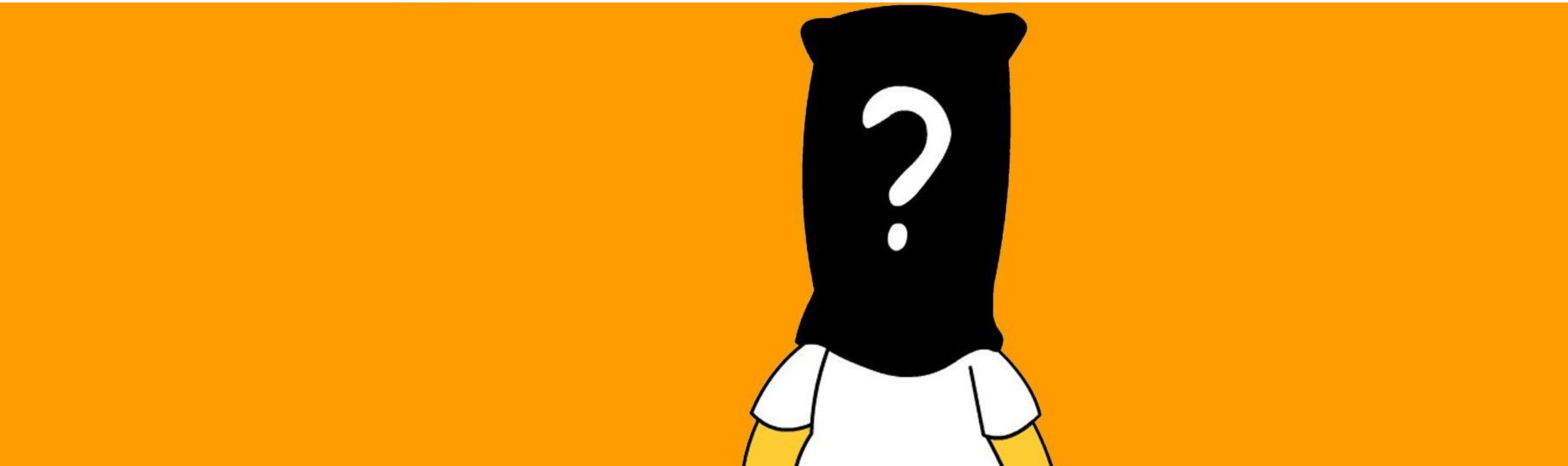
jtsec
BEYOND IT SECURITY

SPANISH CATALOGUE OF QUALIFIED PRODUCTS: A NEW WAY OF USING CC FOR PROCUREMENT

Index

- Who are we?
- Worldwide Procurement Initiatives
- Why a Product Catalogue?
- CPSTIC - Catalogue
- Conclusions

Who are we?



Who are we?

- Jose Ruiz – CTO at jtsec
- jtsec – CC and FIPS 140-2 Consultancy company - Based in Spain
- CCGEN Developers – Common Criteria Documentation Development tool
- More than 10 years of experience working with different labs and CBs as evaluator, lab manager and consultant

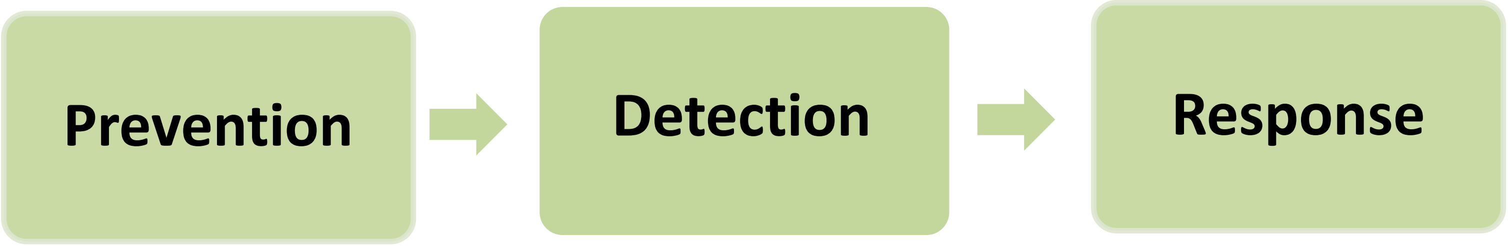
jtsec
BEYOND IT SECURITY

CCGEN
Create Common Criteria
compliant documentation
Simple and Easy

Why are we here?

- We support companies to meet their business expectations. e.g.- sales to governments
- We like initiatives that make life easier
- We think that could be useful for other countries
- My father wanted to visit Canada ;)

The importance of procurement as a prevention tool


Prevention → Detection → Response

Brand value
Reputation
Trustworthy
Integrity
Prestige
Image
Data leakage
Business
DoS

Worldwide Procurement Initiatives

Worldwide Procurement Initiatives

- US Government Requirements

  - ✓ CC is mandatory for all IT products with security features that are deployed in U.S. National Security Systems (NSS)
    - ✓ Products are to be selected from the NIAP PCL, meaning they have met a **NIAP approved Protection Profile**

  - ✓ DoD’s Information Network Approved Products List (DoDIN APL)
    - ✓ Common Criteria and very likely FIPS 140-2 validation are required

Worldwide Procurement Initiatives

- Australian Government Requirements

  ✓ CC is mandatory for all products providing security functions within all Australian Government systems, unless the risks of not using CC products has been appropriately accepted and documented.

  ✓ Products may be selected from the Australian Evaluated Products List (EPL) or the CC portal.

Worldwide Procurement Initiatives

- Canadian Government Requirements

  ✓ CC should be included as a requirement in Government of Canada RFPs/contracts **whenever possible**.

  ✓ Certified products evaluated against the Protection Profile for a given technology class may be selected

Worldwide Procurement Initiatives

- French Government Requirements

  ✓ **Types of certification used for procurement**
  - ✓ Common Criteria Certification
  - ✓ First Level Security Certification – CSPN

  ✓ **Acquisition Policy**:
  - ✓ CSPN for elementary qualification
  - ✓ EAL3+VAN.3+FLR.3 for standard qualification or
  - ✓ EAL4+VAN.5 +IMP.2+ DVS.2+FLR.3 for reinforced qualification

Worldwide Procurement Initiatives

- UK Government Requirements

  ✓ **Types of certification used for procurement**

  - ✓ Common Criteria Certification
  - ✓ Commercial Product Assurance - CPA

  ✓ **CPA:** A security product that passes assessment is awarded Foundation Grade certification - demonstrate good commercial security practice and suitable for lower threat environments.

  ✓ **Should we just use CC?** Ideally, yes

  - x CC does not always represent a necessary or sufficient level of product assurance for the UK public.

¿Why a product catalogue?

Legislation - IT Security products - ENS

- Legal framework
  - ✓ RD 03/2010, 8th January
  - ✓ RD 951/2015, 23rd October by modification of RD 3/2010 -> ENS – National Security Scheme

- Objective:
  - ✓ To establish basic principles and minimum requirements for the protection of information

- Scope of application
  - ✓ Public administration

Legislation - IT Security products - ENS

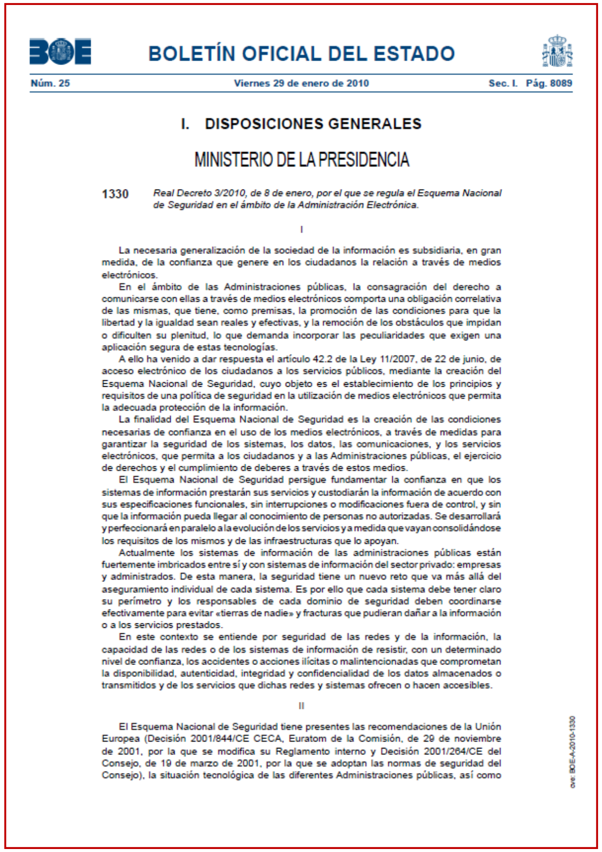
- Information protection. Security dimensions:
  - ✓ Confidentiality
  - ✓ Integrity
  - ✓ Availability
  - ✓ Traceability
  - ✓ Authenticity

- System category:
  - ✓ High
  - ✓ Medium
  - ✓ Basic

Legislation - IT Security products - ENS

- Current situation:

RD 951/2015 of 23rd October, amending RD 3/2010 regulating the ENS in the field of Electronic Administration, ART. 18: “for the procurement of information and communication technology security products to be used by public administrations, those that have **certified the security functions** related to the object of their procurement shall be used in a manner **proportionate to the category of the system** and the level of security identified…”



BOLETÍN OFICIAL DEL ESTADO

Núm. 25 Viernes 29 de enero de 2010 Sec. I. Pág. 8089

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

1330 *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*

I

La necesaria generalización de la sociedad de la información es subsidiaria, en gran medida, de la confianza que genere en los ciudadanos la relación a través de medios electrónicos.

En el ámbito de las Administraciones públicas, la consagración del derecho a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas, que tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

A ello ha venido a dar respuesta el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, mediante la creación del Esquema Nacional de Seguridad, cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Esquema Nacional de Seguridad persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. Se desarrollará y perfeccionará en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que lo apoyan.

Actualmente los sistemas de información de las administraciones públicas están fuertemente imbricados entre sí y con sistemas de información del sector privado: empresas y administrados. De esta manera, la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Es por ello que cada sistema debe tener claro su perímetro y los responsables de cada dominio de seguridad deben coordinarse efectivamente para evitar «tierras de nadie» y fracturas que pudieran dañar a la información o a los servicios prestados.

En este contexto se entiende por seguridad de las redes y de la información, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

II

El Esquema Nacional de Seguridad tiene presentes las recomendaciones de la Unión Europea (Decisión 2001/844/CE CECA, Euratom de la Comisión, de 29 de noviembre de 2001, por la que se modifica su Reglamento interno y Decisión 2001/264/CE del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo), la situación tecnológica de las diferentes Administraciones públicas, así como

cve: BOE-A-2010-1330

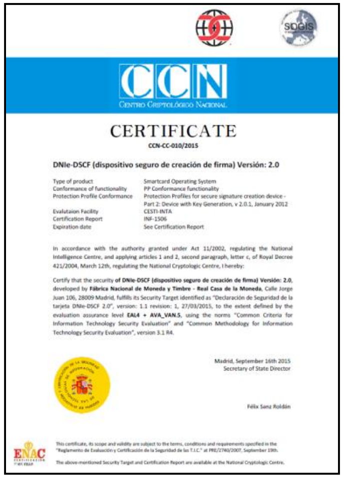
Legislation - IT Security products - ENS

- Moreover, for “High” products category in the ENS:

“**RD 03/2010** of 8th January, regulated by the National Security Scheme (ENS) in the field of electronic administration. Annex 2. section 4.1.5 Certified components: Products or equipment whose safety features and level have been assessed **in accordance to European or International standards** and which are certified by **independent bodies** of recognised standing shall preferably be used. “

Why is not CC the answer?

- What does it mean that a product is certified?
  - ✓ The product has been evaluated taking into account the SFRs and SARs defined in the Security Target
- Who performs the Security Target?
  - ✓ The manufacturer


CENTRO CRIPTOLÓGICO NACIONAL

CERTIFICATE

CCN-CC-010/2015

DNIe-DSCF (dispositivo seguro de creación de firma) Versión: 2.0

Type of product	Smartcard Operating System
Conformance of functionality	PP Conformance functionality
Protection Profile Conformance	Protection Profiles for secure signature creation device - Part 2: Device with Key Generation, v 2.0.1, January 2012
Evalutaion Facility	CESTI-INTA
Certification Report	INF-1506
Expiration date	See Certification Report

In accordance with the authority granted under Act 11/2002, regulating the National Intelligence Centre, and applying articles 1 and 2, second paragraph, letter c, of Royal Decree 421/2004, March 12th, regulating the National Cryptologic Centre, I hereby:

Certify that the security **of DNIe-DSCF (dispositivo seguro de creación de firma) Versión: 2.0**, developed by **Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda**, Calle Jorge Juan 106, 28009 Madrid, fulfills its Security Target identified as "Declaración de Seguridad de la tarjeta DNIe-DSCF 2.0", version: 1.1 revision: 1, 27/03/2015, to the extent defined by the evaluation assurance level **EAL4 + AVA_VAN.5**, using the norms "Common Criteria for Information Technology Security Evaluation" and "Common Methodology for Information Technology Security Evaluation", version 3.1 R4.

Madrid, September 16th 2015
Secretary of State Director

Félix Sanz Roldán

ENAC CERTIFICACIÓN

This certificate, its scope and validity are subject to the terms, conditions and requirements specified in the "Reglamento de Evaluación y Certificación de la Seguridad de las T.I.C." at PRE/2740/2007, September 19th.

The above-mentioned Security Target and Certification Report are available at the National Cryptologic Centre.

Why a product catalogue?

- Certified product → Qualified for use in administration?

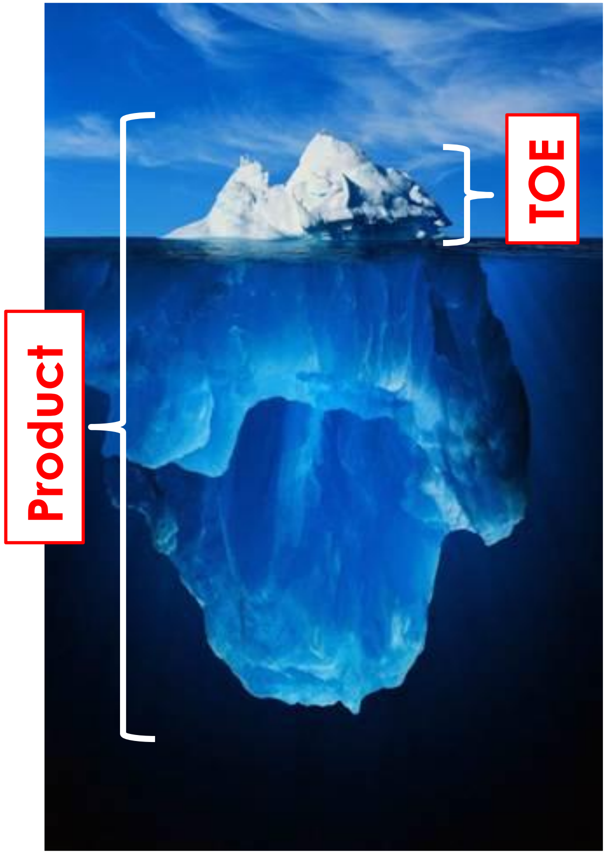
- Only it is suitable if:
  - ✓ The Security Target is complete, consistent and technically accurate.

WARNING:
The ST is performed by the manufacturer!

The CPSTIC. For what?

- Certified product ➡ Qualified for use in administration?

- Only it is suitable if:
  - ✓ The TOE involves the main security functionality of the product.
  - ✓ Unfortunately, sometimes this is not the case



The CPSTIC. For what?

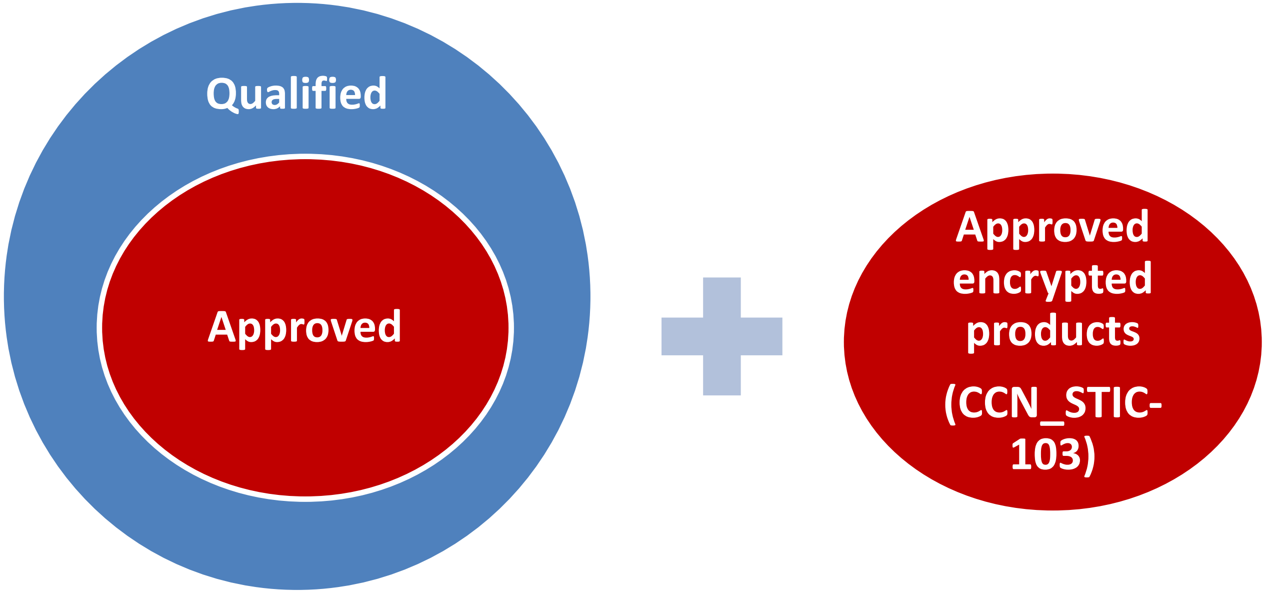
- **Corollary: In order to be able to check if one product is adequately certified, the government agency must have the capacity to:**
  - ✓ Require product certification
  - ✓ Check that the ST is technically suitable
  - ✓ Check that it is complete

A catalogue will ease this task.

The CPSTIC

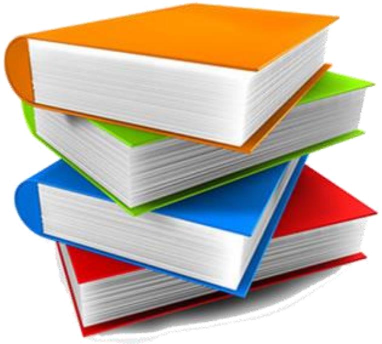
The CPSTIC

- The CPSTIC is the reference catalogue for the acquisition of IT products in public organisms affected by the National Security Scheme (ENS).
- **Scope:**
  - ✓ Qualified products. Sensitive information
  - ✓ Approved products. Classified information



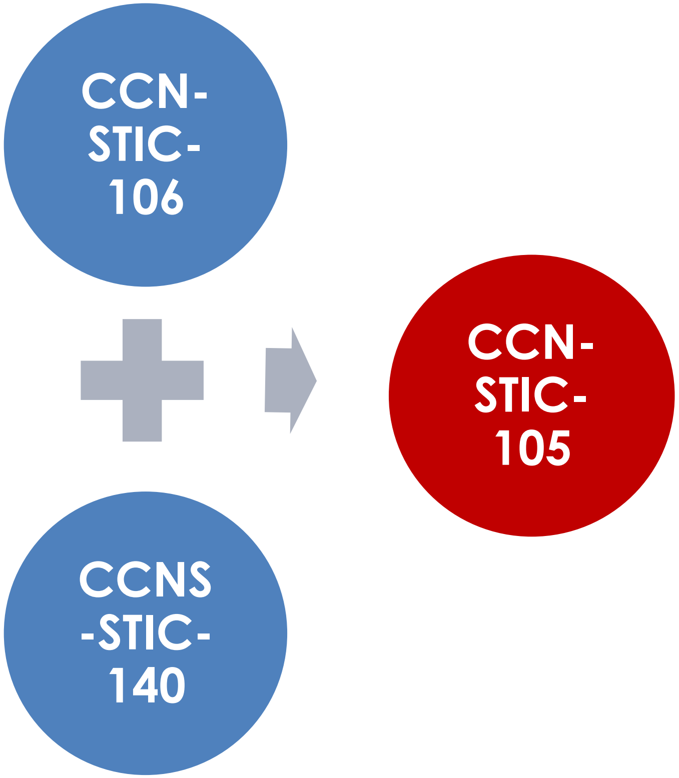
The CPSTIC

- **Scope:**
  - ✓ Which products are suitable to be included?
    - ✓ The products that implement security functionalities in a system in an active manner



The CPSTIC

- **Related legislation:**



✓ CCN-STIC-106. Inclusion procedure of IT products qualified in the CPSTIC

✓ CCN-STIC-140. Reference taxonomies for IT security products

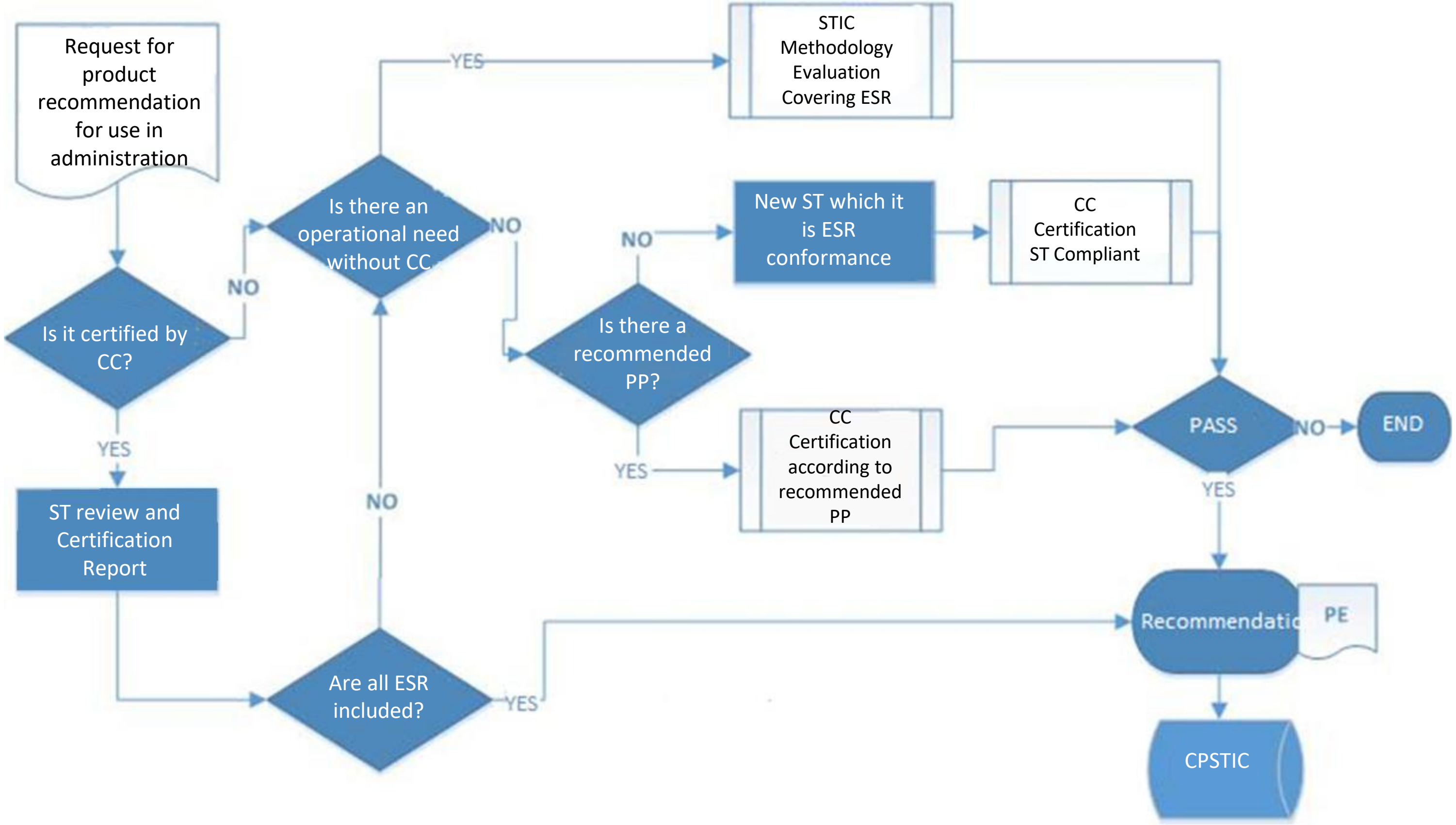
✓ CCN-STIC-105. CPSTIC

The CPSTIC

- **CCN-STIC-106. Inclusion requirements:**
  - ✓ Common Criteria certified products. Low EAL level required. The Security Target shall be checked for compliance with the SFR.
  - ✓ If you do not have Common Criteria certification, an accredited laboratory will perform the evaluation.
- **CC certification may not be required where:**
  - ✓ The product is promoted by the Administration.
  - ✓ It has a strategic interest.
  - ✓ There are no substitute products on the market.
  - ✓ A **STIC evaluation** could be applied.

The CPSTIC

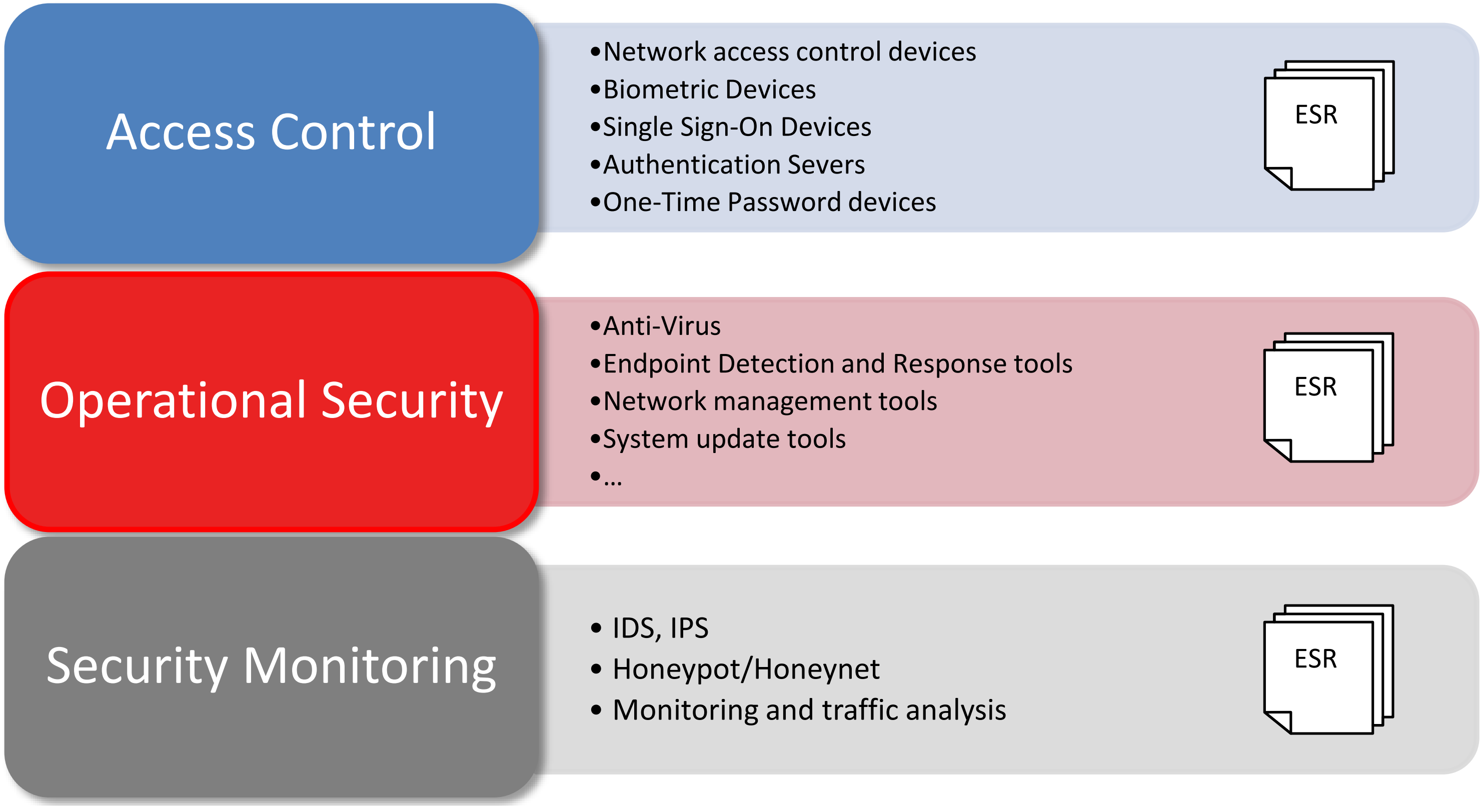
- **Inclusion procedure in the catalogue**



Request for product recommendation for use in administration
Is it certified by CC?
NO
YES
ST review and Certification Report
Is there an operational need without CC
YES
NO
NO
Are all ESR included?
YES
STIC Methodology Evaluation Covering ESR
NO
New ST which it is ESR conformance
CC Certification ST Compliant
Is there a recommended PP?
YES
CC Certification according to recommended PP
PASS
NO
END
YES
Recommendatio
PE
CPSTIC

The CPSTIC - Taxonomy

- **CCN-STIC-140.** Reference taxonomy. Two levels: Category/Family. There are 6 categories and 33 families**.** Example:



Access Control

- Network access control devices
- Biometric Devices
- Single Sign-On Devices
- Authentication Severs
- One-Time Password devices

ESR

Operational Security

- Anti-Virus
- Endpoint Detection and Response tools
- Network management tools
- System update tools
- …

ESR

Security Monitoring

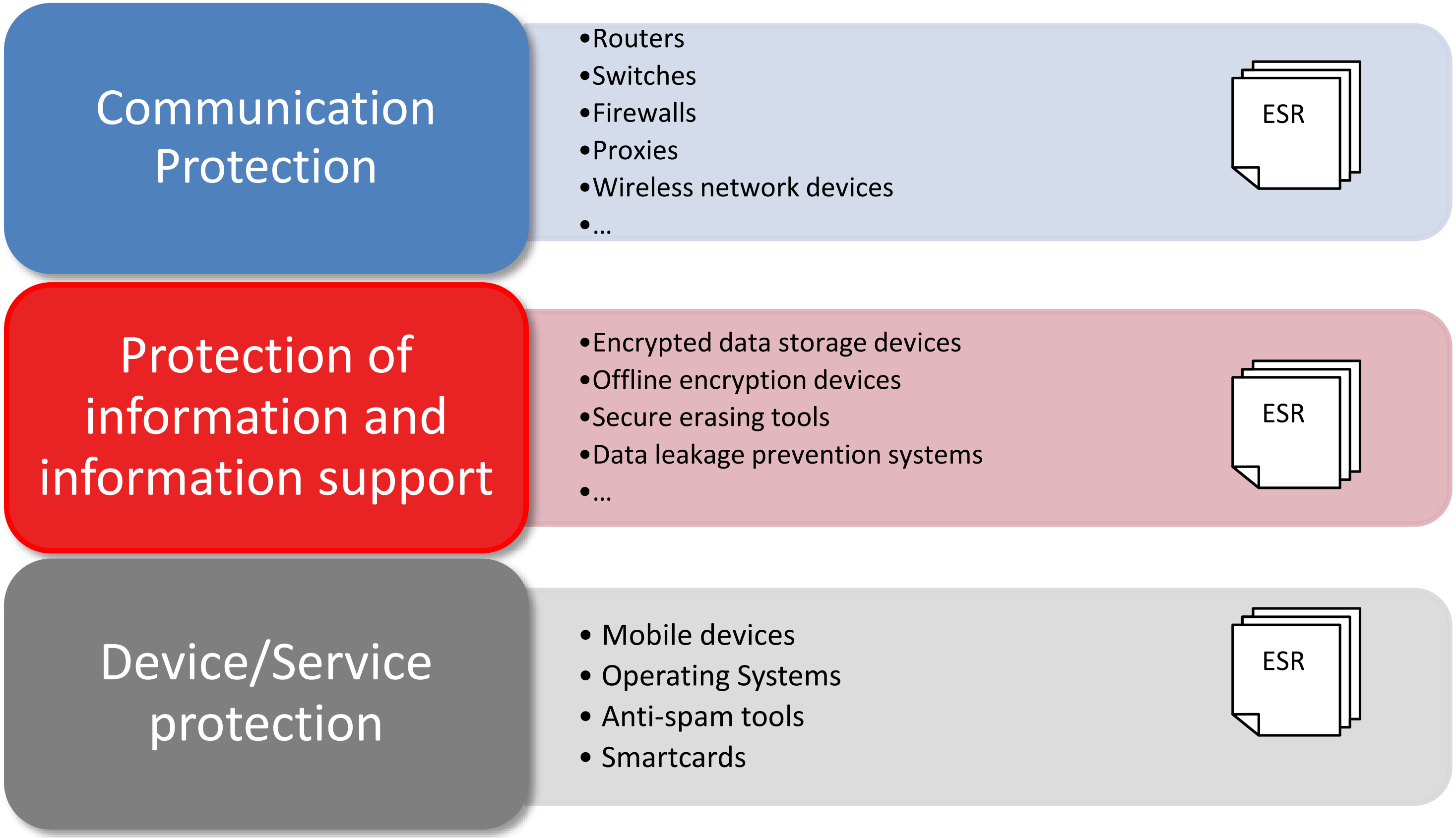
- IDS, IPS
- Honeypot/Honeynet
- Monitoring and traffic analysis

ESR

- For each family, Mandatory Security Requirements have been defined.

The CPSTIC - Taxonomy

- **CCN-STIC-140:** Example:



Communication Protection

- Routers
- Switches
- Firewalls
- Proxies
- Wireless network devices
- …

ESR

Protection of information and information support

- Encrypted data storage devices
- Offline encryption devices
- Secure erasing tools
- Data leakage prevention systems
- …

ESR

Device/Service protection

- Mobile devices
- Operating Systems
- Anti-spam tools
- Smartcards

ESR

The CPSTIC – Family Description

- **Requirements for each family:**
  - ✓ Product family description:
    - ✓ Functionality
    - ✓ Usage case
    - ✓ Device’s scope
    - ✓ CC evaluation requirements
  - ✓ Threats analysis
    - ✓ Environmental hypothesis
    - ✓ Assets
    - ✓ Threats
  - ✓ Mandatory Security Requirements (MSR)

The CPSTIC. Example - Firewall

- "Firewall" family from "Communication Protection" category. Options provided by the catalog:
  - ✓ Evaluation according to the protection profiles internationally defined for this type of product.
  - ✓ Evaluation with EAL2 evaluation level or higher including the SFRs listed in the Protection Profiles
  - ✓ CCRA certificates are recognized (obviously)
    - ✓ YOU CAN BE LISTED IN THE CATALOGUE!!!

The CPSTIC. Example – Secure Erase Tools

- "Secure Erasure Tools" family from "Information Protection and Information Media":
  - ✓ No protection profiles have been published for this family
  - ✓ The catalog includes the ESRs to be assessed during the evaluation
  - ✓ And the evaluation level required (e.g.EAL1)

The CPSTIC - Current status

CPSTIC first version published in Dic2017

If you need to consult it… Where can you find it?

- ✓ CCN-STIC-105 guide. STIC product catalogue (CPSTIC). (https://oc.ccn.cni.es/index.php/en/cis-product-catalogue)
  Periodically will be updated on CCN website

- ✓ Certification Body Web. (https://oc.ccn.cni.es)
  - ✓ 108 qualified products and 18 approved.
  - ✓ 18 different families.
  - ✓ 18 manufacturers.
  - ✓ Continuous growth!

Conclusions

Conclusions

- ❑ Procurement is a key tool for prevention of vulnerabilities
- ❑ There are multiple government initiatives worldwide
- ❑ Just Common Criteria is unfortunately not the answer
- ❑ The CPSTIC is an innovative and flexible mechanism to solve this issue
    - ❑ It is compatible with cPPs avoiding the delays and the cost of cPPs development
    - ❑ Allow other evaluation methodologies to be used and
    - ❑ Allow quick adoption of new technologies

Thank you!

jtsec: Beyond IT Security

c/ Abeto s/n Edificio CEG Oficina 2B
CP 18230 Granada – Atarfe – Spain
hello@jtsec.es

@jtsecES
www.jtsec.es

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

Annex 1. Summary of regulations and interest contacts

- ✓ For qualified products. (HIGH ENS).
- ✓ **CCN-STIC-105 guide.** Security Products Catalogue
- ✓ **CCN-STIC-140 guide.** Reference taxonomy for security products
- ✓ **CCN-STIC-106 guide.** Addition procedure of qualified security products in the CPSTIC.
  - ✓ Available in:
    - ✓ CCN-Cert site: https://www.ccn-cert.cni.es/guias.html
    - ✓ Certification Body site: https://oc.ccn.cni.es