



# A proposal for certificate validity

Certification Body - Spain.  
14th International Common Criteria Conference.

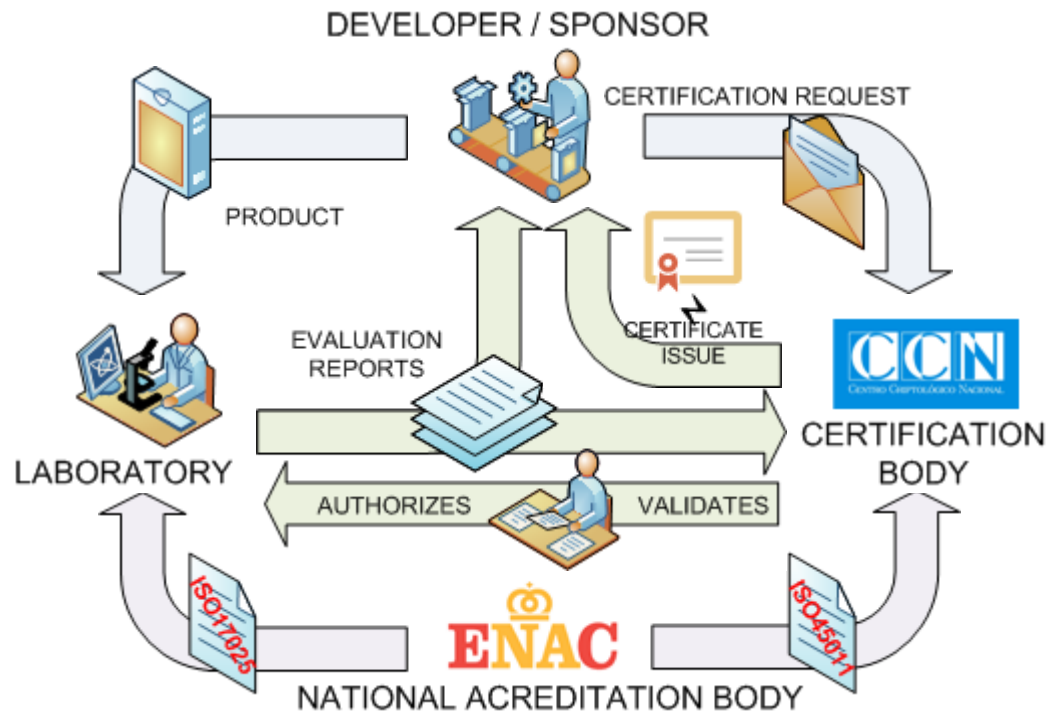
David Cerezo

# Outline

- After the certification
- The Spanish CB experience
- Studying a new certificate validity policy
- Several possible CB services

# The Certification Process

- ▶ Begins with a Sponsor willing to have his product certified...



- ▶ ...and finish with the issue of a certificate.

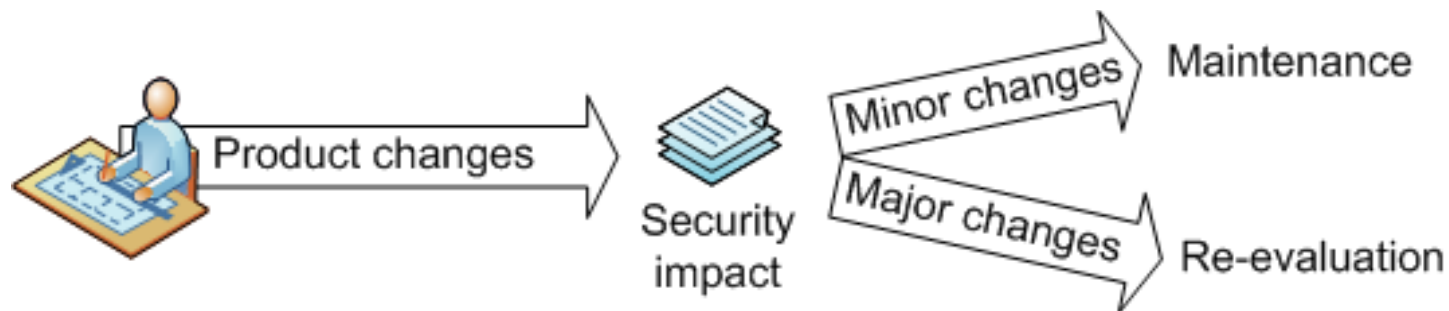
# After the issuance

- ▶ On the Arrangement:
  - ▶ *Certificate recognition and exceptions*
  - ▶ *Publication of certificate and report*
  - ▶ *Use of the CCRA logo*
- ▶ Supporting documents
  - ▶ *Assurance continuity*



# Assurance Continuity

- › Changes in the certified product



- › *Maintenance:*
  - › *Addendum to the certificate*
    - › *Publication of Maintenance Report*
- › *Re-evaluation*
  - › *New evaluation using results of previous evaluation*
    - › *New certificate (and Certificate Report)*

# Assurance Continuity (supplement)

- ▶ Another important point: the changes in the state of the art
  - ▶ *The risk of new vulnerabilities arising in each technology area increases with time*
  - ▶ *Maintaining information security assurance*
- ▶ It's a CB task to develop its own complete *Certificate Validity Policy*

# Spanish CB experience

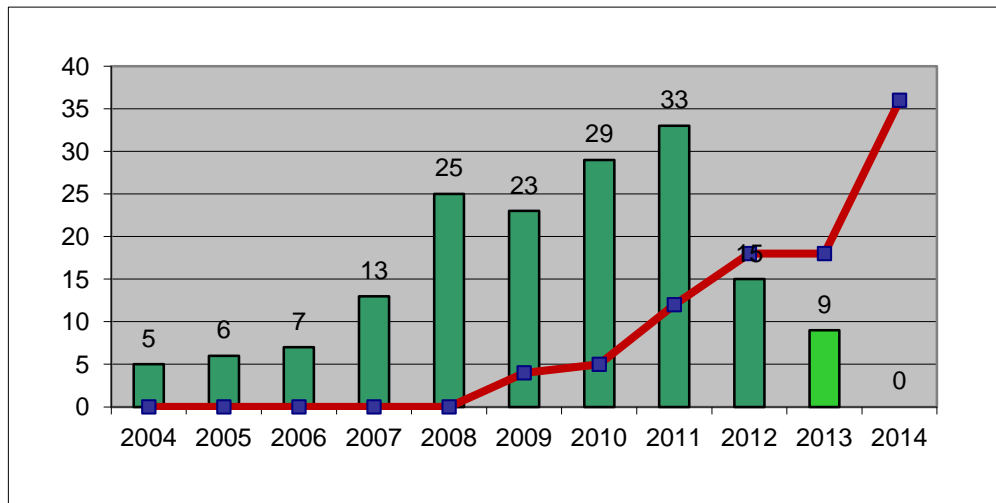


## ➤ Legislation

- *Presidential Order 2740/2007, September 19<sup>th</sup>:*
- *Regulation of the National Scheme for Evaluation and Certification on Information Technology Security*
  - *Certificates will never expire. It will remain valid if there is no change in the conditions that cause its issuance.*
  - *Every two years, the CB will open a new dossier to review the validity of the certificate.*
    - *Changes in technology or state of the art*

# Spanish CB experience

- Consequences
  - Administrative time consuming
  - Reviews made by certifiers not as deep as desired
  - Geometric progression of new reviews



*A change is mandatory!*

New Certifications + Maintenances vs Reviews of validity



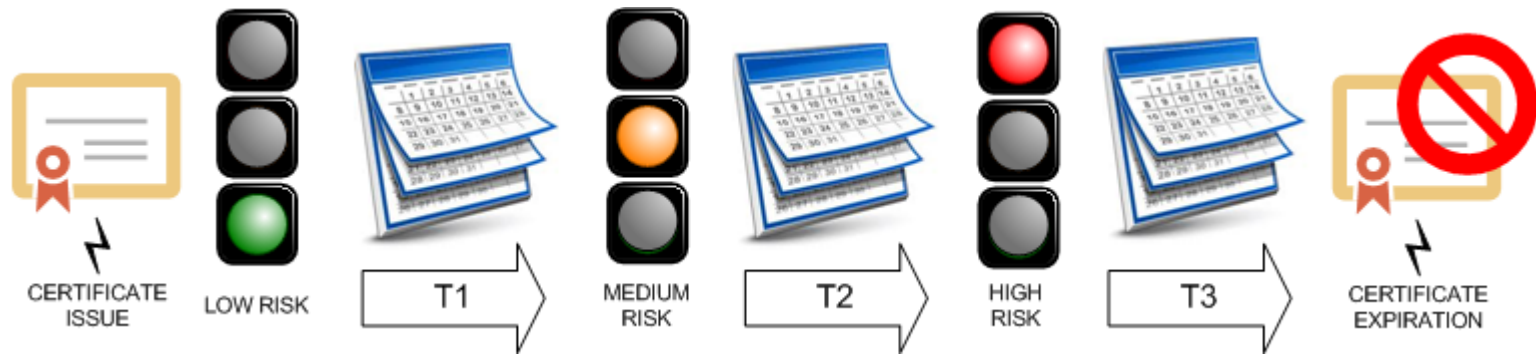
# Present Certificate Validity Policy

- ▶ Points to change
  - ▶ *A certificate cannot be valid forever. They get older to deal with the new security state of the art.*
  - ▶ *Customers should have an easy way to know the health of a certificate in order to plan their procurement.*
  - ▶ *The health of a certificate could be check to know if it keeps fit*
  - ▶ *Some vulnerabilities could appear that call the certificate into question.*

# New Certificate Validity Proposal

- ▶ Key points
  - ▶ *The certificates must have a period of validity*
  - ▶ *This period is divided into 3 risk levels for consuming the certificate (low, medium and high)*
  - ▶ *Reassessments can extend the period of validity (resetting it to low risk)*
  - ▶ *Known vulnerabilities will shorten that period (moving it to high risk)*

# Certificate period of validity

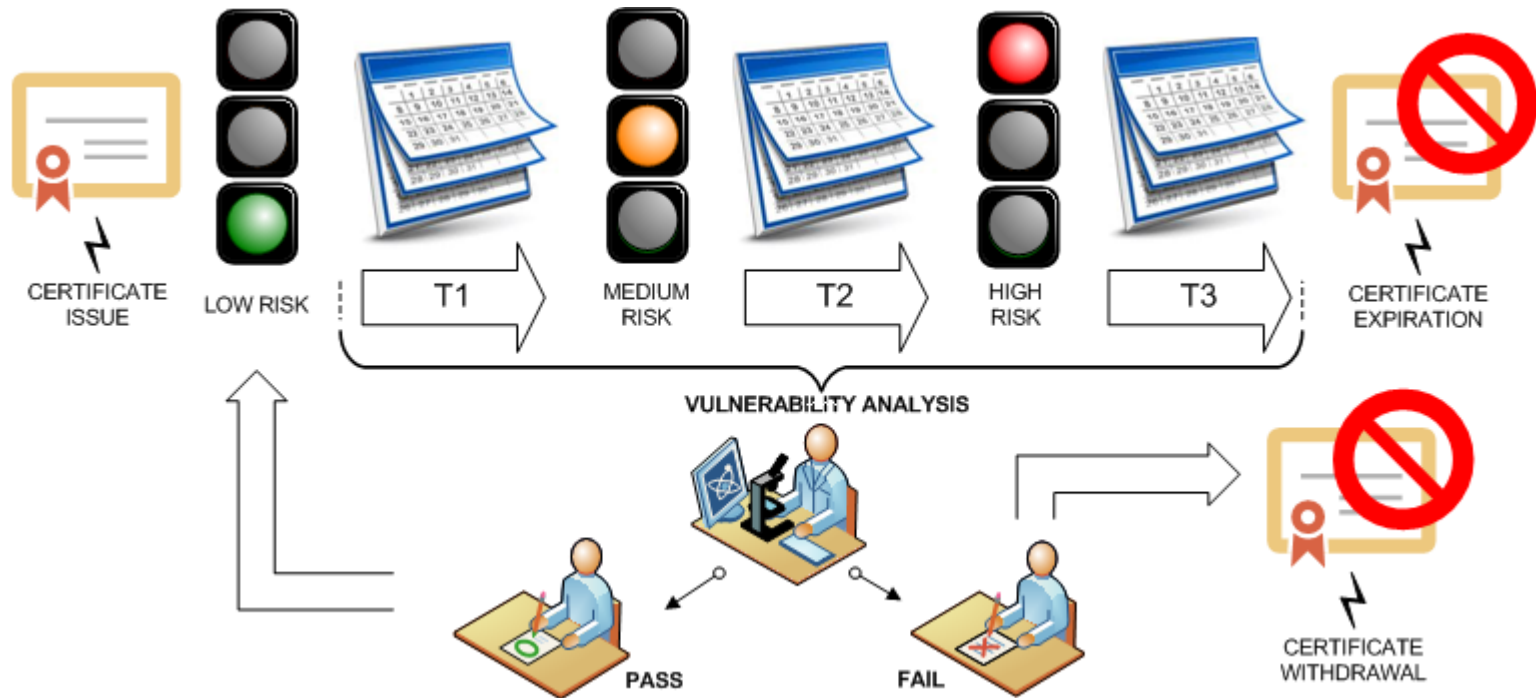


- ▶ **T1: Low risk**
  - ▶ *Probably resistant to the existing vulnerabilities*
- ▶ **T2: Medium risk**
  - ▶ *Could be affected by some new vulnerability*
- ▶ **T3: High risk**
  - ▶ *Not recommended, re-assessment needed*

# Certificate period of validity

- ▶ Time periods
  - ▶ *Could be defined different for different technologies*
    - ▶ The rate of appearance of new vulnerabilities is different between different technologies
  - ▶ *As a first approach they could be:*
    - ▶ T1: 3 years, T2: 2 years and T3: 1 year
- ▶ Limit of validity will end with zombie certificates
- ▶ On the web site it could be published the initial expiration date and its risk level

# Certificate Reassessment

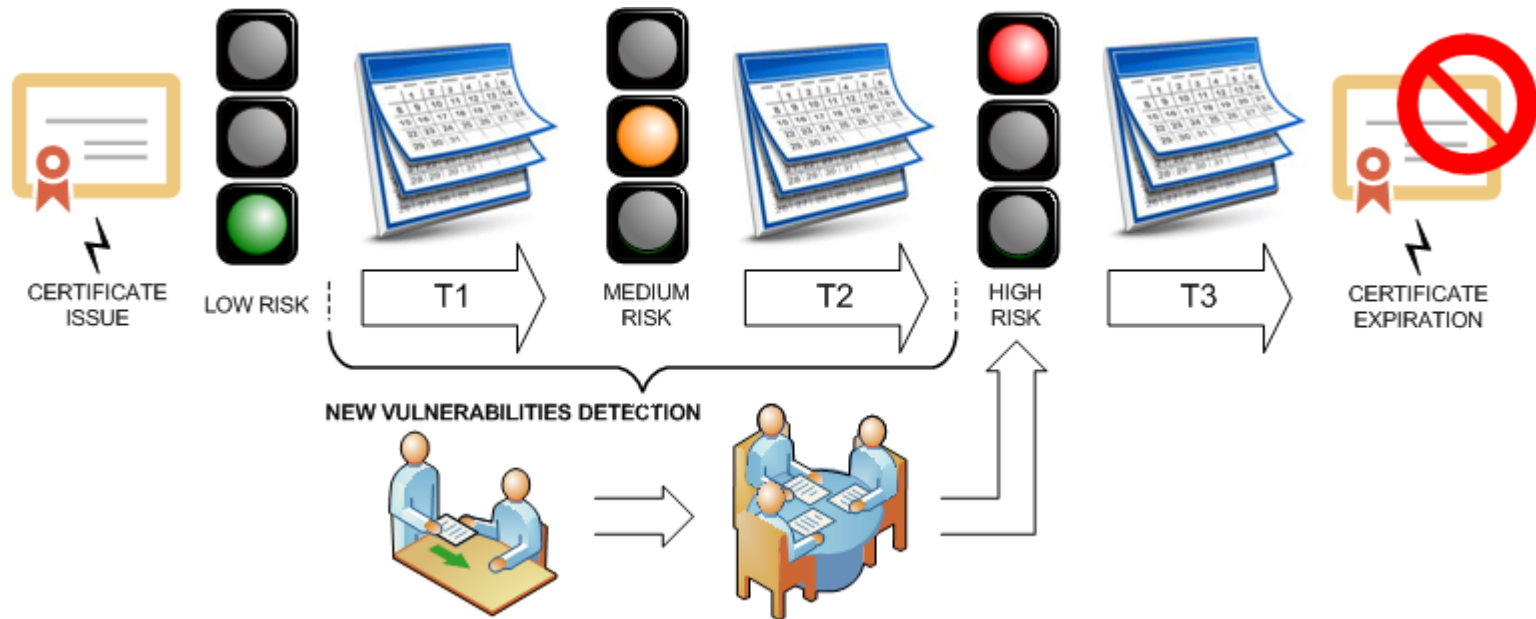


- ▶ Verification of the technical validity of AVA according to the state of the art and related to the scope of the ST.
- ▶ Before certificate expiration it is possible to reset the risk counter by passing a reassessment.

# Certificate Reassessment

- Is a CB service that have to be requested
- The Evaluation Facility will perform the vulnerability analysis
- At the end of a successful reassessment a report will be written and an addendum published on the web
- An unsuccessful reassessment will lead to the withdrawal of the certificate
- If an update of the product is presented solving its security problems it could follow the assurance continuity re-evaluation process

# New vulnerabilities



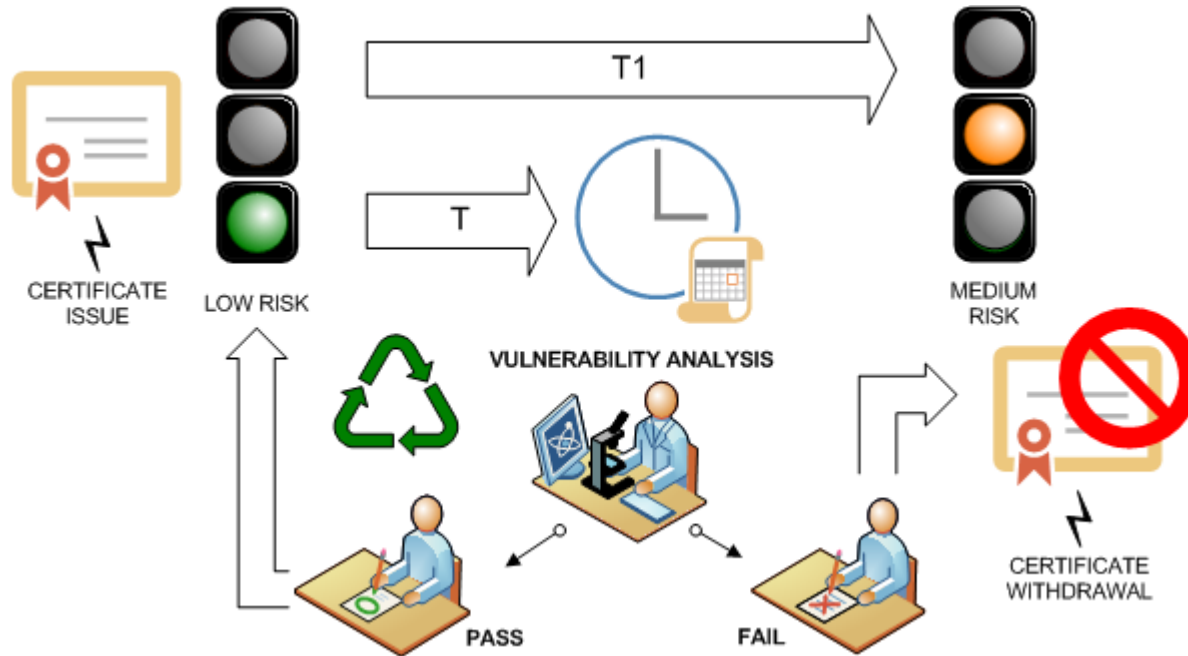
- ▶ During Low and Medium risk time new vulnerabilities could be discovered.
- ▶ If the vulnerability has high possibilities of affecting the certificate's validity it moves it to the high risk level.

# New vulnerabilities

- The discovery of new vulnerabilities could come from different sources:
  - *The CB on its day to day work*
  - *Communication from outside (evaluation facilities, other schemes...)*
- *A careful analysis is needed to forecast that a vulnerability could affect a product's security*
  - *Meeting with the lab to assess the impact*
  - *If it is the decision, inform the sponsor and change the risk status*



# Certificate Surveillance

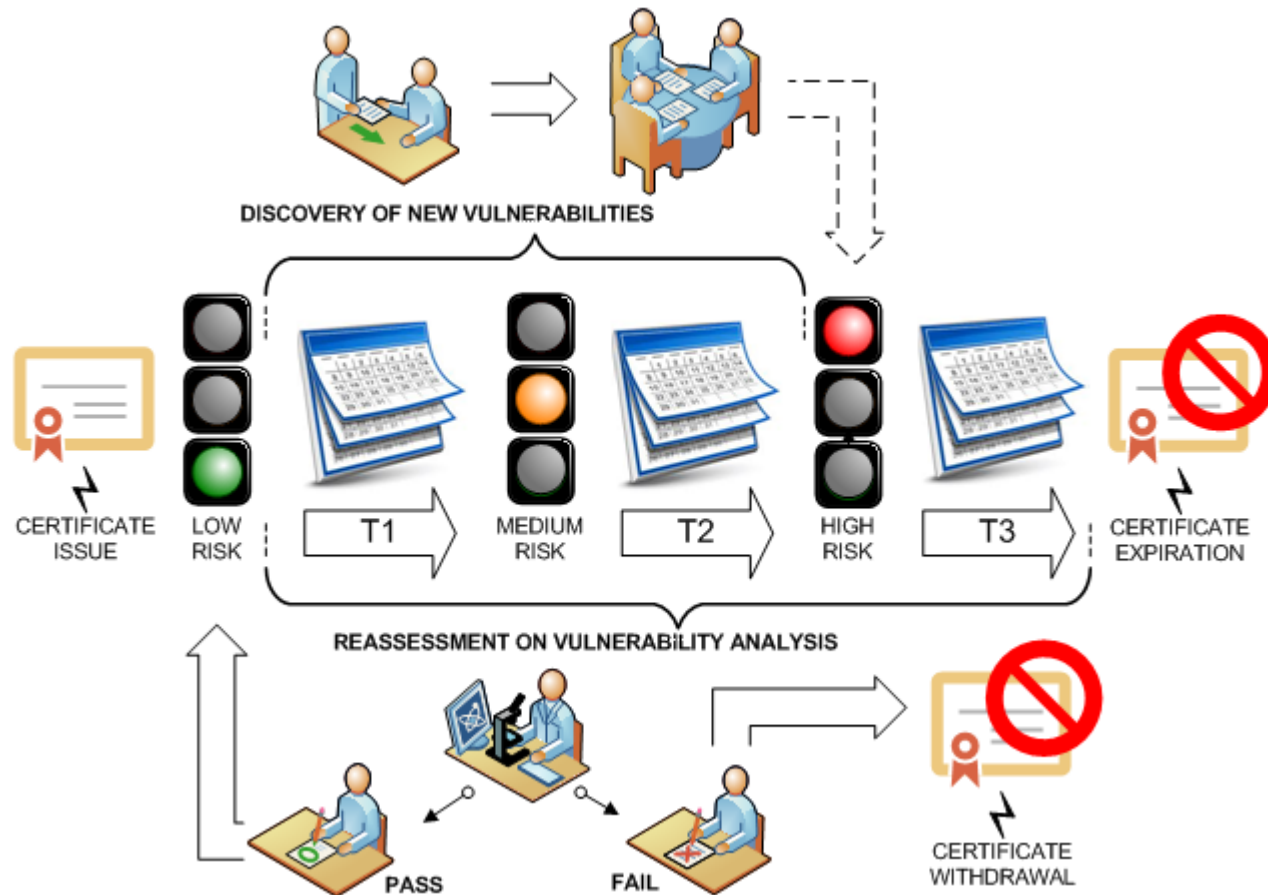


- Optional service for critical products
- Periodic reassessment intended to keep the certificate in a low risk level

# Certificate Surveillance

- It's also a CB service that have to be requested
- The evaluation facility in charge of the surveillance makes an active search for new vulnerabilities and attacks that could affect the product
- At the end of every successful reassessment a report will be written and an addendum published on the web
- On the web site, the certificate could have a special mark to show that it is under a surveillance service

# Assurance continuity II – Changes in the state of the art



# Assurance Continuity (the two aspects)

- ▶ How changes in the product affect the new proposal regarding the changes in the state of the art?
  - ▶ *Maintenance: Same certificate with addendum*
    - ▶ *Expiration date doesn't change*
  - ▶ *Re-evaluation: 2 certificates*
    - ▶ *New certificate has its new own expiration date*

# Certificate recognition

- › Every CB has its own and different certificate validity policy
- › And different services (reassessment, surveillance...) with different names
- › The CC portal recently moves to archive several certificates (expired, withdrawn or simply old?)
- › Confusing for customers
- › Makes difficulties for procurement
- › A harmonized certificate recognition validity is desired

# Conclusions

- The CBs must offer a better supervision of their certificates
- The risk levels and the rules to move between give life to the certificates
- The laboratories will contribute in keeping the certificate status
- The developer will know the resistance of their products
- The consumers will be able to do a better procurement plan based on a more accurate risk analysis.

# Contact Information

- E-mail
  - [organismo.certificacion@cni.es](mailto:organismo.certificacion@cni.es)
- Web Site:
  - [www.oc.ccn.cni.es](http://www.oc.ccn.cni.es)



**ORGANISMO DE CERTIFICACIÓN**

Home  
Certification Body (OC)  
Certification ICT Security  
Laboratories Accreditation  
FAQ  
Documents  
Application forms  
Links

**OC NEWS**

National Cryptologic Centre has certified the following products with Functional Certification

- \*\*Kona102 ePassport [BAC configuration]\*\* Version 1 Revision 1 Update (patch) 2
- \*\*Kona102 ePassport [EAC configuration]\*\* Version 1 Revision 1 Update (patch) 2

- More information -

To implement the level of security appropriate for the organization's aims, these organizations must adopt the necessary organizational and technical measures to prevent the execution of non-desired functions. The user needs certain guarantees regarding the design of the product. The product must be conveniently designed and, besides, must not execute non-desired functions. Nevertheless, the only method available for the user to check such attributes is the **evaluation (1)** of the security of the information system or of some of its parts. That evaluation must be done following strict criteria, with the following **certification (2)** by the part of the organization legally established for that purpose.

National Cryptologic Centre (CCN) as a Certification Body (OC) of the Spanish Evaluation and Certification Scheme of information technologies, which apply to products and systems in this area. It operates under the scope of, as laid out in the Act 11/2002, 6th May, regulating the National Intelligence Centre, and the Royal Decree 421/2004, 12th March, regulating the CCN.

- The National Cryptologic Centre is based on three types of certifications, depending on the security features evaluated:
- Cryptology Certification: products capable of protecting national classified information.
- TEMPEST Certification: encryption equipment and Zoning evaluation
- Functional certification: ITC products and systems evaluated, in accordance with international standard criteria (INTSEC and Common Criteria).

**FUNCTIONAL CERTIFICATION**  
In accordance with international standard criteria (C)

**CRYPTOLOGIC CERTIFICATION**  
Products capable of protecting national classified information

**TEMPEST CERTIFICATION**  
Teams and systems protected against electro-magnetic emissions

In addition, the Certification Body is accredited by the Entidad Nacional de Acreditación, in accordance with the requirements laid out in the standard UNE-EN 45011:1998 for product certification.

Common Criteria  
SOGIS MRA  
How to certify a SICT product?  
Certified Products  
Accredited Laboratories

Contact | Legal Warning | Web Map  
GOBIERNO DE ESPAÑA | MINISTERIO DE LA PRESIDENCIA  
C/Argenta, 20 28023 MADRID  
organismo.certificacion@ccn.cni.es  
Cni-Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.