COMPETENCE
CENTER
CRYPTO &
SECURITY

SESIP A META-FRAMEWORK CERTIFICATION APPROACH

John BOGGIE, Director, Head of Cybersecurity Certification
NXP Semiconductors UK

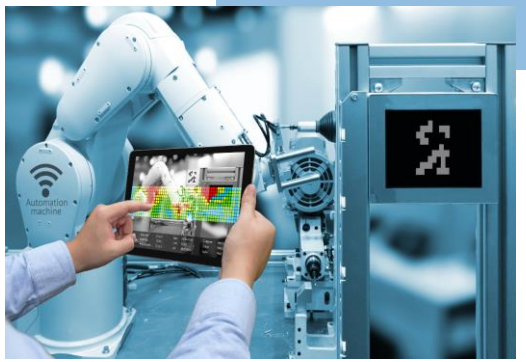
RISC-V SUMMIT SAN JOSE

NXP
SECURE CONNECTIONS
FOR A SMARTER WORLD

The connected world

We are more and more reliant on connected devices. Massive amounts of data are regularly transferred from node to edge to cloud, analysed, with the resulting information, used stored or transferred to other entities.

This will not stop it will only increase, Connected Factories, Connected Cars, Connected infrastructure, Deep learning, etc, etc, etc..

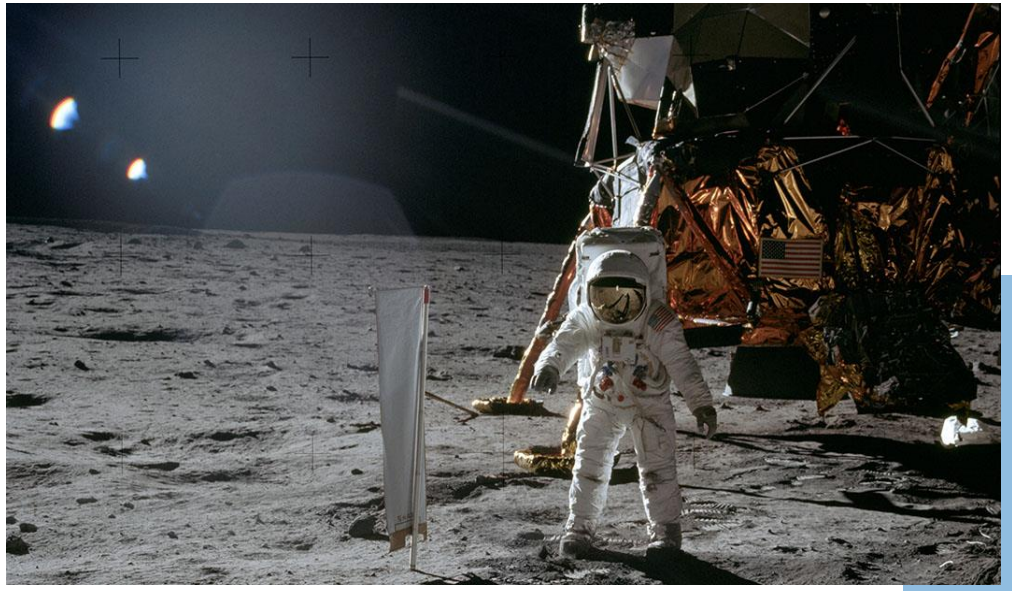


A typical IoT chip

A typical IoT chip includes multiple interfaces multiple processors firmware and cryptographic capabilities.

The NXP i.MX 7ULP has a larger CPU than the computer that the was used in the Apollo 11 capsule.

Fun Fact: NXP Technology was used to transmit and receive information from the Apollo Lunar Module

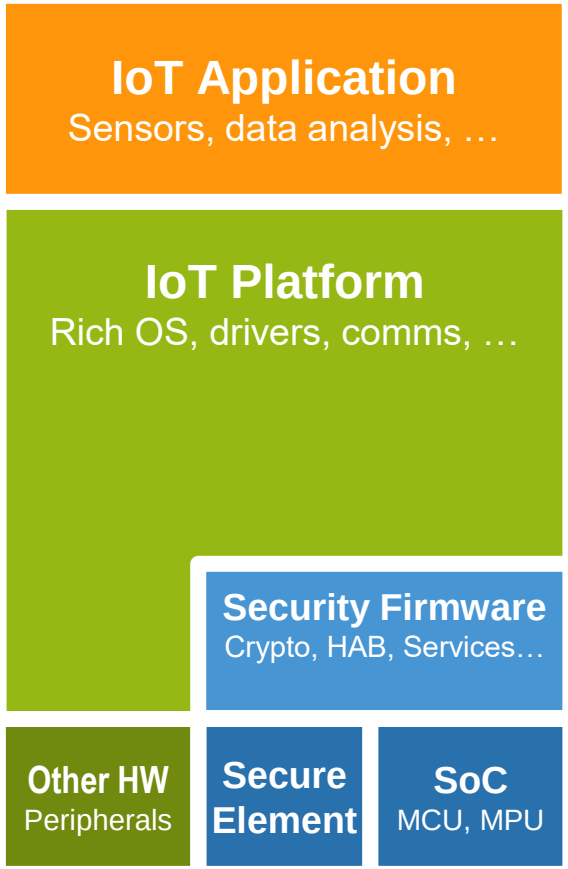


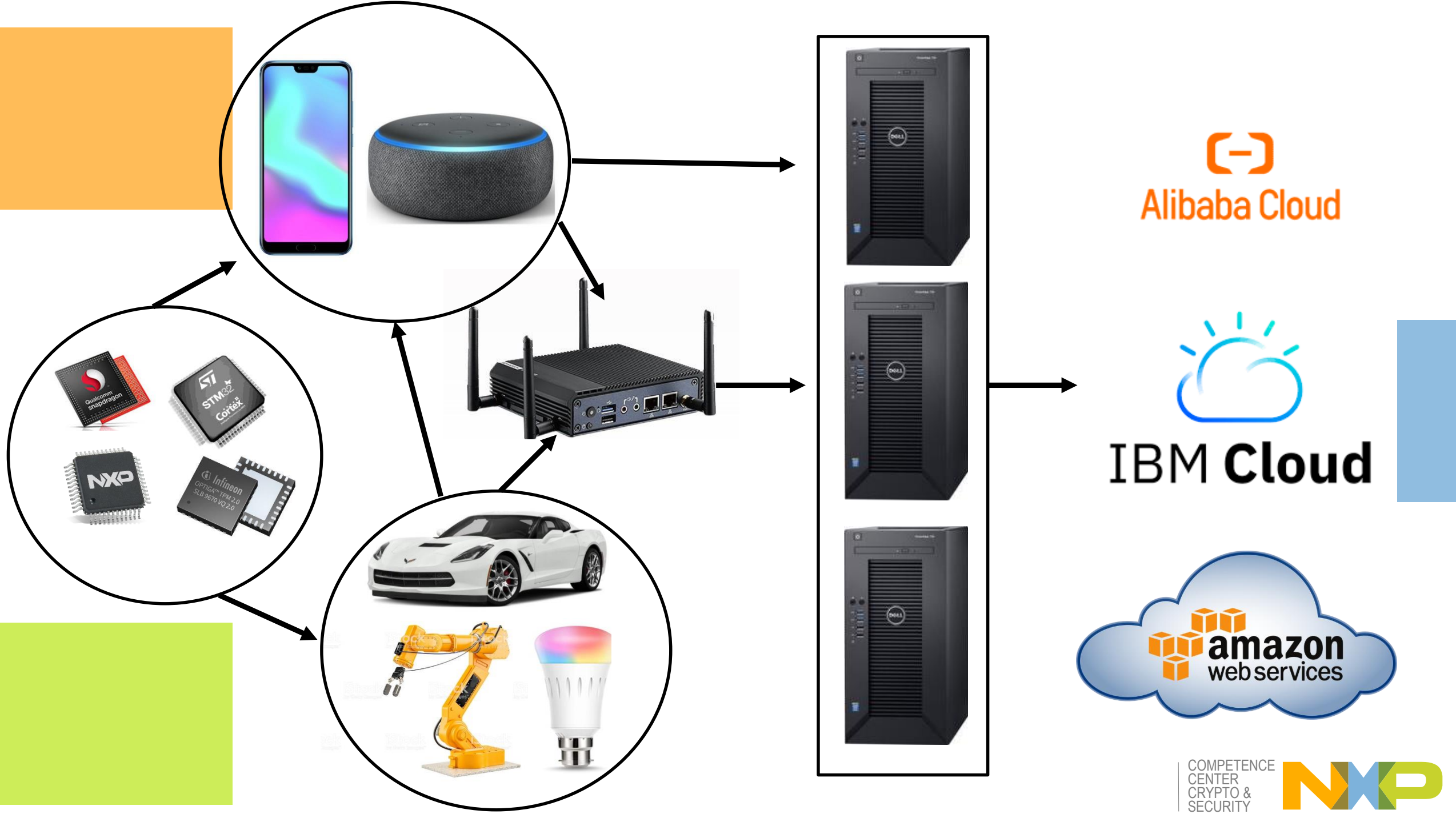
A typical IoT device

Root of Trust , Security FW and services, Rich OS, Comm Stack. Sensors, analytics etc.

The devices is required to:

- Register itself with the cloud service
- Be configurable, including provisioning
- Monitor its operations and perform diagnostics
- Provide analytics to the service provider
- Troubleshoot and report issues to the service provider
- Authenticate and load patches

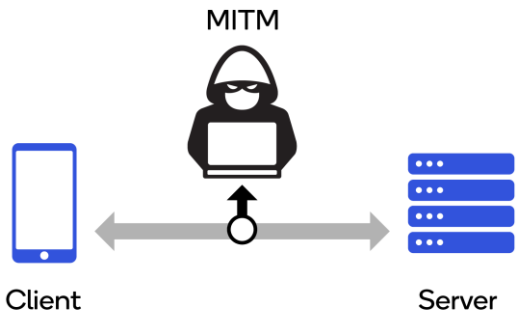



Qualcomm snapdragon
STM32
Cortex
NXP
Infineon
OPTIGA™ TPM 2.0
SLB 9670 VQ 2.0
Alibaba Cloud
IBM Cloud
amazon
web services
COMPETENCE
CENTER
CRYPTO &
SECURITY
NXP

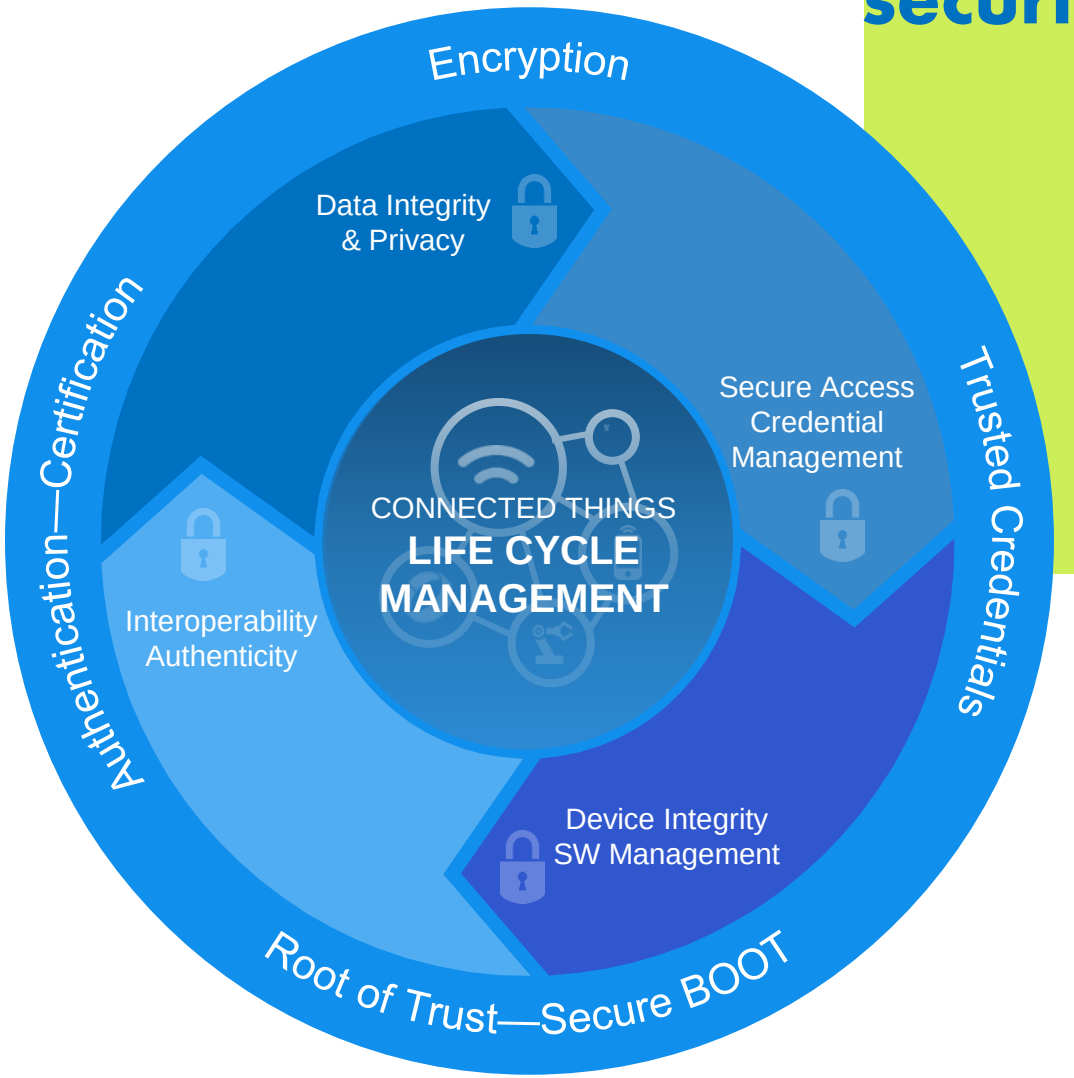
What about security?

Each connected node gathers a large amount of data and passes it to the service provider. This data is valuable so must be protected. Plus if you can control the nodes, actuator or edge then you can access services not paid for by either onboarding rouge nodes or escalating the privileges of a node. There is also DOS, botnets, ransomware etc.

The IoT is a complex system with multiple attack points that if used for malice provide lots of potential for money making or even threats to public safety.



Connected device security



SECURITY CERTIFICATION

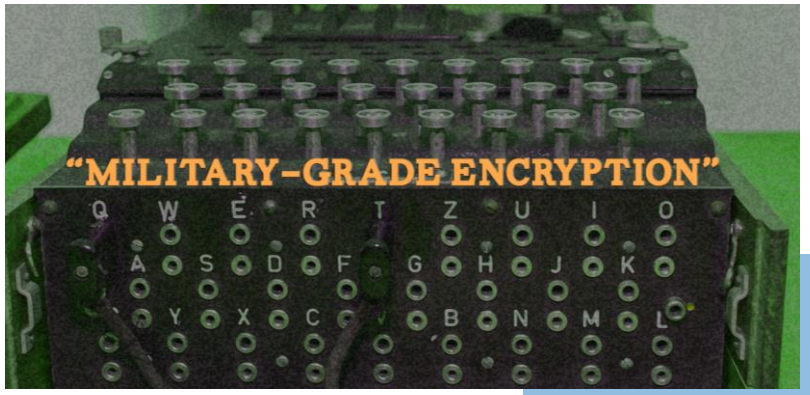
COMPETENCE
CENTER
CRYPTO &
SECURITY

Certification?

One way to ensure that a system has considered security issues is to enforce a security certification as a requirement for the supply chain components or end solutions. Too many companies are making strong security claims with no back-up evidence.

Also the certification landscape is fragmented with multiple competing standards causing confusion for end users and policy makers. For example in Europe as part of the EU Cyber security act a Database of cybersecurity certifications standards is being generated to provide a catalogue of certification standards per Connected Device domain.

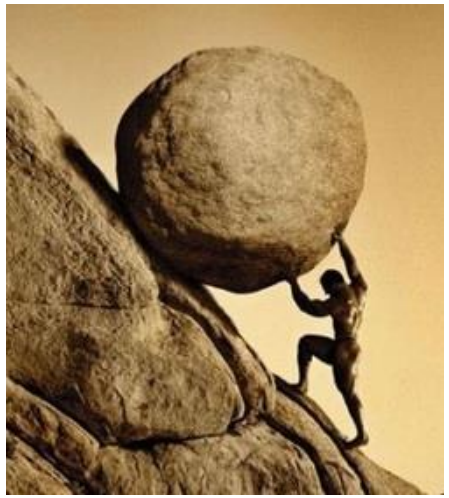
This is also happening in the Charter of Trust partnership where members are looking at cyber security standards and how they fit together through the supply chain of a cyber security product.



Enough is enough!
What do we need?

Look we need to be realistic here it is not easy generating a standard it takes a lot of work and effort. So no one is going to let their baby go, “we fought long and hard for this, and we believe our standard is the greatest in the universe”. So instead of deleting or removing standards let’s work together to link them and fill gaps where they exist.

Also we should make the process easy, user friendly and as much as possible re-use what already exists.



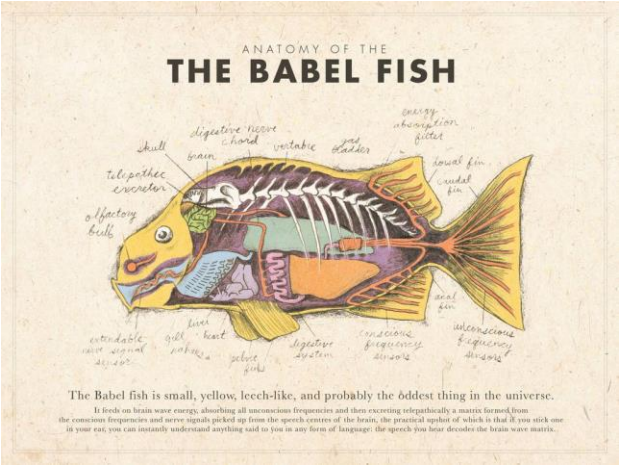
SECURITY EVALUATION STANDARD FOR IOT PLATFORMS
A META FRAMEWORK APPROACH

COMPETENCE
CENTER
CRYPTO &
SECURITY
NXP

WTF is a Metaframework?

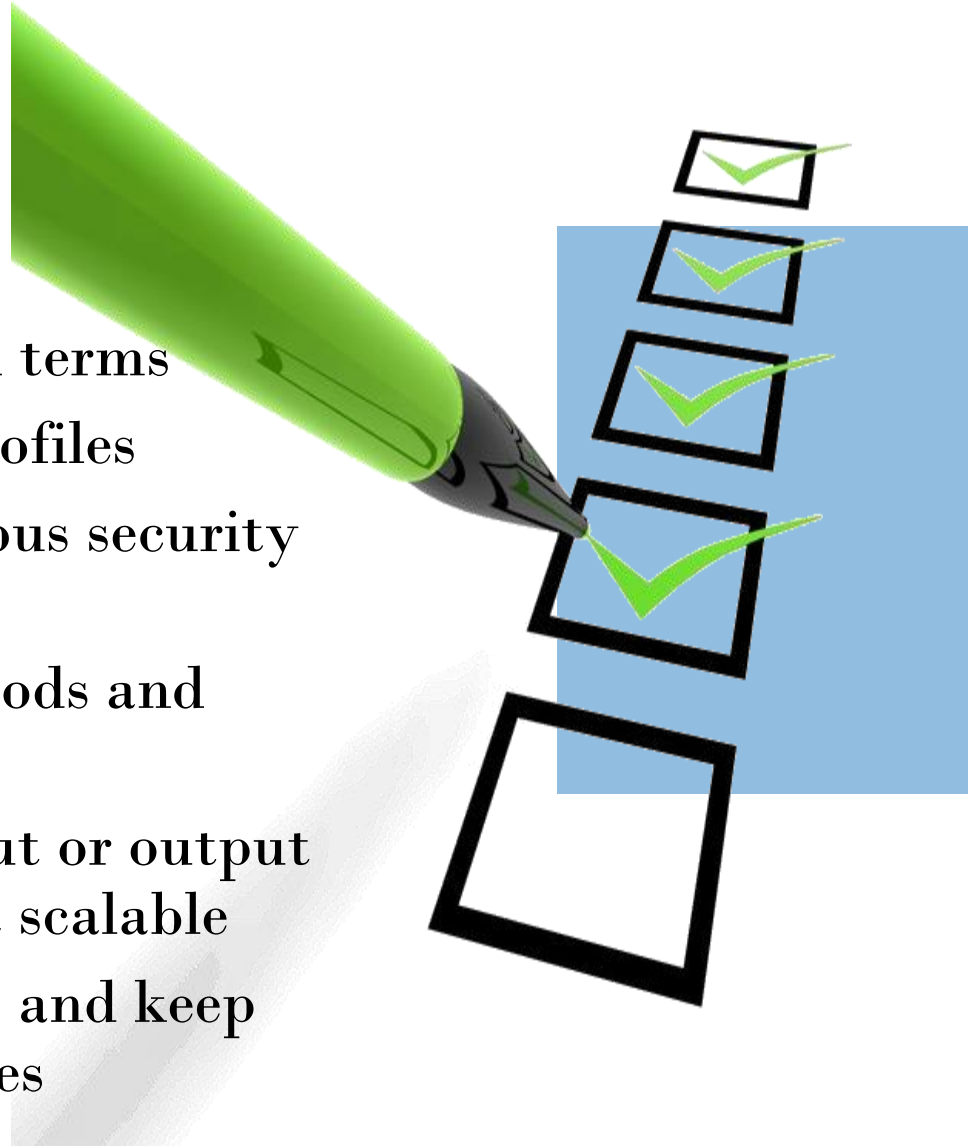
"**A framework** that has a set of core interfaces for common services and a highly extensible backbone for integrating components and services. The structure is open and flexible to incorporate other concrete **frameworks** and components." Java Web Application Definition

Or to make it clearer an interpretation tool defining a common language used to glue or link standards together.

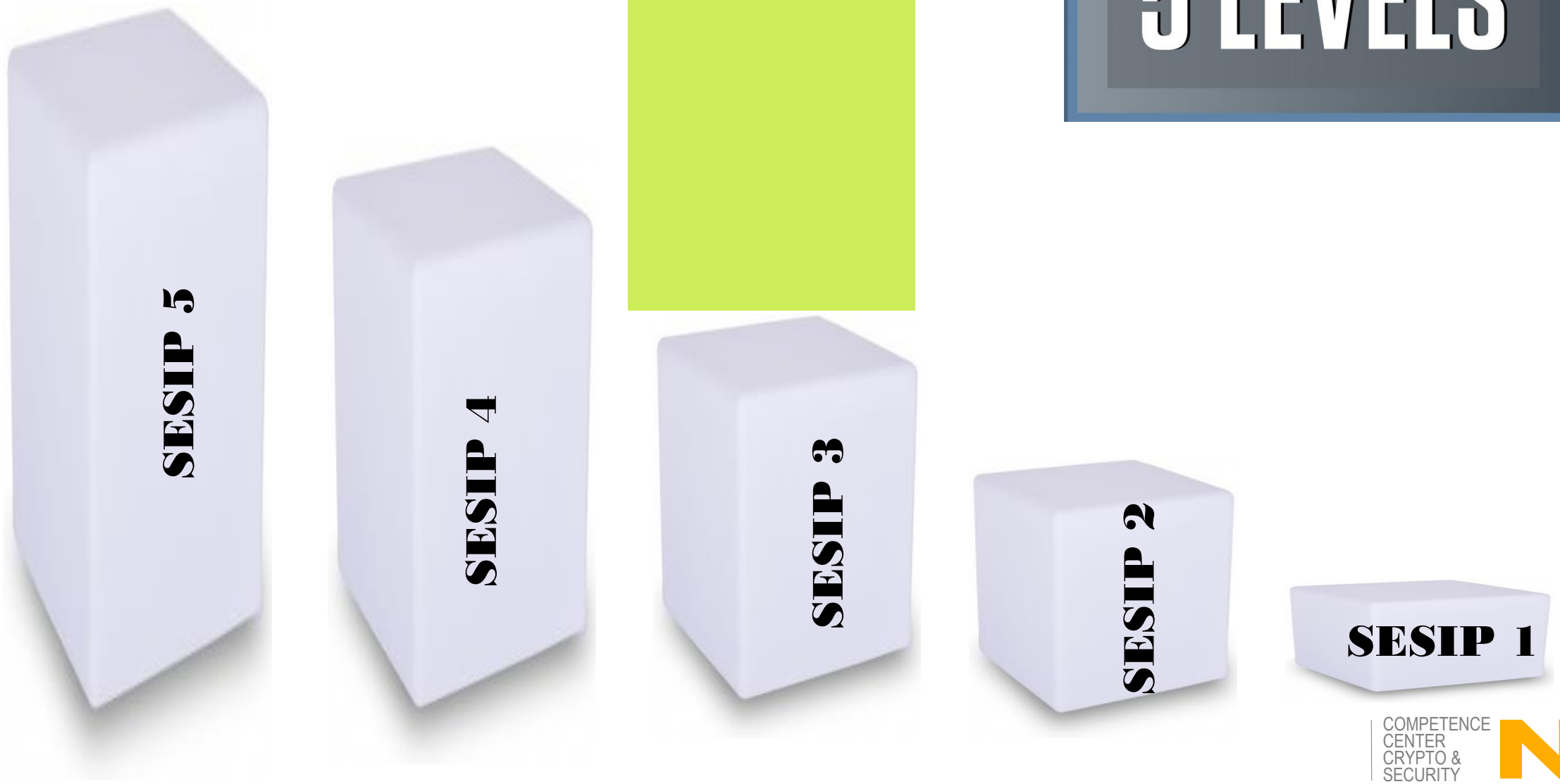


So let's build something based on some key goals.

1. Make it understandable, no confusing definitions and terms
2. Flexible, different certification levels and attacker profiles
3. Usable, allow product integrators to re-use the previous security testing to achieve their certification
4. Ease of use, provide templates and well defined methods and process steps
5. Unifying, make it flexible enough to re-use as an input or output to other certification schemes, make it global make it scalable
6. Relevant, ensure that patching is an integral concept and keep testing state of the art by building strong communities



5 LEVELS



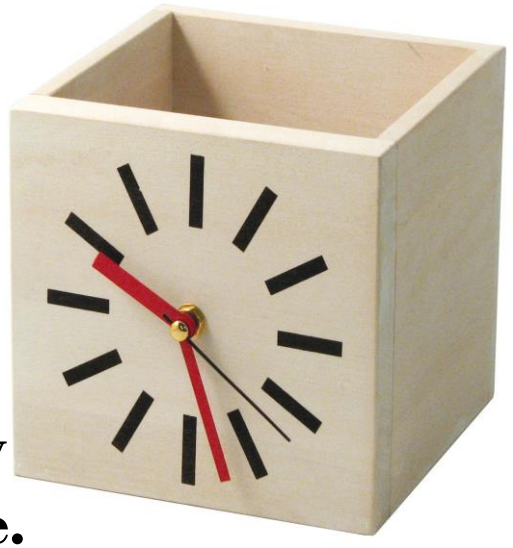
COMPETENCE CENTER CRYPTO & SECURITY

COMMON CRITERIA
CERTIFIED
EAL4+

A full EAL4+ AVA.VAN.5 Certification allowing harmonization and re-use of existing state of the art SOG-IS common criteria certifications. Allowing developers to use high assurance testing to provide a secure Root of Trust/PSA, that can be used to decrease the requirements for SW and applications built on top.

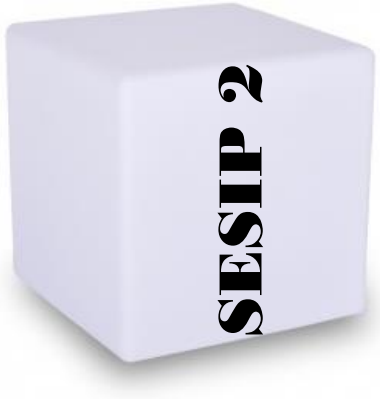
An optimized Common Criteria based certification using the SESIP assurance methodology. Only applicable work units, optimization of others.

This is a highly optimized Common Criteria Certification.



A time boxed certification to allow developers to fully understand the length of time a certification will take. This can be considered as a AVA_VAN.3 certification, it includes a Vulnerability Analysis and a targeted test campaign. The length of time for both VA and testing is defined according to the defined time limits as agreed by the technical community.

SESIP 2 gives the ability to have a push button or automated test campaign. This is envisioned to include known vulnerabilities for a technology and/or implementation. The vulnerability database is built from published or known weakness, and can be in the form of either a code review or an automated test bench.



SESIP 1 is a self declaration performed by the company and verified by the certification body. This level of certification allows a company to achieve a certificate for their product. This certificate is meaningful as it relies on the testing performed on the supply chain parts that make up the end solution/device. The idea is that the CB verifies the security claims made by confirming that the lower layers have been tested and that the company has integrated the layers correctly into their product. It allows a company with little security expertise to achieve a meaningful security certificate.

SESIP certification of a product

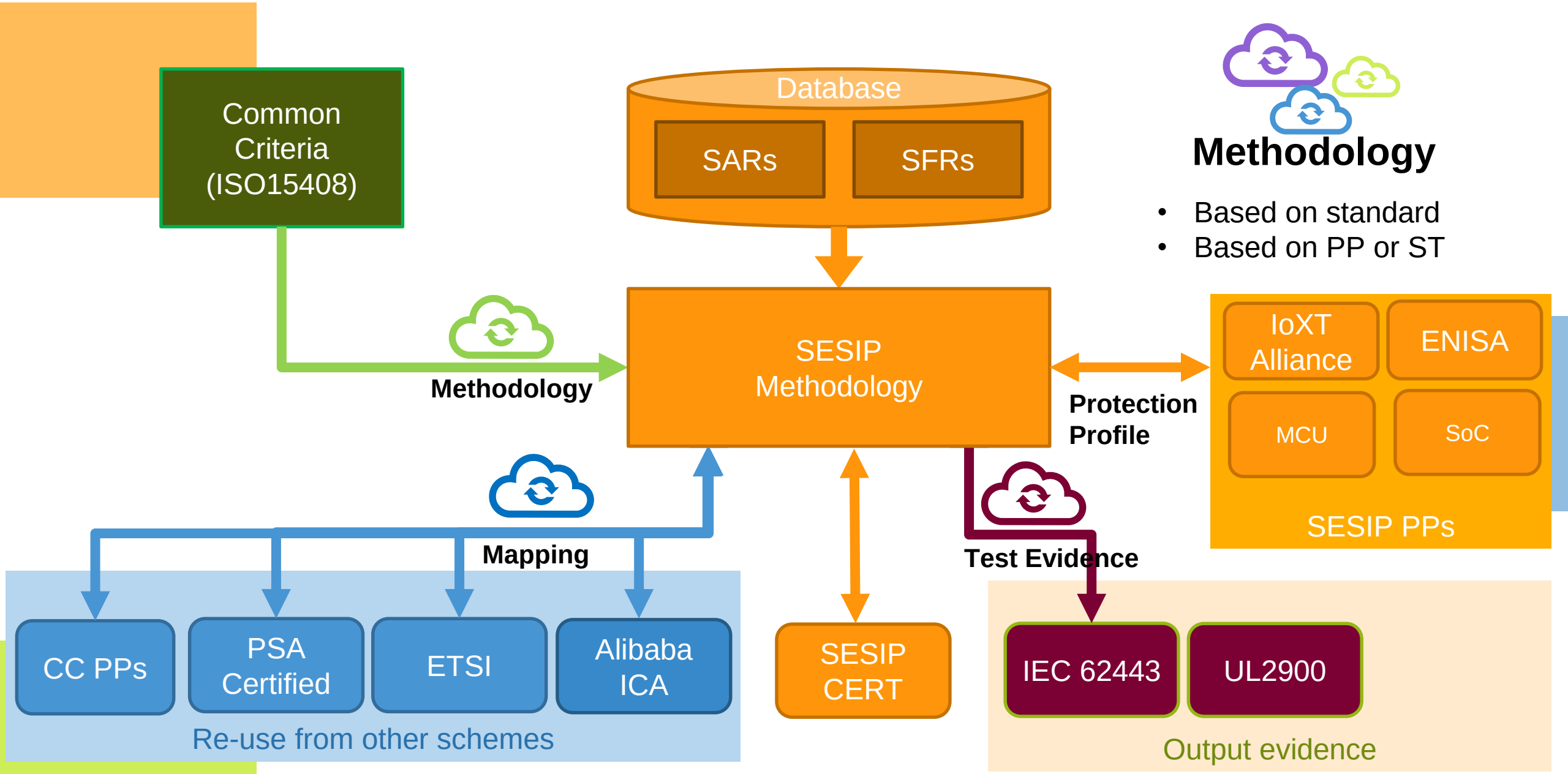
SESIP 4 – Root of Trust/PSA: Optimized Common Criteria Certification using the SESIP methodology

SESIP 3 – Secure Microcontroller: Time boxed VA and test campaign taking about 25 man days for each

SESIP 2 – RTOS: Source code and implementation analysis, backed up with some automated open port and fuzzing testing. Verification that applications are sandboxed.

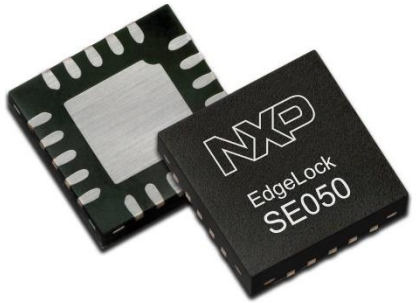
SESIP 1 – Device: Self –declaration to show that the end product has taken into account any security recommendations and that all certificates are in place.

COMPETENCE CENTER CRYPTO & SECURITY



COMPETENCE CENTER CRYPTO & SECURITY

SESIP as a meta-framework



EAL6+ SOG-IS– Re-use of the existing BSI and NSCIB Certificates

PSA Certified Level 2– PSA Security Target has been translated to SESIP Language.

Also mapping to the SESIP ICA PP allows an ICA PP ICA Level 3 to be achieved.

SESIP 2 – RTOS: Source code and implementation analysis, backed up with some automated open port and fuzzing testing. Verification that applications are sandboxed.

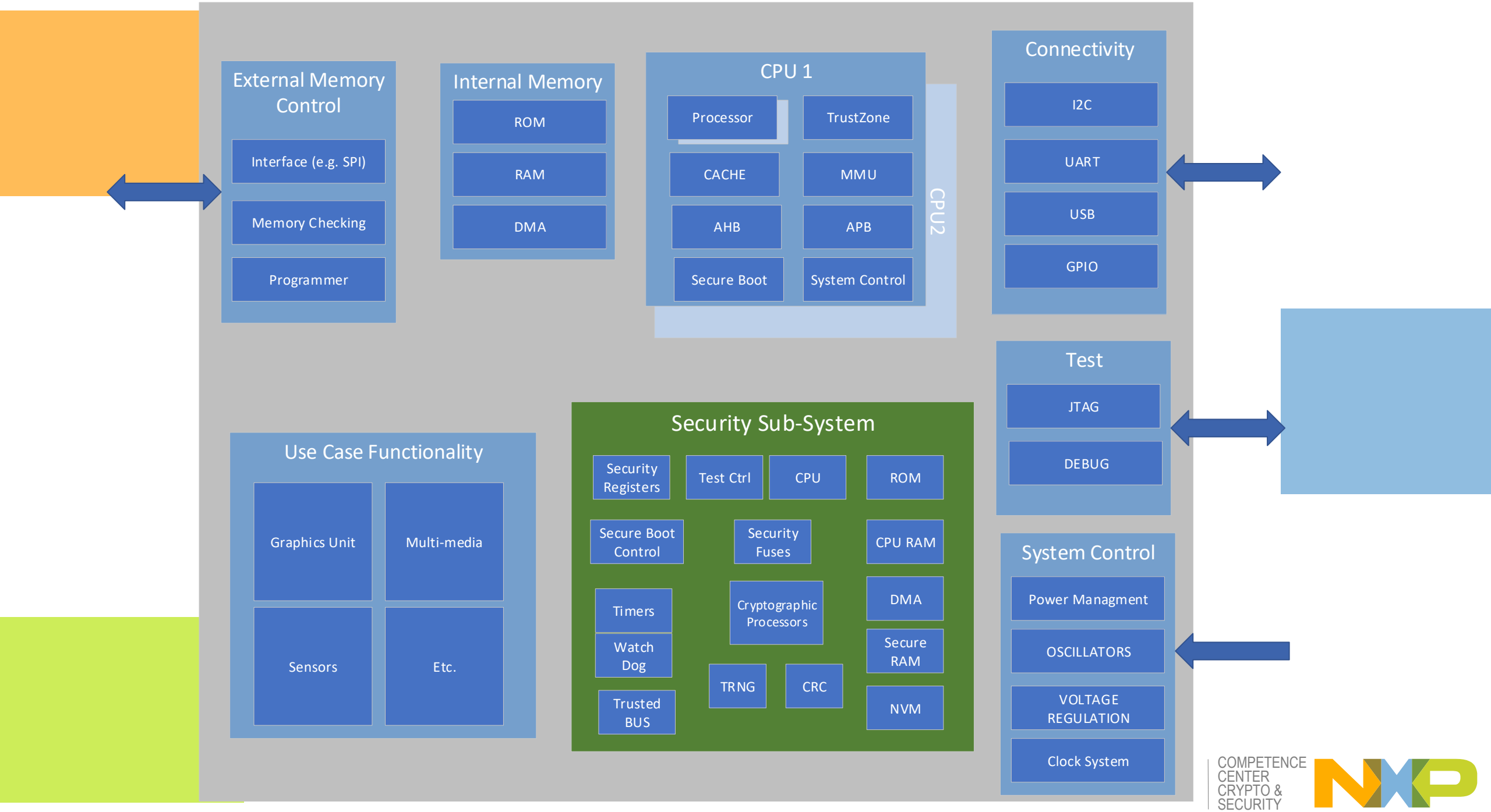
Using the IoXT Security pledge protection profile a SESIP Level 1 verification is performed using self-declaration. UL 2900 achieved by using security testing proof.

ETSI TS 103 645 – Proof is also achieved

SESIP NXP AND RISC-V

COMPETENCE
CENTER
CRYPTO &
SECURITY

NXP


External Memory Control
Interface (e.g. SPI)
Memory Checking
Programmer
Internal Memory
ROM
RAM
DMA
CPU 1
Processor
TrustZone
CACHE
MMU
AHB
APB
Secure Boot
System Control
CPU2
Connectivity
I2C
UART
USB
GPIO
Test
JTAG
DEBUG
Use Case Functionality
Graphics Unit
Multi-media
Sensors
Etc.
Security Sub-System
Security Registers
Test Ctrl
CPU
ROM
Secure Boot Control
Security Fuses
CPU RAM
Timers
Cryptographic Processors
DMA
Watch Dog
Secure RAM
TRNG
CRC
Trusted BUS
NVM
System Control
Power Managment
OSCILLATORS
VOLTAGE REGULATION
Clock System
COMPETENCE CENTER CRYPTO & SECURITY

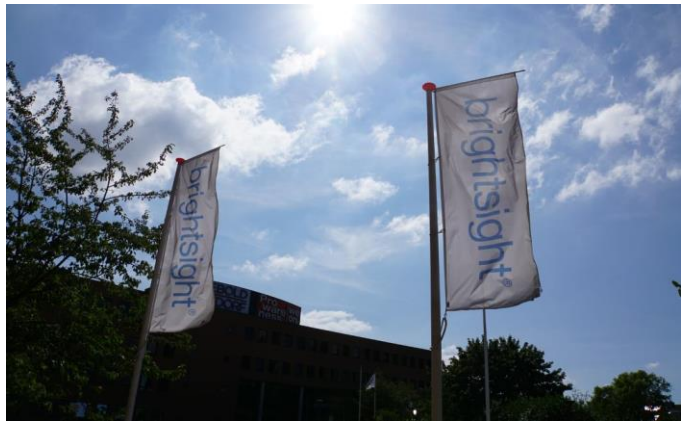
STATUS AND PARTNERSHIPS

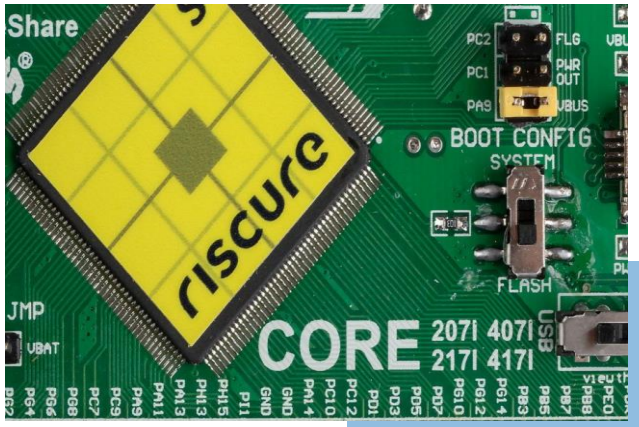
SESIP

SESIP Version 1.3 is live online

https://www.trustcb.com/iot/sesip/

Security Target Template also online





SRC security consulting

COMPETENCE CENTER CRYPTO & SECURITY

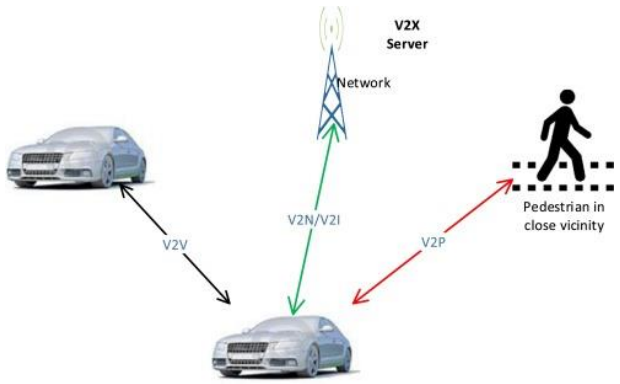
NXP

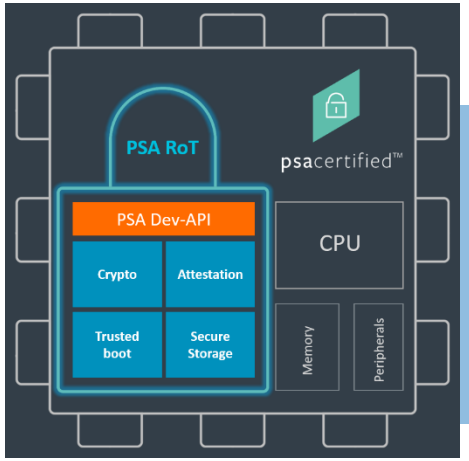
Mapping with SESIP

SESIP can be used to map standards one example is PSA (Platform Security Architecture), the Protection Profile can be mapped directly to SESIP where gaps exist the SESIP catalogue of SFRs was updated, this allows interoperability between the 2 standards.

The existing Protection Profiles already generated for Common Criteria can also be used with SESIP, the SESIP catalogue was originally generated from ISO 15408 therefore any PP generated can map to SESIP both for SFR and SAR.

Other standards can also be mapped e.g. IEC 62443, this can re-use the security testing from SESIP and linked standards.





Generating Protection Profiles with SESIP

SESIP

Obviously SESIP can be used to generate a Protection Profile from a list of requirements both as a framework for example the ioxt Alliance Pledges, ENISA IoT best practices, Charter of Trust Principle 3 Security by default, ETSI IoT Requirements etc.

Or, a list of requirements for a standard can be used to generate a protection profile for SESIP, for example the Alibaba ICA IoT Security requirements level 3.

ioXt
internet of secure things

Charter of Trust

COMPETENCE CENTER CRYPTO & SECURITY

Protection Profile Status

- Generic Secure MCU/MPU Draft Transferring to Global Platform end of 2019
  - Attacker Profile Draft Ready
  - Attacker rating tables Draft Ready
- AliBaba ICA Level 3 PP Ready for Release Initial pilot due to complete end of 2019
- Baseline IoT Product PP Underway – Uses a superset of baseline requirements from various standards and associations

Note: Eurosmart is working on a 3S in a SoC PP due Q3 2020

Partnerships

SESIP Donated to Global Platform using the fast track process.

Alibaba accepts SESIP as a certificate for the Alibaba ICA cloud association; Protection Profile, Security Target Template and acceptance procedure due to be published ready

Generic MCU/MPU Draft PP ready

Mapping to PSA Certified level 1 and 2 complete.

Mapping to IEC 62443

Work underway to push into standardization

SECURE CONNECTIONS FOR A SMARTER WORLD