CPU •Security features: Secure Boot, PSA and Post Quantum Crypto Libraries, Authentication, Integrity, Secure Update 	Not mandatory	Compliant with SESIP 3 AVA_VAN.3 certification	Delivered as a synthesizable RTL for flexibility and easy integration	Not applicable (RTL only)

Evolutionary IP Architecture for multiple designs



What's next

- Follow/anticipate evolution of certification standards/schemes
 - EUCC, SESIP, FIPS
 - Application-specific standards and protection profiles
- Check/anticipate adoption rate by the industry
 - Impact on costs and time-to-market
 - Certification reusability problem
 - Not all semiconductor companies are motivated by independent certifications/evaluations
 - Decide for appropriate security assurance level
- Necessity for security certification labs to extend their capacities
- Necessity for chip/IP providers to have scalable and upgradable security offers



Thank you!

