SESIP INTRODUCTION

NXP SEMICONDUCTORS

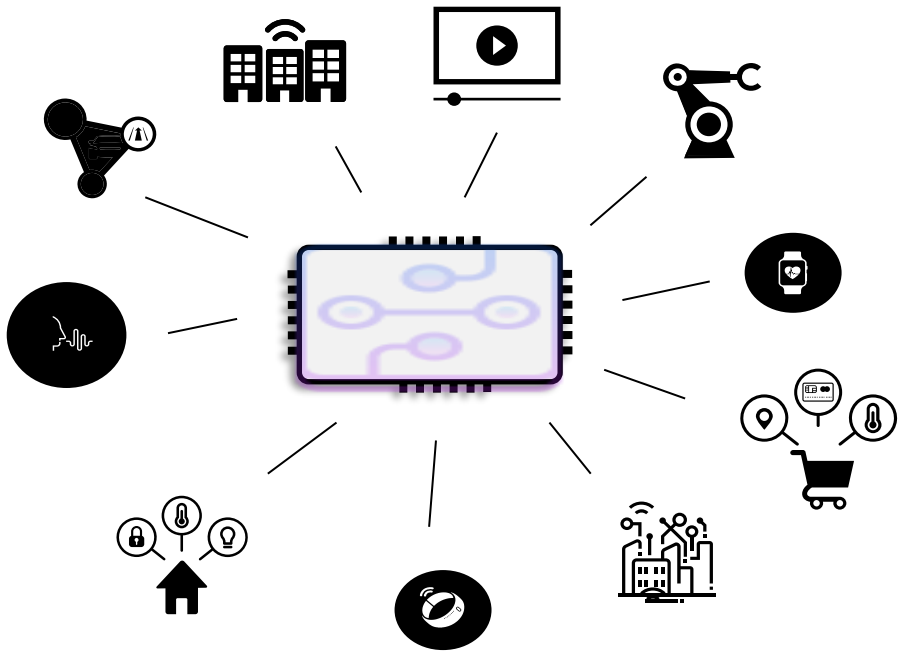
OCTOBER 19, 2022

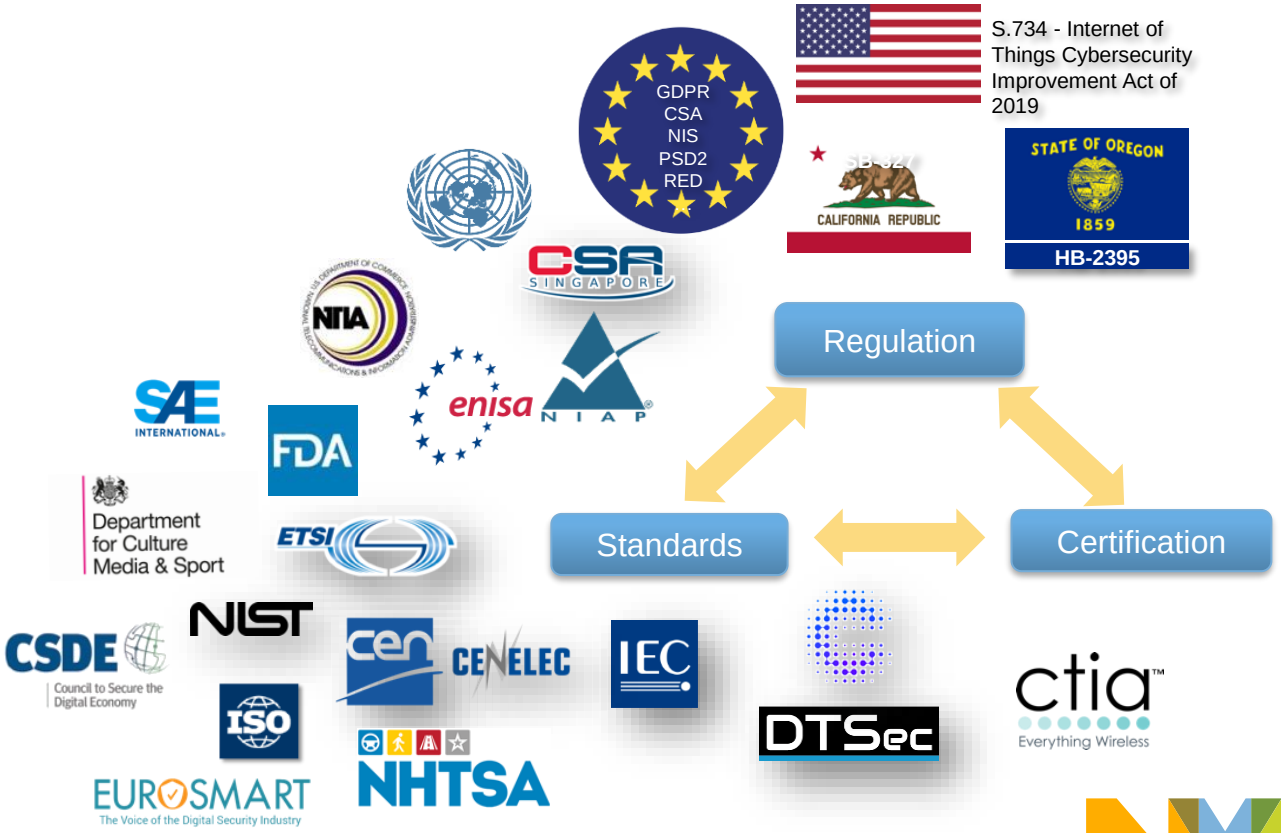
SECURE CONNECTIONS
FOR A SMARTER WORLD

Challenge 1 - IoT ecosystem

Many IoT standards and regulations

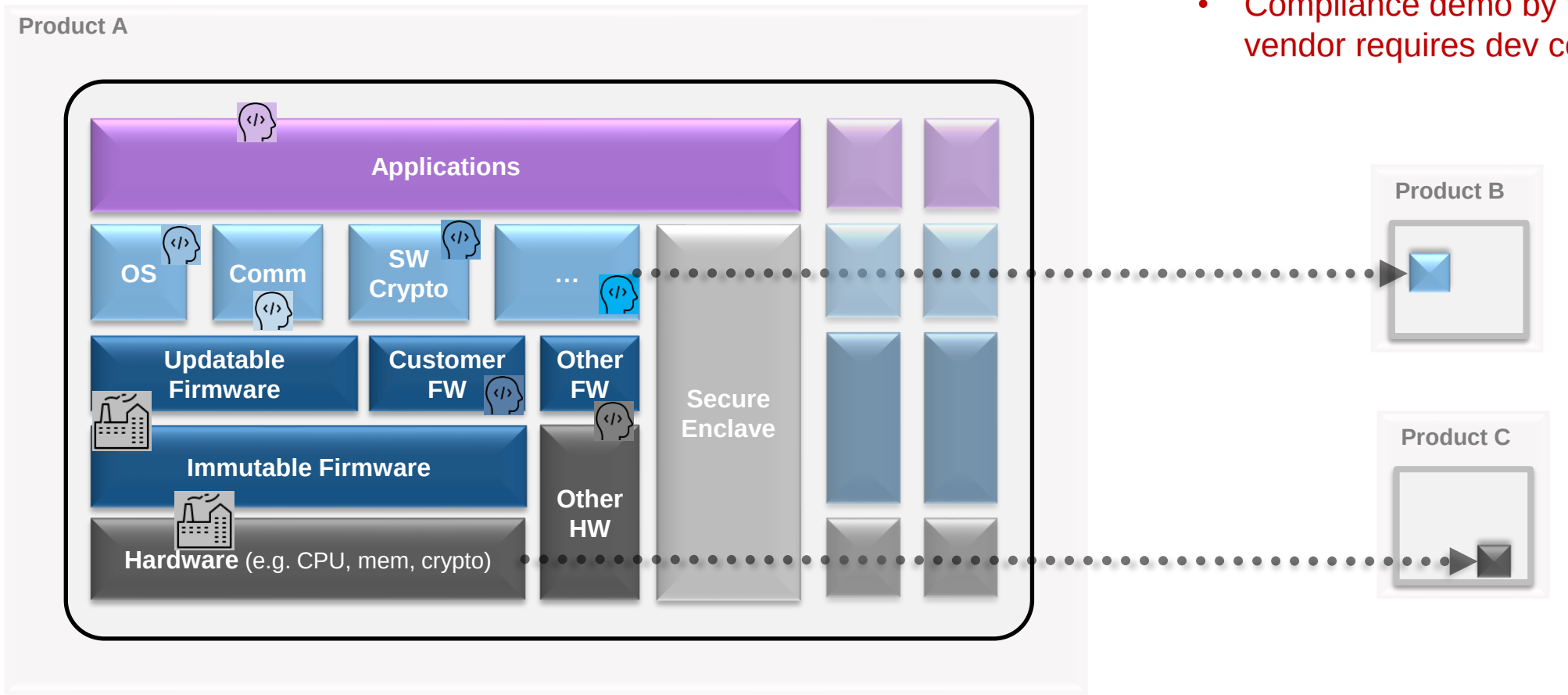
Complex and costly





Challenge 2 – IoT products complexity

Several modules
Different developers



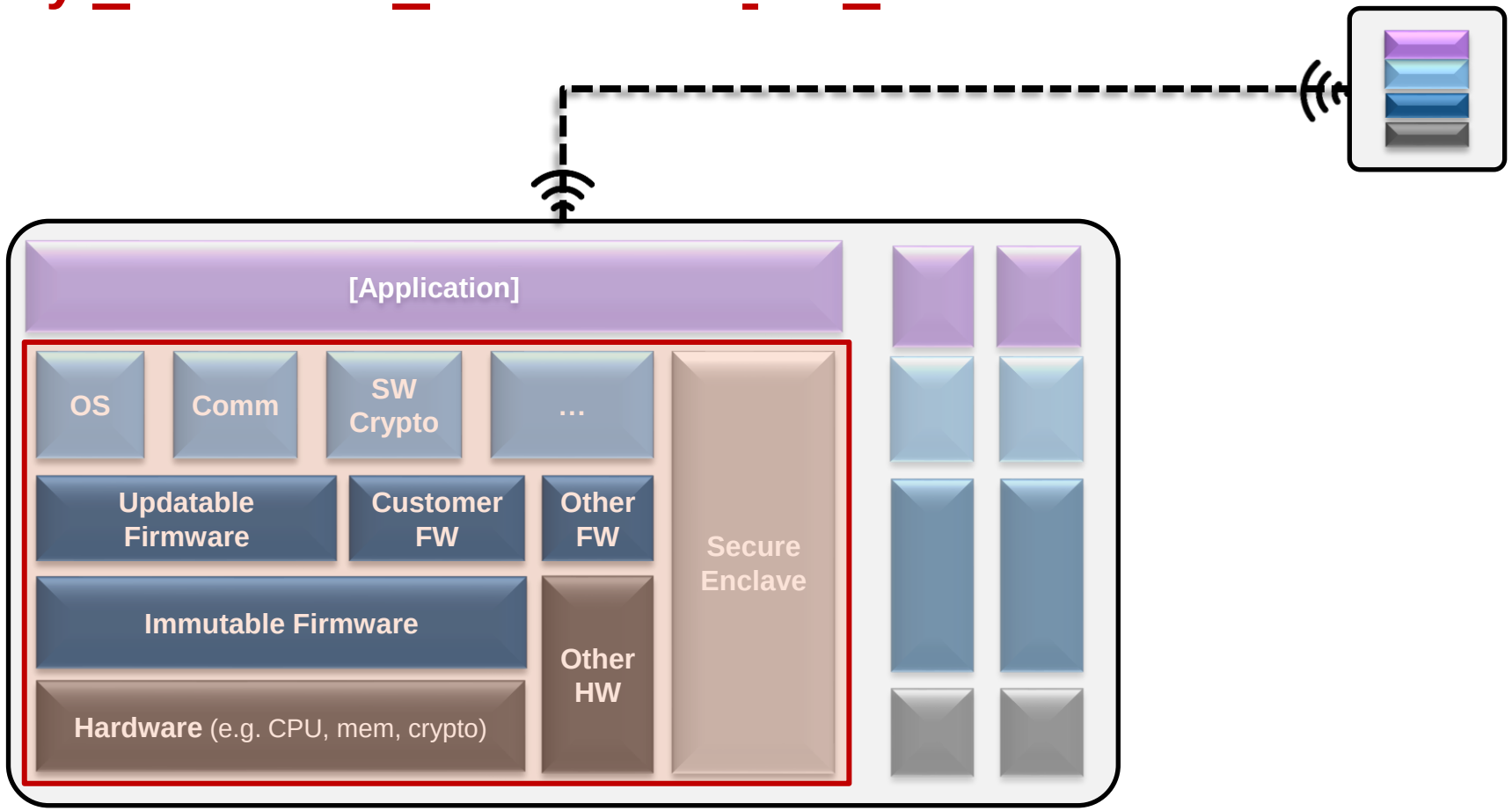
Several final products

- 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

Security Evaluation Standard for IoT Platform

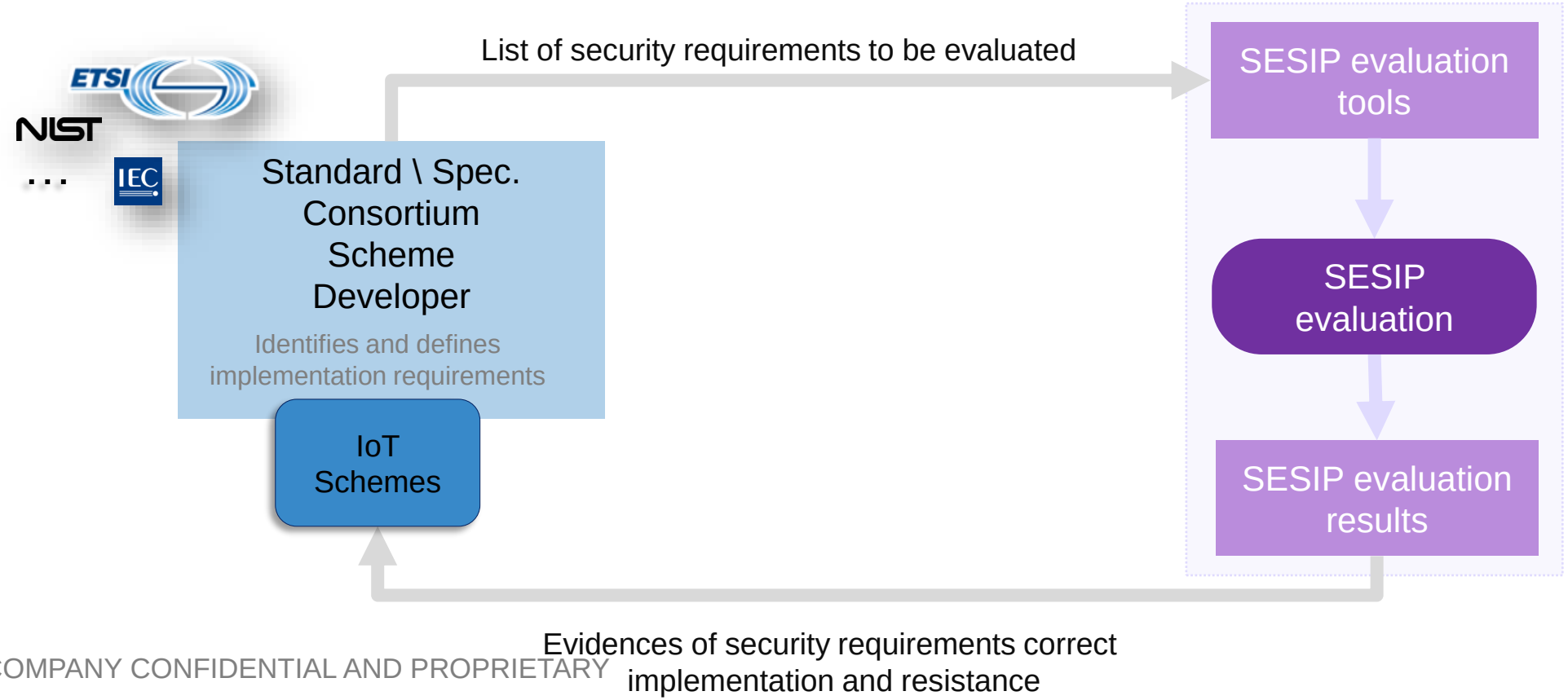
IoT Platform (platform)
Security features of IoT devices



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**”



Composition and reuse

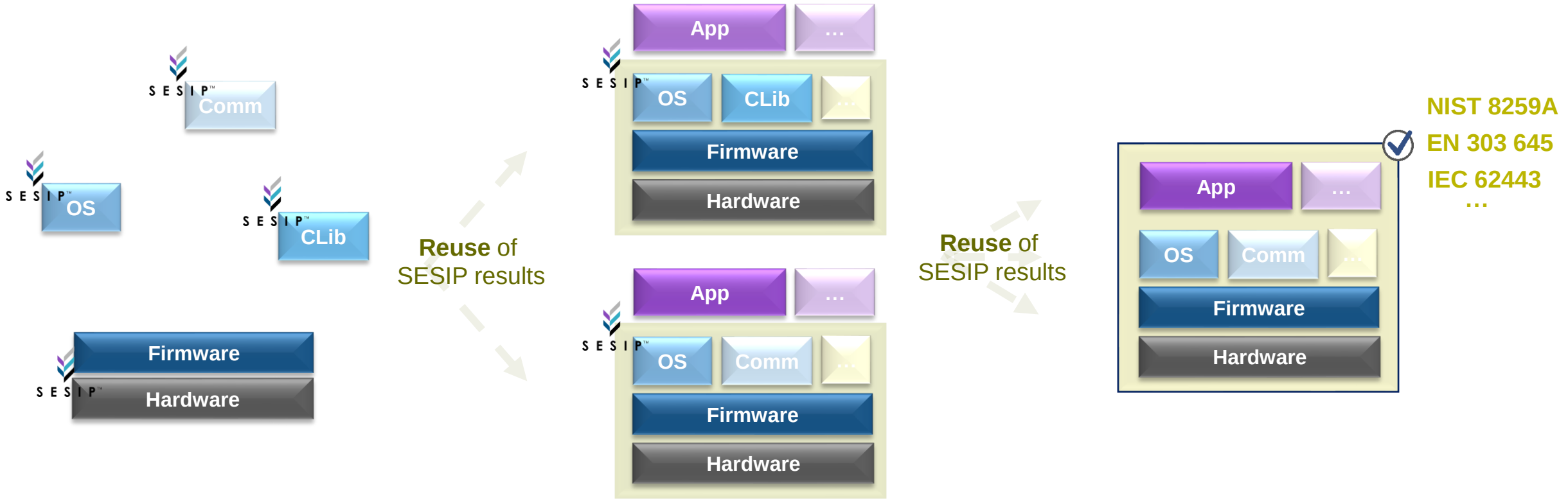
Security of **components (platform parts)**

Security of **platforms**
Composition

Security of **devices**

Prove component **security** to customers

Support customers in **compliance demonstration**



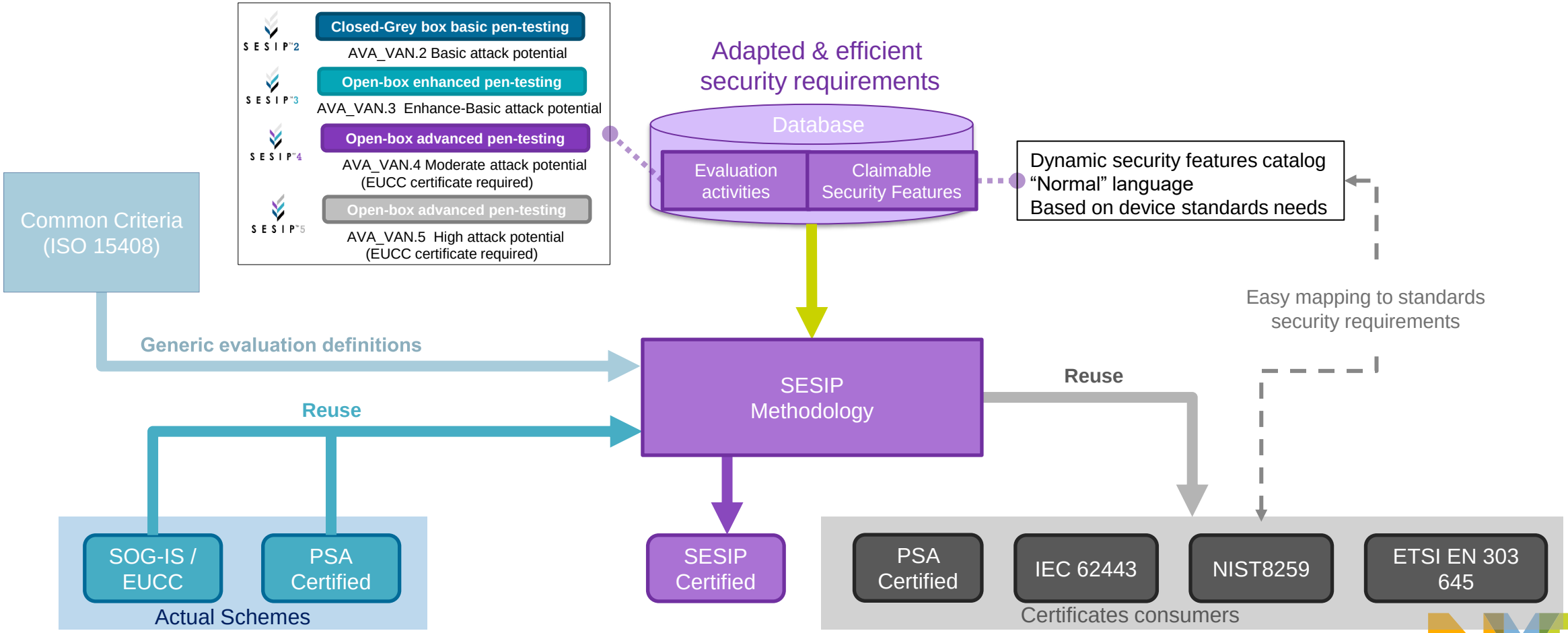
Component developers

Device developers
(e.g manufacturers Customers)

Harmonization between standards

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

⇒ Reusable results



Mappable Security Functional Requirements

- **SFRs** => security feature/service to be evaluated

Understandable & Intuitive

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

Mappable Security Functional Requirements

Selectable IoT features

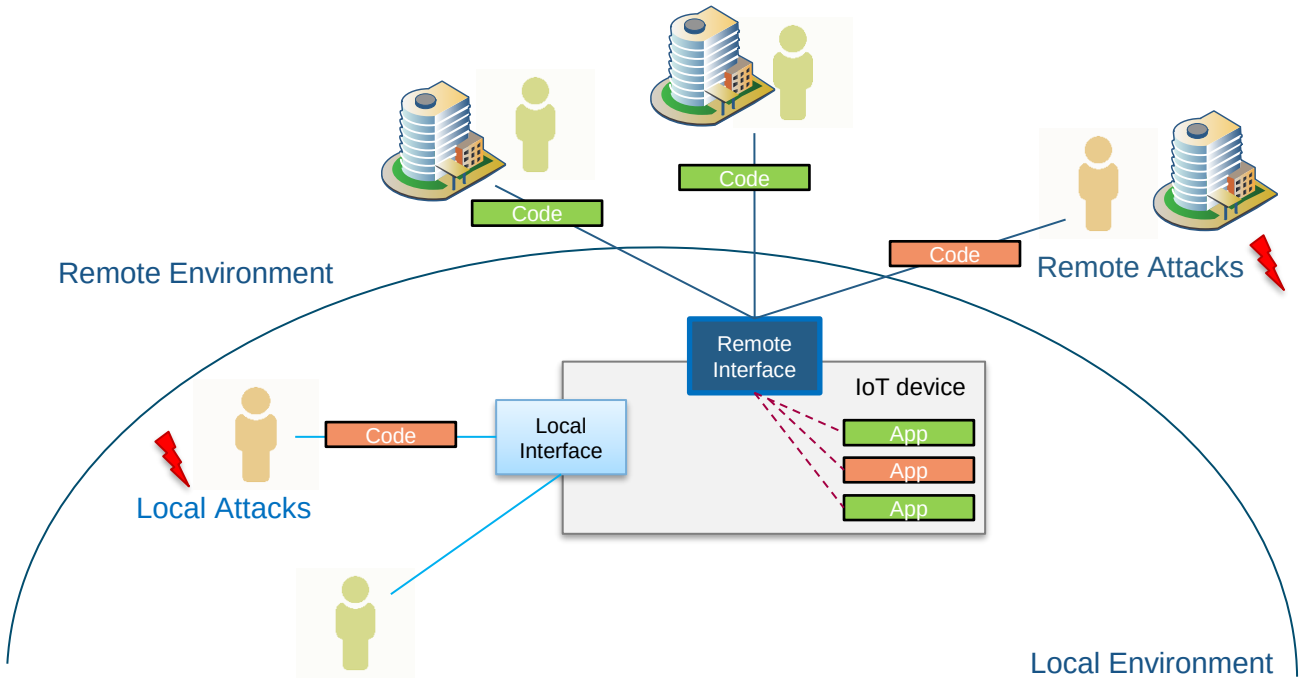
Identification & Attestation	Product Life Cycle	Cryptographic functionality	Secure communications	Compliance functionality	Extra attacker resistance
Verification of platform identity	Factory reset of platform	Cryptographic operation	Secure communication support	Secure Storage	Limited physical attacker 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

Efficient Security Assurance Requirements & Levels

Self-assessment
Utilizing public tools to discover publicized potential vulnerabilities

AVA_VAN.1 – Resistance to Basic Attack potential

Black-Grey box penetration testing
Adding vulnerability analysis and penetration testing

AVA_VAN.2 – Resistance to Basic Attack potential

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

AVA_VAN.3 – Resistance to Enhance-Basic Attack potential

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

AVA_VAN.4 – Resistance to Moderate Attack potential

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

AVA_VAN.5 – Resistance to High Attack potential

Efficient Security Assurance Requirements & Levels

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

Efficient Security Assurance Requirements & Levels

SESIP™2

Black-Grey 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

Efficient Security Assurance Requirements & Levels

White-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

Efficient Security Assurance Requirements & Levels

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

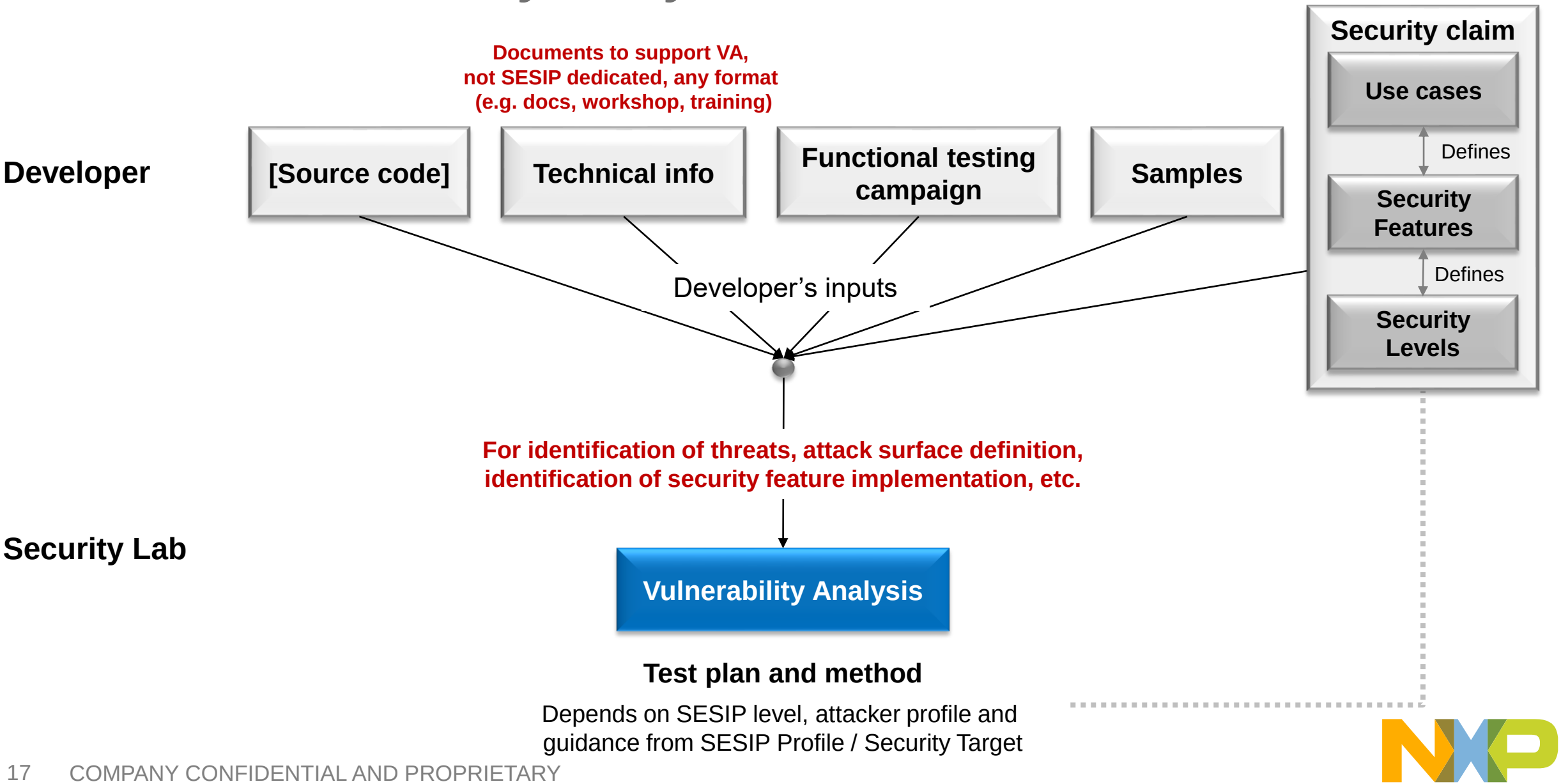
Efficient Security Assurance Requirements & Levels

SESIP™5

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

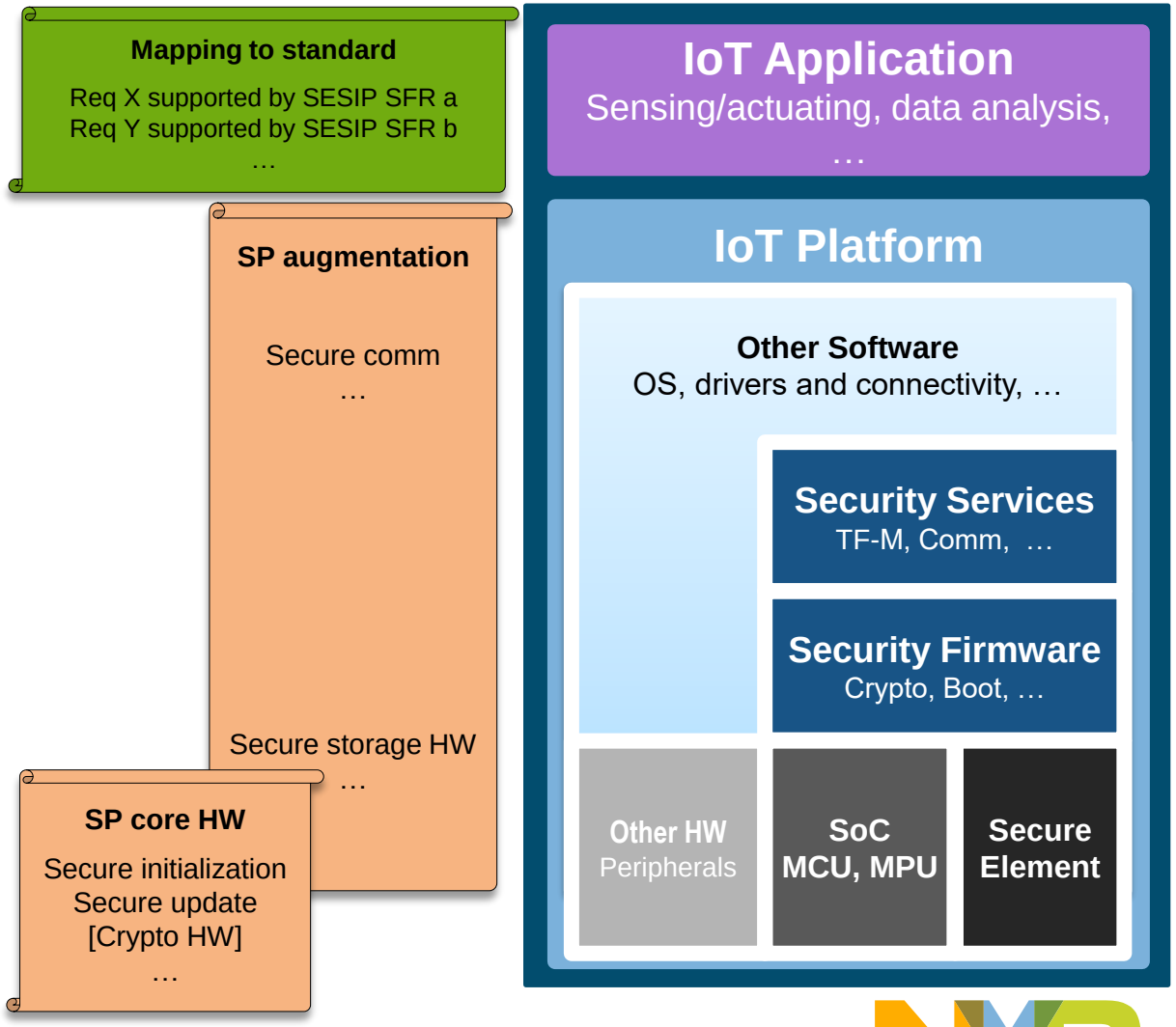
	SESIP 1	SESIP 2	SESIP 3	SESIP 4	SESIP 5
Security Target	X	X	X	X	X
User guidance (prepa/install/ope…)	X	X	X	X	X
Functional specification		X	X	X	X
Design implementation information					X
Security mechanisms				X	X
Configuration Management			X	X	X
Environment Audit				X	X
Flaw remediation process	X	X	X	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

Focus on Vulnerability Analysis

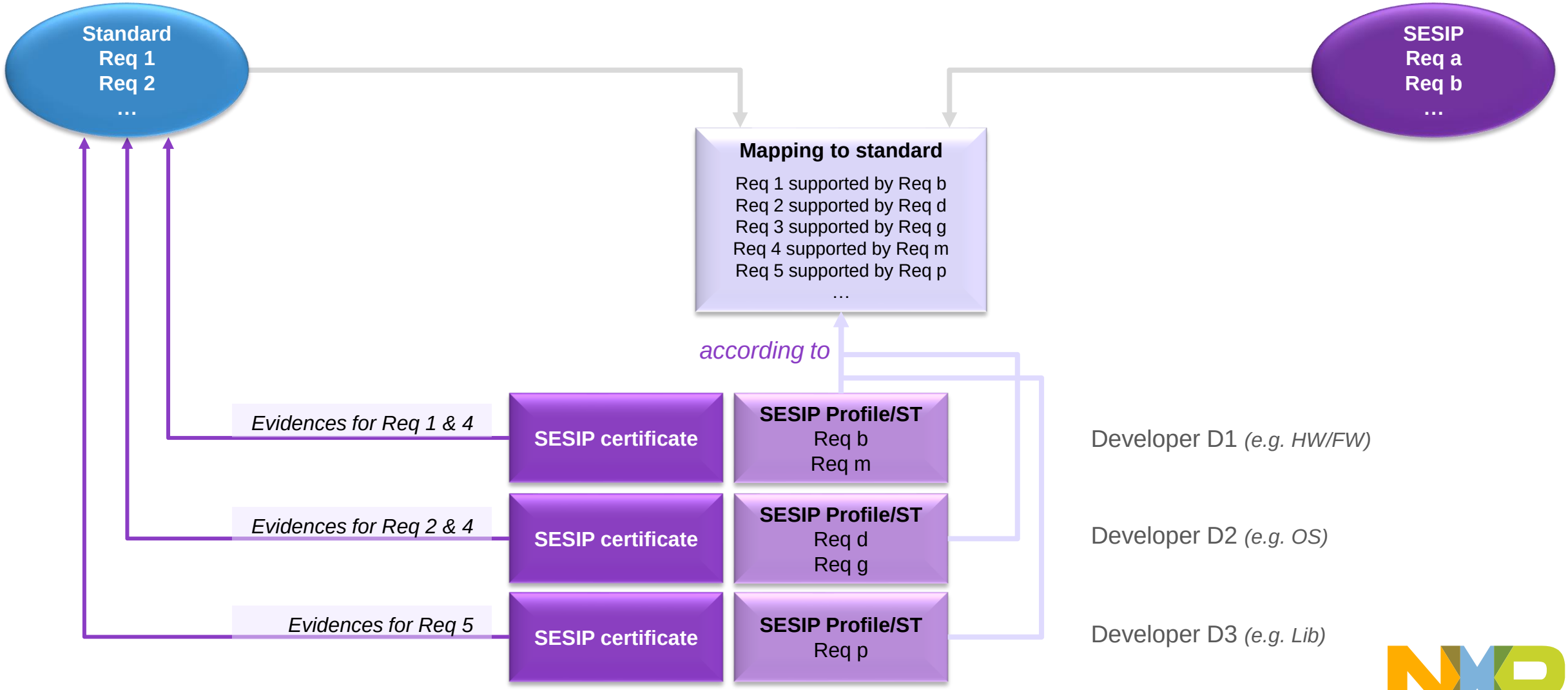


SESIP Extended tools

- **Security Targets**
  - Security claim of a specific product
- **SESIP Profiles**
  - Generic requirements per type of products
  - Ensure comparability between certificates
  - Written upon need by stakeholders
  - e.g. core MCU/MPU, PSA L2 & L3, Secure Memory, communication controllers (others ongoing)
- **SESIP Mappings**
  - Map SESIP SFRs & SARs to standards requirements
  - Allow the reuse of SESIP evaluation results for compliance demonstration to standards
  - e.g. NIST 8259A, ETSI 303 645, IEC 62443 (others ongoing)



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

No universal default passwords

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

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
  - Current SESIP methodology published by GlobalPlatform
  - GlobalPlatform SESIP Licensing for harmonization of SESIP operations
    - 1 SESIP scheme licensed (TrustCB)
    - Several SESIP labs licensed (Applus, Riscure, SGS BrightSight) or under licensing
- Under CEN/CENELEC adoption
  - Current WI, could become a European Norm in Summer 2023

SESIP Strengths

- Reuse based on composition and mappings => cost and time reduction
- Aligned with main IoT device standards requirements, align-able with future ones
- Assurance Levels and Requirements for all use cases: from verified self-declaration to highest testing level
- Cover 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, NIST, CCC; work ongoing with others: ETSI, FIDO, CSA/Matter

SECURE CONNECTIONS
FOR A SMARTER WORLD