
jtsec
BEYOND IT SECURITY
Cybersecurity certification
for European market

José Ruiz Gualda

jtsec Beyond IT Security

jruiz@jtsec.es

- Computer Engineer (University of Granada)
- Expert in Common Criteria, LINCE and FIPS 140-3
- Member of the SCCG (Stakeholder Cybersecurity Certification Group) at the European Commission.
- Editor of LINCE as UNE standard
- Editor in JTC13 WG3 of the FITCEM Methodology
- European Commission editor for the ERNCIP group "IACS Cybersecurity Certification".

jtsec Beyond IT Security

Cybersecurity Company providing evaluation and consultancy services in different technical domains (Smart Cards, Hardware and Software)

Developers of unique tools for Common Criteria (CCToolbox) and LINCE (LINCEToolbox)

Actively involved in standardization activities (ISO, CEN/CENELEC, ISCI WGs, ENISA CSA WGs, CCUF, CMUF, ERNCIP, …)

Members of the SCCG (Stakeholder Cybersecurity Certification Group)

Speakers at different events in the sector such as ICCC, ICMC, CCN-CERT, EUCA or ENISE).

First LINCE laboratory accredited by CCN (Spanish Certification Body).

We are now part of Applus Laboratories

ABOUT APPLUS+ LABORATORIES

ASIA

Our facilities in Asia

2 Labs (Shangai & Seoul)

4 Sales and Technical Services

Some of our Asian customers

CyberSecurity MALAYSIA
An agency under MOSTI

winbond

Lenovo

HUAWEI

>500
Technical professionals
专业技术人员

18.000
Sqm of testing facilities
测试实验室占地面积

2005
Since established
成立时间

accredited
by major international organisations 收获主要国际认证

Our brands

Applus laboratories

Applus RA RELIABLE ANALYSIS

Applus CFI

INDEX

INDEX

Introduction

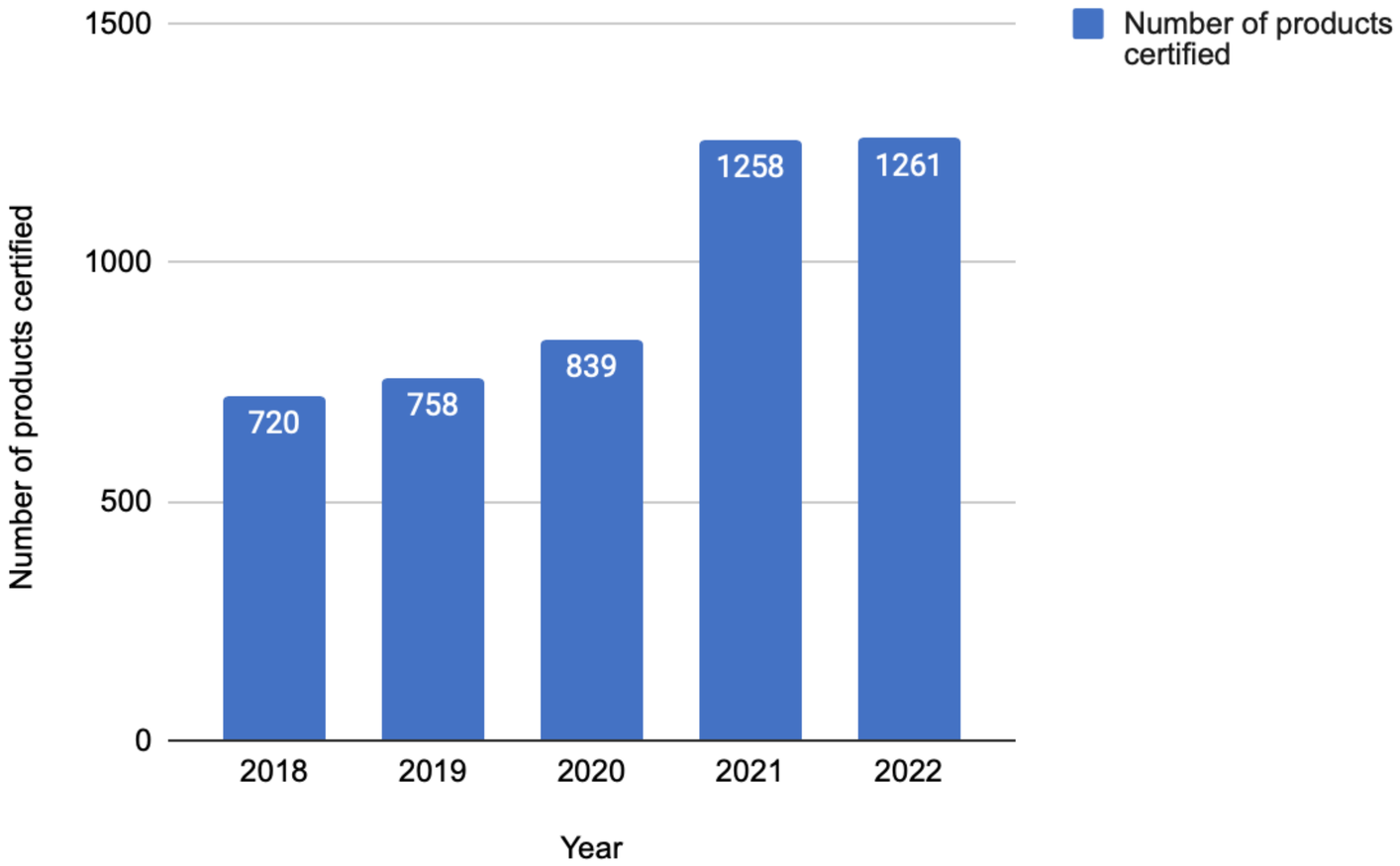
The market is not only Common Criteria. It's much bigger

Bundesamt
für Sicherheit in der
Informationstechnik

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

Introduction

Number of products certified in the last 5 years



INDEX

Certification schemes & methodologies

ICT Products (Common Criteria)

Common Criteria
An international standard (ISO/IEC 15408) published in 1994 and the most recognized certification used for assessing security in ICT products.

- Scope: International (more than 30 countries)
- Validity of the certificate: 5 years

Certification schemes & methodologies

ICT Products (Fixed-time)

LINCE
Is an evaluation and certification methodology for ICT security products developed by the Spanish Certification Body (CCN).

- Scope: Spain
- Validity of the certificate: 5 years

CSPN
Developed by ANSSI, certifies the robustness of a technological product, based on a conformity analysis and intrusion tests carried out by a CESTI.

- Scope: France
- Validity of the certificate: 5 years

Certification schemes & methodologies

ICT Products (Fixed-time)

BSZ

Is based on predictable evaluation times and ensures a reasonable level of expenditure for product. The evaluation follows a risk-driven approach that establishes a high level of trust in the security statements.

- Scope: Germany
- Validity of the certificate: 2 years

Bundesamt für Sicherheit in der Informationstechnik

BSPA

Is requested for Dutch government agencies as well as product manufacturers that want to get a security-specific certificate for their products.

- Scope: The Netherlands
- Validity of the certificate: 3 years

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

Certification schemes & methodologies

ICT Products (IOT Platforms)

SESIP
Provides a common and optimized approach for evaluating the security of connected products that meets the specific compliance, security, privacy and scalability challenges of the evolving IoT ecosystem.

- Scope: International
- Validity of the certificate: 2 years

PSA
Provides standardized resources to help resolve the growing fragmentation of IoT requirements and ensure security is no longer a barrier to product development.

- Scope: International
- Validity of the certificate: N/E

GP TEE
Defines an open security architecture for consumer and connected devices using a TEE to secure devices, enabling development & deployment of secure services.

- Scope: International
- Validity of the certificate: User fixes the period for the re-assessment.

SESIP™

psacertified™

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Certification schemes & methodologies

ICT Products (IOT)

ioXt

The program measures a product against each of the eight ioXt principles with clear guidelines to quantify the appropriate level of security required for a specific product

- Scope: International
- Validity of the certificate: N/E

CSA

Ignites creativity and collaboration in the IoT by developing, evolving and promoting universal open standards that enable all objects to securely connect and interact.

- Scope: International
- Validity of the certificate: Valid for the useful life of the product.

Certification schemes & methodologies

ICT Products (IOT Labels)

Germany
The IT Security Label creates transparency for consumers, revealing basic security features of IT products.

- Scope: Germany
- Validity of the certificate: 2 years

Finland
Created by Traficom in 2020, the requirements of the Label are based on ETSI EN 303 645 and have been prioritized using the OWASP IoT TOP 10 Threat List (2018)development.

- Scope: Finland
- Validity of the certificate: N/E

Singapore
Smart devices are rated according to their levels of cybersecurity provisions. Enables consumers to identify products with better cybersecurity provisions and make informed decisions.

- Scope: Singapore
- Validity of the certificate: 3 years

Certification schemes & methodologies

ICT Products (Crypto)

FIPS 140-3
Developed by NIST defines the requirements to be satisfied by a crypto module in order to protect sensitive information.

- Scope: International
- Validity of the certificate: 5 years

Certification schemes & methodologies

ICT Products (Industrial, operational technology in automation & control systems)

IECEE - IEC 62443 4-1 & 4-2

These two standards provide detailed requirements for IACS products. throughout their lifecycle.

- Scope: International
- Validity of the certificate: Can vary depending on the certifying body and the specific program the organization adheres to.

ISA Secure

Certifies off-the-shelf products, systems & development practices. Certifications are developed and maintained by their membership

- Scope: International
- Validity of the certificate: can vary depending on the certifying body and the specific program the organization adheres to.

Certification schemes & methodologies

ICT Products (Transport)

MiFare
Based on various levels of the ISO/IEC 14443 Type A 13.56 MHz contactless smart card standard. It uses AES and DES/Triple-DES encryption standards, as well as an older proprietary encryption algorithm, Crypto-1.

- Scope: International
- Validity of the certificate: 5 years

FeliCa
Is an IC Card technology that supports the entire life cycle of IC cards including application dev, card issuance, personalization & daily operation.

- Scope: Hong Kong, Singapore, Japan, Indonesia, Macau, the Philippines and the United States
- Validity of the certificate: 10 years

Calypso
Ensures multi-sources of compatible products enabling the interoperability between some operators offering a ticketing system including evolutions toward mobile phones, account-based ticketing or public key infrastructure

- Scope: International
- Validity of the certificate: 7 years

Calypso

Certification schemes & methodologies

ICT Products (Identity & digital signature)

FIDO

The FIDO protocols use standard public key crypto techniques to provide stronger authentication and are designed from the ground up to protect user privacy

- Scope: International
- Validity of the certificate: No expiration

eIDAS

Set the standards and criteria for simple electronic signature, advanced electronic signature, qualified electronic signature, qualified certificates and online trust services.

- Scope: European Union
- Validity of the certificate: 5 years

Certification schemes & methodologies

ICT Products (Payment Cards)

Payment
Certifications from private companies focused on payment security playing crucial role due to the sensitive nature and potential risks.

- Scope: International
- Validity of the certificate: Depends

Certification schemes & methodologies

ICT Products (POI Categories)

PCI

Payment Terminals are evaluated using the PCI standard. Depending on the technology used we can find PCI-PTS, PCI-SPOC, PCI-MPOC, PCI-CPOC

- Scope: International
- Validity of the certificate: Depending on the version of the norm and the approval class of the product

Common. SECC

Covers POIs deployed at merchants in Germany and the UK. Requires that terminals are evaluated for security using Common Criteria (CC).

- Scope: Germany & UK
- Validity of the certificate: 6 years.

Certification schemes & methodologies

ICT Products (Mobility)

MDCert
Is a certification program under development by GSMA. It's based mainly on the ETSI TS 103732. It has potential implications for further developments under 5G, eIDAS 2 and eventually CRA

- Scope: International
- Validity of the certificate: N/E

APP Defense Alliance
It's primarily based on OWASP guidance and tools. The program is working since 2022 and its formalization in a scheme will follow later this 2023.

- Scope: International
- Validity of the certificate: N/E.

GSMA™

App Defense Alliance

Certification schemes & methodologies

ICT Products (5G)

NESAS

The purpose of the scheme is to audit and test network equipment vendors, and their products, against a security baseline. The scheme has been defined by industry experts through GSMA and 3GPP.

- Scope: International
- Validity of the certificate: 2 years

NESAS CCS-GI

This national certification scheme for 5G mobile network equipment allows equipment vendors to demonstrate compliance with required security features through an IT security certificate.

- Scope: Germany
- Validity of the certificate: 2,5 years.

GSMA™

INDEX

Overview of the main EU policies on cybersecurity

CSA (CyberSecurity Act)

Definition

Proposes the creation of a **common European framework for the certification of "cybersecure" ICT products and services.**

One of the main objectives of the Cybersecurity Act is to **increase the competitiveness** and growth of European companies. Key to this is the ability to issue **cybersecurity certificates recognized throughout Europe** for systems, processes and products while minimizing their cost.

The Cybersecurity Act aims to achieve this objective by creating a common European framework for the **development of common schemes for cybersecurity certification.**

The Cybersecurity Act or CSA sets out three levels of assurance **(basic, substantial and high)**

Level	What is tested?	Objective	Minimum assesstment
High	Compliance and robustness	Preserving sovereignty, protecting the citizen and industry from criminal organizations	Pentesting State-of-the-Art attacks
Substantial	Compliance and robustness	Prevent scalable attacks on medium/high cost devices	Absence of public vulnerabilities Compliance testing
Basic	Compliance	Prevent massive attacks on low-cost devices	Technical documentation review Self-assessment

Overview of the main EU policies on cybersecurity

URWP (Union Rolling Work Programme)

Definition

Created by the European Commission defines the priorities at European level in terms of cybersecurity certification. It is a document to be taken into account by manufacturers, Public Bodies and companies related to the cybersecurity certification sector.

The URWP contains a series of strategic lines of action, five to be precise, which focus on improving cybersecurity in the European Union as a whole, covering both the public and private sectors:

- International cooperation
- Standardization
- Risk management
- Security by design and security by default
- Consistency between schemes

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

Overview of the main EU policies on cybersecurity

CRA (Cyber Resilience Act)

Definition

The CRA is an initiative that **aims to ensure that vendors establish appropriate cybersecurity safeguards in the digital products** they sell. By establishing cybersecurity requirements before and after a product is marketed, the CRA will strengthen the security and resilience of the entire supply chain for the benefit of businesses and end consumers.

The main mission of the Cybersecurity Resilience Act is to **fill existing gaps in legislation by creating horizontal legislation defining European cybersecurity standards** for digital products and services, as currently EU product-specific legislation mostly covers security aspects and addresses cybersecurity only partially.

Requirements for manufacturers

- **Security by design and by default** for all products within the scope of the regulation.
- Cybersecurity requirements throughout the **life cycle** (before and after the product is placed on the market).
- **Vulnerability management** and (whenever possible) **security patching**.
- **Transparency of the supply chain** of hardware or software components.
- **Enumeration of software components.**
- **End-user information** on the cybersecurity level of the product.
- **Security reporting requirements** for each product.
- **Post-market security support requirements** (probably limited to a period of 5 years after commercialization).

Overview of the main EU policies on cybersecurity

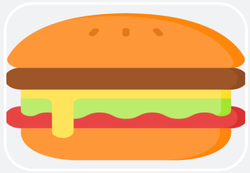
NIS2

Definition

The NIS2 directive will establish a set of requirements for the **cybersecurity risk management of critical entities**, in particular those related to **energy, health, transport and digital infrastructure.**

The directive aims at **eliminating divergences between the member states** regarding cybersecurity and reporting obligations to the public authority. To this end, it sets minimum standards and establishes **mechanisms for effective cooperation between the competent authorities** of each EU Member State. Provides for **heavy sanctions** to ensure enforcement

Sectors affected by NIS 2



Food

Manufacturers

Postal & Courier

Providers of electronic communications

Space

Public Administration

Digital Services

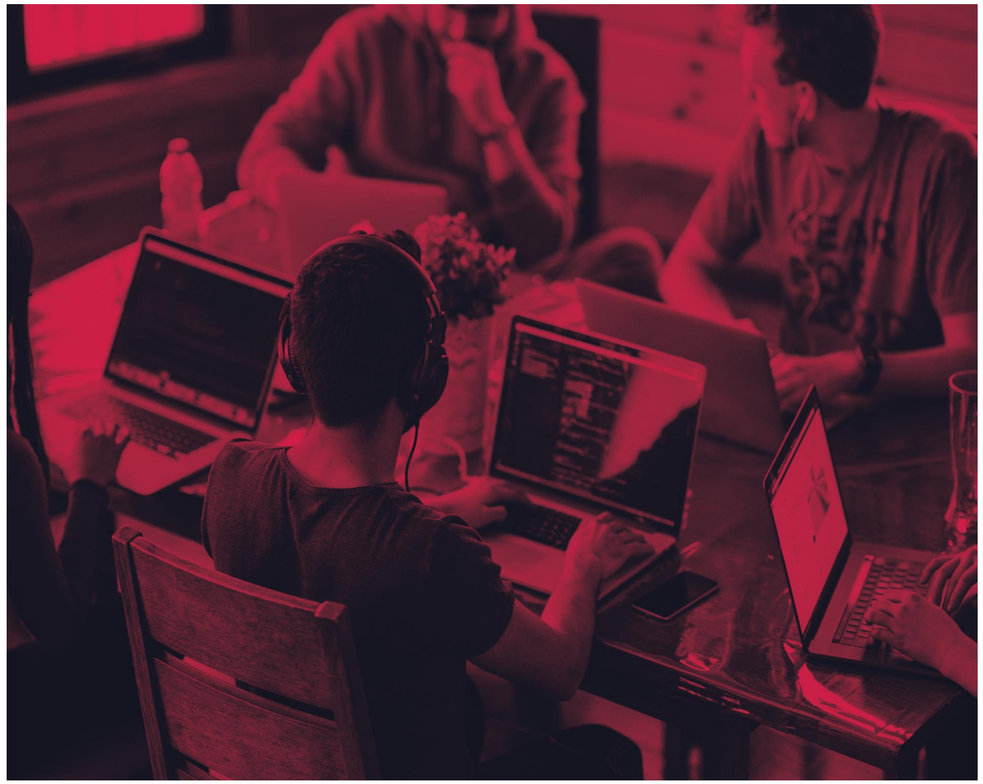
Waste water and waste management

NIS2 Directive

INDEX

Recommendations for the European Market

- Cybersecurity certification **requirements already in force (e.g. EIDAS)**
- Other **regulations will come in the following years (e.g. CRA).** This implies **mandatory requirements for manufacturer**s to be able to do business in Europe
- **Methodologies and schemes** developed in **Europe** will be used.
- **Prepare in advance** for the introduction on the European market. E.g. Patch management strategy or Cybersecurity by design takes time.
- Certifications involve both financial and personnel efforts for manufacturers. **These certifications are not simple to achieve.**
- **Stay up to date!** Follow standardization efforts! **Changes are coming!!**




jtsec
BEYOND IT SECURITY
Thank you