EU CYBERSECURITY ACT CONFERENCE 2022

CROSS STANDARD AND SCHEME COMPOSITION

MAY 2022

SUBJECT

The proliferation of new cybersecurity standards/schemes shows the interest of all the stakeholders to require cybersecurity for ICT products. On the other hand, a need for harmonization/recognition between standards/schemes is needed. Otherwise, there could be too many standards that become non-cost-effective for developers certifying their products

For instance, almost every IoT vertical has its own set of cybersecurity standards. But IoT devices and it, is supply chain is not limited within a single vertical. In fact, the contrary holds, that building blocks of an IoT device find appliance in a couple of other verticals. Assuming that these building blocks demonstrated cybersecurity compliance of some form, say for a particular vertical, it will be key for the economy to not repeat those proofs of compliance but instead accept across standards and schemes where applicable

This talk will highlight the importance of the acceptance of certification and standard compliance results across different schemes or security standards. We will show examples (e.g., smart metering in France with de-facto acceptance of underlying CC results, SESIP to IEC62443-4-2) where this has been applied successfully, but will also look at existing standards or schemes where this would be possible (e.g. EUCC, FITCEM, etc) or proposals on how to apply this for Industrial IoT (IACS ERNCIP recommendations to the EU commission)

ABOUT US

José Ruiz:

- Co-Founder & CTO
- Common Criteria, FIPS 140-2 & 3 Expert
- Member of the SCCG (Stakeholder Cybersecurity Certification Group)
- ICCC Former Program Director
- Editor at thematical group “IACS Cybersecurity certification “.
- Editor at JTC13 WG3: “Cybersecurity Evaluation Methodology for ICT products”

ABOUT US

Fabien Deboyser:

- Security Certification Expert
- Common Criteria, FIPS 140-2 & 3, PCI-HSM, SESIP & ISO17025 Expert
- Member of ISO/CEN committees: TC 224, ISO19790, ISO17825
- Eurosmart CDI representative
- Former Common Criteria laboratory director

Everything Safe & Secure

Sense

Everything
Aware

Think

Everything
Smart

Connect

Everything
Connected

Act

Everything
Efficient

HORIZONTAL CERTIFICATION SCHEME IS IN DEMAND TO ADDRESS VARIOUS REQUIREMENTS

Government Legislation:

- European Cyber Security Act
- Singapore CSL
- S.734 - Internet of Things Cybersecurity Improvement Act of 2019
- Cal. SB-327

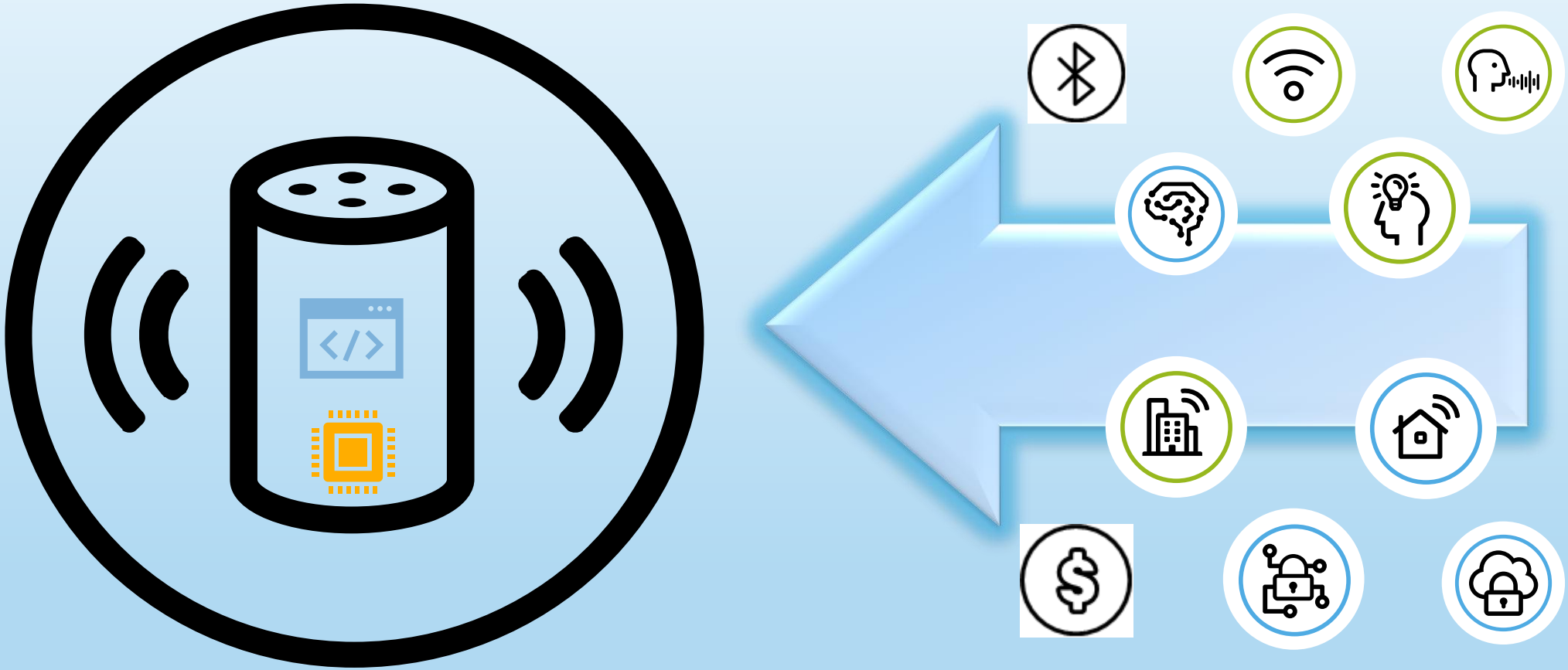
Baseline Requirements:

- CSA/MATTER (Zigbee etc)
- ETSI 303 645 (Consumer)
- NISTIR 8259 (Device Manufacturers)
- UL 2900 (SW)

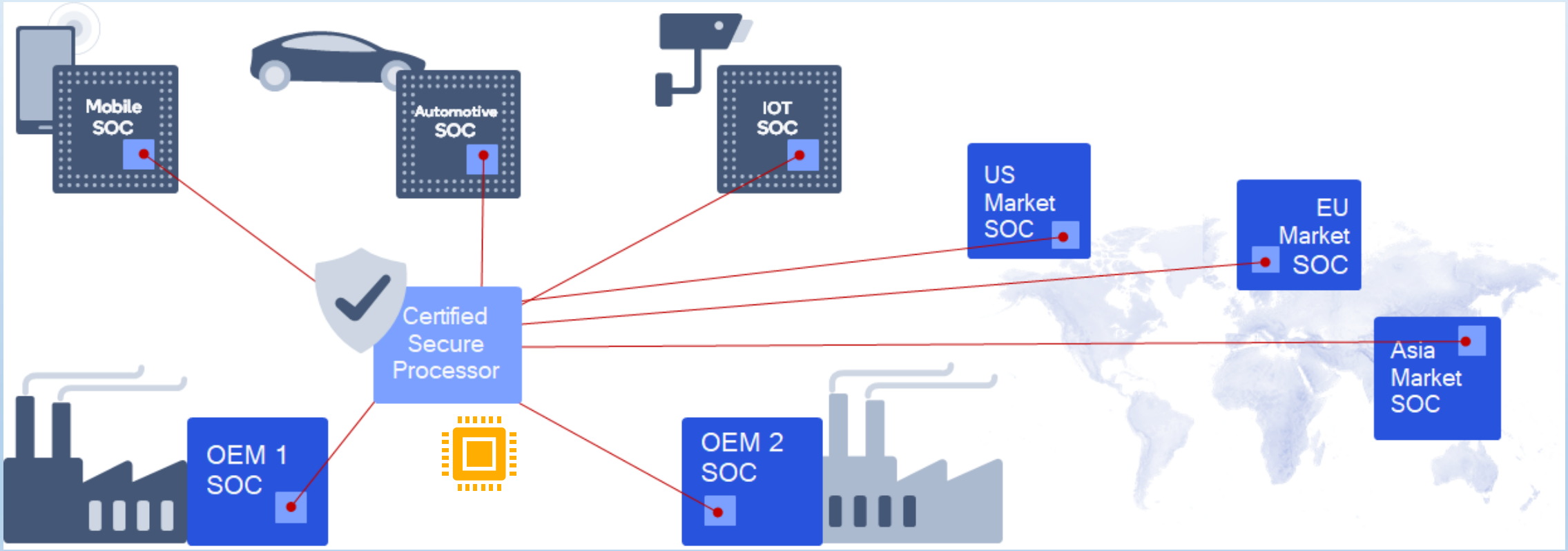
Sector Specific:

- ISO/SAE 21434 (Auto)
- IEC 62443 (Industrial)
- NFC/FiRa/CCC
- Hospital & at-home Patient Monitoring
- Personal Health & Fitness Monitoring

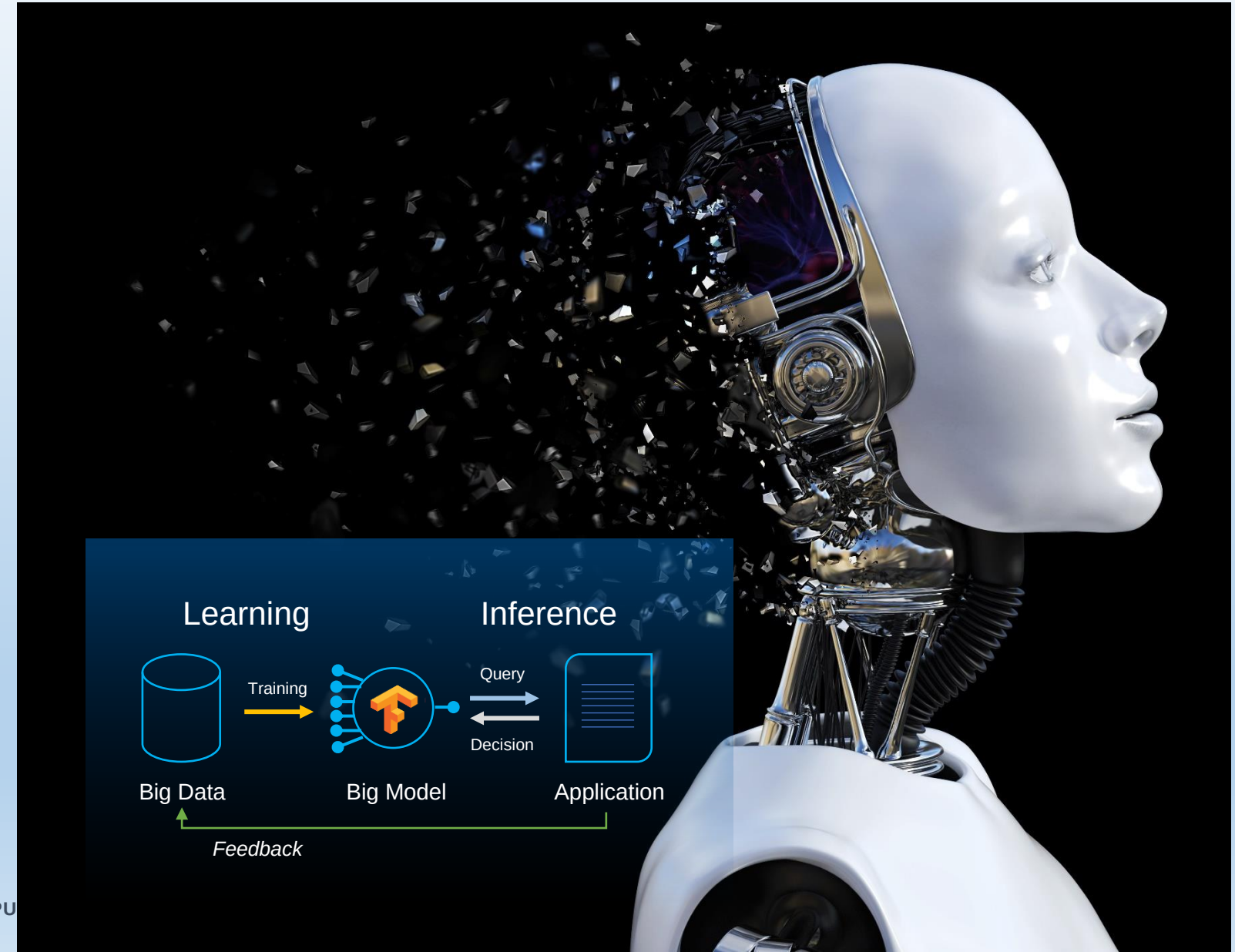
CURRENT SITUATION = VENDOR PERSPECTIVE



CURRENT SITUATION = VENDOR PERSPECTIVE



SECURITY WILL CONSTANTLY EVOLVE IN REAL TIME



Connected devices are always online and can be monitored for unusual behaviour using AI both in the cloud and more and more at the edge.

Security profiles can be loaded and adapted in real time

CURRENT SITUATION = LABORATORY PERSPECTIVE

No mutual recognition

PRODUITS CERTIFIÉS CSPN

Stormshield Network Security Pare-feu Industriel SNi40 Suite logicielleVersion 2.3.4

Référence : 2016/11
Date : 27/07/2016

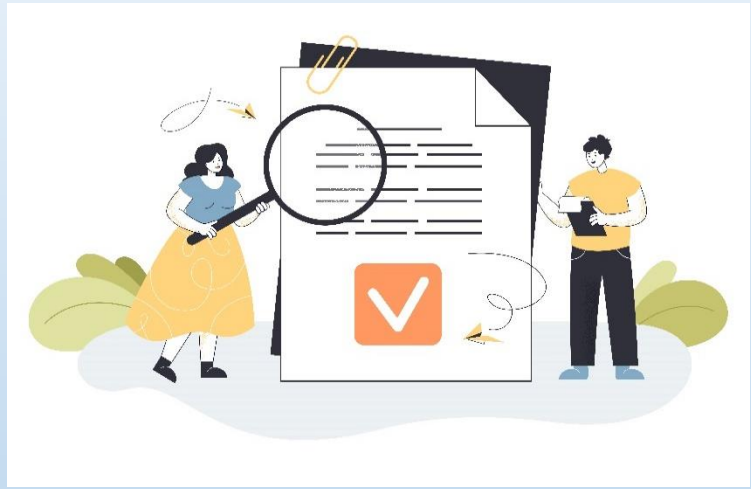
Catégorie : **Pare-feu**
Référentiel : **Certification de sécurité de premier niveau**
Développeur(s) / Commanditaire(s) : **/ Stormshield**
Centre d'évaluation : **Oppida**

OC-CCN ABOUT OC CERTIFIED PRODUCTS CIS PRODUCT CATALOGUE TYPES OF CERTIFICATION REQUESTS AND FORMS

HOME » CIS PRODUCT CATALOGUE » LIST OF QUALIFIED PRODUCTS » STIC PRODUCTS » STIC PRODUCTS CATEGORIES » PROTECTION OF COMMUNICATIONS » STORMSHIELD NETWORK SECURITY UTM/ FIREWALL (APPLIANCES DESDE SN200 A SN6100 EN 4 COMPILACIONES DISTINTAS: S, M, L Y XL). 3.10.1

Stormshield Network Security UTM/NG-Firewall (Appliances desde SN200 a SN6100 en 4 compilaciones distintas: S, M, L y XL). 3.10.1

Standards checking the same work

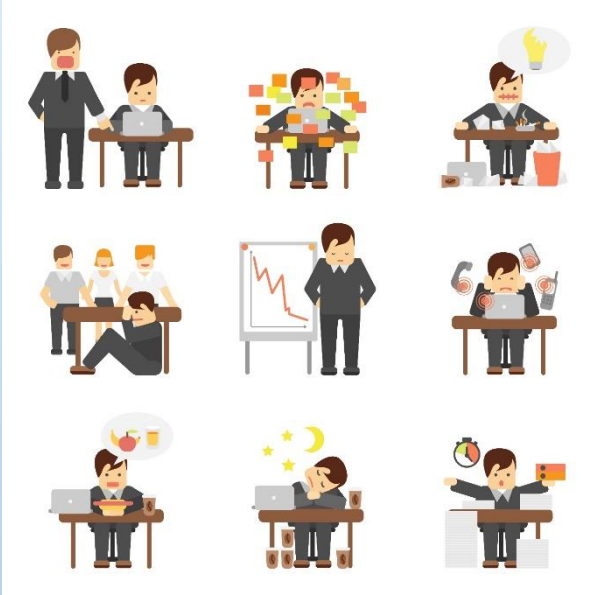


EMVCo

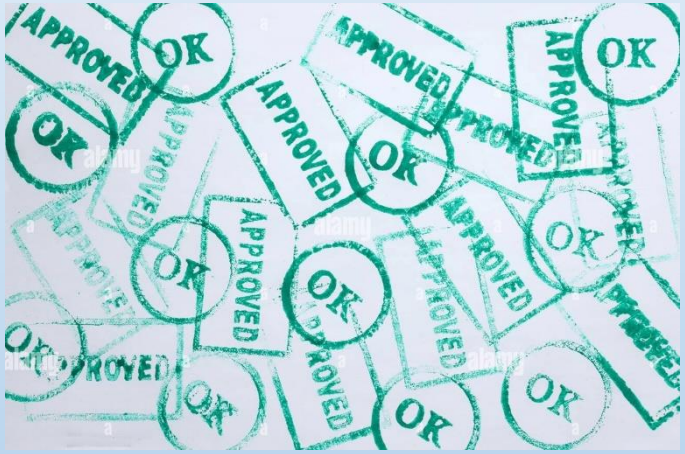
Common Criteria

Chaos of certifications and overlapping of standards/schemes

PROBLEMS FROM THE LABORATORY PERSPECTIVE



Lack of personnel



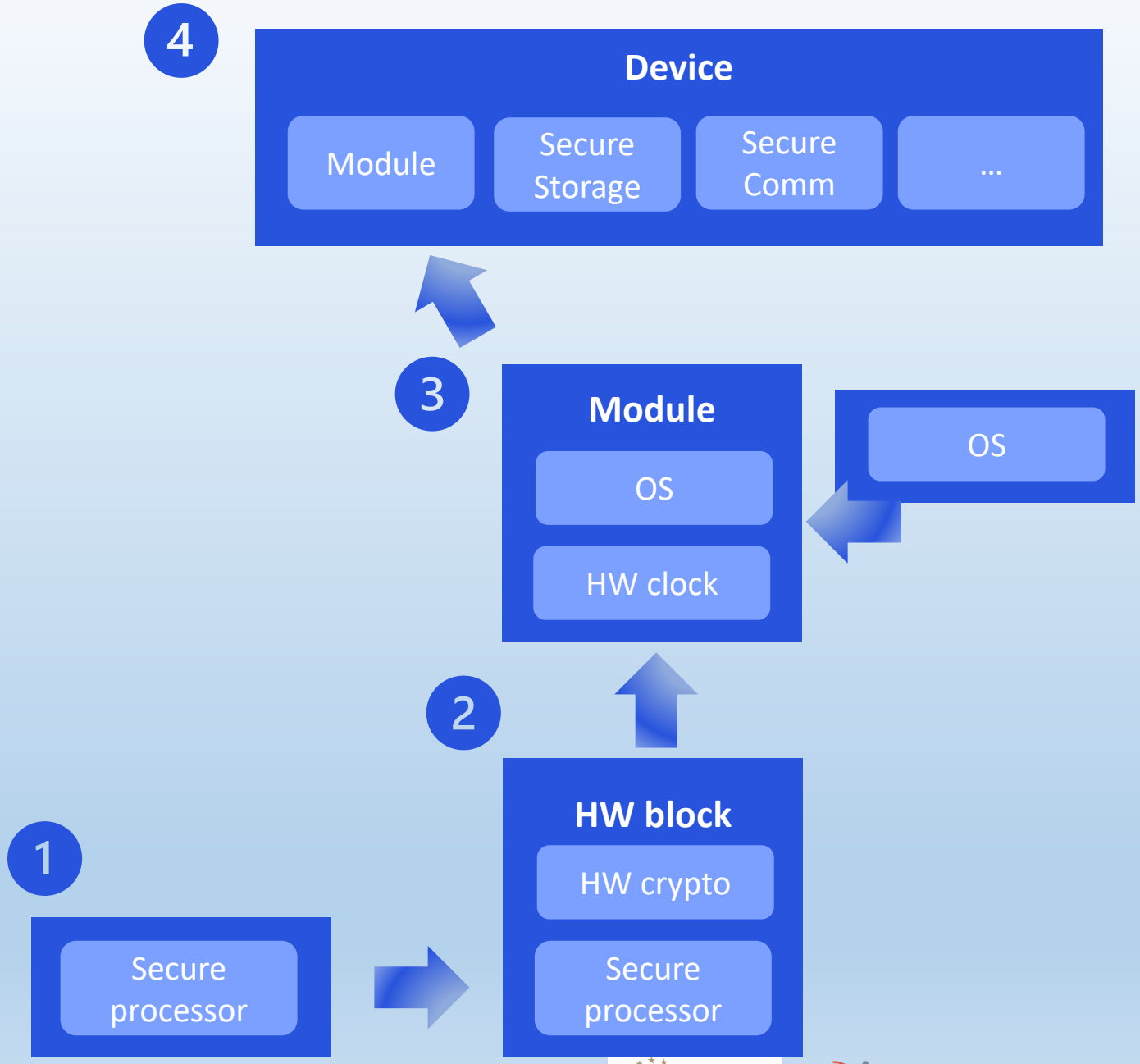
Too Many Accreditation Audits


WHAT IS
CROSS STANDARD AND SCHEME COMPOSITION?
imgflip.com

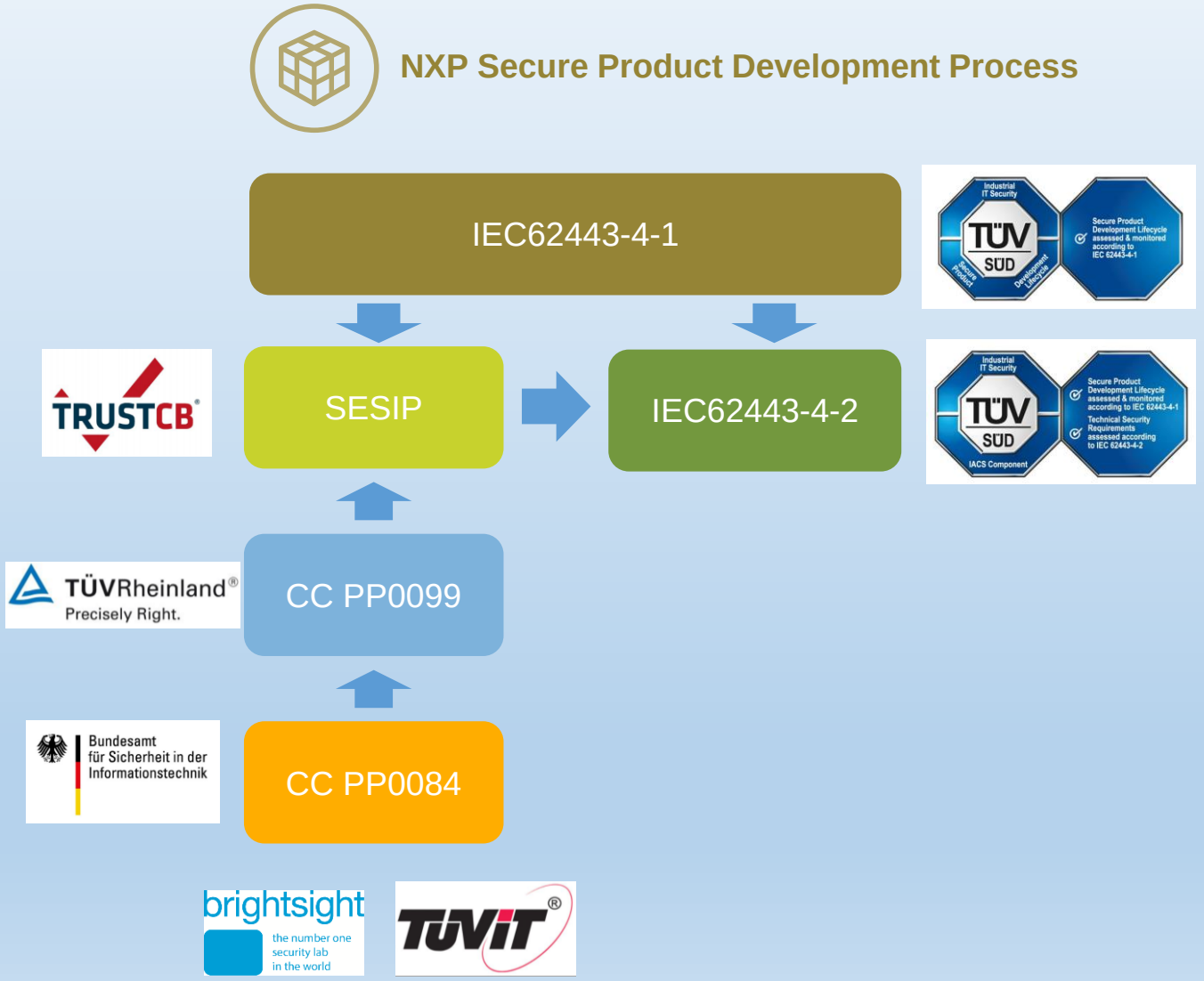
WHAT IS COMPOSITION?

- The art of putting “things together”, to create harmony

- In security certification:
  - the art of reusing existing compliance proofs without re-evaluation, re-audit or re-testing
  - This can be done within a scheme or multiple schemes



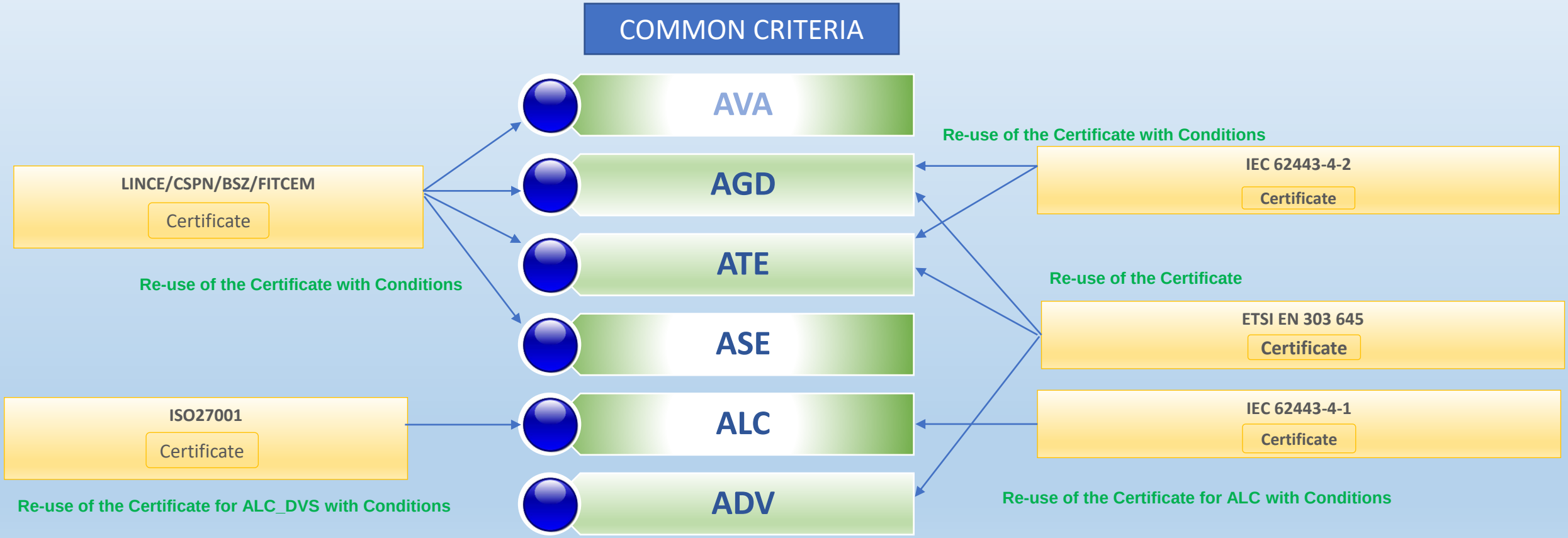
SOLUTIONS FROM THE VENDOR PERSPECTIVE = CROSS SCHEME AND COMPOSITION IN PRACTICE



CROSS STANDARD & SCHEME COMPOSITION

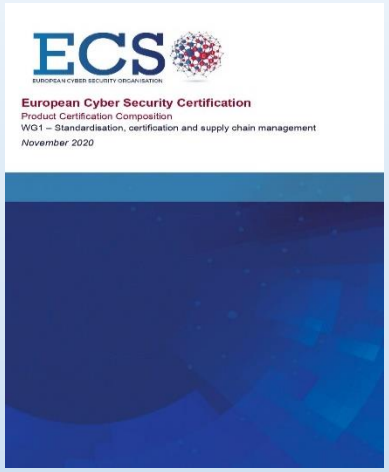
Cross Standard & Scheme composition

To reuse existing compliance proofs across different certification schemes or standards without (or only limited) re-evaluation, re-audit or re-testing.



INTERESTING INITIATIVES FROM THE LAB PERSPECTIVE

Mutual recognition – CSPN & BSZ

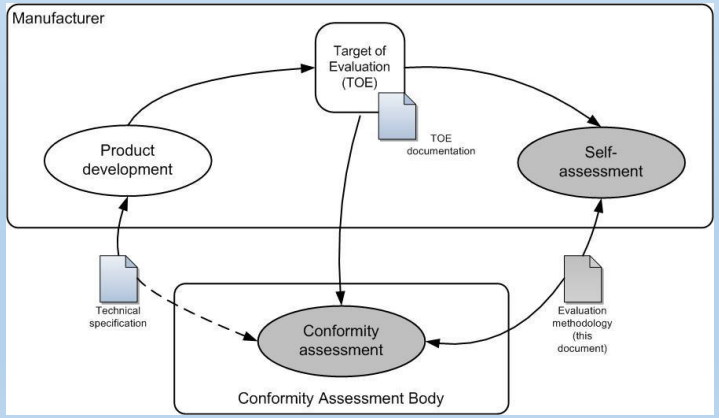


ECSO – Product Certification Composition

Scheme	Current phase	Upcoming Phase	Sectors involved
EUCC	Approval pending	Convert the scheme into European Law	Information and Communication Technology (ICT) products
Cloud Services	Modifications to the draft after public consultation	Approval of the candidate scheme by the European Commission	Cloud service providers
5G	Ad-hoc Working Group created for the development of the draft	Development of the first draft	Devices that are part of the 5G infrastructure
IoT	Included in the URWP	Request from the European Commission for the creation of the candidate scheme	To be defined, potentially any device considered as IoT
IACS	Included in the URWP	European Commission's request for the creation of the candidate scheme	Industry and industrial component manufacturers

URWP – New Schemes

IACS ERNCIP Recommendations – Definition of the scheme



FITCEM

Food for thoughts

Recognition between countries for lightweigths schemes or

A ligthweight horizonal scheme in Europe under the CSA

Bundesamt
für Sicherheit in der
Informationstechnik

Nederlands Schema
voor Certificatie op het
gebied van IT-Beveiliging
(NSCIB)

Food for thoughts

New version of Common Criteria includes exact conformance

Common Criteria

LET'S USE IT!

LET'S INNOVATE!

Eg.- Develop an PP for IoT devices mandating an ETSI certificate + AVA_VAN activities

This will allow to reuse the ETSI certificate saving a lot of time related to the CC certification

Food for thoughts

- **Technical WGs to discuss technical details/challenges of Cross Standard and scheme composition at ENISA**

- **New Cybersecurity Act schemes should integrate cross standard and scheme composition from the very beginning**

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Questions?

Thanks

José Ruiz
jruiz@jtsec.es

Fabien Deboyser
fabien.deboyser@nxp.com