RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

EVALUATION ET CERTIFICATION DE LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

1. La certification
   a. Généralités
   b. Accords de reconnaissance
   c. Processus de certification

2. les Critères Communs
   a. La TOE
   b. Quelques notions
   c. L'évaluation

3. La cotation d'attaque
   a. Comment coter une attaque
   b. L'exemple de la carte à puce
   c. Exemples de cotation

1. LA CERTIFICATION

La certification en France

Les acteurs de la certification

3 acteurs :

Organisme de certification
CCN

Centres d'évaluation de la sécurité et des technologies de l'Information (CESTI)

Fabricant de produits de sécurité (ou commanditaire)

→ le décret 2002-535 établit le cadre juridique et les procédures réglementaires régissant la certification des produits de sécurité informatique en France.

La certification en France

Les acteurs de la certification : laboratoires agréés (CESTI)

Les portées d'agrément détaillées figurent sur le site internet de l'ANSSI

acceis
Centre d'expertises en cybersécurité

AMOSSYS

cea leti

edsi
The Embedded Security Experts

Oppida
apave

Quarkslab

SERMA GROUP

CESTI matériel

Lexfo

SYNACKTIV

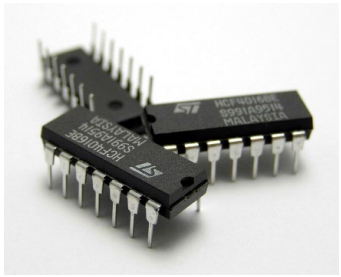
THALES

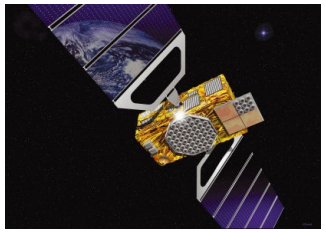
*Les centres d'évaluation sont **agréés** par le Centre de Certification National pour effectuer des évaluations techniques des produits de sécurité informatique soumis à certification.*

Site web : Voir les centres d'évaluation | ANSSI

La certification en France

Les acteurs de la certification : les développeurs





La certification en France

Critères Communs (CC)

Schéma international : accords de reconnaissance

CCRA

- Accord mondial ouvert à tous
- 31 pays membres
- Les certificats émis sont reconnus à un certain niveau d'assurance (EAL2)

EUCC

- Schéma européen de cyber sécurité
- Tous les pays européens sont membres de l'accord
- Tous les certificats sont reconnus

Site web : https://www.commoncriteriaportal.org/ Accords de reconnaissance mutuelle des Critères Communs | ANSSI

La certification en France : Processus de certification

Enregistrement	•Lancement des travaux d'évaluation
Re0 (optionnel)	•Mise au point de l'évaluation •Intérêt de cette réunion si primo évaluation ou projet pilote
Re1 (optionnel)	•Validation du plan de tests
Réception(s) RTE	•Réception incrémental du RTE (RTI) en provenance du CESTI •**Mode tunnel uniquement en CSPN** •Relecture du RTE •Échanges avec le CESTI via une fiche de revue qui consigne anomalies / remarques / points à clarifier
Certification ou clôture	•Si FAIL alors lettre de clôture (ce qui arrive très peu en CC) •Si PASS alors rédaction du rapport de certification + certificat puis décision de certification puis circuit de validation / signature

La certification en France

Questions ?

2. LES CRITÈRES COMMUNS (CC)

Critères Communs (CC)

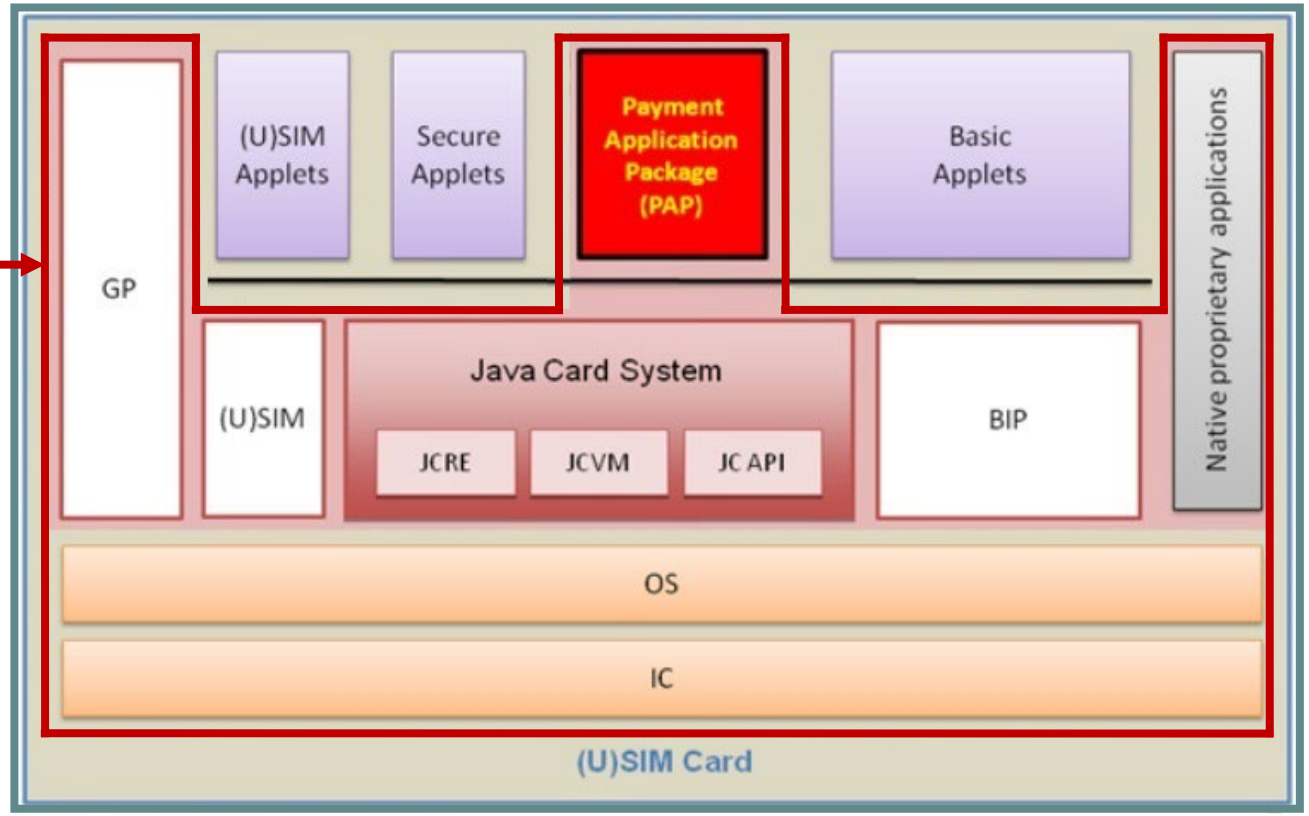
Cible d'évaluation / Target of Evaluation / TOE

Produit

Tests de vulnérabilités

TOE

Tests de conformité



Autres exemples de TOE :

- Un logiciel
- Un système d'exploitation
- Un circuit-intégré (IC)
- Une passerelle
- Un HSM

Critères Communs Partie 1

la cible de sécurité

- Cible de sécurité / Security Target / ST
- Spécification du besoin de sécurité, cahier des charges de l'évaluation
  - Description des biens (ce qu'il faut défendre), menaces, hypothèses, objectifs de sécurité
  - Identification du produit
  - Description du cycle de vie
  - Description de la cible d'évaluation
  - Description des fonctions de sécurité évaluées
  - Niveau d'évaluation

Les Critères Communs (CC)

Quelques notions

- Ensemble de règles auquel un produit peut se conformer
- Plusieurs niveaux: EAL (Evaluation Assurance Level)

EAL 1, EAL 2, …, EAL 7

  - Niveau de conformité ADV, AGD, ALC, ASE, ATE
  - Niveau de résistance aux attaques **AVA_VAN**

	Range of values*	TOE resistant to attackers with attack potential of:
	0-15	No rating
AVA_VAN.1 - 2 →	16-20	Basic
AVA_VAN.3 →	21-24	Enhanced-Basic
AVA_VAN.4 →	25-30	Moderate
AVA_VAN.5 →	31 and above	High

Table 11: Rating of vulnerabilites for CC v3

Les CC

Tests de pénétration

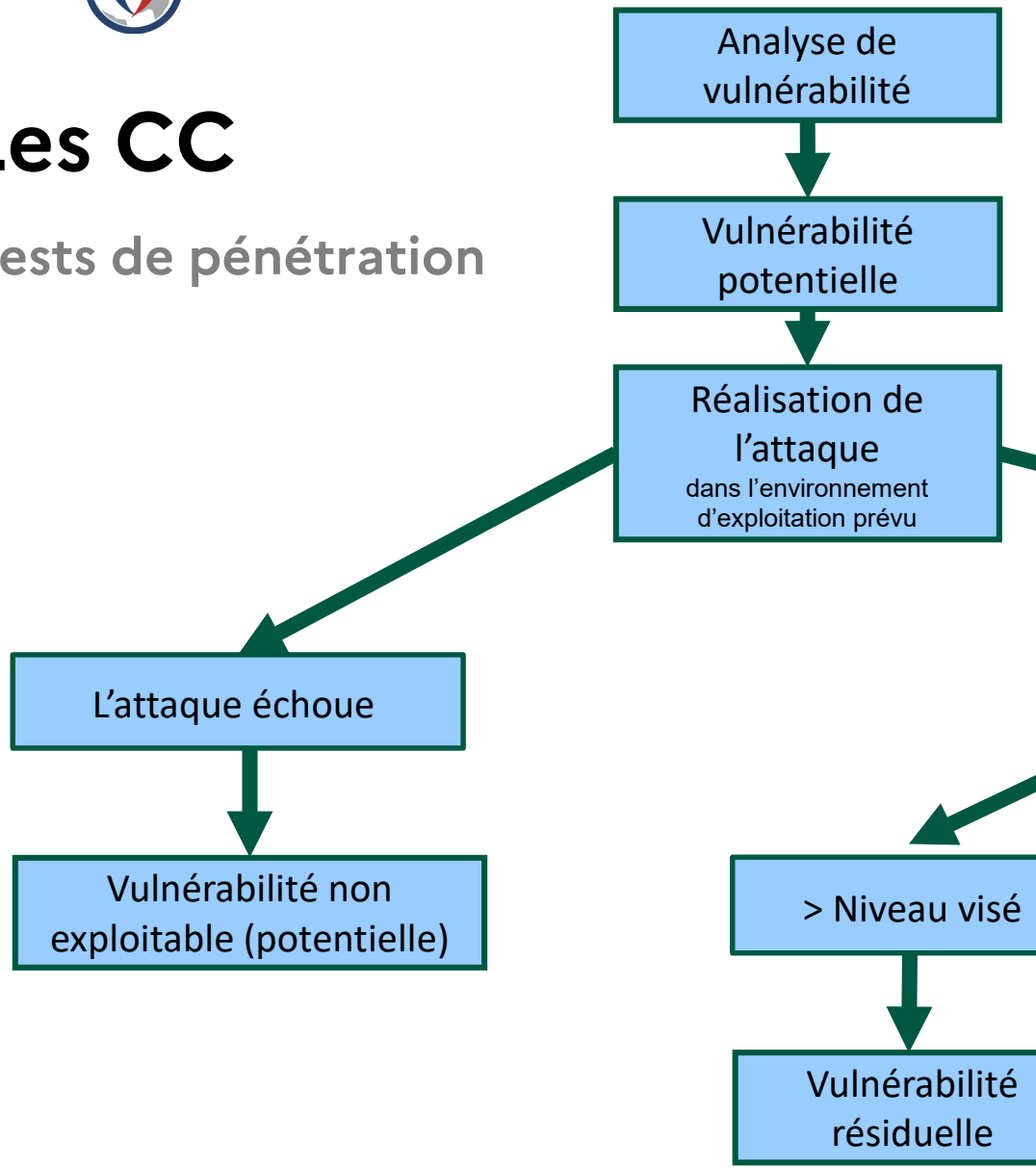


Table de cotation du JHAS pour les Smartcards

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
> four months[4]	6	10
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Critical+	9	*
Not practical	*	*
Access to TOE (1)		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (2)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples/Samples with known secrets		
Public	0	NA
Restricted	2	NA
Sensitive	5	NA
Critical	9	NA
Not practical (Samples with known secrets only)	*	NA

Table 13: Final table for the rating factors

Les Critères Communs (CC)

Questions ?

3. LA COTATION D'ATTAQUE

Les Critères Communs (CC)

Le niveau AVA_VAN pour les cartes à puce

Comment coter une attaque ?

→5 critères

- ***Temps passé***
- ***Niveau d'expertise***
- ***Connaissance du produit***
- ***Accessibilité au produit***
- ***Equipement nécessaire***

→A chaque critère une table de cotation et une table de cotation par domaine…

Cotation des attaques sur cartes à puces

Le niveau AVA_VAN pour les cartes à puce

La méthode générale des CC a été interprétée afin de :

- Distinguer l'effort d'Identification de l'attaque (trouver l'attaque) et l'effort d'Exploitation de l'attaque (reproduire l'attaque).
- Reformuler l'effort pour accéder au produit.
- Procurer certains privilèges à l'évaluateur tout en les prenant en compte dans la cotation.

→ *Application of Attack Potential To SmartCard*

Exemple de cotation pour une attaque par injection de fautes

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Layman: pas d'expertise particulière

Proficient: connaissance d'attaques classiques et concepts de sécurité

Expert: **connaissances des algorithmes, protocoles, structures HW, principes et concepts de sécurité – techniques et outils pour définir de nouvelles attaques**

Multiple Expert: niveau « expert » sur différents niveaux d'attaque (par exemple manipulation HW et crypto)

Exemple de cotation pour une DPA - Differential Power Analysis

Exploitation de la consommation électrique obtenue lors de l'exécution d'opérations sensibles

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Standard: oscilloscope de base, lecteur de carte, PC…

Specialized: oscilloscope haut de gamme, microscope UV

Bespoke: FIB (Focused Ion Beam), AFM (Atomic Force Microscope)…

Multiple Bespoke: équipements « bespoke » sur différents niveaux de l'attaque

Exemple de cotation pour une DPA - Differential Power Analysis

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples (rated according to access to open samples)		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Prenons un cas optimiste, sans prendre en compte la connaissance de la TOE sur un produit accessible au grand public

Et comptons les points :

TOTAL = 23 points

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Table 11: Rating of vulnerabilites for CC v3

4. CONCLUSION

Merci pour votre attention

Questions ?