Security Conference 2022

SESIP - Scheme Overview, Objectives and Relations and Complementarities with Other Schemes

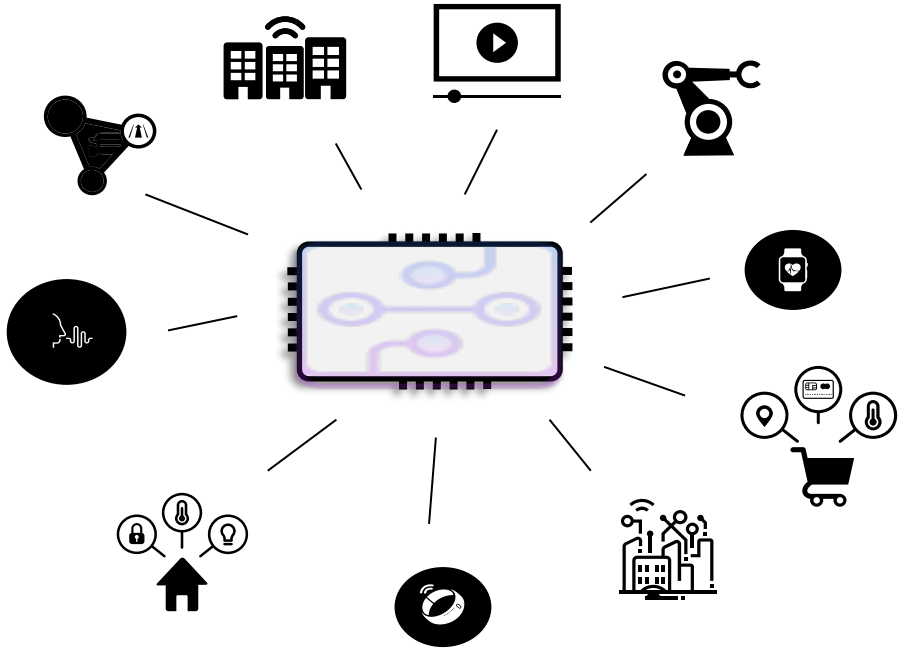
Eve Atallah – NXP Semiconductors

04/10/2022

Challenge 1 - IoT ecosystem

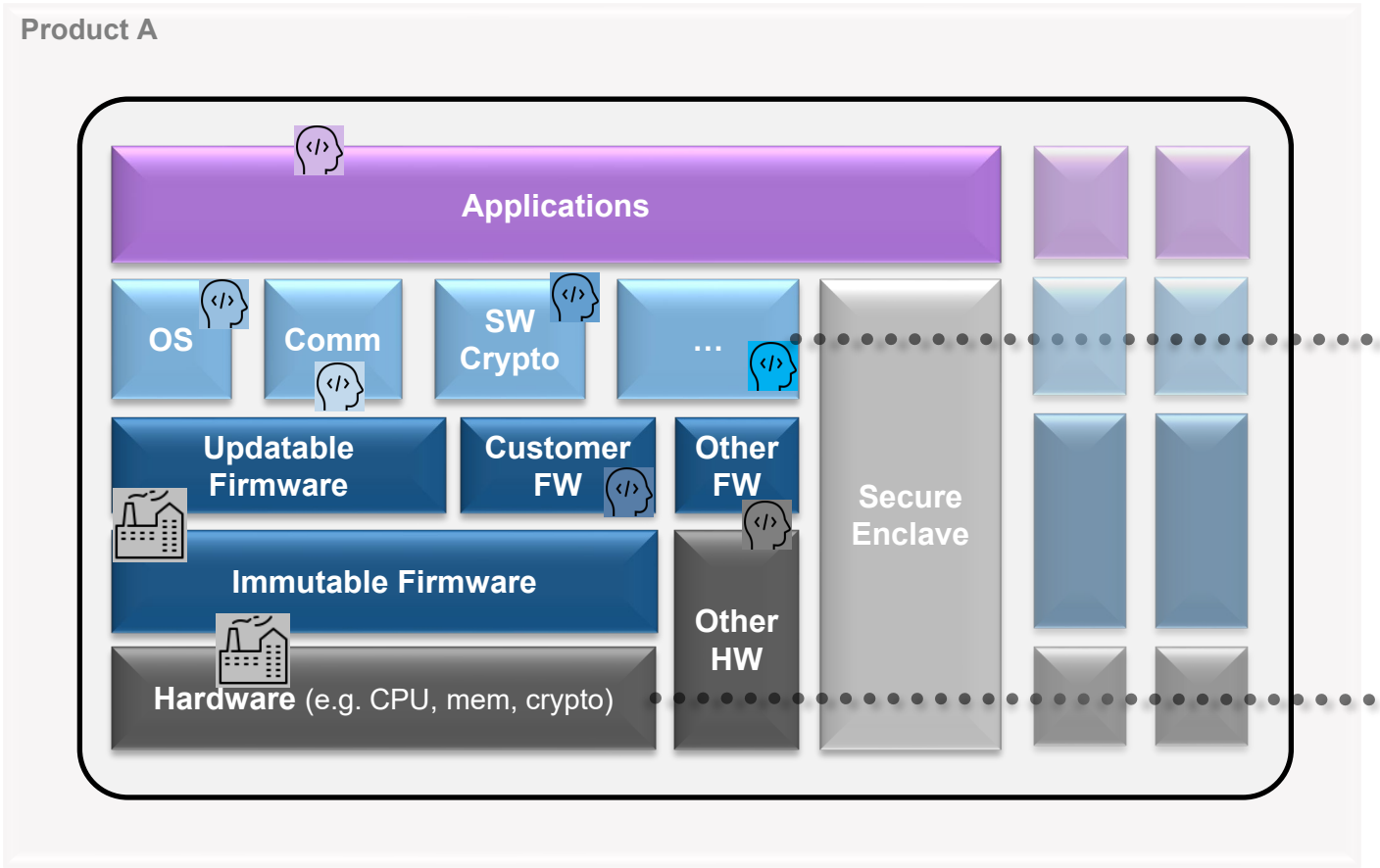
Many IoT standards and regulations

Complex and costly



Challenge 2 – IoT products complexity

Several modules
Different developers

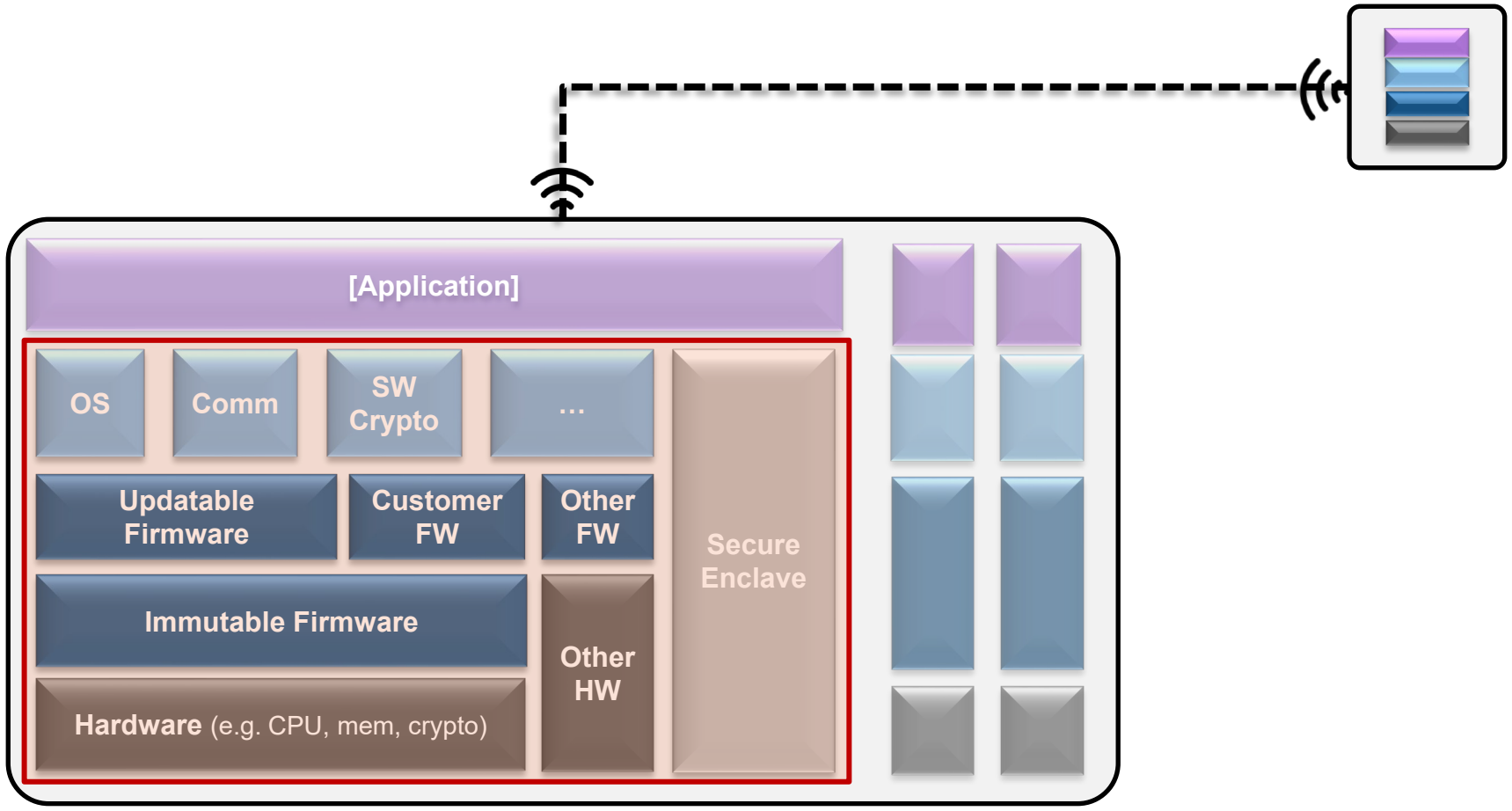


Several final products

- Full re-testing per products time and cost consuming
- Compliance demo by final device vendor requires dev components support

SESIP - Security Evaluation Standard for IoT Platform

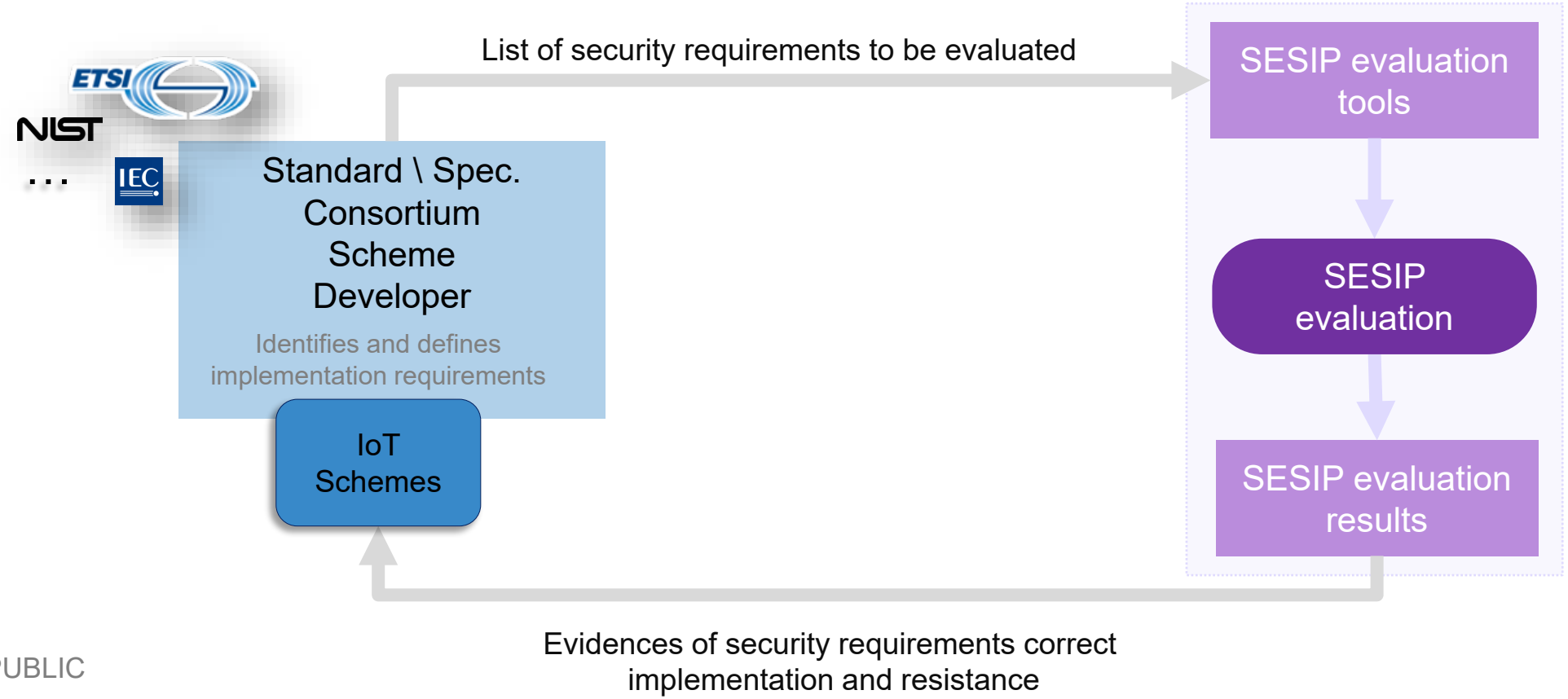
IoT Platform (platform)
Security features of IoT devices



SESIP scope representation example

SESIP role in current IoT ecosystem

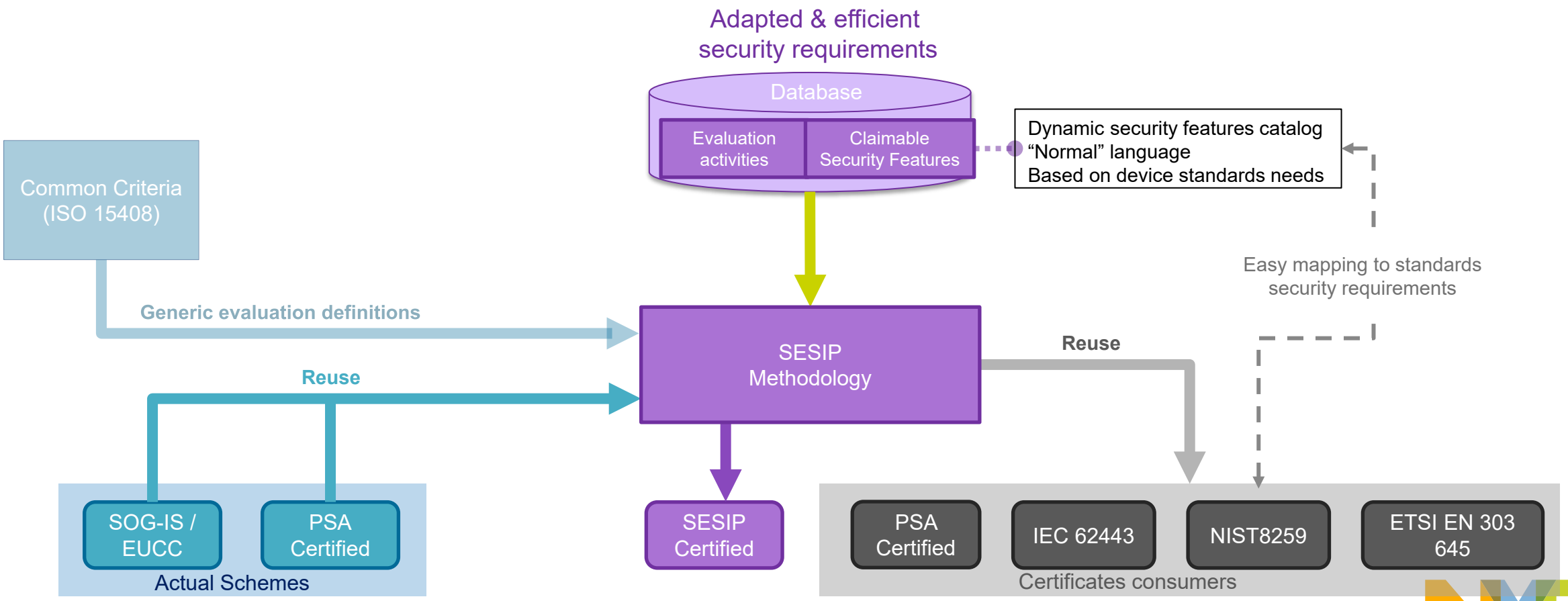
Not an implementation requirements standard – “security features to be **implemented**”
Evaluation standard – “security features to be **evaluated**”



Harmonization between standards

- Catalogue of mappable security requirements, selected upon need
- Efficient evaluation activities, depending on assurance levels

⇒ Reusable results



Composition and reuse

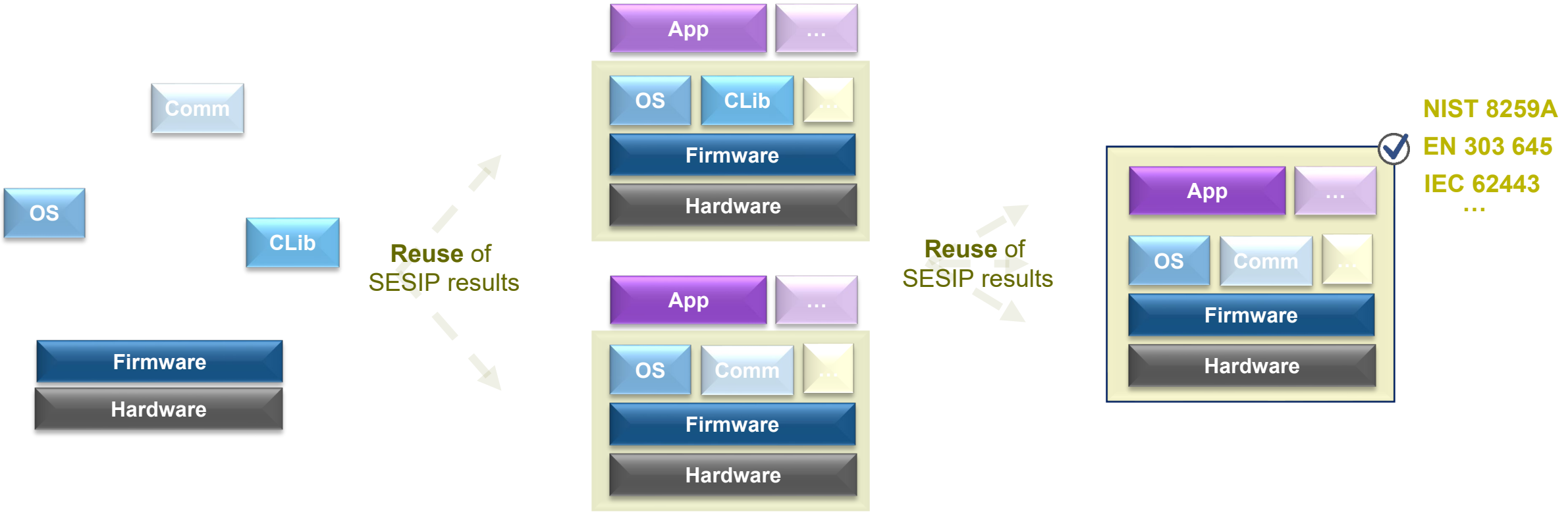
Security of **components (platform parts)**

Security of **platforms**
Composition

Security of **devices**

Prove component **security** to customers

Support customers in **compliance demonstration**



Component developers

Device developers
(e.g manufacturers Customers)

Mappable Security Features

- Security feature/service claimable and to be evaluated

Secure initialization of platform

Requirement

The platform ensures its authenticity and integrity during the platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to *<list of controlled states>*.

Value

Users, developers and evaluators can trust that the platform verified its authenticity and integrity at start-up, hence an operational product is running on a secure platform.

Considerations

A platform detecting a breach of authenticity or integrity may offer “Factory reset of platform”, “Secure update of platform”, or “Decommission of platform” functionality to recover a given product.

- Requirement: covers a **full security goal**.
- Value: explains benefit and use case.
- Consideration: guidance to use and fulfill the SFR

Understandable & Intuitive

Mappable Security Features

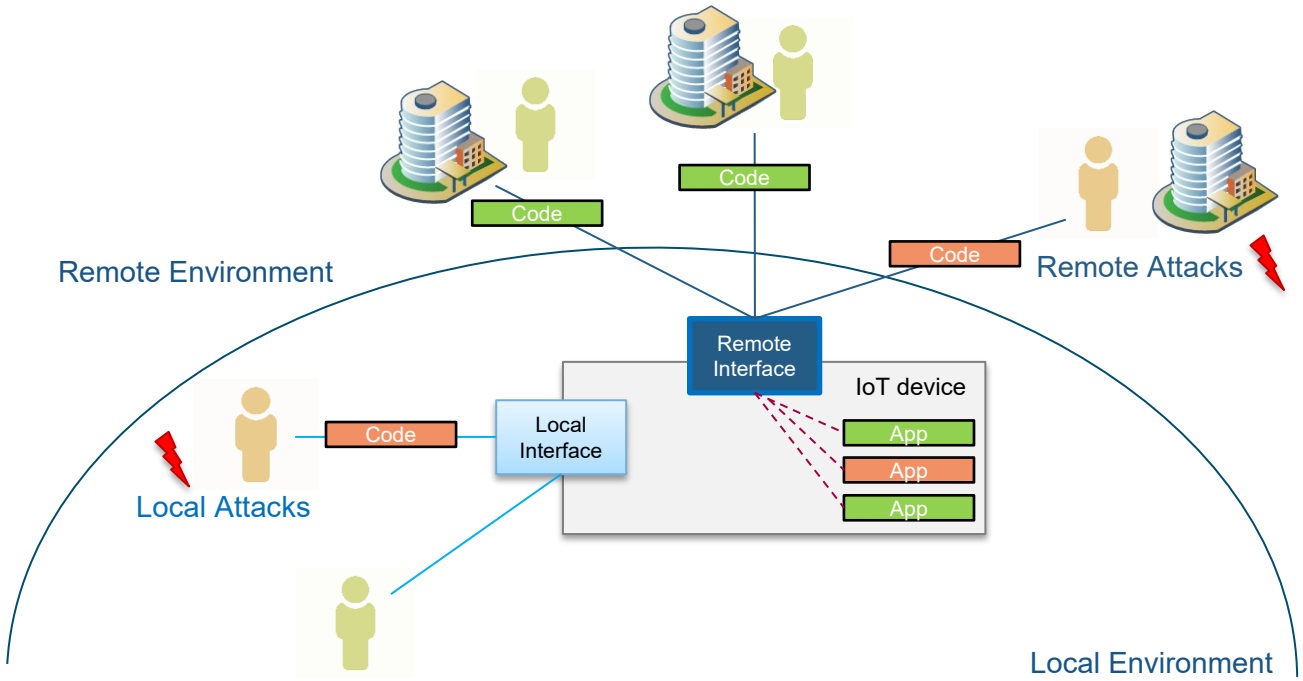
Selectable IoT features

Identification & Attestation	Product Life Cycle	Cryptographic functionality	Secure communications	Compliance functionality	Extra attacker resistance
Verification of platform identity	Factory reset of platform	Cryptographic operation	Secure communication support	Secure Storage	Limited physical attacker resistance
Verification of platform instance identity	Decommission of platform	Cryptographic random number generation	Secure communication enforcement	Secure encrypted storage	Physical attacker resistance
Attestation of platform genuineness	Field return of platform	Cryptographic KeyStore		Secure External Storage	Software attacker resistance: isolation of platform
Attestation of application genuineness	Secure update of platform	Cryptographic key generation		Residual information purging	Software attacker resistance: isolation of platform parts
Attestation of platform state	Secure install of application			Audit log generation and storage	Software attacker resistance: isolation of application parts
Attestation of application state	Secure update of application			Secure debugging	
Secure initialization of platform	Secure uninstallation of application			Reliable index	

New features added in next version
Definition of proprietary SFRs possible upon need

Realistic attack contexts

Attacks context adapted to real use cases



- **Default context**
  - Remote attacks only
  - Trusted code only
- **With local attacks**
  - Physical attacker resistance
- **With untrusted code**
  - Software attacker resistance

Focus on Vulnerability Analysis

Developer

Documents to support VA,
not SESIP dedicated, any format
(e.g. docs, workshop, training)

[Source code] | Technical info | Functional testing campaign | Samples

Developer's inputs

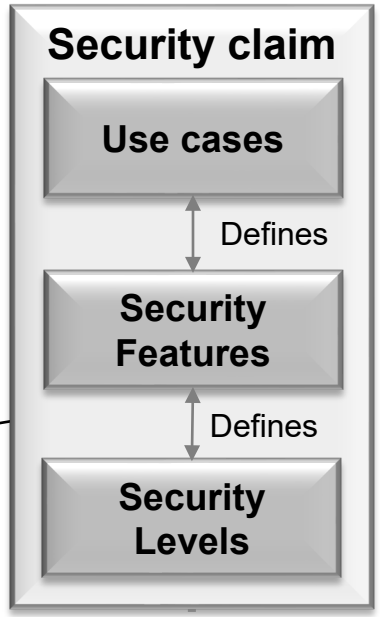
Security Lab

For identification of threats, attack surface definition,
identification of security feature implementation, etc.

Vulnerability Analysis

Test plan and method

Depends on SESIP level, attacker profile and
guidance from SESIP Profile / Security Target



Relevant Security Leveling

Self-assessment
Utilizing public tools to discover publicized potential vulnerabilities

	SESIP 1	SESIP 2	SESIP 3	SESIP 4	SESIP 5
Security Target	X	X	X	X	X
User guidance (prepa/install/ope…)	X	X	X	X	X
Functional specification		X	X	X	X
Design implementation information					X
Security mechanisms				X	X
Configuration Management			X	X	X
Environment Audit				X	X
Flaw remediation process	X	X	X	X	X
Source code			X	X	X
Functional testing	X (self-checking)	X	X	X	X
Penetration testing	VAN.1 (Survey)	VAN.2	VAN.3	VAN.4	VAN.5

Relevant Security Leveling

Closed/Semi-closed box penetration testing
Adding vulnerability analysis and penetration testing

	SESIP 1	SESIP 2	SESIP 3	SESIP 4	SESIP 5
Security Target	X	X	X	X	X
User guidance (prepa/install/ope…)	X	X	X	X	X
Functional specification		X	X	X	X
Design implementation information					X
Security mechanisms				X	X
Configuration Management			X	X	X
Environment Audit				X	X
Flaw remediation process	X	X	X	X	X
Source code			X	X	X
Functional testing	X (self-checking)	X	X	X	X
Penetration testing	VAN.1 (Survey)	VAN.2	VAN.3	VAN.4	VAN.5

Relevant Security Leveling

Open-box vulnerability analysis and penetration testing
Adding source code review

	SESIP 1	SESIP 2	SESIP 3	SESIP 4	SESIP 5
Security Target	X	X	X	X	X
User guidance (prepa/install/ope…)	X	X	X	X	X
Functional specification		X	X	X	X
Design implementation information					X
Security mechanisms				X	X
Configuration Management			X	X	X
Environment Audit				X	X
Flaw remediation process	X	X	X	X	X
Source code			X	X	X
Functional testing	X (self-checking)	X	X	X	X
Penetration testing	VAN.1 (Survey)	VAN.2	VAN.3	VAN.4	VAN.5

Relevant Security Leveling

Reuse of SOG-IS/EUCC CC evaluation
More evidences and higher attack potential

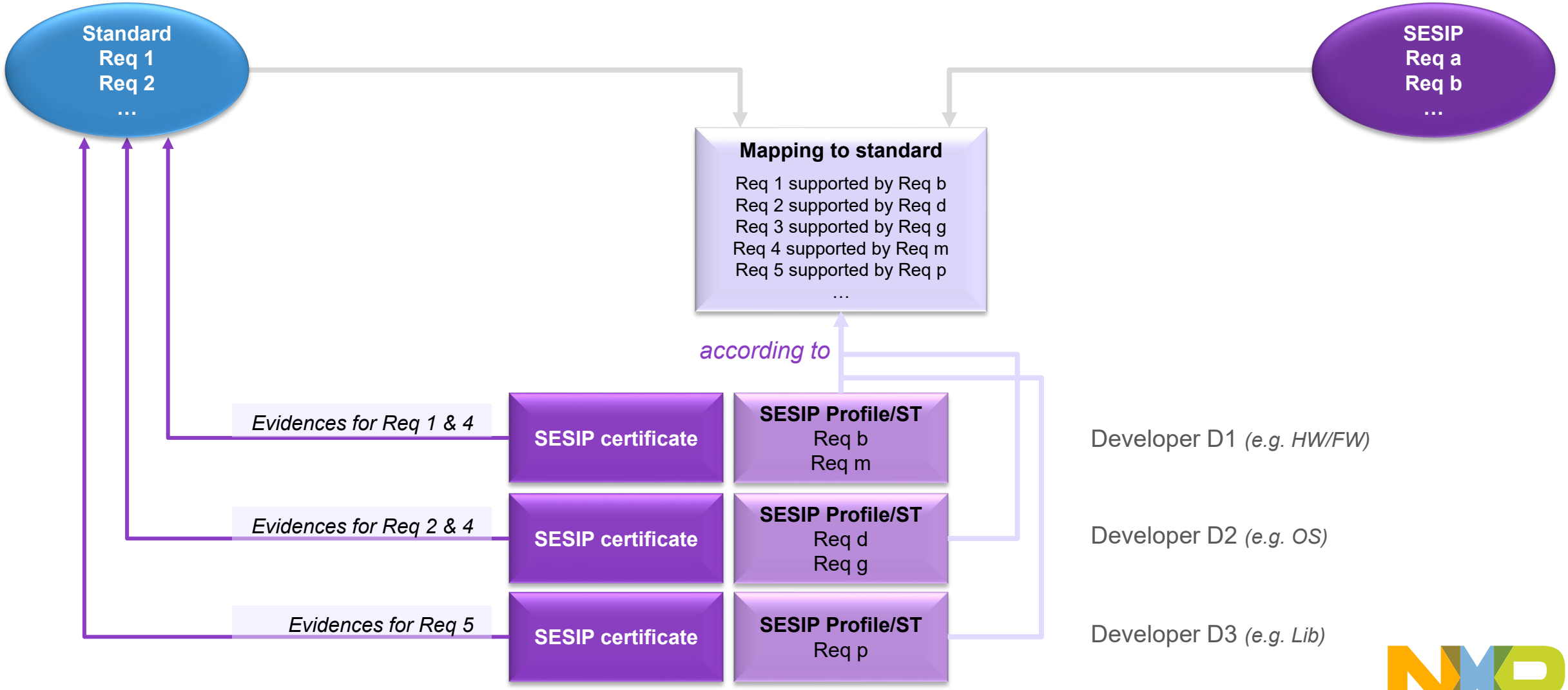
	SESIP 1	SESIP 2	SESIP 3	SESIP 4	SESIP 5
Security Target	X	X	X	X	X
User guidance (prepa/install/ope…)	X	X	X	X	X
Functional specification		X	X	X	X
Design implementation information					X
Security mechanisms				X	X
Configuration Management			X	X	X
Environment Audit				X	X
Flaw remediation process	X	X	X	X	X
Source code			X	X	X
Functional testing	X (self-checking)	X	X	X	X
Penetration testing	VAN.1 (Survey)	VAN.2	VAN.3	VAN.4	VAN.5

Relevant Security Leveling

Reuse of SOG-IS/EUCC CC evaluation
More evidences and higher attack potential

	SESIP 1	SESIP 2	SESIP 3	SESIP 4	SESIP 5
Security Target	X	X	X	X	X
User guidance (prepa/install/ope…)	X	X	X	X	X
Functional specification		X	X	X	X
Design implementation information					X
Security mechanisms				X	X
Configuration Management			X	X	X
Environment Audit				X	X
Flaw remediation process	X	X	X	X	X
Source code			X	X	X
Functional testing	X (self-checking)	X	X	X	X
Penetration testing	VAN.1 (Survey)	VAN.2	VAN.3	VAN.4	VAN.5

SESIP Mappings & Profiles for compliance demonstration



SESIP Mapping with EN 303 645 & 103 701

EN 303 645 / TS 103 701

SESIP Mapping

EN 303 645 Provision x.y

Covered by

SESIP Security Features
+ refinements

Authenticated Access Control
***Refinement 1**: Authentication by password – 5.1-1*
***Refinement 2**: Password generation rules – 5.1-1, 5.1-2*

No universal default passwords

IXIT TSO x.y/*

Covered by

SESIP User Guidance Analysis
+ refinements

The developer shall include information required in IXIT TSO related to claimed Provisions in [TS103701].

The evaluator shall check that user guidance includes the information required in IXIT TSO related to claimed Provisions in [TS103701].

Test Group x.y/*

Covered by

SESIP Functional Testing
+ refinements

The evaluator shall ensure that the functional testing campaign includes all test cases related to claimed Provisions in [TS103701].

Current and next SESIP operations

- Current SESIP methodology published by GlobalPlatform
  - GlobalPlatform SESIP Licensing for harmonization of SESIP operations
- Under CEN/CENELEC adoption
  - Current WI, could become a European Norm in Summer 2023
- Liaison Statement sent to ETSI TC Cyber group
  - To agree on Mapping/Profile approach and work on Mapping/Profile finalization
  - To recognize SESIP certificates to allow reuse and optimization of efforts

Conclusion

- Reuse based on composition and mappings => cost and time reduction
- Aligned with main IoT device standards requirements, align-able with future ones
- SESIP levels for all use cases: from verified self-declaration to highest testing level
- All connected products and use cases – wide range of products
- Full certification scheme already existing, significant number of certificates
- Support by many industry stakeholders, actively promoting and maintaining
- Already recognized by other players: PSA, ETSI (TS 103 732), NIST, CCC; work ongoing with others: FIDO, CSA/Matter

SECURE CONNECTIONS
FOR A SMARTER WORLD