SESIP CERTIFICATION

A scalable Certification for IoT – RISC-V Community

John Boggie / Eric Vétillard

IoT Certification

NXP Semiconductors

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD

Background

The Connected World is becoming a reality

Edge to Node

Smart Infrastructure

Smart Manufacturing & Robotics

Smart Retail

Wearables

Smart Media & Education

Smart Home

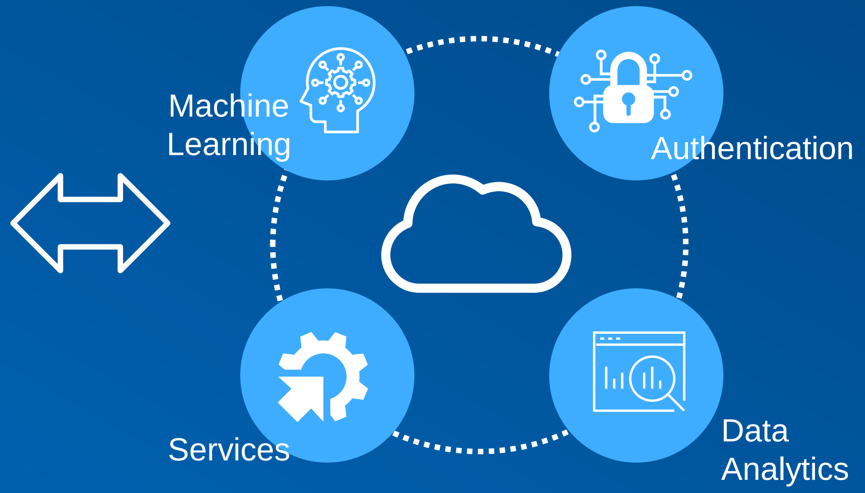
Smart Health

Smart City

Smart Transportation

Smart Assistant

Cloud Infrastructure



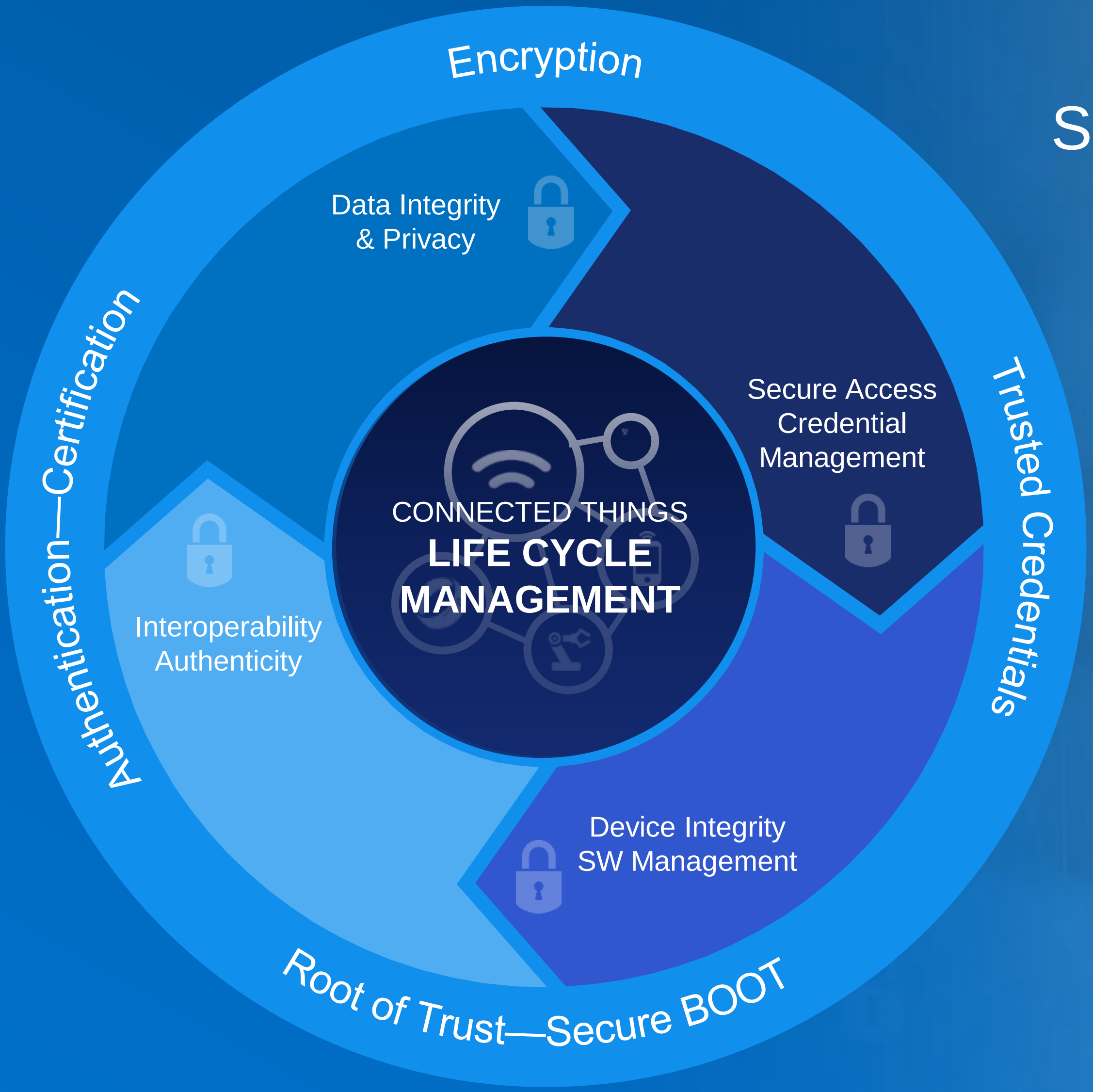
Sensing

Connectivity

Processing (incl. AI/ ML)

Safety & Security

What does a secure system look like

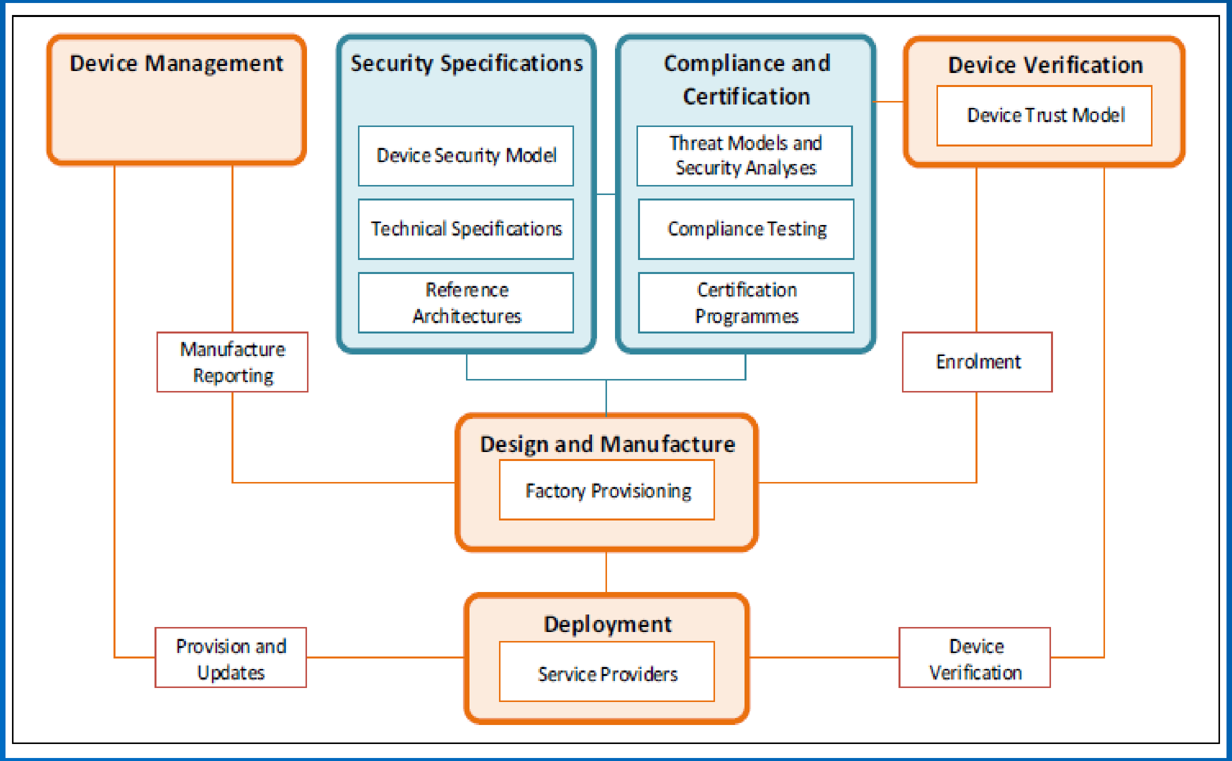

Encryption
Trusted Credentials
Root of Trust—Secure BOOT
Authentication—Certification
Data Integrity & Privacy
Secure Access Credential Management
Device Integrity SW Management
Interoperability Authenticity
CONNECTED THINGS
LIFE CYCLE MANAGEMENT

Security & Privacy by Design

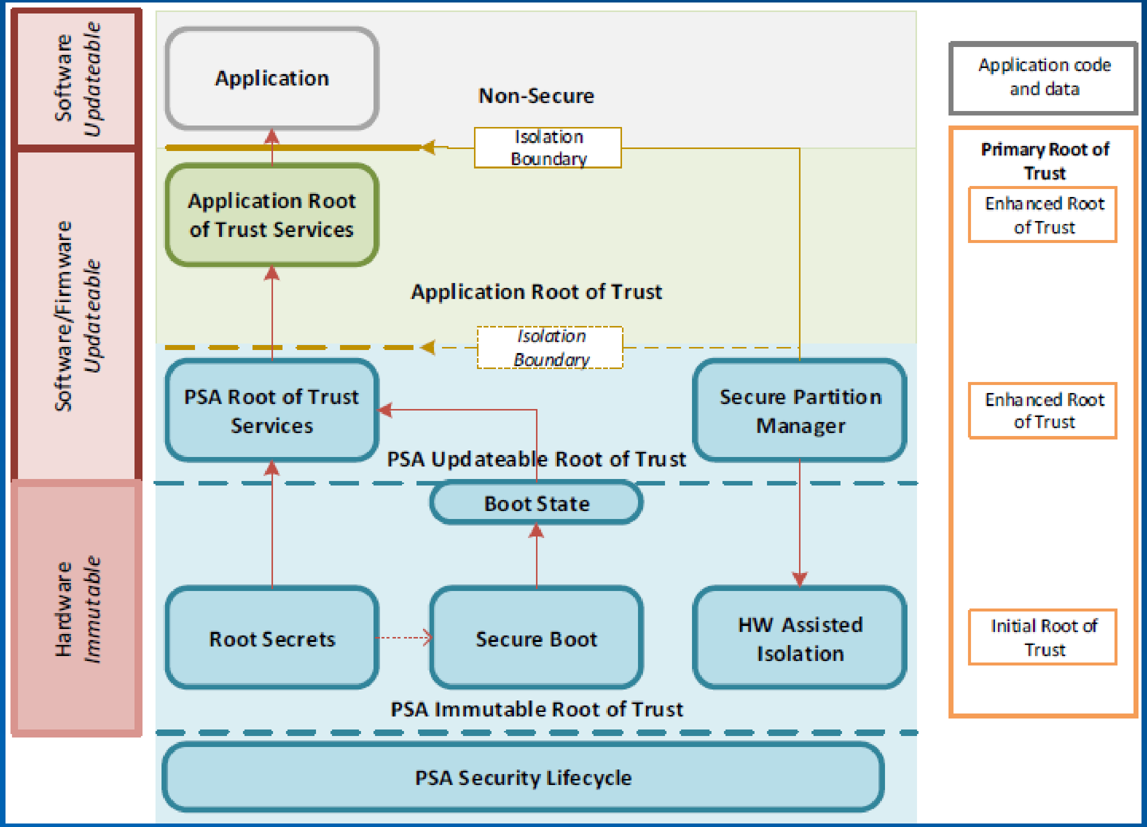
EMVCo
fido ALLIANCE
UL
enisa
GLOBALPLATFORM
GSMA
NXP MIFARE
FeliCa CERTIFIED
arm
IoT Security Foundation
SOGIS
IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT
Common Criteria Users Forum
CYBER ESSENTIALS
SGS
CAR 2 CAR
COMMUNICATION CONSORTIUM
DEKRA
ISASecure
SECURITY VISA
ANSSI
AUTO ISAC
Applus IDIADA
FIPS
Level 3 Validated
140-2

ARM PSA

The PSA Vision of the IoT Ecosystem



PSA defines a vision for the entire IoT ecosystem, centered around specifications and compliance & certification



PSA’s vision is centered around the Root of Trust, which is defined by the PSA specifications. It relies on a Secure Processing Environment (SPE), which runs on TrustZone/M’s Secure mode (like a lightweight TEE).

PSA Certified

Trust Signals

Certification is performed by accredited third-party laboratories

Each device makes a claim of PSA Level 1/2/3

Cloud based services can make risk judgements based on the certification level

Centered around PSA

Strongly linked to the PSA framework and its compliance program

Focuses on features defined in PSA and on the implementation of a device’s Root-of-Trust

Three Levels

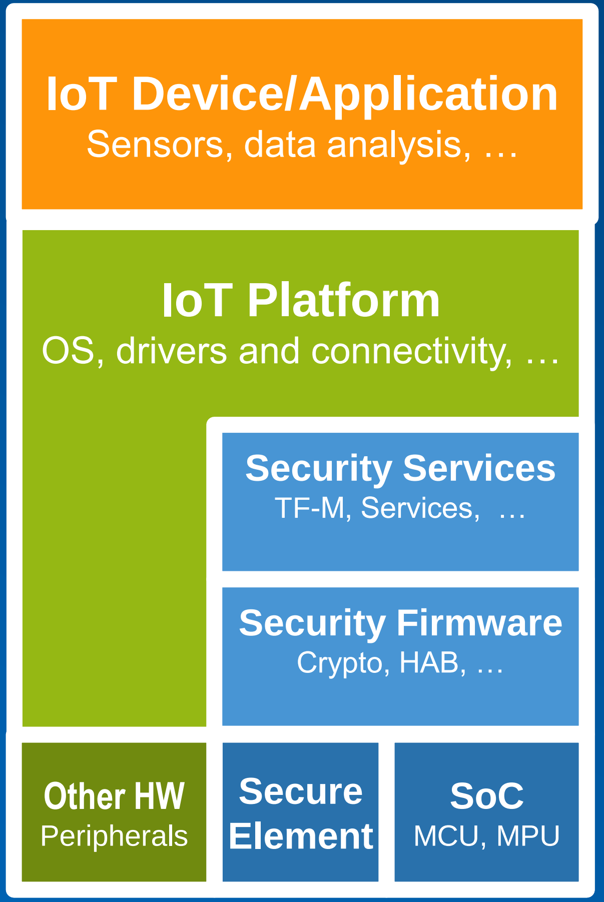
Level 1 is a declaration about good IoT security hygiene

Level 2 is an evaluation focused on the device’s Secure Processing Environment

Level 3 is an evaluation that requires a high assurance Secure Element

SESIP

IoT Application	**Using the platforms' services** - Reducing the risk of doing security wrong
IoT Platform	**Offering low level security services** - Secure connectivity, secure interfaces - Application SW separation
Root of Trust	**Protecting most sensitive assets** - Keys, FW integrity, Secure boot, Crypto primitives, …



IoT Device/Application
Sensors, data analysis, …

IoT Platform
OS, drivers and connectivity, …

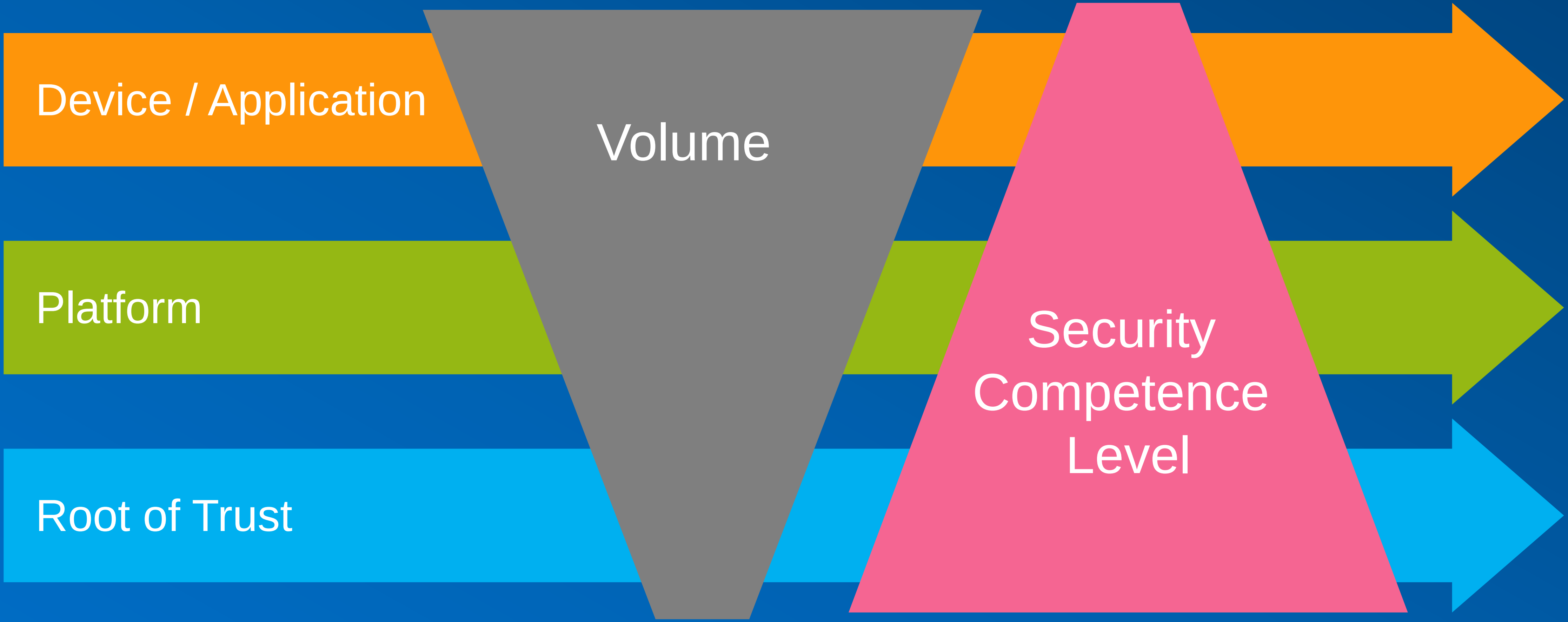
Security Services
TF-M, Services, …

Security Firmware
Crypto, HAB, …

Other HW
Peripherals

Secure Element

SoC
MCU, MPU



Device / Application

Platform

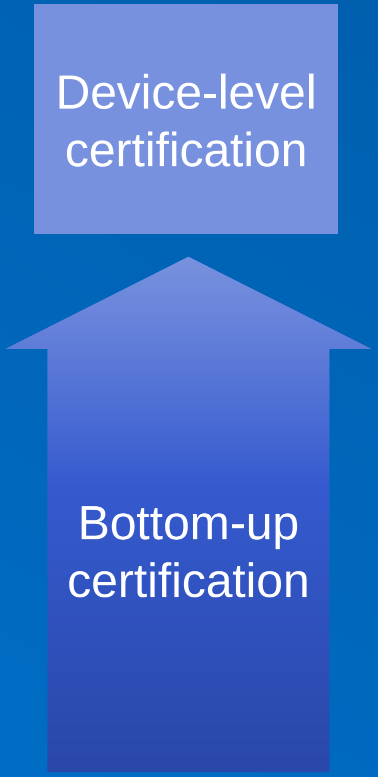
Root of Trust

Volume

Security Competence Level

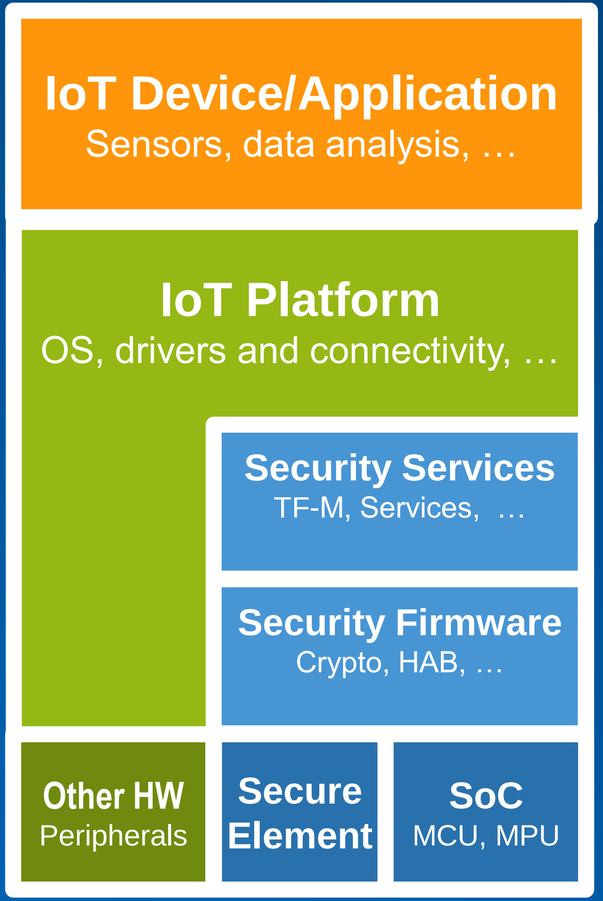
SESIP

Security
Evaluation
Scheme for
I oT
Platforms


Device-level certification

Bottom-up certification

IoT Application	**Using the platforms' services** - Reducing the risk of doing security wrong
IoT Platform	**Offering low level security services** - Secure connectivity, secure interfaces - Application SW separation
Root of Trust	**Protecting most sensitive assets** - Keys, FW integrity, Secure boot, Crypto primitives, …


IoT Device/Application
Sensors, data analysis, …

IoT Platform
OS, drivers and connectivity, …

Security Services
TF-M, Services, …

Security Firmware
Crypto, HAB, …

Other HW
Peripherals

Secure Element

SoC
MCU, MPU

SESIP is a Variant of Common Criteria

- Following all mandatory aspects of the ISO15408 standard
- A variant that simplifies certification for a specific use case
  - A fixed set of SFRs, described in plain text for accessibility
    - Describing IoT-centered security requirements
  - A custom set of assurance levels, based on CC standard assurance requirements
    - Focusing on vulnerability analysis rather than processes
  - Limited options in the levels for better readability

- Two main benefits
  - Defining a flexible and efficient schemes for IoT platforms and components
  - Showing a methodology to derive variants from ISO15408

1: Understandable – No confusing definitions and terms

2: Flexible – Different levels and attack 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 up to date by building strong communities

Further concerns about PSA Certified

Interesting but not sufficient

- PSA Certified mandates a scope that includes a Trusted Firmware
  - Good for low-level developers
  - Concern for chip/IP vendors
- PSA Certified stops at the Root-of-Trust level
  - No coverage of platform certification
  - Root-of-Trust remains too low for most "real" IoT developers

Actions

- SESIP is designed to be more flexible
  - Any platform component can be certified
    - SoC, software IP, hardware IP
    - Root-of-Trust, OS, full platform
  - Every element is certified for its own contribution to a system's security
- A choice must be made
  - Simple, proprietary, shiny scheme
  - Complete, open, real scheme

SESIP

Flexible – Usable: The SESIP Levels

SESIP 1	**Self-Declaration**	**Self declaration assessed by a third party lab – No product checking – Checking if existing security certifications are in place and up to date and that procedures have been followed – Allows an integrator to achieve a meaningful certificate proving correct security implementation**
SESIP 1+	**Black Box Testing**	**Black box testing with a time limited penetration test campaign. Intended as an entry level for components or for security testing on an already certified Root-of-Trust**
SESIP 2	**White Box**	**White box certification with a time limited vulnerability assessment and security testing**
SESIP 2+	**White Box Extended**	**Deep investigation of how the security is implemented test time depends on the security claims**
SESIP 3	**High Assurance**	**Full EAL4+ Certification using AVA_VAN.5 intended as a way of re-using existing SOG-IS CC or as a place holder for later certification approaches**

Flexible – Usable: Various Attacker Profiles

Remote/Proximity Attacks: Tests the connectivity of the product and whether it can be manipulated or intercepted by an attacker remotely with access to the communication to or from the device

Software Attacks: If an external entity can load software to the device this profile would check that the product has sufficient isolation to ensure critical assets and functions cannot be compromised

Local/Physical Attacks: The attacker is considered to have physical access to the device. Attacks would include abuse of local ports (USB, Wireless interfaces) or reactivating test features. Also invasive/semi-invasive attacks e,g. probing, side channel

In practice: Major Deliverables for SESIP

ITP-1: Self

- Security target
  - Including a self-assessment rationale

ITP-1+: Black-box

- Security target
  - Functional specification
  - User documentation
  - Admin documentation
  - Flaw reporting
  - Vulnerability survey

ITP-2: White-box

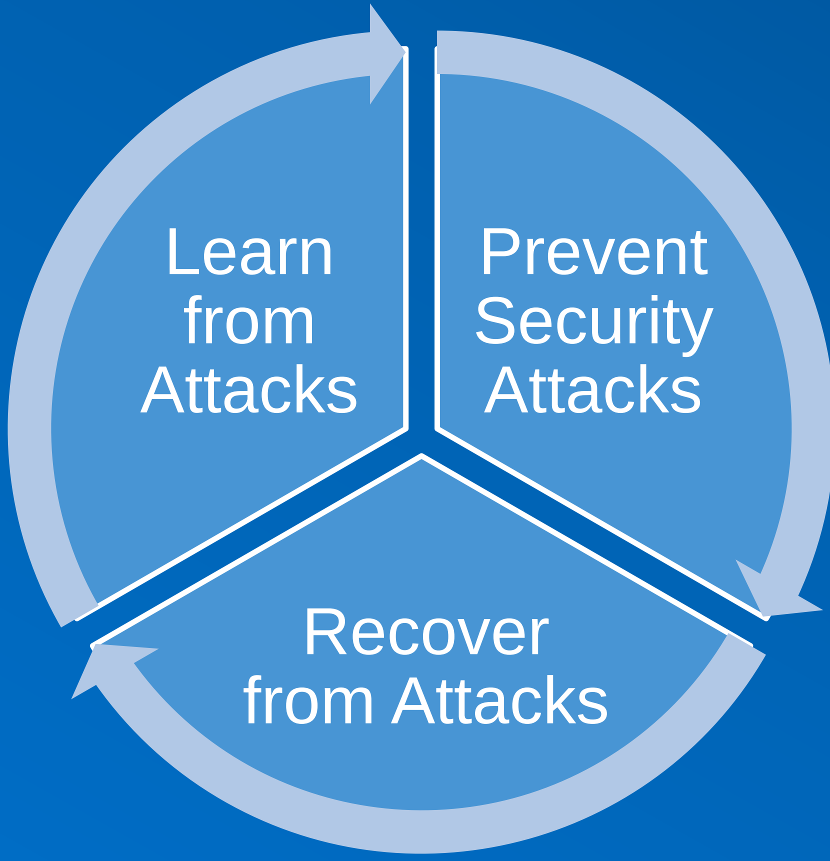
- Same as ITP-1+ +
  - Implementation
  - Mapping to claims
  - Conf Mgmt coverage
  - Vulnerability analysis

Improvement from CC by only considering useful docs

Assurance Components for SESIP Levels

Category	ITP-1	ITP-1+	ITP-2 / ITP-2+
Security target	ASE_INT.1: ST Introduction ASE_OBJ.1: Security reqs for operational env *ASE_REQ.3: Listed Security Requirements* ASE_TSS.1: TOE Summary Specification	ASE_INT.1: ST Introduction ASE_OBJ.1: Security reqs for operational env *ASE_REQ.3: Listed Security Requirements* ASE_TSS.1: TOE Summary Specification	ASE_INT.1: ST Introduction ASE_OBJ.1: Security reqs for operational env *ASE_REQ.3: Listed Security Requirements* ASE_TSS.1: TOE Summary Specification
Development		ADV_FSP.4: Complete functional spec	ADV_FSP.4: Complete functional spec *ADV_IMP.3: Complete mapping of impl to SFRs*
Guidance documents		AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures	AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures
Lifecycle support	ALC_FLR.2: Flaw reporting procedures	ALC_FLR.2: Flaw reporting procedures	ALC_CMC.1: Labelling of the TOE ALC_CMS.1: TOE CM Coverage ALC_FLR.2: Flaw reporting procedures
Tests		ATE_IND.1: Independent testing: conformance	ATE_IND.1: Independent testing: conformance
Vulnerability assessment		AVA_VAN.1: Vulnerability survey	AVA_VAN.2: Vulnerability analysis (ITP-2) AVA_VAN.3-4: (ITP-2+)

Relevant – Keep the product up to date



Partnered with industry experts to keep testing at the required level, with balanced risk assessment.

SESIP regards product maintenance and software updates as an integral part of the product. The mechanism “Secure Update of Platform” is mandatory for all SESIP levels.

Flaw remediation addresses developers policies and processes for fixing security flaws this is also require on all levels.

It can be thought of in this way SESIP does not only look at the product now but how it also evolves to mitigate attacks in the future.

SESIP IN ACTION

PUBLIC

Example: The Robot Vacuum Cleaner

SESIP 1	Self-Declaration	Application	Remote	Application developer uses the existing certificates and has a third party verify they have integrated the components correctly and that communications are protected
SESIP 1	Self-Declaration	Platform	Remote Software	The Application developer would like to have the Platform SW patches verified before release so he mandates a self declaration and has it verified
SESIP 1+	Black Box Testing	Platform	Remote Software	Penetration test campaign of 14 days showing protection against known SW attacks and proving that the Application is isolated from accessing master keys
SESIP 2	White box testing	SoC	Remote Software Local/Physical	Developer is producing general purpose Microcontrollers that can be used in multiple products. He has them verified to a broad range of attacks, as he does not know the end application

Example: How SESIP integrates with other Standards- Industrial HSM

ISO 62443	Industrial Standard	HSM	IECEE	The end product is certified as an HSM node using the testing below as an input to ISO 62443 Industry 4.0
SESIP 1+	Rich OS and Application	Platform	Remote	Product integrator adds SW and Application from third parties and has the product tested to ensure that it is not vulnerable to Communication manipulation. He also declares that it is not possible to patch in the field
ARM PSA Level 2	Arm PSA	SoC	SESIP 2	Secure Element is integrated with a PSA Certified Microcontroller
CC EAL4+ AVA_VAN.5	BSI CC Certificate	Secure Element	SESIP 3	Secure Element is equivalent to ITP 3

SESIP and RISC-V

PUBLIC

SESIP and RISC-V

SESIP's vision

- Security standards should not be proprietary
  - NXP is the initiator, a support, and an early adopter, not the owner
  - TrustCB is the initial CB, not the owner
- SESIP is intended to become a standard
  - An official variant of ISO 15408
  - Currently exploring JTC13 politics

Useful to RISC-V

- SESIP applies to IoT components
  - Including hardware IP and products
  - Helping to build reusable evidence
- SESIP is open for business
  - Pilot certifications are possible today at levels 1, 1+, and 2.
  - Getting certified is good for the community
  - Supporting the scheme and providing very valuable input to improve the scheme

We need an open standard for IoT

SESIP NEEDS THE SUPPORT OF MORE VENDORS

Where do we stand today

Significant progress

- Definition of the scheme
  - An initial scheme document with levels and functional scope, and a ST template
  - Pilots (SESIP1 done, SESIP2 in progress)
- Some interfaces to other schemes
  - Technical alignment with Arm PSA
- support
  - From other vendors
  - From IoT stakeholders
  - From BSI and NSCIB

Further work

- Enlarge the SESIP ecosystem
  - To involve a larger group of contributors
  - To work efficiently and get validation
- Consolidation work required
  - Based on current and further pilots
  - Editing SFRs, building attacker models
- Moving to official support
  - Submission to JTC13

Thank you!

john.boggie@nxp.com
eric.vetillard@nxp.com

NXP | CONNECTS