Standardization Support for the upcoming EU semiconductor manufacturing industry

CEN/CENELEC

About me

- **José Manuel Pulido:**
- Lead Cybersecurity Consultant and Senior Cybersecurity Evaluator at jtsec
- Common Criteria expert
- CCToolbox developer
- More than 10 years of experience in cybersecurity technologies
- Speaker at several conferences including ICCC20, ICCC21 and ICCC22

About us

- Cybersecurity **evaluation** & consultancy **services**
- Common Criteria, LINCE, IEC 62443-4-1 , IEC 62443-4-2 and ETSI EN 303 645 accredited lab.
- **Highly Involved in standardization** activities (ISO, CEN/CENELEC, ISCI WGs, ENISA CSA WGs, CCUF, ERNCIP, …)
  - Editors of FITCEM, LINCE or ISO/IEC TS 9569 Patch Management
- Members of the SCCG (Stakeholder Cybersecurity Certification Group)

Landscape and motivation – EU Chips Act

- Cybersecurity standards for ICT products are aligned with and can support EU Chips Act objectives

NON-EU CHIP MANUFACTURING INDUSTRY

- Exponential demand of chips across different industries
- High dependency with non-EU countries for chip production
- Low resilence of the supply chain to crisis events

- Compliance of production processes with EU regulations
- Security improvement of the supply chain
- Mitigate the impact of crisis in chip-based industry

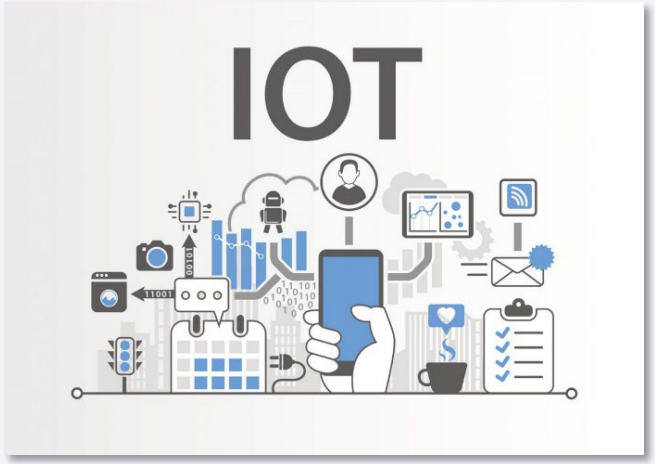
Security standardization needs in chip-based products

Security ICs and Smartcards

- Payment industry.
- National IDs, passports.
- Mobile wallets.

- **High** assurance security certifications required

IoT and general-purpose Devices



- Always connected devices.
- Breaches could compromise home and corporate networks.

- **Medium-Low** assurance security certifications required.

Security standards for chip-based products shall provide security assurance on:

- Security specifications
- Functional security testing
- Vulnerability analysis and penetration testing
- Security user guidance.
- Development and lifecycle assurance, which includes **chip design and manufacturing security assessment**.

EU Cybersecurity standards for chip-based products

Common Criteria

- Low, medium and high assurance. Best-suited for high.
- Specific assurance and methodologies for Security ICs.
- Assurance evaluation of the production and supply chain lifecycle.

EUCC

- Low, medium and high assurance.
- Reuses all assurance levels from Common Criteria, without site security

FITCEM (EN 17640)

- Modular framework adaptable to different assurance needs.
- Meant to replace national standards in Europe (LINCE, BSZ, BSPA, CSPN)
- Fixed time evaluation.

SESIP

- Specific for IoT platforms – Vertical standard
- Supports low, medium and high assurance.
- High assurance evaluations require a previous CC evaluations.

ETSI EN 303 645

- Designed for consumer IoT devices.
- No high assurance evaluations.
- Focused on functional security requirements and provisioning.

☑ Addresses security of chip production in design and manufacturing centers.

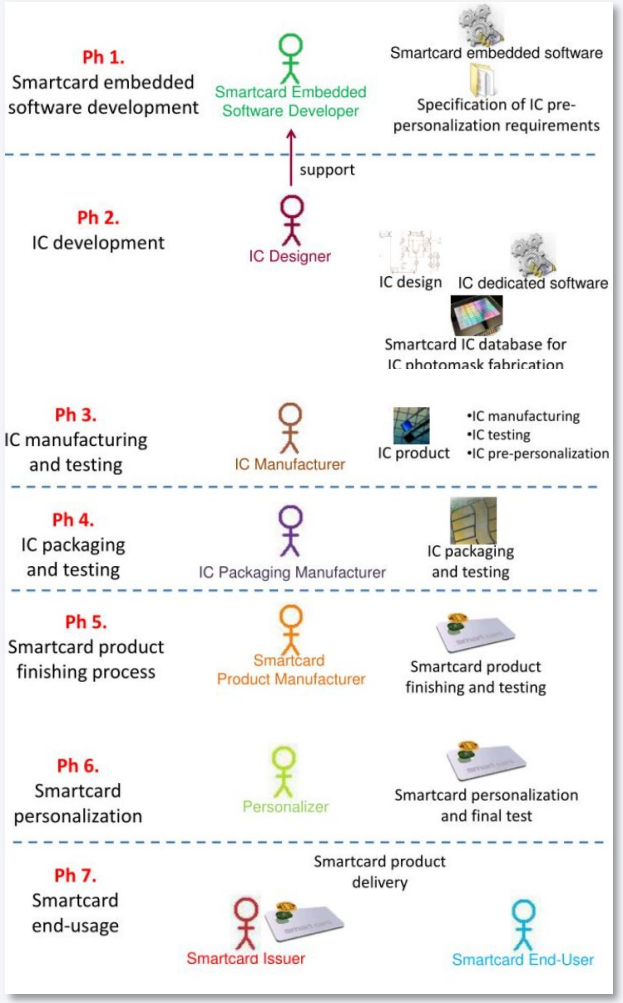
☑ Audits to development and production centers included in evaluations

☑ Production lifecycle security to be addressed in next version of the standard (under development)

☑ Security of chip production only addressed through CC

☒ Chip lifecycle and production not assessed

Lifecycle of high-assurance semiconductors



- IC Developers perform:
  - Design of IC circuit.
  - IC FW development
  - IC SW development
  - IC Unit-testing
  - IC logical testing
  - Design of test program for fabs
  - Design personalization program
  - Monitoring /handling of fab testing output

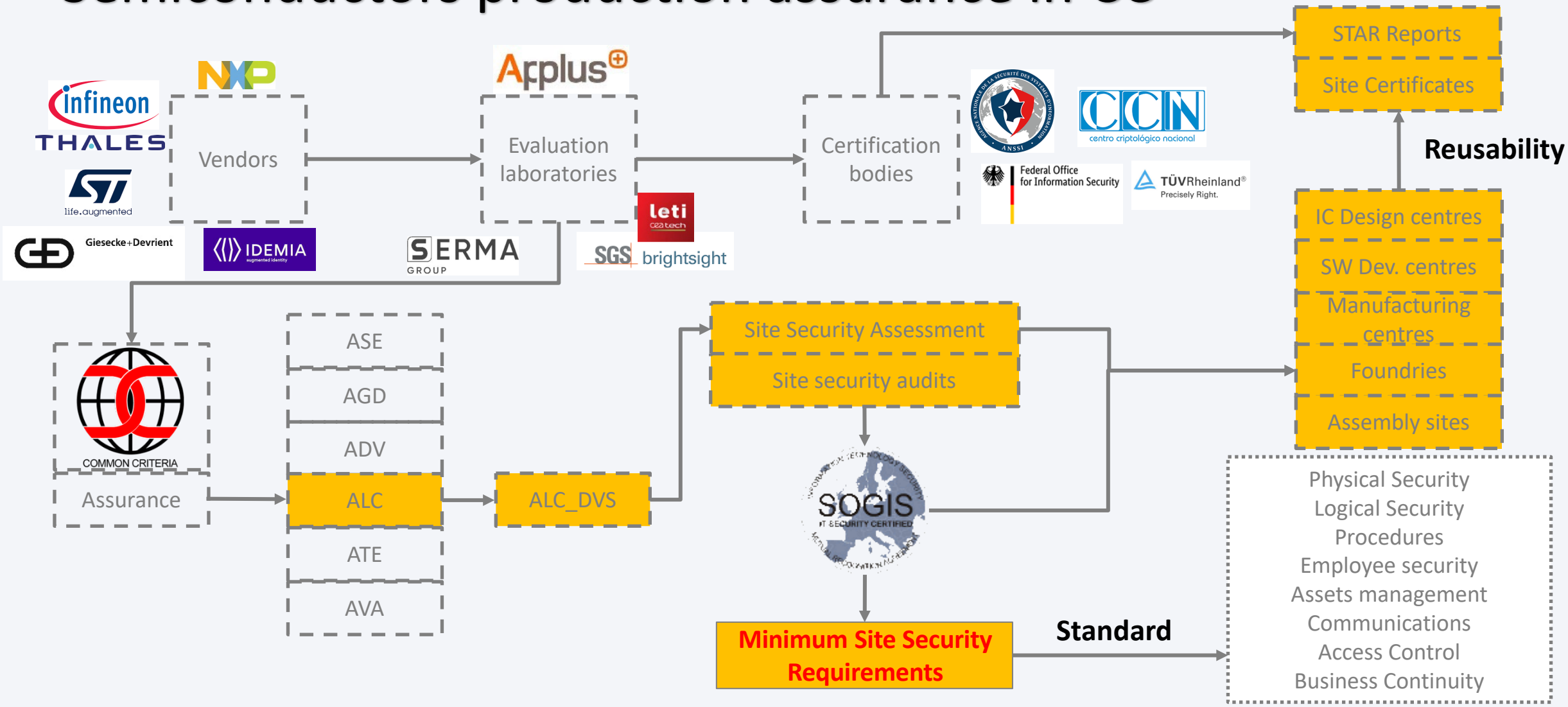
- Huge share of EU vendors
- Decision making in all critical aspects of the device
- **Decision making and talent are based in EU**
- **EU countries are leaders and pioneers in IC industry**

- Fabs/SATs perform:
  - Manufacturing
  - Packaging
  - Finishing and execution of volume testing
- Pre-personalization usually performed in SATs at large-volume scale

- Mostly outside EU (Asia)
- Manufacture ICs designed mainly in EU
- Run test & QA programs designed at EU with no decision making
- Requires specialized equipment and facilities

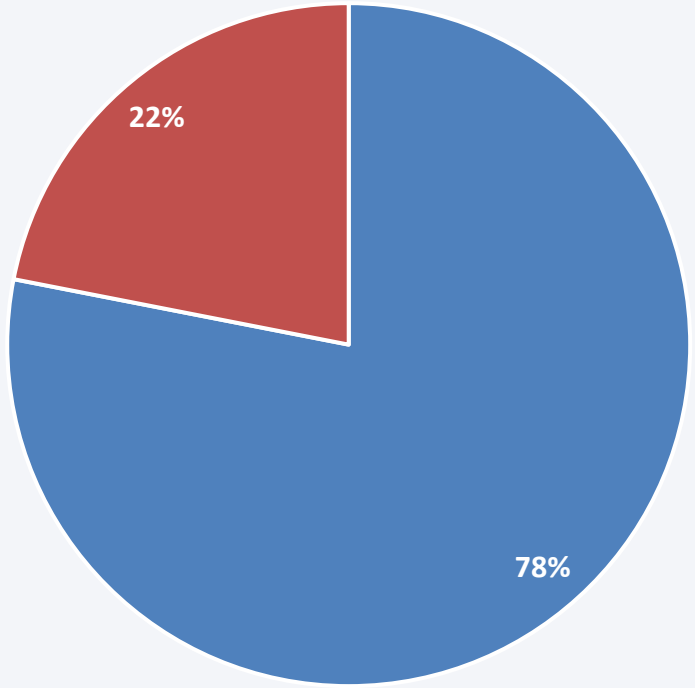
- **EU has the tradition and talent but lacks manufacturing centers to control the full production loop**

Semiconductors production assurance in CC

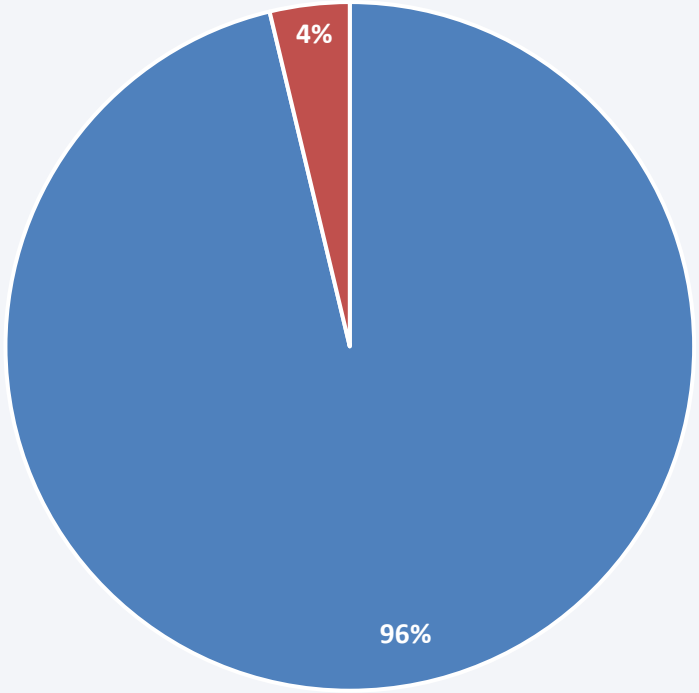


Security ICs evaluation share in EU (5 years - CC)

Vendors of certified Security ICs



Security IC evaluations in Europe



Lifecycle assessment in certifications without high assurance

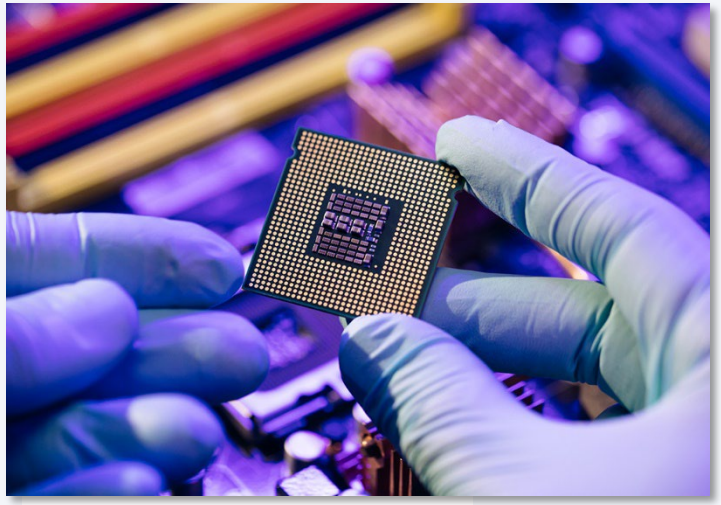
Security certifications without High assurance needs	Lifecycle security assessment
Swift and cost-effective. Useful when no high security needs. Suitable for consumer IoT and general-purpose devices.	Security in development and production is not addressed. Lack of control on development and production environments could result in: • Sensitive information leaks. • Introduction of vulnerabilities

- ETSI EN 303 645
- FITCEM Basic
- CC/SESIP under EAL3
- EUCC below High

- There is no ad-hoc methodology addressing production and lifecycle security in certifications without high-assurance needs.
- Options to fill this gap:
  - Mandatory life cycle evaluation as a requirement to produce semiconductors undergoing security evaluations. (e.g. ISO/IEC 27001).
  - Ad-hoc lightweight standard that considers life cycle evaluation in a cost-effective way, supporting reusability
    - Currently being worked in FITCEM
- Solutions shouldn't affect cost and speed, and should support reusability.

Standards are ready to support EU semiconductors industry

- Horizontal standards (CC, EUCC, FITCEM) are ready to cover all sectorial domains that use semiconductors.
- Vertical standards such as SESIP (IoT platforms) and ETSI EN 303 645 (Consumer IoT) cannot not be taken as a to-go option for all sectorial domains.
- High assurance standards (CC, MSSR) already consider the whole lifecycle security, including manufacturing centers.
- Evaluations without high assurance needs, don't cover lifecycle and production security. It needs to be defined if it will be a requirement for the future market.



Common Criteria

ETSI EN 303 645 V2.1.1 (2020-06)

EUROPEAN STANDARD

SESIP

Industry is ready to support EU semiconductor production

EU vendors:

- Are semiconductors market leaders.
- Have a long tradition in semiconductors industry.
- Have massive talent and expertise in the field.

EU schemes and laboratories:

- Have almost whole world-market share in Security ICs.
- Have massive experience auditing manufacturing sites in the context of security evaluations.
- Have historically contributed to enhance security in non-EU manufacturers.

EU **standards, vendors, schemes and labs** will be a cornerstone in the transition to EU semiconductor manufacturing companies.

- They will greatly contribute to improve security, monitoring and regulation compliance in semiconductor production.
- They will support to create resilience to supply chain disruptions.

Contact

jtsec Beyond IT Security

Granada & Madrid – Spain

hello@jtsec.es

@jtsecES

www.jtsec.es

"Any fool can make something complicated. It takes a genius to make it simple."
Woody Guthrie