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)

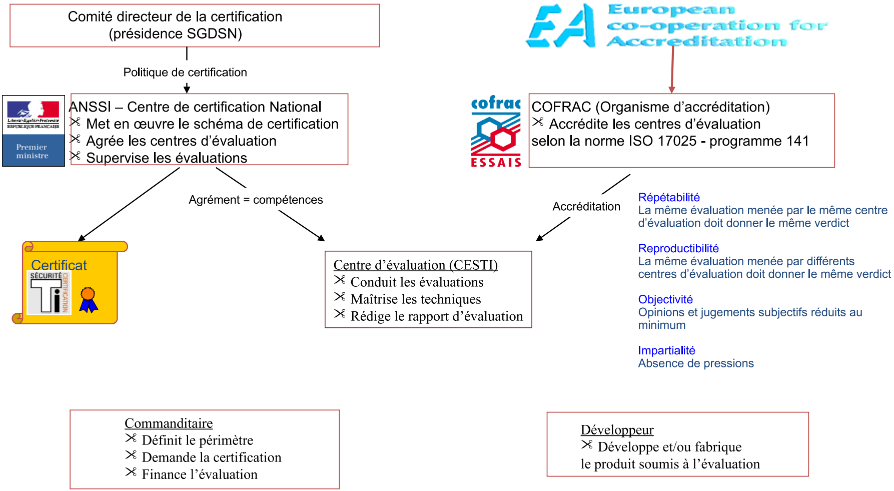
How to ensure security level of SE?

- 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



Comité directeur de la certification
(présidence SGDSN)

Politique de certification

ANSSI – Centre de certification National
- Met en œuvre le schéma de certification
- Agrée les centres d'évaluation
- Supervise les évaluations

Agrément = compétences

COFRAC (Organisme d'accréditation)
- Accrédite les centres d'évaluation

selon la norme ISO 17025 - programme 141

Accréditation

Centre d'évaluation (CESTI)
- Conduit les évaluations
- Maîtrise les techniques
- Rédige le rapport d'évaluation

Répétabilité
La même évaluation menée par le même centre d'évaluation doit donner le même verdict

Reproductibilité
La même évaluation menée par différents centres d'évaluation doit donner le même verdict

Objectivité
Opinions et jugements subjectifs réduits au minimum

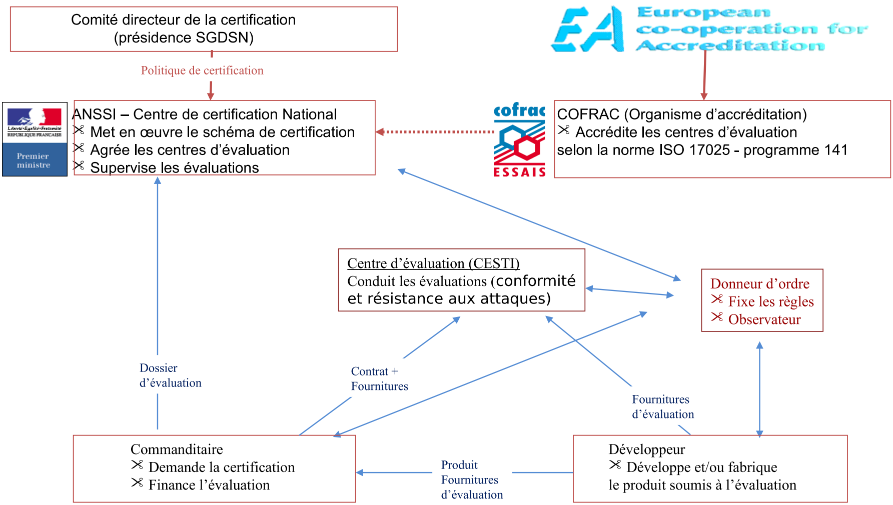
Impartialité
Absence de pressions

Commanditaire
- Définit le périmètre
- Demande la certification
- Finance l'évaluation

Développeur
- Développe et/ou fabrique

le produit soumis à l'évaluation

The Common Criteria Scheme in France



Comité directeur de la certification (présidence SGDSN)

Politique de certification

ANSSI – Centre de certification National
- Met en œuvre le schéma de certification
- Agrée les centres d'évaluation
- Supervise les évaluations

COFRAC (Organisme d'accréditation)
- Accrédite les centres d'évaluation selon la norme ISO 17025 - programme 141

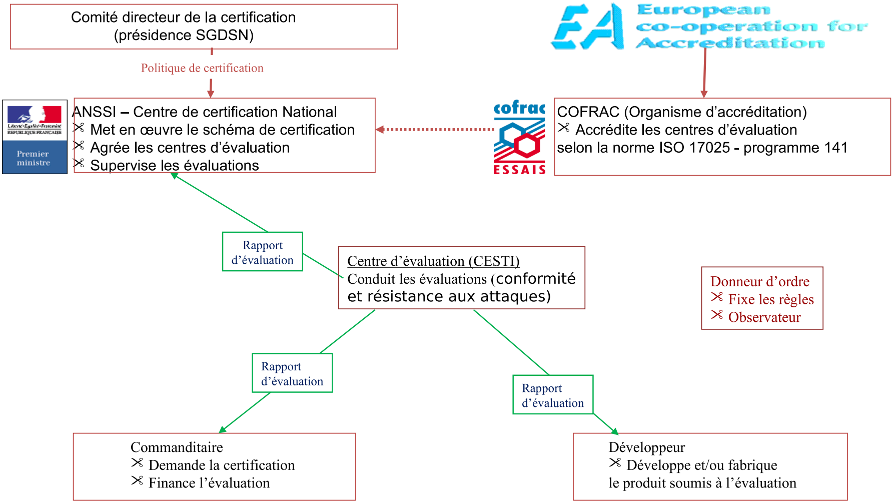
Centre d'évaluation (CESTI)
Conduit les évaluations (conformité et résistance aux attaques)

Donneur d'ordre
- Fixe les règles
- Observateur

Commanditaire
- Demande la certification
- Finance l'évaluation

Développeur
- Développe et/ou fabrique le produit soumis à l'évaluation

The Common Criteria Scheme in France



Comité directeur de la certification
(présidence SGDSN)

Politique de certification

ANSSI – Centre de certification National
⤫ Met en œuvre le schéma de certification
⤫ Agrée les centres d'évaluation
⤫ Supervise les évaluations

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
European co-operation for Accreditation
cofrac
ESSAIS

COFRAC (Organisme d'accréditation)
⤫ Accrédite les centres d'évaluation
selon la norme ISO 17025 - programme 141

Rapport d'évaluation

Centre d'évaluation (CESTI)
Conduit les évaluations (conformité et résistance aux attaques)

Donneur d'ordre
⤫ Fixe les règles
⤫ Observateur

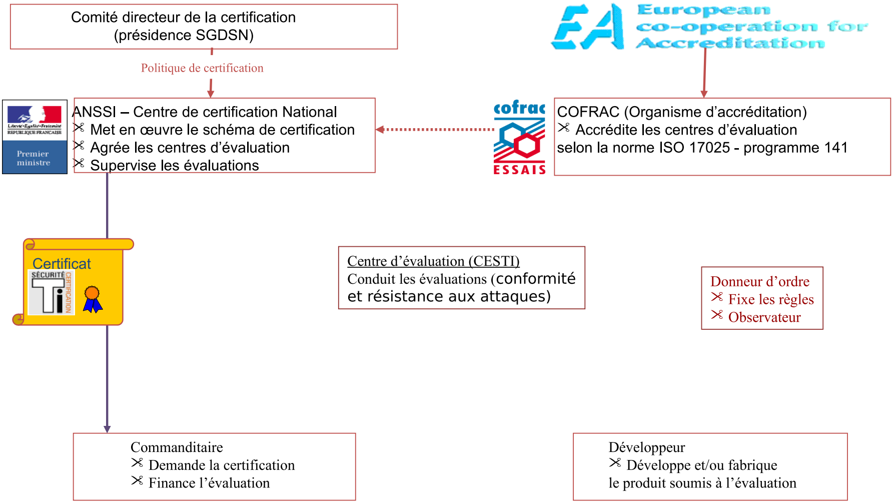
Rapport d'évaluation

Rapport d'évaluation

Commanditaire
⤫ Demande la certification
⤫ Finance l'évaluation

Développeur
⤫ Développe et/ou fabrique
le produit soumis à l'évaluation

The Common Criteria Scheme in France



Comité directeur de la certification (présidence SGDSN)

Politique de certification

ANSSI – Centre de certification National
⤫ Met en œuvre le schéma de certification
⤫ Agrée les centres d'évaluation
⤫ Supervise les évaluations

COFRAC (Organisme d'accréditation)
⤫ Accrédite les centres d'évaluation selon la norme ISO 17025 - programme 141

Centre d'évaluation (CESTI)
Conduit les évaluations (conformité et résistance aux attaques)

Donneur d'ordre
⤫ Fixe les règles
⤫ Observateur

Commanditaire
⤫ Demande la certification
⤫ Finance l'évaluation

Développeur
⤫ Développe et/ou fabrique le produit soumis à l'évaluation

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?

VISA DE SÉCURITÉ

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION • ANSSI •

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€)

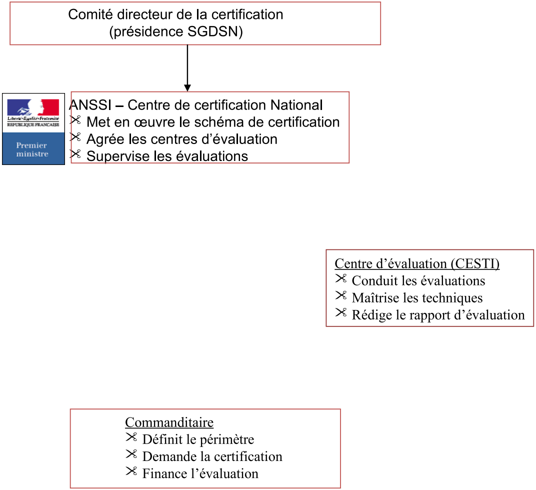
VISA DE SÉCURITÉ

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI ·

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)



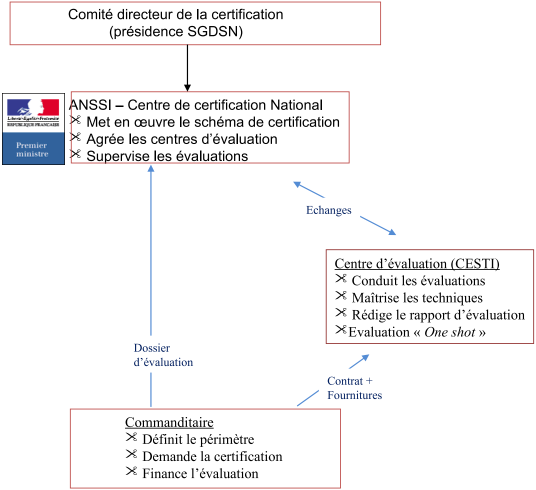
Comité directeur de la certification
(présidence SGDSN)

ANSSI – Centre de certification National
- Met en œuvre le schéma de certification
- Agrée les centres d'évaluation
- Supervise les évaluations

<u>Centre d'évaluation (CESTI)</u>
- Conduit les évaluations
- Maîtrise les techniques
- Rédige le rapport d'évaluation

<u>Commanditaire</u>
- Définit le périmètre
- Demande la certification
- Finance l'évaluation

Certification de Sécurité de Premier Niveau (CSPN)



Comité directeur de la certification
(présidence SGDSN)

ANSSI – Centre de certification National
- Met en œuvre le schéma de certification
- Agrée les centres d'évaluation
- Supervise les évaluations

Echanges

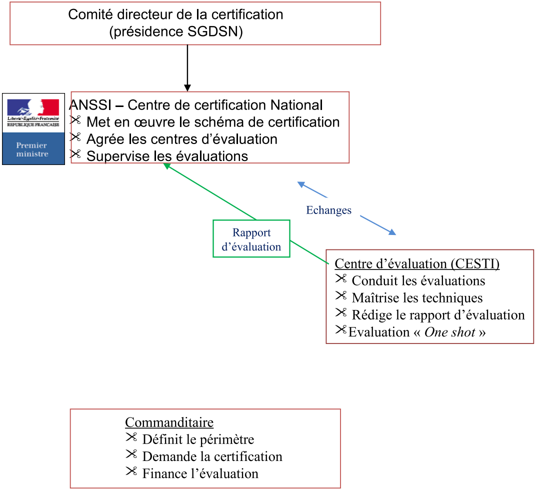
Centre d'évaluation (CESTI)
- Conduit les évaluations
- Maîtrise les techniques
- Rédige le rapport d'évaluation
- Evaluation « *One shot* »

Dossier d'évaluation

Contrat + Fournitures

Commanditaire
- Définit le périmètre
- Demande la certification
- Finance l'évaluation

Certification de Sécurité de Premier Niveau (CSPN)



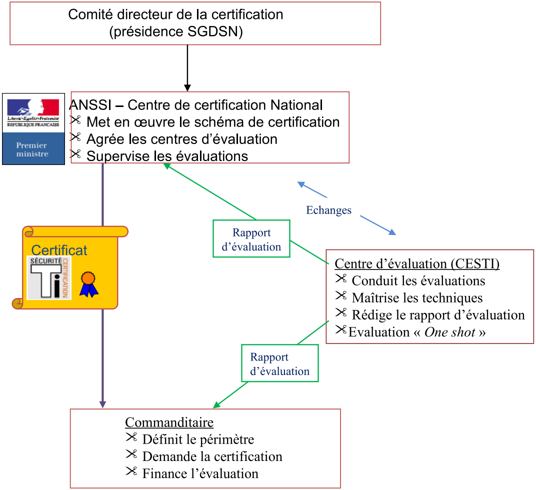
Comité directeur de la certification
(présidence SGDSN)

ANSSI – Centre de certification National
- Met en œuvre le schéma de certification
- Agrée les centres d'évaluation
- Supervise les évaluations

Centre d'évaluation (CESTI)
- Conduit les évaluations
- Maîtrise les techniques
- Rédige le rapport d'évaluation
- Evaluation « *One shot* »

Commanditaire
- Définit le périmètre
- Demande la certification
- Finance l'évaluation

Certification de Sécurité de Premier Niveau (CSPN)



Comité directeur de la certification
(présidence SGDSN)

ANSSI – Centre de certification National
- Met en œuvre le schéma de certification
- Agrée les centres d'évaluation
- Supervise les évaluations

Centre d'évaluation (CESTI)
- Conduit les évaluations
- Maîtrise les techniques
- Rédige le rapport d'évaluation
- Evaluation « *One shot* »

Commanditaire
- Définit le périmètre
- Demande la certification
- Finance l'évaluation

Licensed ITSEFs

SERMA
SAFETY & SECURITY

LEXFO

AMOSSYS

leti
cea tech

Quarkslab
SECURING EVERY BIT OF YOUR DATA

THALES

TL Trusted labs
Creating trust in a connected world

edsi
The Embedded Security Experts

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

SYNACKTIV
DIGITAL SECURITY

Licensed ITSEFs

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

SERMA
SAFETY & SECURITY

leti
cea tech

THALES

edsi
The Embedded Security Experts

Licensed ITSEFs

Agreements for **Software and Networks**

LEXFO

AMOSSYS

Quarkslab
SECURING EVERY BIT OF YOUR DATA

THALES

Trusted labs
Creating trust in a connected world

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

SYNACKTIV
DIGITAL SECURITY

Licensed ITSEFs

Agreements for ***Equipements matériels avec boîtiers sécurisés***

SERMA SAFETY & SECURITY — AMOSSYS

OPPIDA EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION — SERMA SAFETY & SECURITY

leti ceatech

THALES

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>