



Certification and IoT

Guillaume Bouffard (guillaume.bouffard@ssi.gouv.fr)

Agence nationale de la sécurité des systèmes d'information

23 Mai 2019

Until now ...

Security features are made on specific devices

- Payment
- Identity
- Travel
- ...

Until now ...

Security features are made on specific devices

- Payment
- Identity
- Travel
- ...

Devices

- Smartcard
- Embedded secure element (SE)

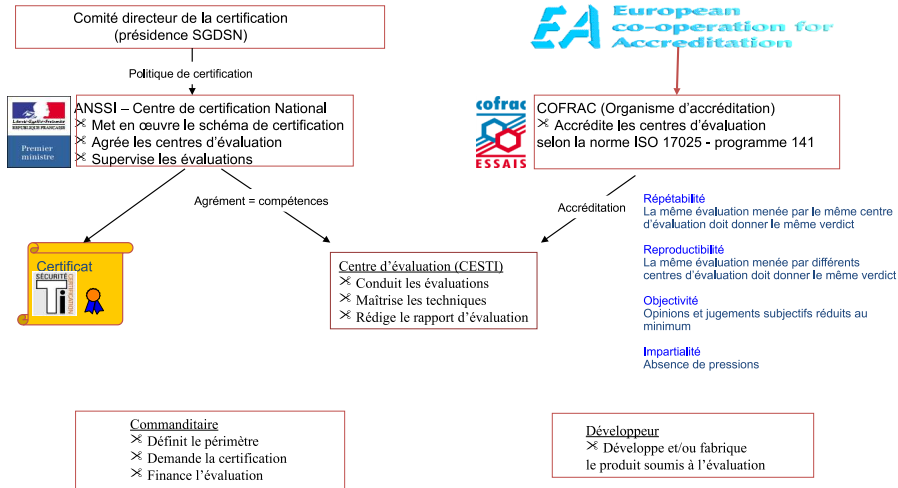
How to ensure security level of SE?

- **Customers** specify the security requirements.
- **Developers** implement security requirements in the product.
- **ITSEFs** evaluate the product security level.
- **Certification Body** certify products and checks each step of the evaluation process.

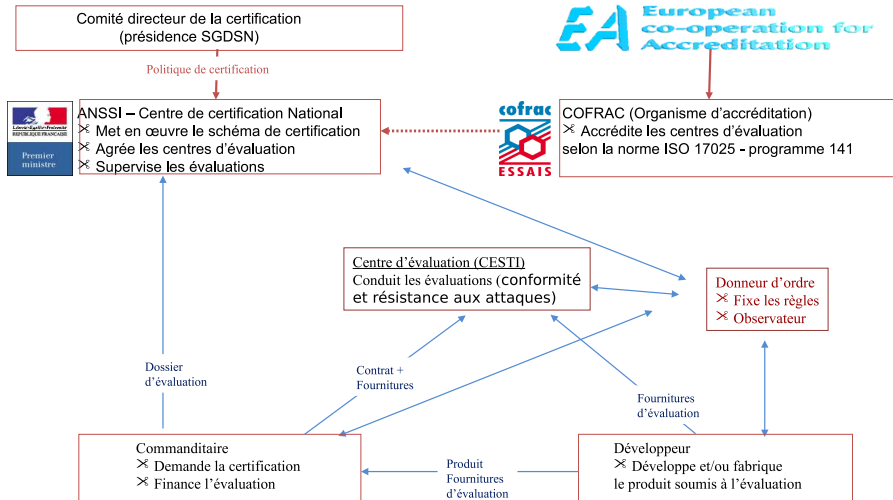
The Common Criteria

- Common Criteria is an international standard (ISO/IEC 15408) for certification of secure products.
- International recognition

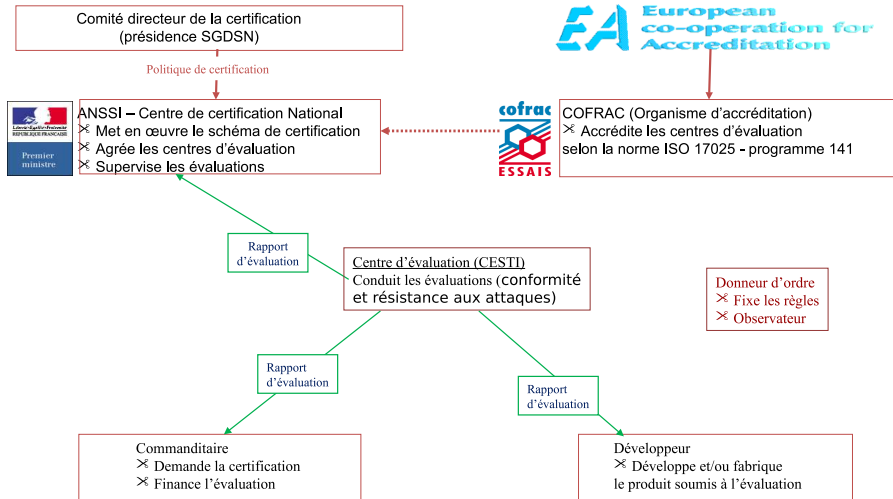
The Common Criteria Scheme in France



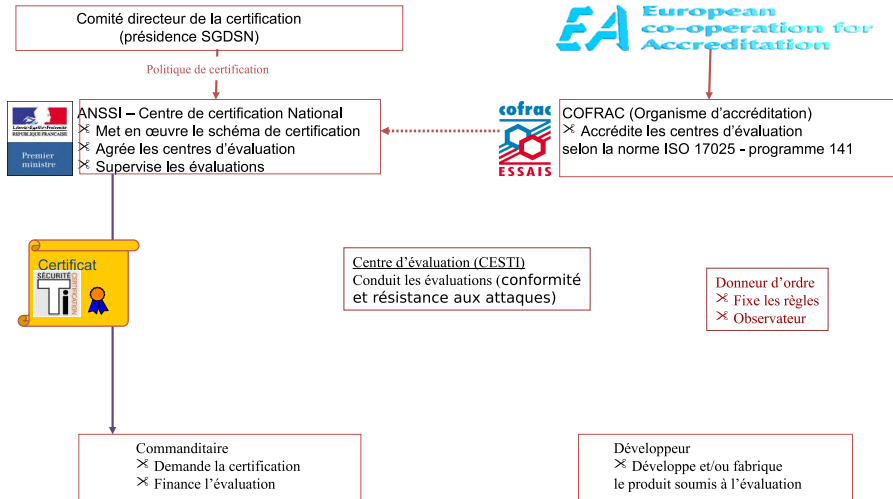
The Common Criteria Scheme in France



The Common Criteria Scheme in France



The Common Criteria Scheme in France



Evaluation level

- Several certification classes exist:

Level	Description
EAL1	Functionally Tested
EAL2	Structurally Tested
EAL3	Methodically Tested and Checked
EAL4	Methodically Designed, Tested and Reviewed
EAL5	Semiformally Designed and Tested
EAL6	Semiformally Verified Design and Tested
EAL7	Formally Verified Design and Tested

- For each class may be *augmented*:
 - ▶ For instance: a smartcard can be evaluated as:
EAL4 + ALC_DVS.2 + AVA_VAN.5
- Each evaluation is not time constraint.

A new world comes with new usages

- Secure features moves to unsecured component:
 - ▶ SoC/TEE
 - ▶ Whitebox crypto

A new world comes with new usages

- Secure features moves to unsecured component:
 - ▶ SoC/TEE
 - ▶ Whitebox crypto
- Each 6-month/year: a new version of a component is released.

A new world comes with new usages

- Secure features moves to unsecured component:
 - ▶ SoC/TEE
 - ▶ Whitebox crypto
- Each 6-month/year: a new version of a component is released.
- But, are we able to evaluate that?



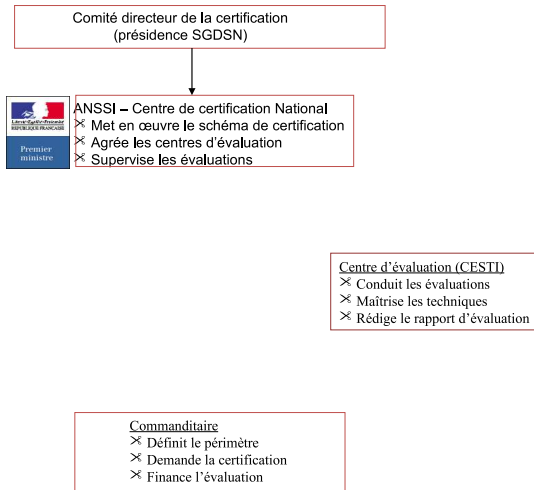
CC	CSPN
EAL 1 to 7	Only one level
Grey/white box	Black box
International certification recognition	No recognition
No time constraint	25md (+10 for crypto)
Product update during the evaluation	Fixed product version
Developer must provide compliant docs	No specific knowledge
Very expensive (60 to 200k€)	Relatively low cost (25 to 35k€)



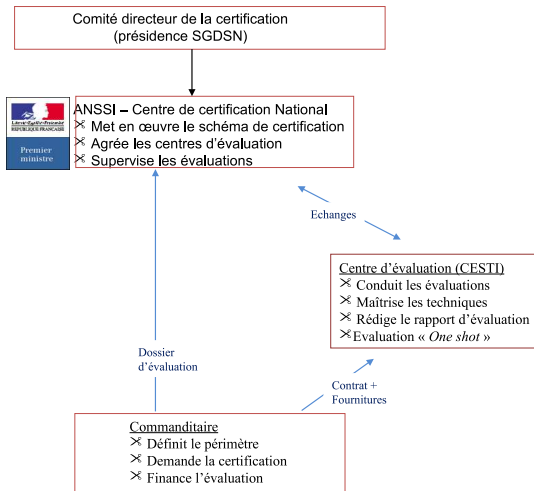
CC	CSPN
EAL 1 to 7	Only one level
Grey/white box	Black box
International certification recognition	No recognition
No time constraint	25md (+10 for crypto)
Product update during the evaluation	Fixed product version
Developer must provide compliant docs	No specific knowledge
Very expensive (60 to 200k€)	Relatively low cost (25 to 35k€)

- CPSN-like scheme available in Germany (BSZ — Accelerated Security Certification) and Spain (LINCE).

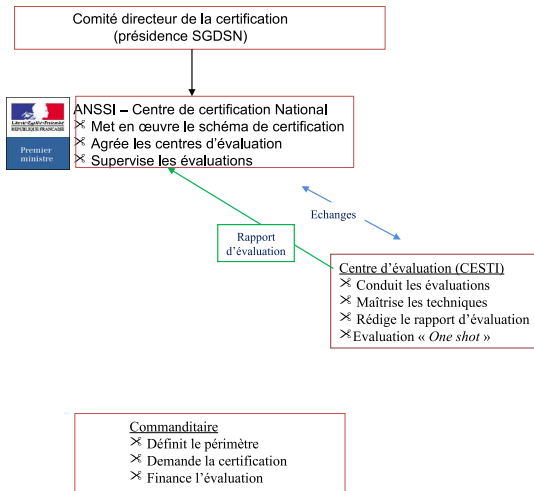
Certification de Sécurité de Premier Niveau (CSPN)



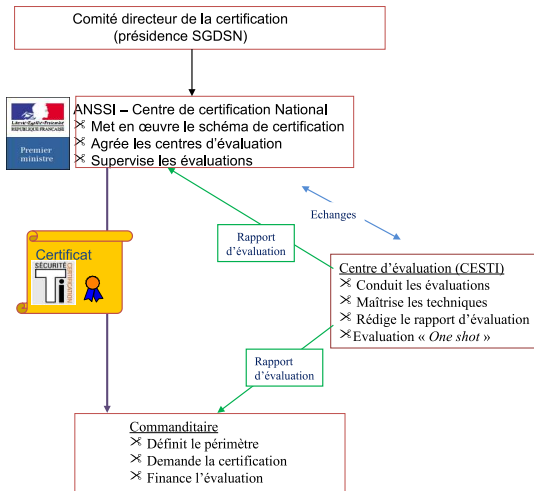
Certification de Sécurité de Premier Niveau (CSPN)



Certification de Sécurité de Premier Niveau (CSPN)



Certification de Sécurité de Premier Niveau (CSPN)



Licensed ITSEFs



Licensed ITSEFs

Agreements for **Electronic, microelectronic components and embedded software**



THALES



Licensed ITSEFs

Agreements for **Software and Networks**



Licensed ITSEFs

Agreements for *Équipements matériels avec boîtiers sécurisés*



Short List of CSPN products

- A full list is available there:

<https://www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/>

- Random-chosen CPSN products:

- ▶ Ledger Nano S version 1.5.1 (14/02/2019)
- ▶ Mécanisme de cloisonnement runtime de KNOX Workspace version 2.3 (03/12/2015)
- ▶ Sous-système de chiffrement de disques dm-crypt Noyau Linux 4.4.2 – cryptsetup 1.7.0 (16/06/2016)
- ▶ HP Sure Start Hardware Root of Trust, en version A0, embarqué sur la puce NPCE586HA0MX (16/03/2017)

Conclusion

- Currently, there is not scheme to evaluate IoT devices.
- Several approaches exist (CSPN, or property scheme) without **international recognition**.

Questions?

Guillaume Bouffard
<guillaume.bouffard@ssi.gouv.fr>