Certification Critères Communs appliquée aux circuits électroniques

Alexandre Gavriloff (ANSSI/CCN)

L’ANSSI

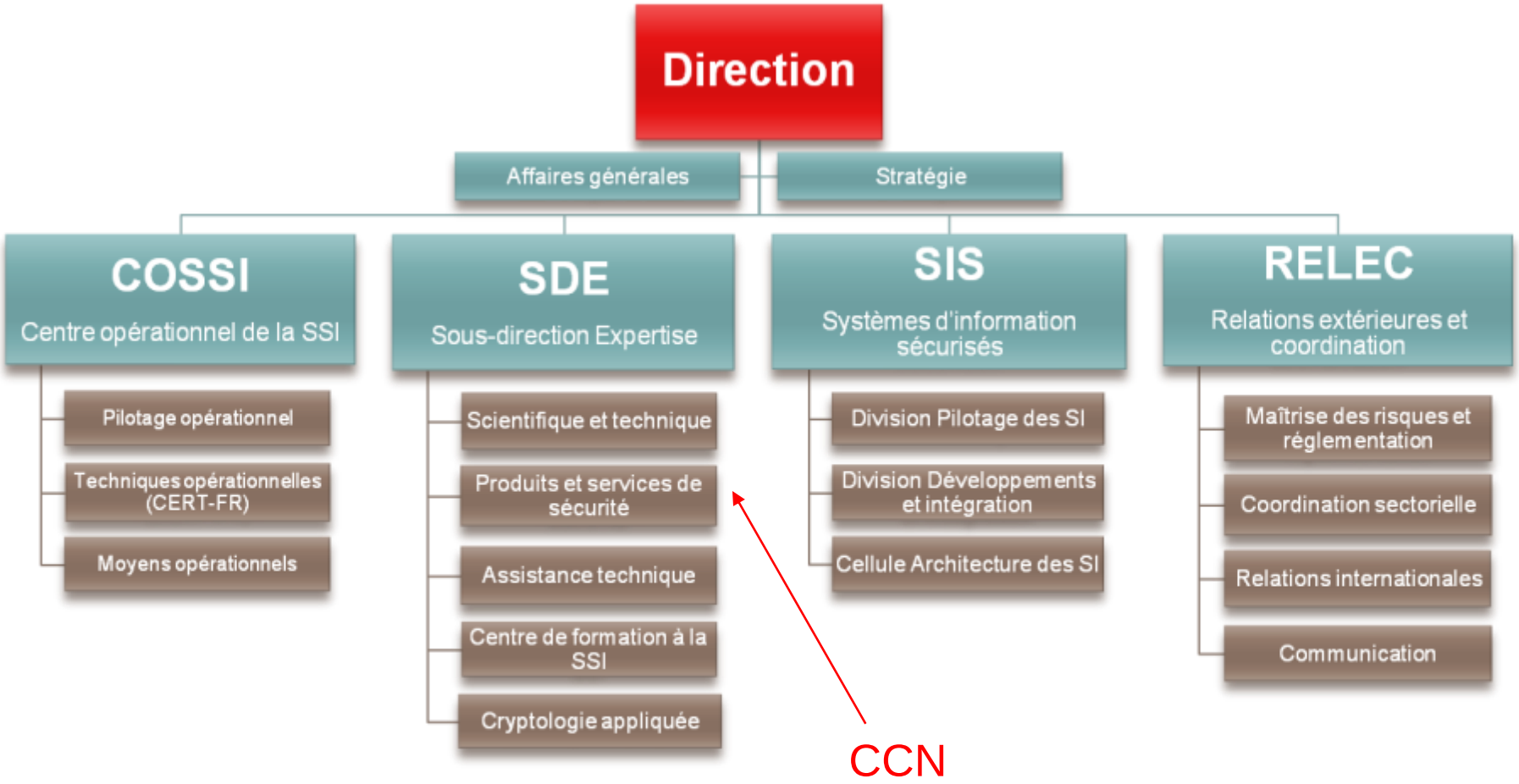
L'ANSSI

- **Agence Nationale de la Sécurité des Systèmes d'Informations**
  - Créée en 2009 par décret
  - Rattachée au Secrétariat Général de la Défense et Sécurité Nationale (SGDSN)
  - Liée directement au Premier Ministre
- **Réservoir de compétences au profit de l'état et des Organisme d'importance Vitale (OIV)**

L'ANSSI

- **Objectifs**
  - Doter la France de véritables capacités en SSI
    - Stratégie, Livre Blanc, LPM*
  - Être une puissance mondiale de Cyberdéfense
- **Moyens**
  - Prévention
    - Réglementation, labellisation, conseil, formation…
  - Défense
    - Gestion d'incident, réponses aux crises…

L'ANSSI


Direction
Affaires générales
Stratégie
COSSI
Centre opérationnel de la SSI
Pilotage opérationnel
Techniques opérationnelles (CERT-FR)
Moyens opérationnels
SDE
Sous-direction Expertise
Scientifique et technique
Produits et services de sécurité
Assistance technique
Centre de formation à la SSI
Cryptologie appliquée
SIS
Systèmes d'information sécurisés
Division Pilotage des SI
Division Développements et intégration
Cellule Architecture des SI
RELEC
Relations extérieures et coordination
Maîtrise des risques et réglementation
Coordination sectorielle
Relations internationales
Communication
CCN

La certification

Centre de Certification National

Créé le 1 avril 1995

- **Décret 2002-535**
- **Service public (impartial, gratuit)**
- **Schéma d'évaluation et de certification**
  - Évaluation CC (Microcircuits, cartes, logiciels…)
  - Évaluation CSPN (Pare-feu, communication sécurisée, contrôle d'accès, stockage sécurisé…)
  - Maintenance (Continuité de l'assurance après une modification non sécuritaire du produit)
  - Surveillance (Tests de résistance d'un produit après certification)

La certification

- **Agrément des laboratoires**

La certification

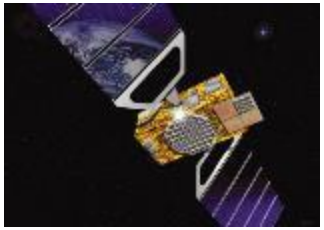
- **Des industriels utilisant le schéma français**

La certification

- **Des industriels du « domaine public »**

La certification

- **Des produits connus ?**



La certification

Label délivré par le PM

Critères Communs

CSPN

Assurance

Conformité

Qu’est ce que c’est ?

Reconnaissance

Cible de sécurité

Profil de protection

Standards

Analyse de vulnérabilité

CESTI

Qualification

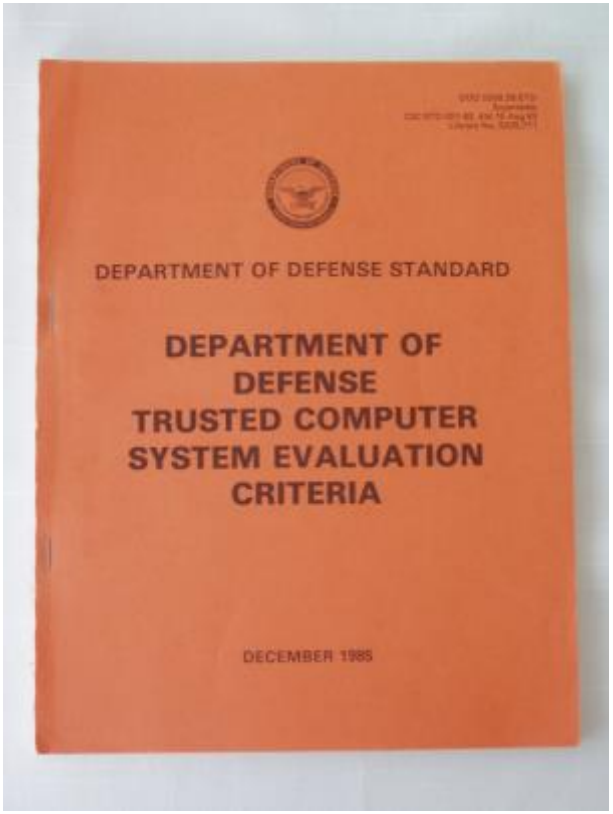
Agrément

La certification

- **Principes**
  - Attester de la conformité de l'objet soumis à évaluation à un référentiel d'évaluation en utilisant des critères et une méthodologie d'évaluation
  - Estimation de l'efficacité des contre-mesures de sécurité
  - Différentes certifications (CC, CSPN, EMVCO, Fips, ISO…)
  - Différents niveaux d'évaluation (« EAL » 1 → 7)
  - 3 acteurs principaux
    - Développeur
    - Evaluateur
    - Certificateur

La certification

- **Un peu d'histoire…**



La certification

- **Un peu d'histoire des CC…**
- **1983 USA Orange Book TCSEC***
- **1990 FR UK NL GE ITSEC****
- **1993 CANADA CTCPEC*****
- **1995 US, Europe, Canada Common Criteria**
- **…**
- **2012 CC, version 3.1 révision 4**

- ***TCSEC Trusted Computer System Evaluation Criteria**
- ****ITSEC Information Technology Security Evaluation Criteria**
- *****CTCPEC Canadian Trusted Computer Product Evaluation Criteria**

La certification

- **Deux objectifs**
  - Développer des critères d'évaluation harmonisés entre les nations
  - Assurer la reconnaissance des certificats entre les nations

Accords internationaux de reconnaissance

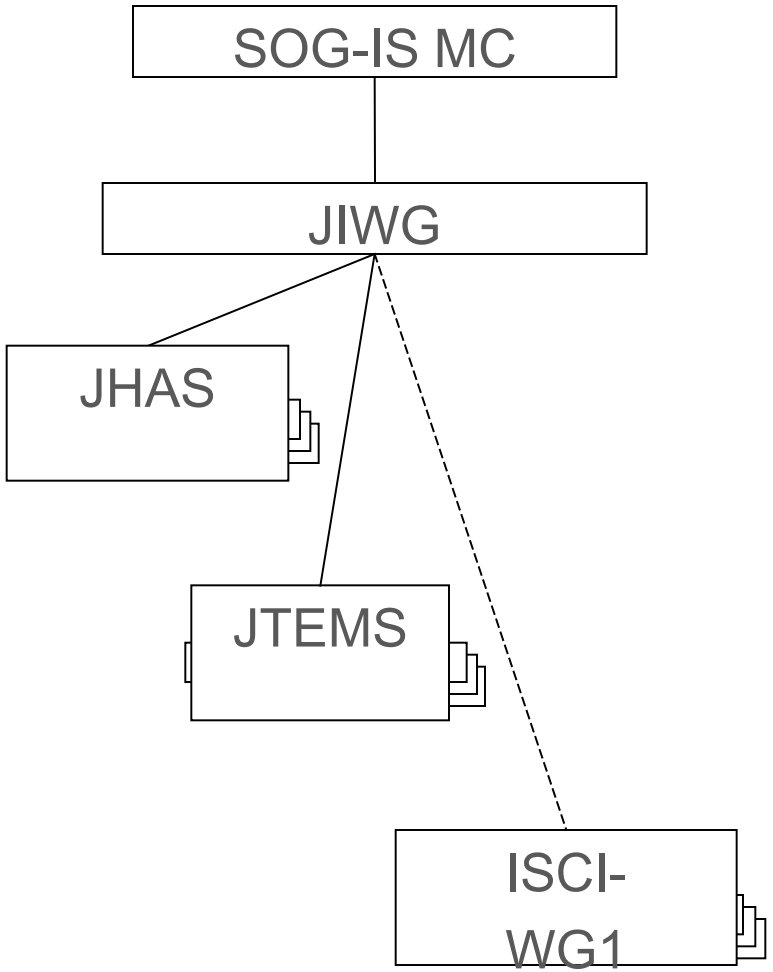
- **Contenu des accords de reconnaissance:**
  - Impose que les participants soient des Etats
  - Repose sur le principe de la certification à travers l'accréditation (EN45011, EN17025)
  - Crée le groupe de management de l'accord
  - Impose des audits périodiques des organismes de certification des Etats
  - Fixe les normes d'évaluation utilisées
  - Indique les règles de la reconnaissance (par ex: cible de sécurité et rapport de certification publics)
  - …

SOGIS

- **SOGIS : Senior Officials Group Information Systems Security**
  - Accord Européen
  - Ouvert aux pays de l'UE et de l'AELE*
  - 1998 création
  - 2010 dernière mise à jour
- **Reconnaissance des certificats CC**
  - Jusqu'à EAL 7 (niveau d'éval. max.)
    - Cartes à puce
    - Security Boxes
  - EAL4 (niveau moyen)
  - 5 pays qualifiés pour la carte à puce
    - France, Allemagne, Angleterre, Hollande, Espagne

Site web : http://www.sogis.org/

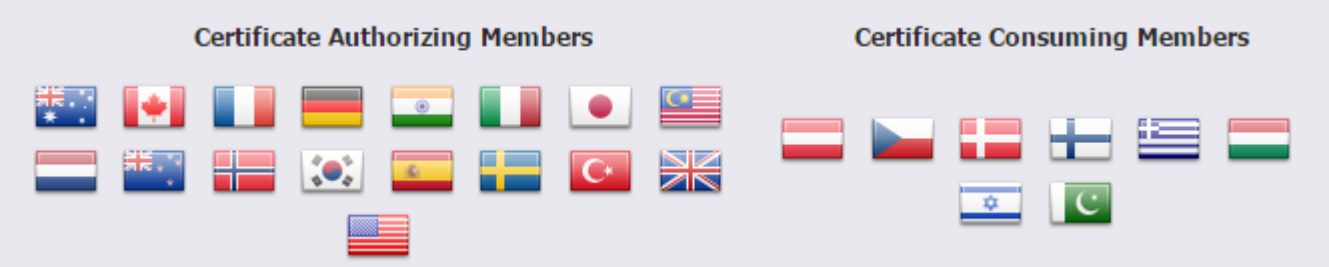
SOGIS



- **Managment Comitee**
  - Accepte les nouveaux membres
  - Décisions sur politique de certification
- **Joint Interpretations Working Group**
  - Développement de critères et de leurs interprétations et orientation des WGs
- **JIL Hardware related Attacks Subgroup**
  - Groupe de travail sur les aspects « attaque » des Cartes à puce
- **JIL Terminal Evaluation Methodology Subgroup**
  - Groupe de travail sur les aspects « attaque » des terminaux
- **International Security Certification Initiative**
  - Groupe de travail sur la technologie d'évaluation Carte à Puce

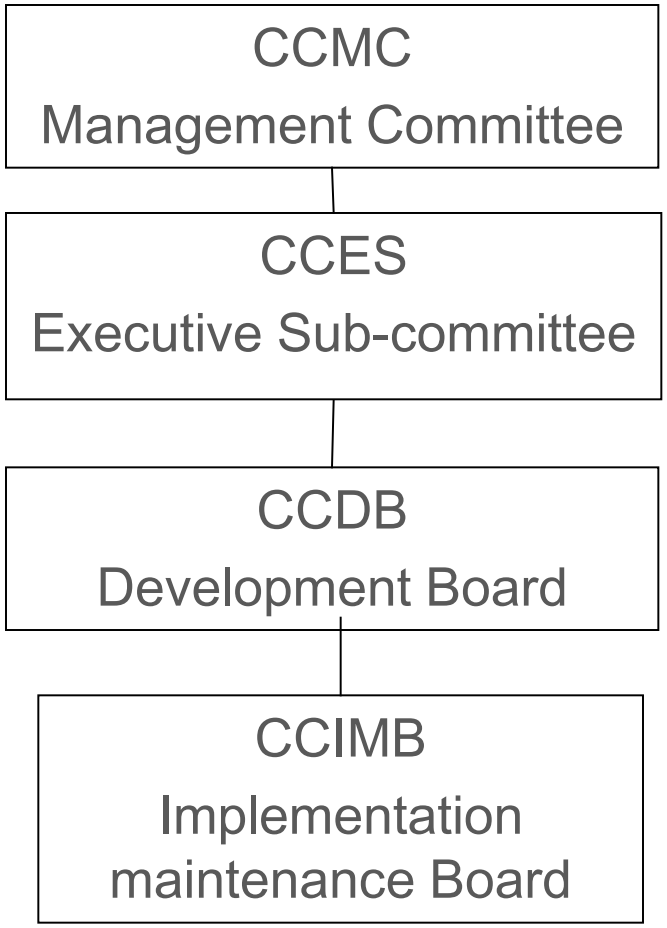
CCRA

- **CCRA : Common Criteria Recognition Arrangement**
  - Accord mondial
    - ouvert à tous les pays
    - 2000 création
    - 2014 dernière maj
  - Reconnaissance des certificats CC
  - Jusqu'à EAL 2 (niveau bas)
  - 25 pays



Site web : https://www.commoncriteriaportal.org/

CCRA



- **Décide les critères reconnus**
- **Accepte les nouveaux membres**

- **Gestion de la reconnaissance des certificats**
- **Promotion des Critères Communs**

- **Orientations pour le développement et la maintenance de la norme**
- **Harmonisation entre les schémas**

- **Développement et maintenance de la norme**

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

Les critères communs (la vision carte à puce)

Les critères communs

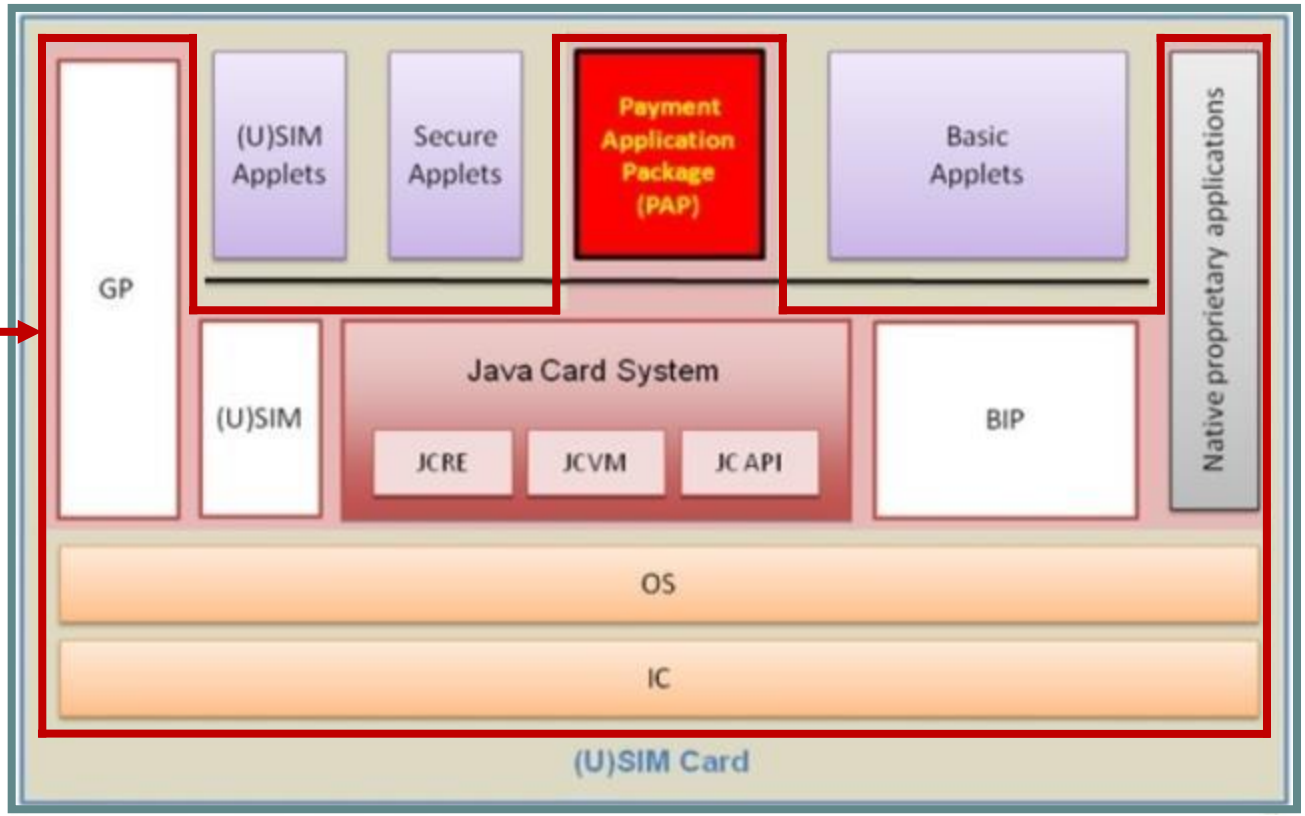
- **TOE : Target Of Evaluation – Cible d'évaluation**
  - La partie du produit soumise à évaluation

Produit

Tests de vulnérabilités

TOE

Tests de conformité



Les critères communs

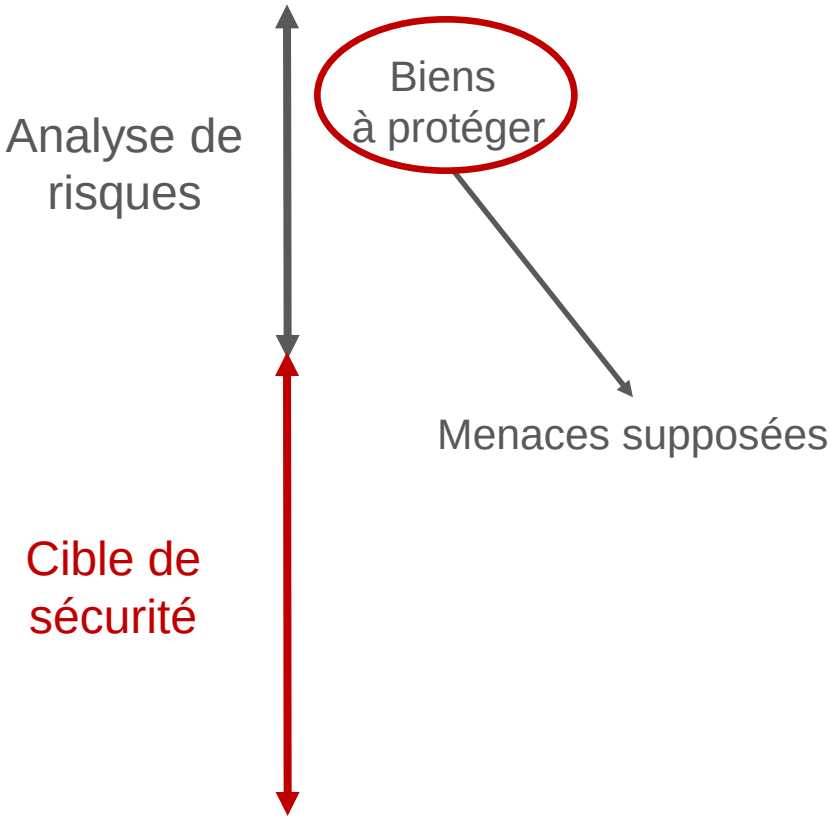
- **Quelques notions indispensables !**
  - ST Security Target - Cible de sécurité
    - Spécification du besoin de sécurité
    - Définition de ce qui est, et ce qui n'est pas, évalué (cahier des charges)

Les critères communs

- **Quelques notions indispensables !**
  - ST Security Target - Cible de sécurité
    - Biens, menaces, objectifs de sécurité (sur la TOE et l'environnement), hypothèses (restrictions d'usage)
    - Identification du produit (unique)
    - Cible d'évaluation (TOE)
    - Fonctions de sécurité évaluées
    - Cycle de vie
    - Niveau d'évaluation EAL
    - Document initial pour lancer une certification
    - Vérification par CCN (non trompeuse, cohérente, charges…)
    - Peut évoluer au cours de l'évaluation
      - Des vulnérabilités identifiées en évaluation peuvent être couvertes par des hypothèses
      - De nouvelles fonctions de sécurité peuvent être ajoutées

Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport



Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport

Analyse de risques

Biens à protéger

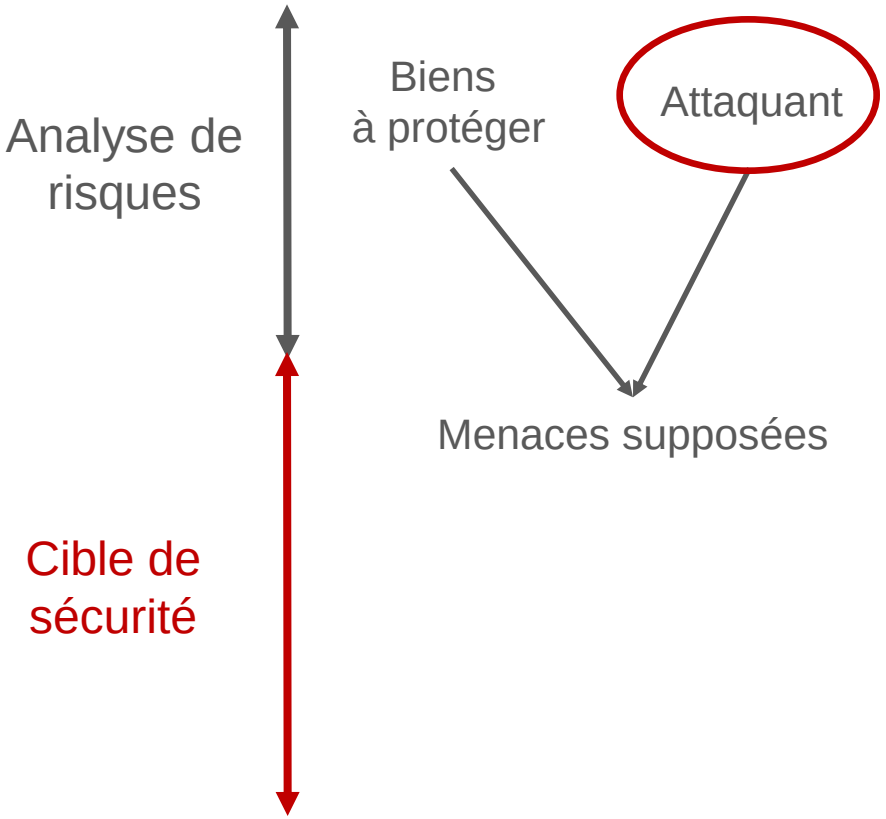
- Données stockées dans la TOE
- Données échangées avec le terminal
- Données de traçabilité
- Clefs cryptographiques…

Menaces supposées

Cible de sécurité

Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport

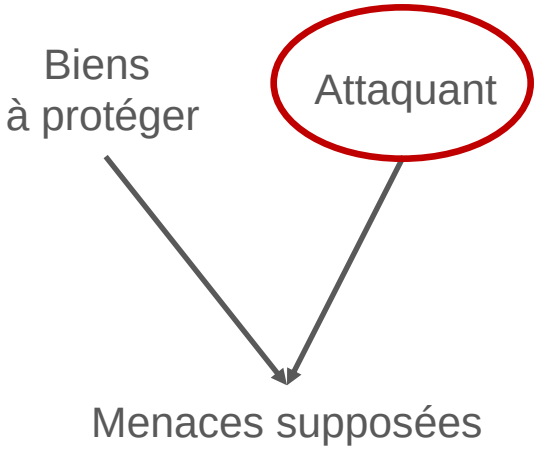


Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport

Analyse de risques

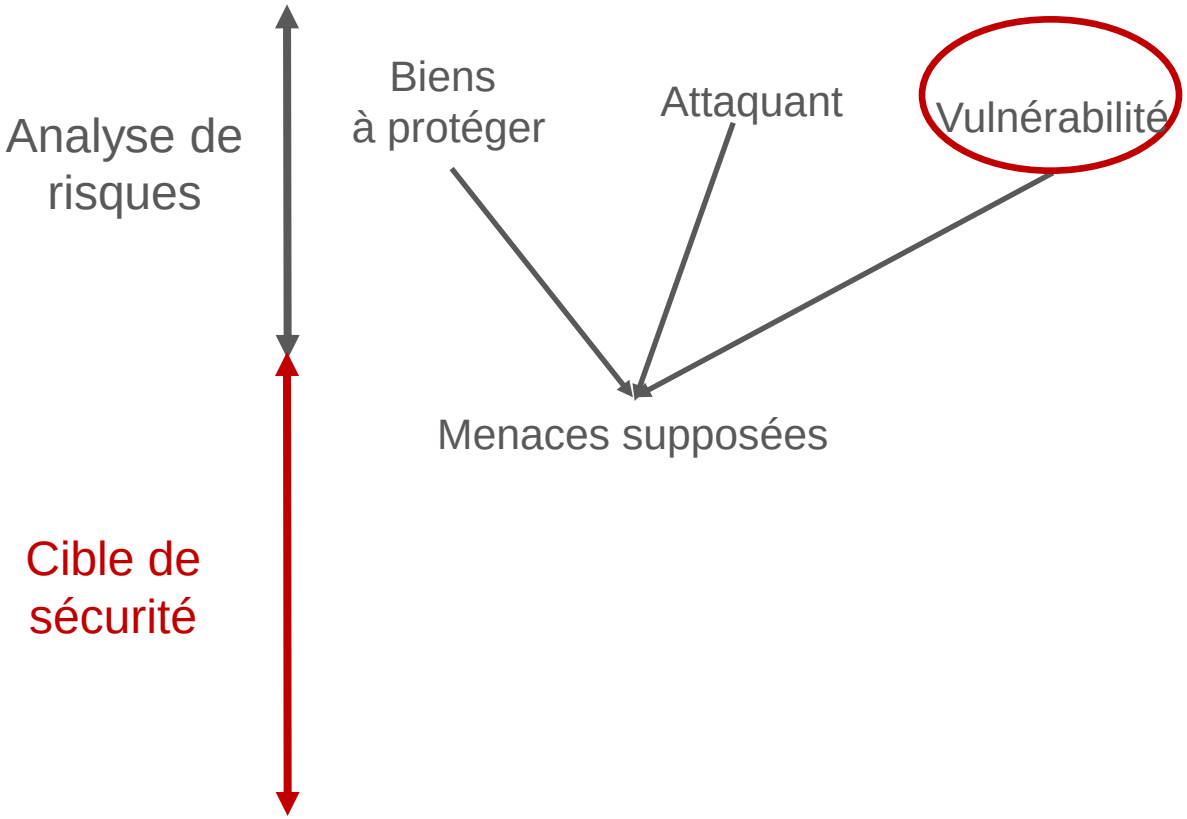
Cible de sécurité



- Toute personne ou processus voulant nuire à la sécurité de la TOE définie dans la ST
- Détenteur du passeport
- Manipulateur du passeport

Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport

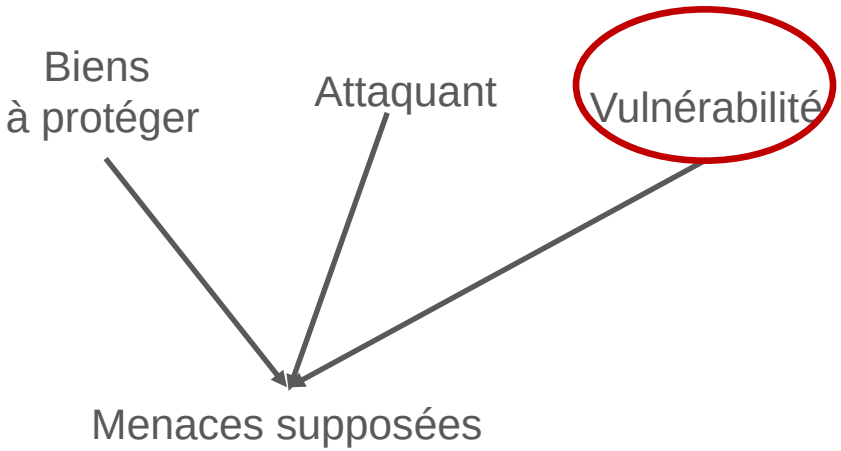


Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport

Analyse de risques

Cible de sécurité



- Imitation du système d'inspection
- Ecoute des communications
- Modification des données ou des fonctions de sécurité
- Effacement des données
- Fuite d'information
- Clonage du passeport

Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport

Analyse de risques

Cible de sécurité

Biens à protéger

Attaquant

Vulnérabilité

Menaces supposées

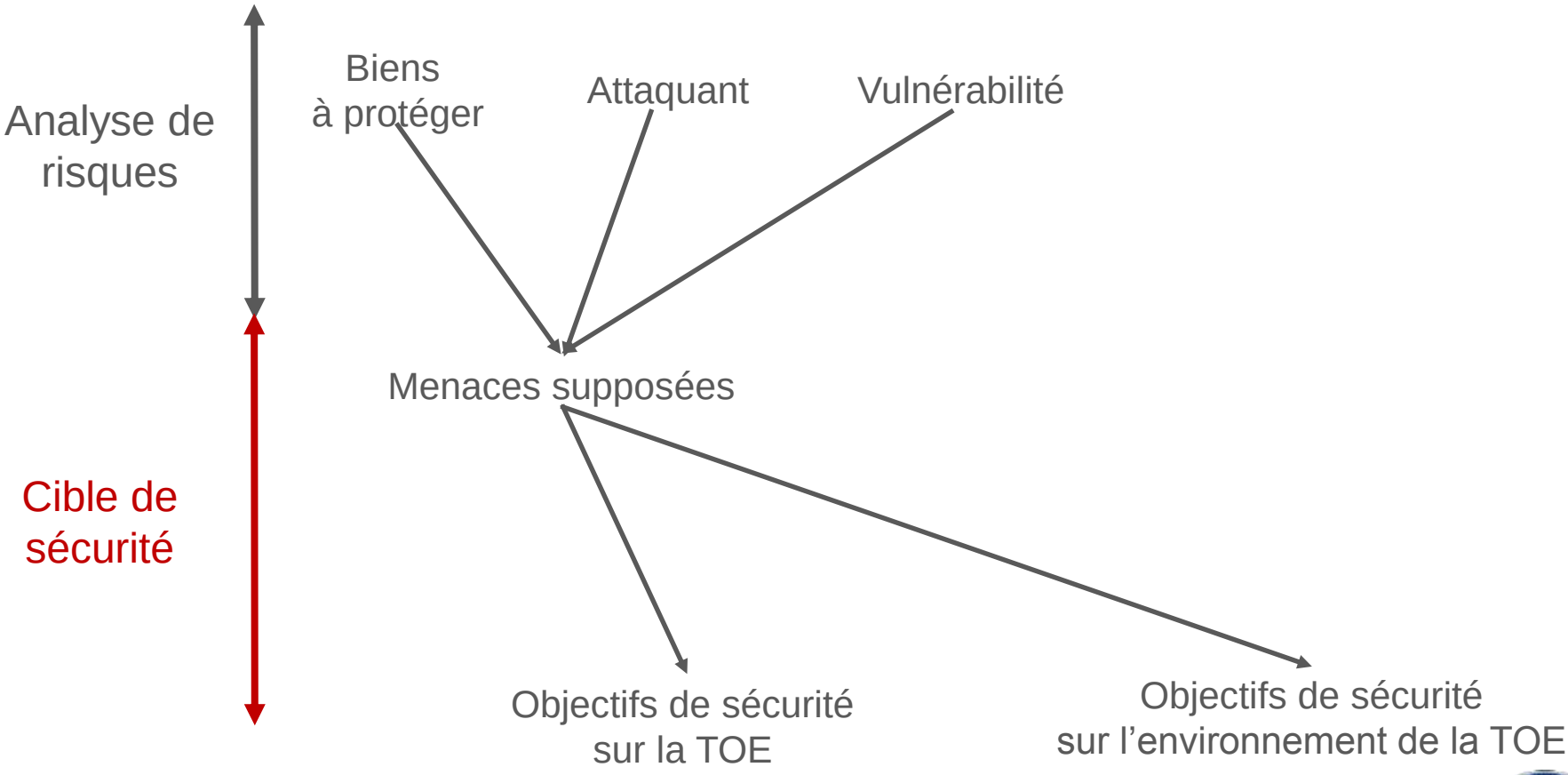
- Données stockées dans la TOE
- Personne possédant un ou plusieurs documents « légitimes »
- Clonage du passeport

T.Counterfeit	**Counterfeit of travel document chip data**
Adverse action:	An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveller by possession of a travel document. The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.
Threat agent:	having high attack potential, being in possession of one or more legitimate travel documents.
Asset:	authenticity of user data stored on the TOE

http://www.ssi.gouv.fr/IMG/certificat/ANSSI-CC-cible_2014-77en.pdf

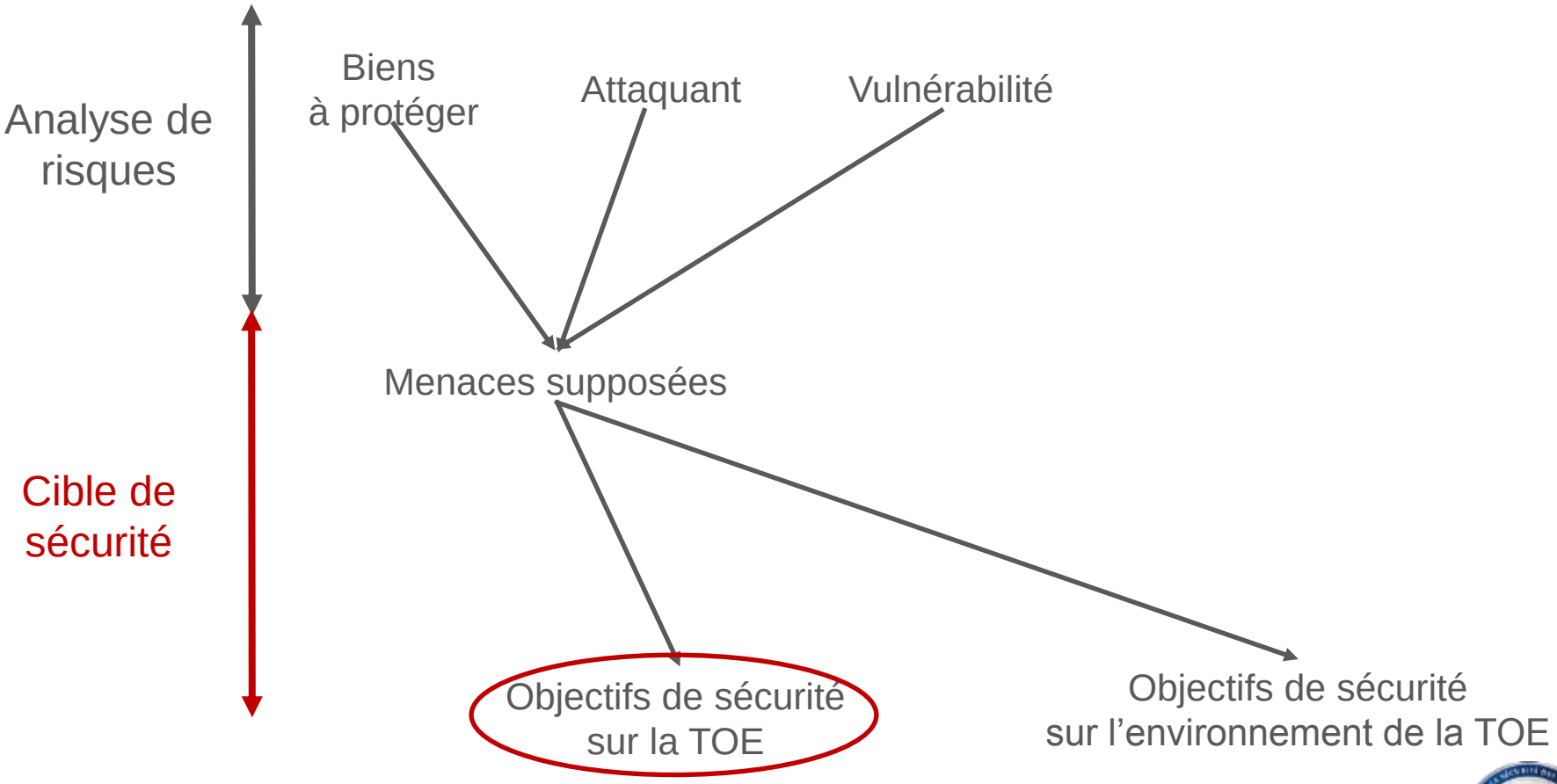
Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport



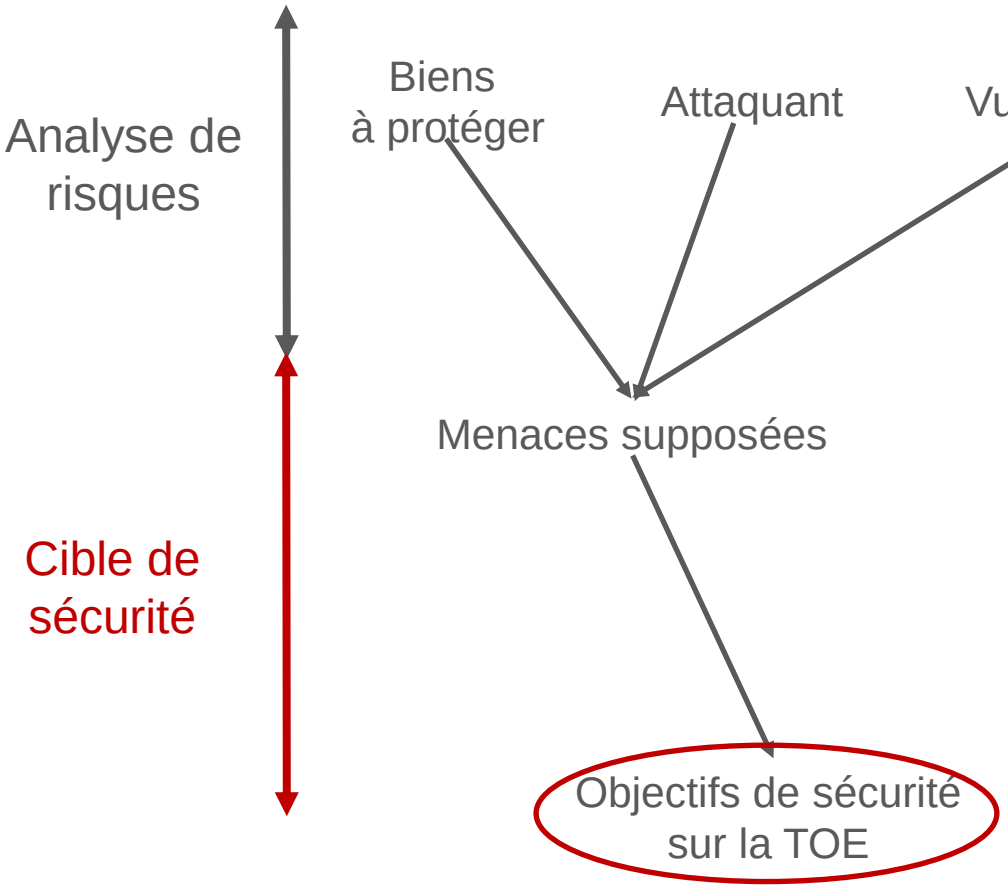
Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport



Les critères communs

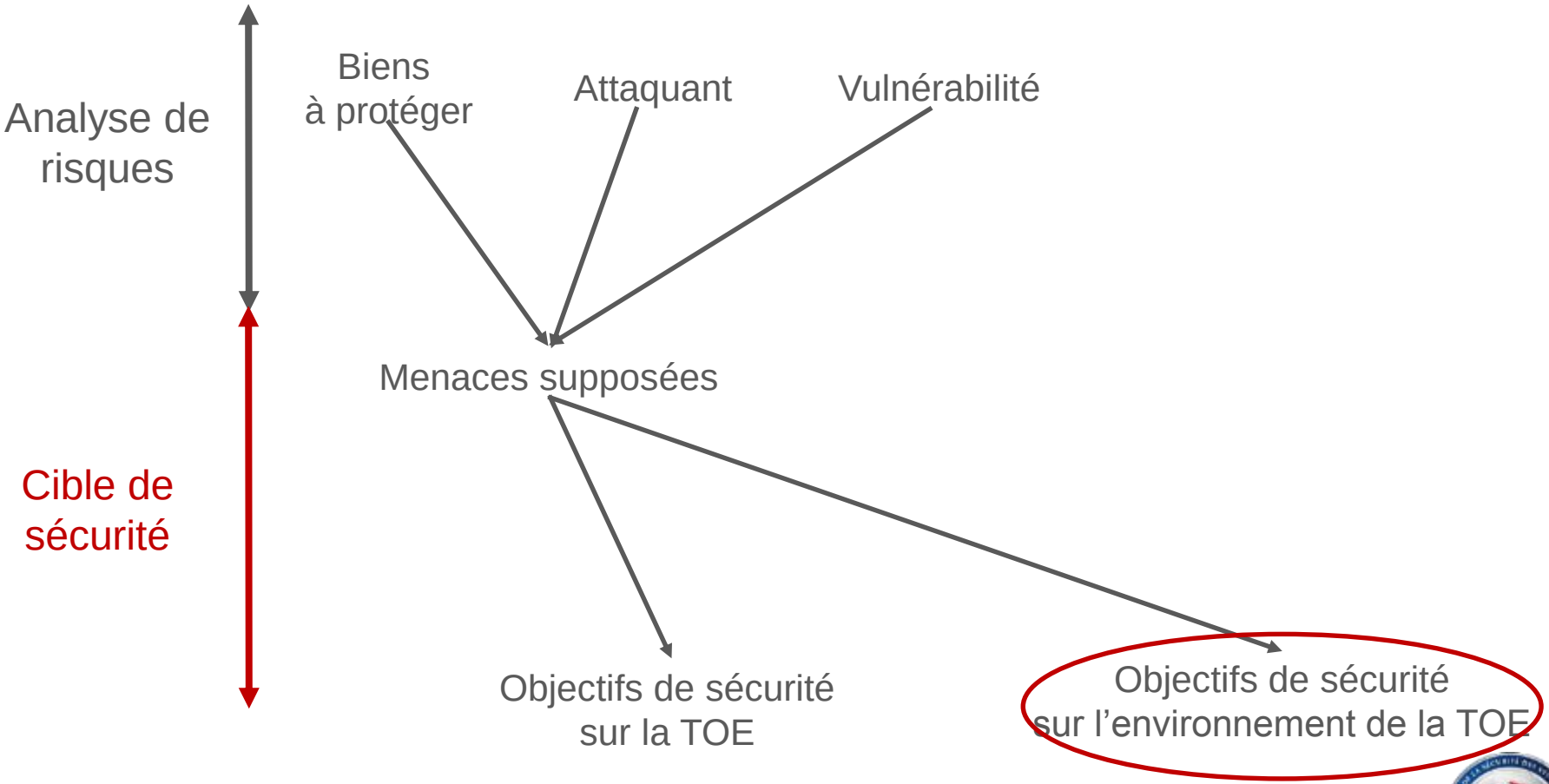
- **Quelques notions indispensables !**
  - ST Exemple du passeport



- La TOE doit assurer l'intégrité des données de l'utilisateur stockées dans le passeport et échangées pendant les communications avec le terminal
- La TOE doit assurer l'authenticité des données de l'utilisateur échangées avec le terminal
- La TOE doit assurer la confidentialité des données de l'utilisateur
- La TOE doit empêcher la récolte des données de traçabilités
- La TOE doit être protégée contre la fuite d'information, falsification, le dysfonctionnement…

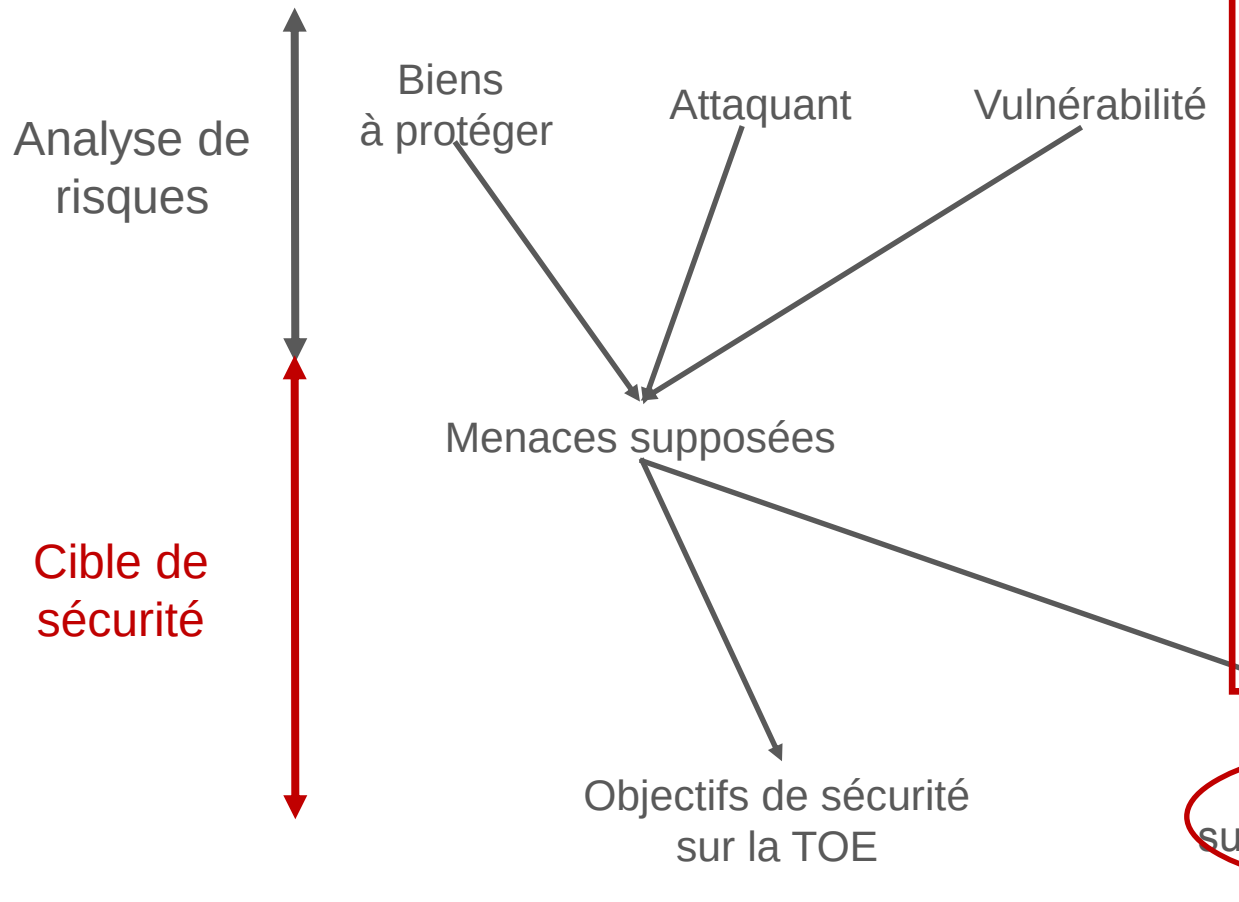
Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport



Les critères communs

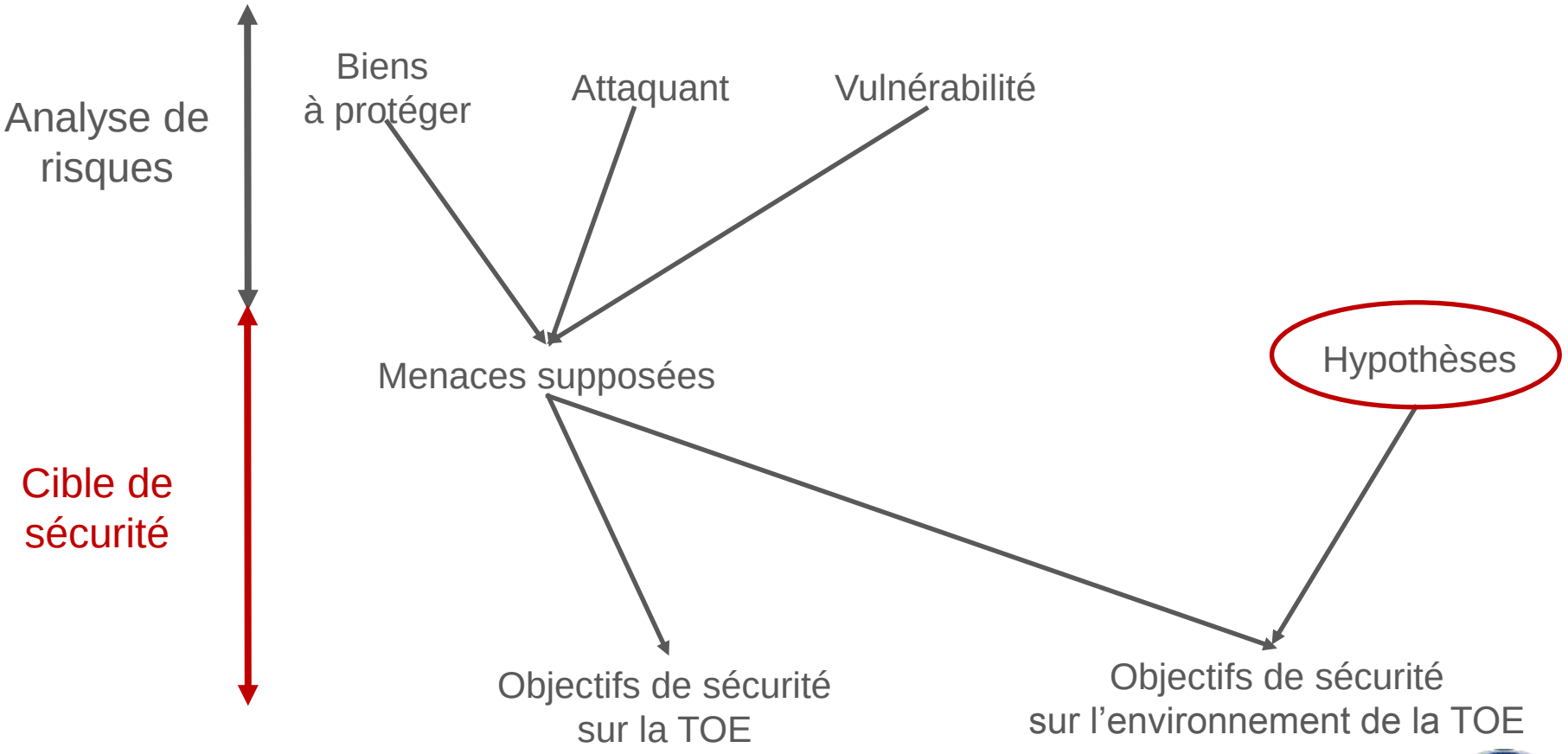
- **Quelques notions indispensables !**
  - ST Exemple du passeport



- L'émetteur du passeport doit le délivrer et accepter l'usage du terminal conformément aux lois et régulations en vigueur
- L'émetteur du passeport doit s'assurer que les agents de personnalisation inscrivent les bonnes données (identité, biométrie…)
- Le terminal doit respecter certaines règles (crypto, protocoles, confidentialité…)
- Le pays émetteur doit respecter certaines règles (infrastructures de clefs publiques, examen du passeport du voyageur pour vérifier son authenticité…)

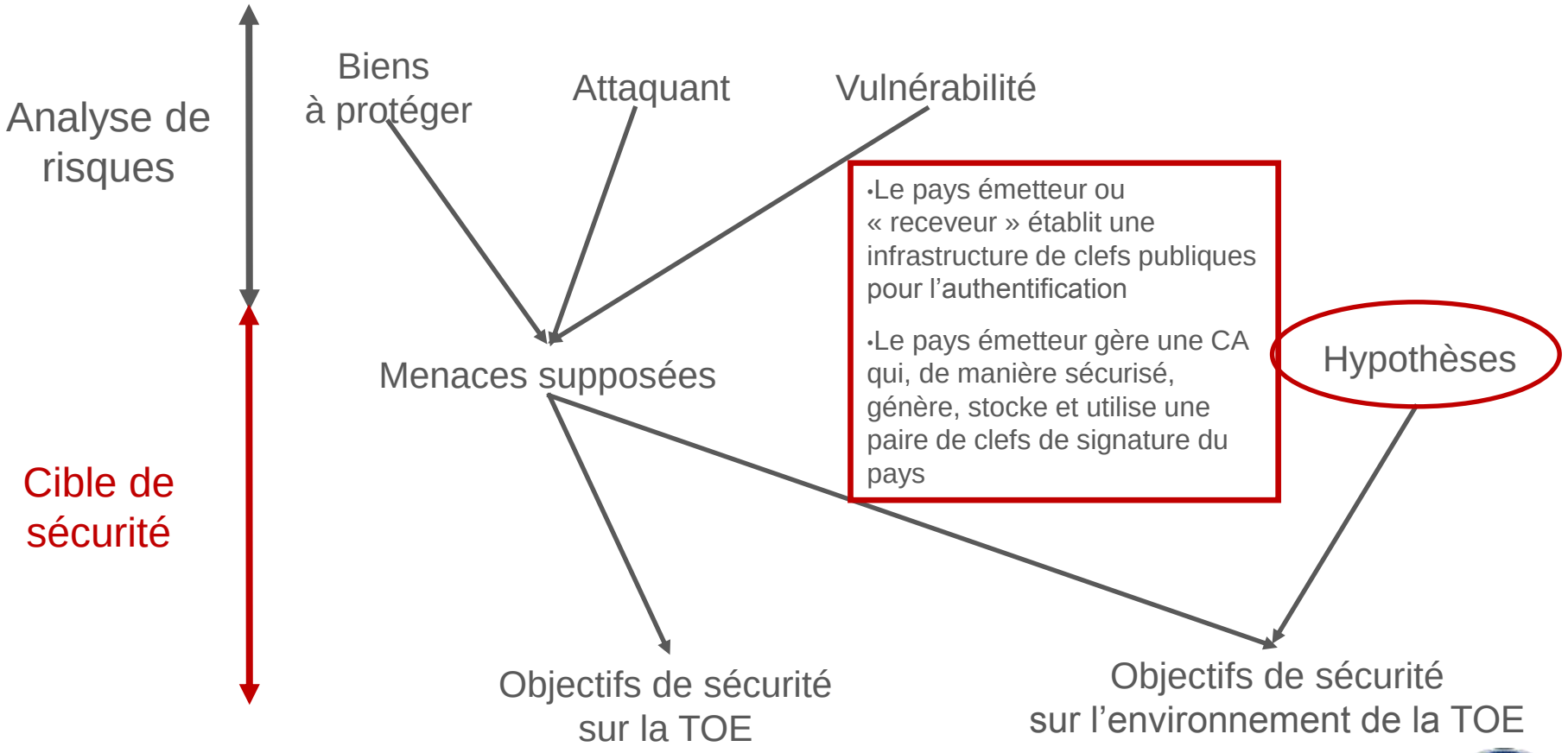
Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport



Les critères communs

- **Quelques notions indispensables !**
  - ST Exemple du passeport



Les critères communs

- **Quelques notions indispensables !**
  - PP Protection Profile – Profil de protection
    - Cible générique pour un type de produit défini et pour un usage donné
      - Contient déjà la trame (biens, menaces, objectifs…)
      - Défini déjà le besoin de sécurité
  - Rédaction par un ensemble de commanditaires ou d'acteurs d'un type de produit (PP passeport, PP SSCD, PP tachographe, PP JavaCard…)
  - Intérêt: permet de s'assurer qu'un produit est conforme à un besoin de sécurité déterminé (pas de modification de la TOE en cours d'évaluation pour échapper à des vulnérabilités)

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

Les critères communs

- **Les CC**
  - Ensemble de règles auquel un produit peut se conformer
  - Plusieurs niveaux: « EAL » (1->7)
    - Niveau de conformité ADV, AGD, ALC, ASE, ATE
    - Niveau de résistance aux attaques AVA_VAN

Les CC

Classe	Famille	EAL 1	2	3	4	5	6	7	Intitulé du composant
ADV: Développement	ADV_ARC		1	1	1	1	1	1	Security Architecture Description
	ADV_FSP	1	2	3	4	5	5	6	Functional specification
	ADV_IMP				1	1	2	2	Implementation
	ADV_INT					2	3	3	Internals structure
	ADV_SPM						1	1	Security policy model
	ADV_TDS		1	2	3	4	5	6	TOE Design
AGD: Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	Preparative procedures
ALC: Support au cycle de vie	ALC_CMC		2	3	4	4	5	5	Configuration management capabilities
	ALC_CMS	1	2	3	4	5	5	5	Configuration management scope
	ADO_DEL		1	1	1	1	1	1	Delivery
	ALC_DVS			1	1	1	2	2	Development security
	ALC_FLR								Flaw remediation
	ALC_LCD			1	1	1	1	2	Life Cycle definition
	ALC_TAT				1	2	3	3	Tools and technique
ASE: Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	Security requirements
	ASE_SPD		1	1	1	1	1	1	Security Problem definition
	ASE_TSS	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	Analysis of coverage
	ATE_DPT			1	1	3	3	4	Depth
	ATE_FUN		1	1	1	1	2	2	Functional testing
	ATE_IND	1	2	2	2	2	2	3	Independent testing
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	Vulnerabilty Analysis

Les CC

EAL

Classe	Famille	1	2	3	4	5	6	7	Intitulé du composant
ADV: Développement	ADV_ARC		1	1	1	1	1	1	Security Architecture Description
	ADV_FSP	1	2	3	4	5	5	6	Functional specification
	ADV_IMP				1	1	2	2	Implementation
	ADV_INT					2	3	3	Internals structure
	ADV_SPM						1	1	Security policy model
	ADV_TDS		1	2	3	4	5	6	TOE Design
AGD: Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	Preparative procedures
ALC: Support au cycle de vie	ALC_CMC		2	3	4	4	5	5	Configuration management capabilities
	ALC_CMS	1	2	3	4	5	5	5	Configuration management scope
	ADO_DEL		1	1	1	1	1	1	Delivery
	ALC_DVS			1	1	1	2	2	Development security
	ALC_FLR								Flaw remediation
	ALC_LCD			1	1	1	1	2	Life Cycle definition
	ALC_TAT				1	2	3	3	Tools and technique
ASE: Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	Security requirements
	ASE_SPD		1	1	1	1	1	1	Security Problem definition
	ASE_TSS	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	Analysis of coverage
	ATE_DPT			1	1	3	3	4	Depth
	ATE_FUN		1	1	1	1	2	2	Functional testing
	ATE_IND	1	2	2	2	2	2	3	Independent testing
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	Vulnerabilty Analysis

50

« The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST claim conformance »

« The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST claim conformance »

« The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST claim conformance »

« The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented »

2. CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIM

Common criteria Version:

This ST conforms to CC Version 3.1 [CC-1] [CC-2] [CC-3]

Conformance to CC part 2 and 3:

CC Part 2 extended,

– CC Part 3 conformant.

The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; [CEM] has to be taken into account.

2.2 PP CLAIM,

The eTravel Essential 1.0 BAC+AA security target claims strict conformance to the Protection Profile "Machine Readable Travel Document with ICAO Application, Basic Access Control ([PP-MRTD-BAC]).

The TOE also claims conformance to other Protection Profiles. This is described in other Security Targets:

- The eTravel Essential 1.0 EAC on PACE security target claims strict conformance to [PP-MRTD-EAC].
- The eTravel Essential 1.0 SAC security target claims strict conformance to [PP-MRTD-SAC].

2.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL4 augmented with ALC_DVS.2 defined in CC part 3 [CC-3].

2.4 CONFORMANCE STATEMENT

This ST strictly conforms to [PP-MRTD-BAC].

« The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST claim conformance »

« The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented »

2. CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIM

Common criteria Version:

This ST conforms to CC Version 3.1 [CC-1] [CC-2] [CC-3]

Conformance to CC part 2 and 3:

CC Part 2 extended,

– CC Part 3 conformant.

The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; [CEM] has to be taken into account.

2.2 PP CLAIM,

The eTravel Essential 1.0 BAC+AA security target claims strict conformance to the Protection Profile "Machine Readable Travel Document with ICAO Application, Basic Access Control ([PP-MRTD-BAC]).

The TOE also claims conformance to other Protection Profiles. This is described in other Security Targets:

- The eTravel Essential 1.0 EAC on PACE security target claims strict conformance to [PP-MRTD-EAC].
- The eTravel Essential 1.0 SAC security target claims strict conformance to [PP-MRTD-SAC].

2.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL4 augmented with ALC_DVS.2 defined in CC part 3 [CC-3].

2.4 CONFORMANCE STATEMENT

This ST strictly conforms to [PP-MRTD-BAC].

Les CC

EAL

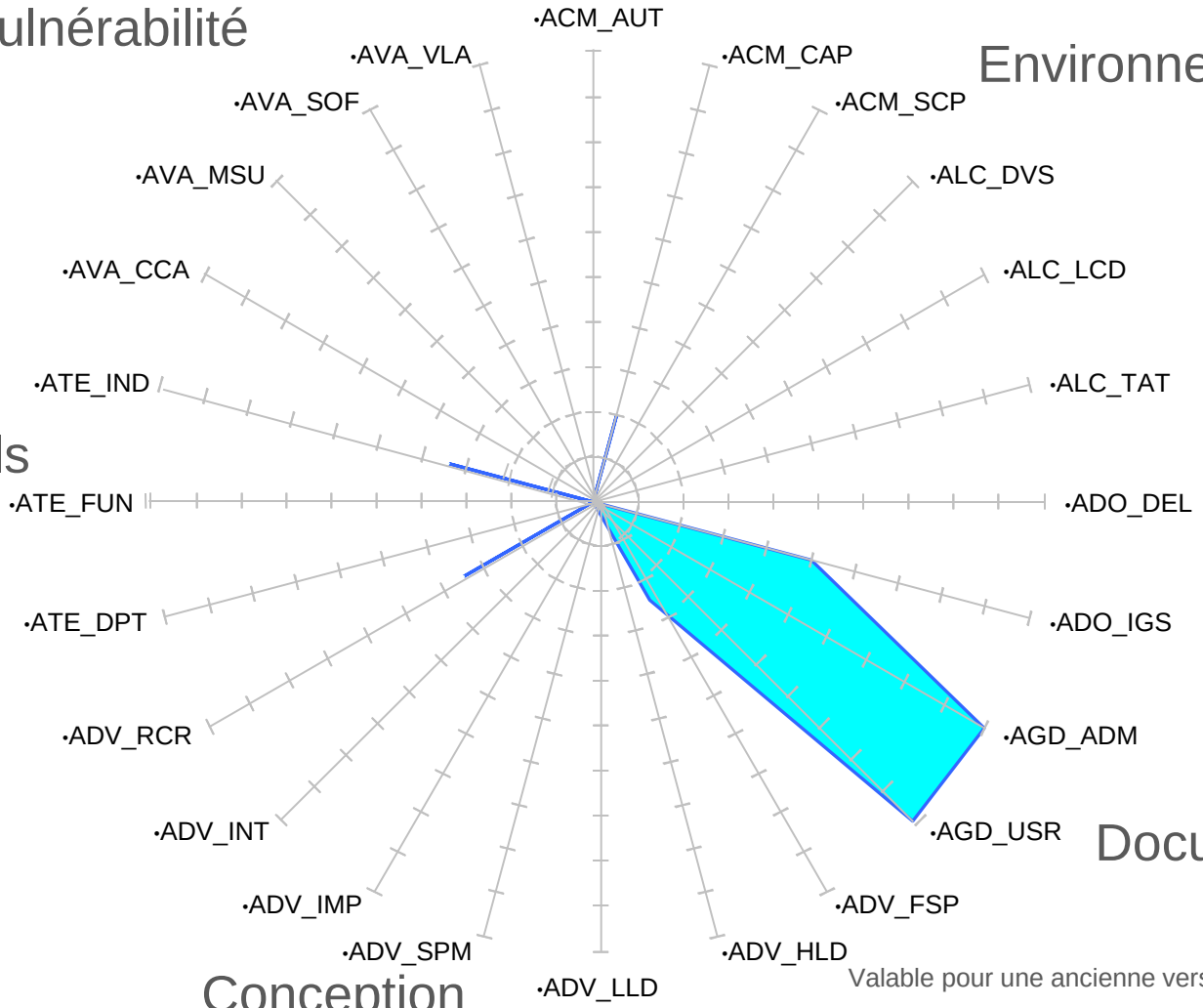
Classe	Famille	1	2	3	4	5	6	7	Intitulé du composant
ADV: Développement	ADV_ARC		1	1	1	1	1	1	Security Architecture Description
	ADV_FSP	1	2	3	4	5	5	6	Functional specification
	ADV_IMP				1	1	2	2	Implementation
	ADV_INT					2	3	3	Internals structure
	ADV_SPM						1	1	Security policy model
	ADV_TDS		1	2	3	4	5	6	TOE Design
AGD: Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	Preparative procedures
ALC: Support au cycle de vie	ALC_CMC		2	3	4	4	5	5	Configuration management capabilities
	ALC_CMS	1	2	3	4	5	5	5	Configuration management scope
	ADO_DEL		1	1	1	1	1	1	Delivery
	ALC_DVS			1	1	1	2	2	Development security
	ALC_FLR								Flaw remediation
	ALC_LCD			1	1	1	1	2	Life Cycle definition
	ALC_TAT				1	2	3	3	Tools and technique
ASE: Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	Security requirements
	ASE_SPD		1	1	1	1	1	1	Security Problem definition
	ASE_TSS	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	Analysis of coverage
	ATE_DPT			1	1	3	3	4	Depth
	ATE_FUN		1	1	1	1	2	2	Functional testing
	ATE_IND	1	2	2	2	2	2	3	Independent testing
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	Vulnerabilty Analysis

Les critères communs

Analyse de vulnérabilité

Environnement

Test fonctionnels



Documentation

EAL 1

Conception

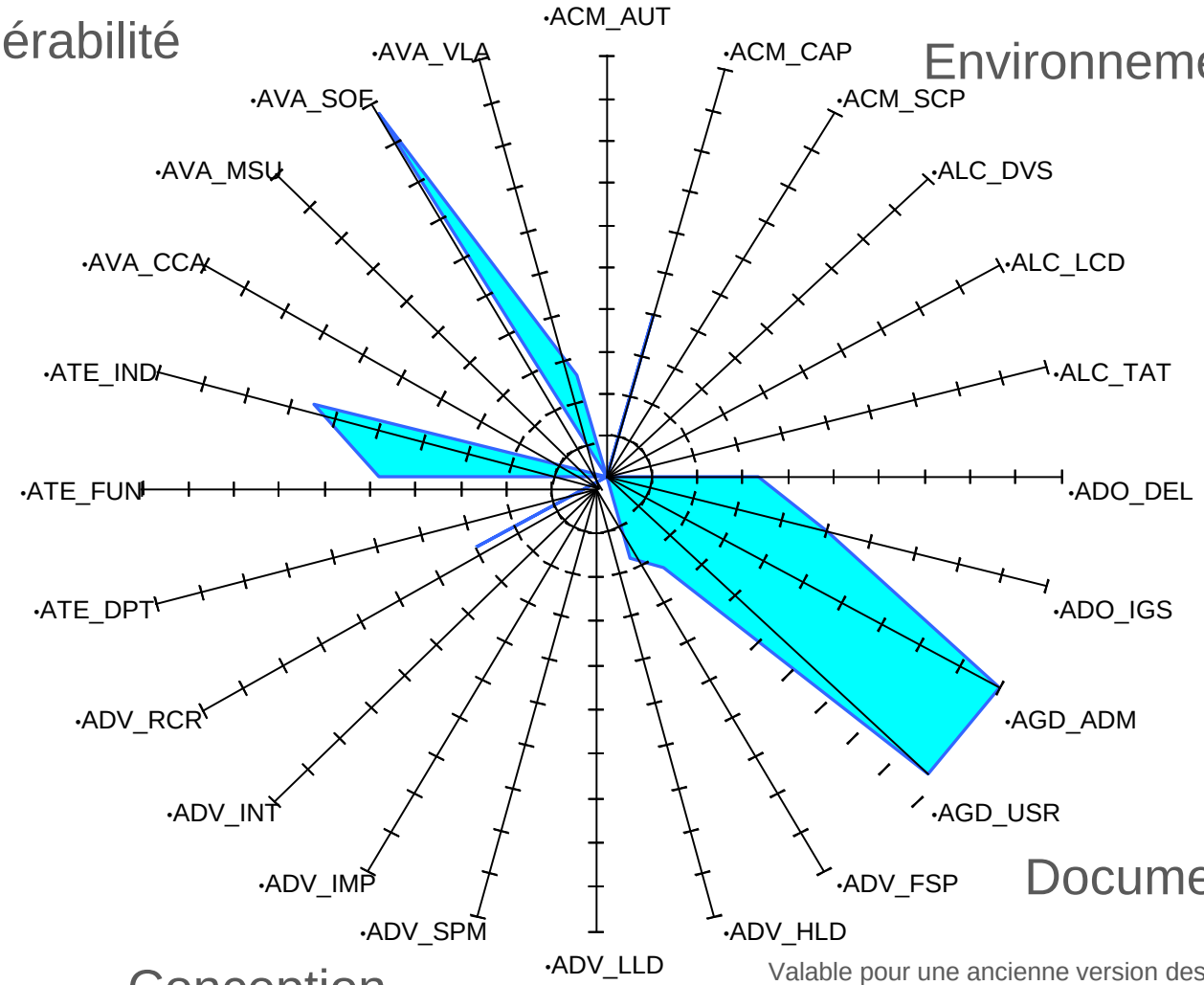
Valable pour une ancienne version des Critères Communs

Les critères communs

Analyse de vulnérabilité

Environnement

Test fonctionnels



EAL 2

Documentation

Conception

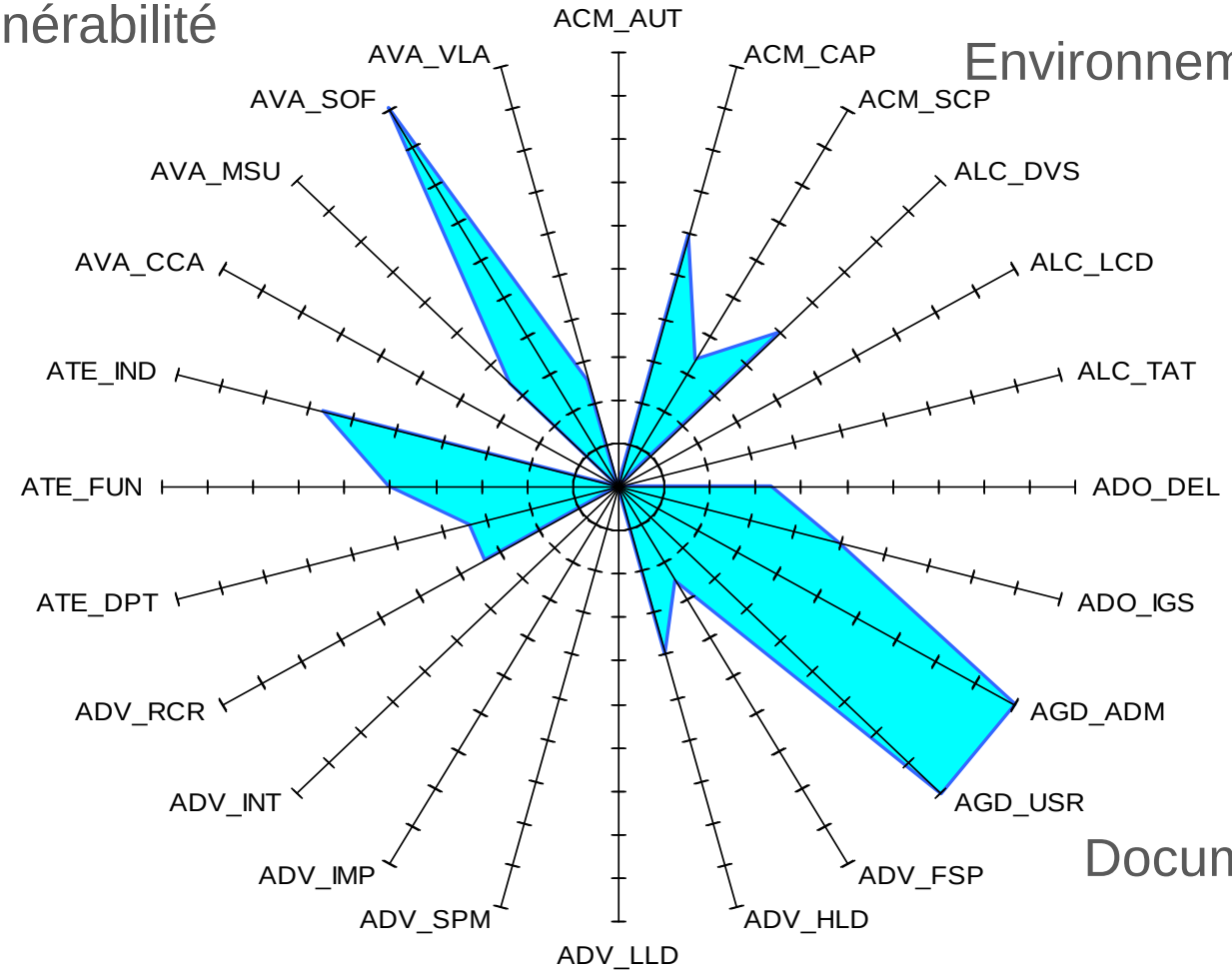
Valable pour une ancienne version des Critères Communs

Les critères communs

Analyse de vulnérabilité

Environnement

Test fonctionnels



Documentation

EAL 3

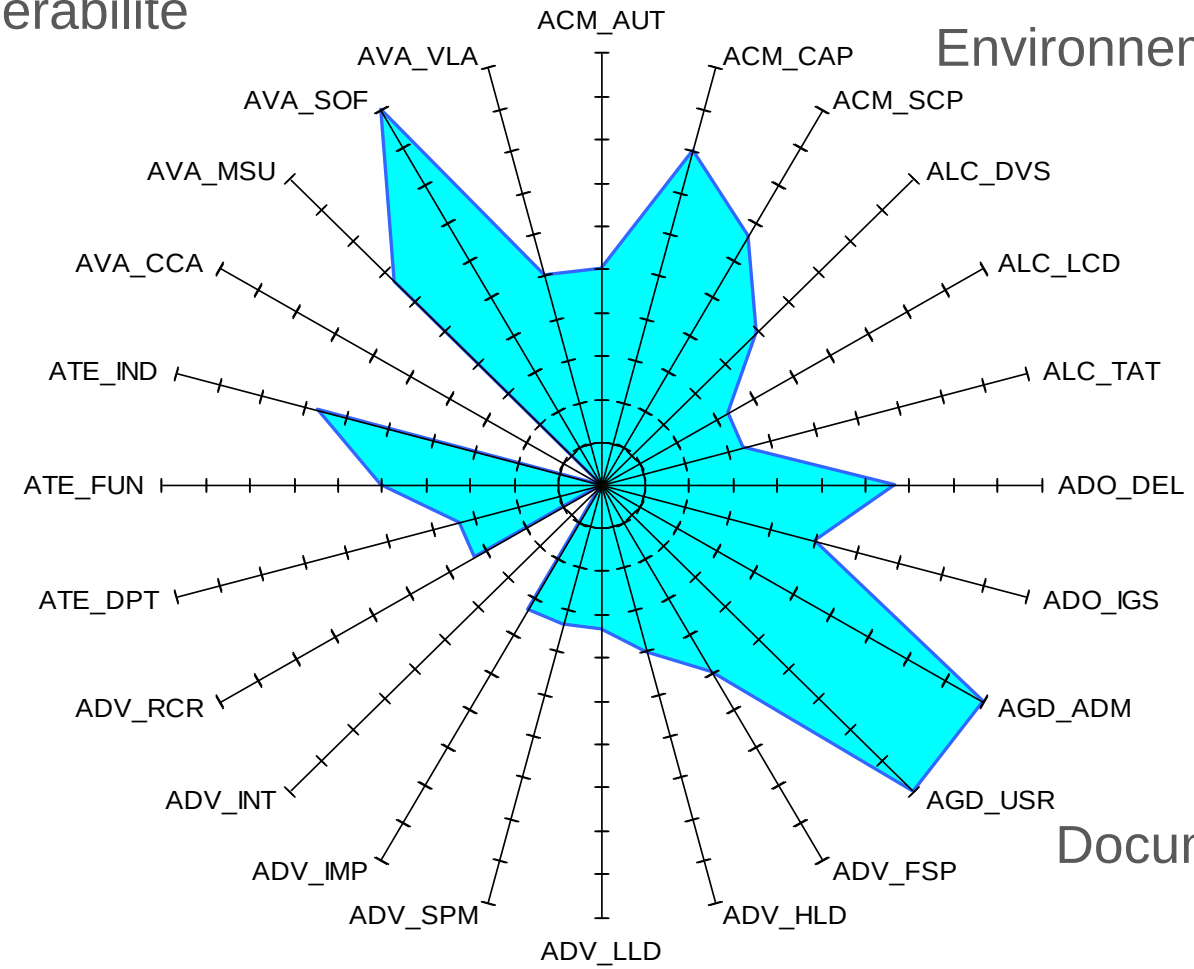
Conception

Valable pour une ancienne version des Critères Communs

Les critères communs

Analyse de vulnérabilité

Environnement



Test fonctionnels

Documentation

EAL 4

Conception

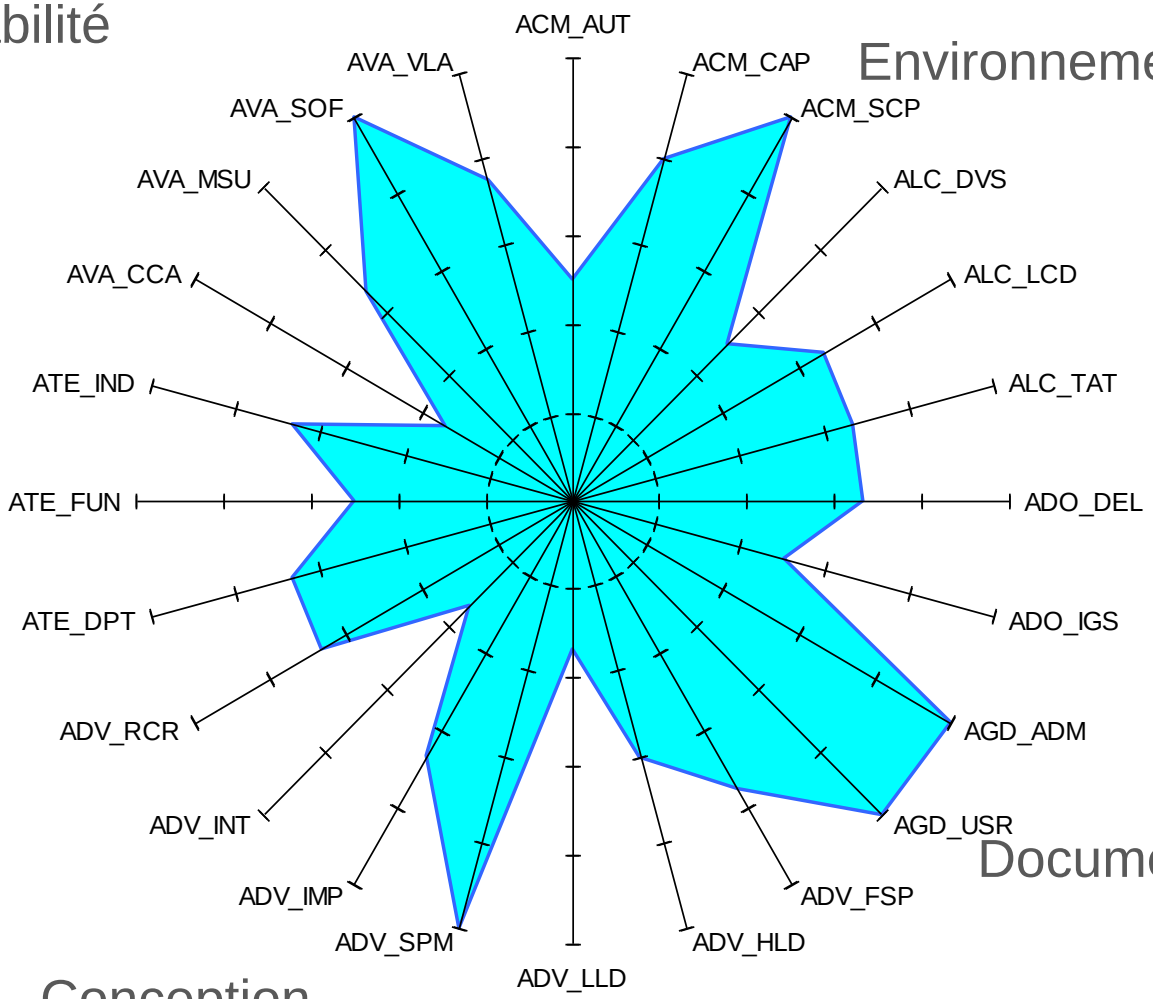
Valable pour une ancienne version des Critères Communs

Les critères communs

Analyse de vulnérabilité

Environnement

Test fonctionnels



Documentation

EAL 5

Conception

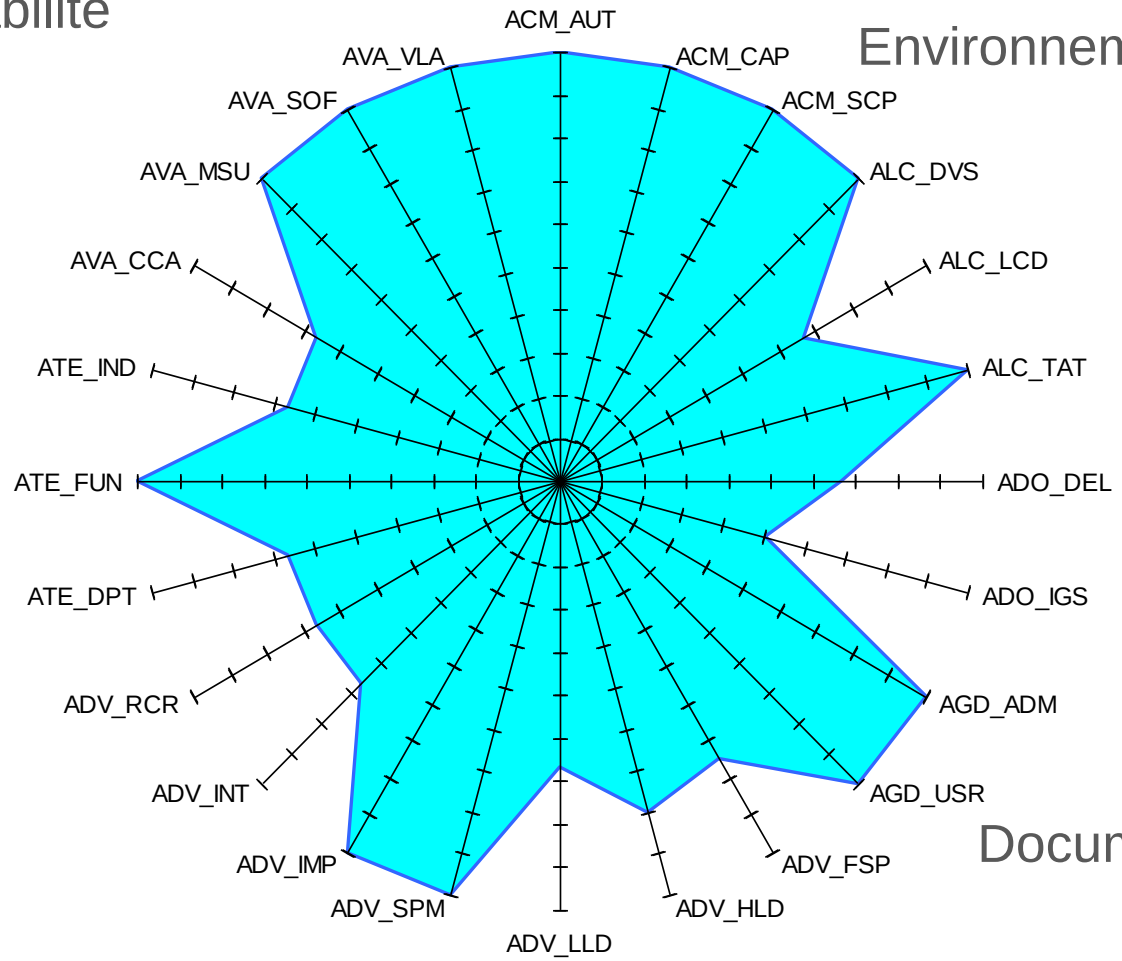
Valable pour une ancienne version des Critères Communs

Les critères communs

Analyse de vulnérabilité

Environnement

Test fonctionnels



Documentation

EAL 6

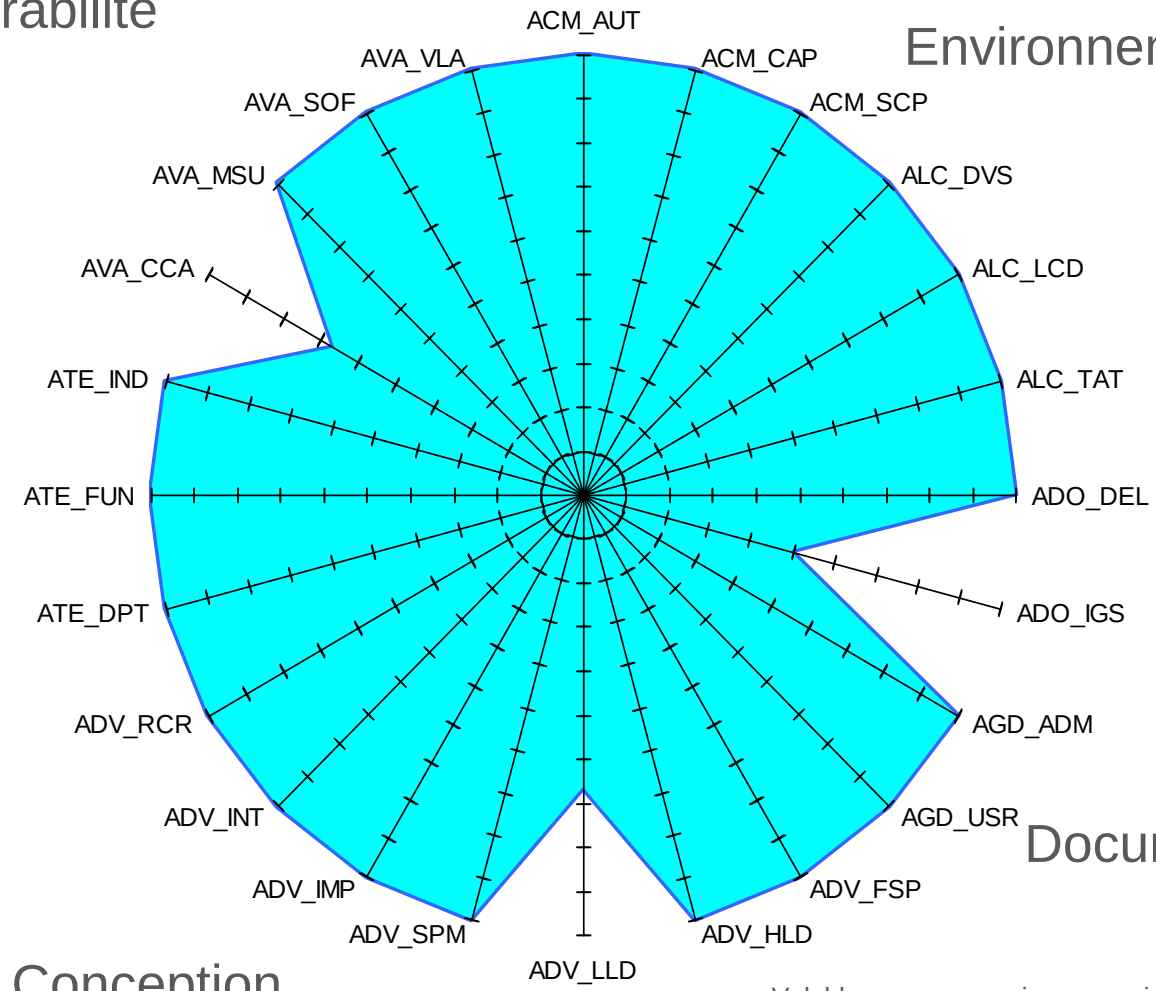
Conception

Valable pour une ancienne version des Critères Communs

Les critères communs

Analyse de vulnérabilité

Environnement



Test fonctionnels

Documentation

EAL 7

Conception

Valable pour une ancienne version des Critères Communs

Les critères communs

- **Niveau des certification de produit en général…**
  - Microcircuits EAL5-6, AVA_VAN.5
  - Cartes à puce EAL4-5, AVA_VAN.5
  - Logiciels EAL3, AVA_VAN.3

Les critères communs

- **Le niveau AVA_VAN**
  - Dans les critères*: succinct mais objectif !

Les critères communs

- **Le niveau AVA_VAN**
  - Dans les critères*: succinct mais objectif !
    - “The developer shall provide the TOE for testing”

Les critères communs

- **Le niveau AVA_VAN**
  - Dans les critères*: succinct mais objectif !
    - “The developer shall provide the TOE for testing”
    - “The TOE shall be suitable for testing”

Les critères communs

- **Le niveau AVA_VAN**
  - Dans les critères*: succinct mais objectif !
    - “The developer shall provide the TOE for testing”
    - “The TOE shall be suitable for testing”
    - “The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE”

Les critères communs

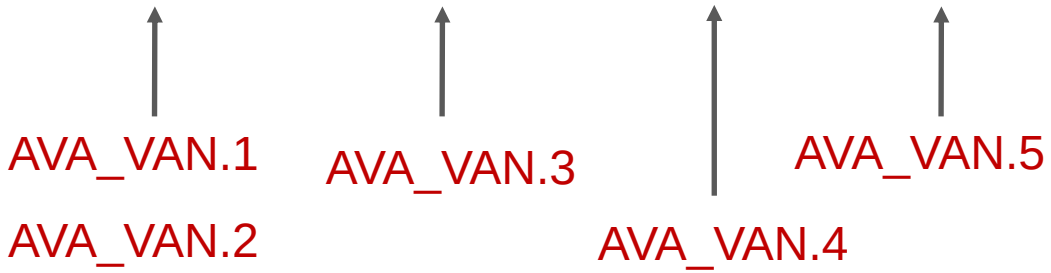
- **Le niveau AVA_VAN**
  - Dans les critères*: succinct mais objectif !
    - “The developer shall provide the TOE for testing”
    - “The TOE shall be suitable for testing”
    - “The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE”
    - “The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE”

Les critères communs

- **Le niveau AVA_VAN**
  - Dans les critères*: succinct mais objectif !
    - “The developer shall provide the TOE for testing”
    - “The TOE shall be suitable for testing”
    - “The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE”
    - “The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE”
    - “The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing Basic / Enhanced-Basic / Moderate / High attack potential”

Les critères communs

- **Le niveau AVA_VAN**
  - Dans les critères*: succinct mais objectif !
    - “The developer shall provide the TOE for testing”
    - “The TOE shall be suitable for testing”
    - “The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE”
    - “The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE”
    - “The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing Basic / Enhanced-Basic / Moderate / High attack potential”



Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
  - Avec un table de cotation :

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

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
  - Avec un table de cotation :

AVA_VAN.1-2 →

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

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
  - Avec un table de cotation :

AVA_VAN.1-2 →
AVA_VAN.3 →

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

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
  - Avec un table de cotation :

AVA_VAN.1-2 →
AVA_VAN.3 →
AVA_VAN.4 →

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

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
  - Avec un table de cotation :

	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 critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment définir le potentiel d'attaque (Basic – enhanced-basic, moderate et High) ?
  - Avec un table de cotation :

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

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?
    - 5 critères:
      - Temps passé

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?
    - 5 critères:
      - Temps passé
      - Niveau d'expertise

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?
    - 5 critères:
      - Temps passé
      - Niveau d'expertise
      - Connaissance du produit

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?
    - 5 critères:
      - Temps passé
      - Niveau d'expertise
      - Connaissance du produit
      - Nombre d'échantillons nécessaire

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?
    - 5 critères:
      - Temps passé
      - Niveau d'expertise
      - Connaissance du produit
      - Nombre d'échantillons nécessaire
      - Equipement nécessaire

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?
    - 5 critères:
      - Temps passé
      - Niveau d'expertise
      - Connaissance du produit
      - Nombre d'échantillons nécessaire
      - Equipement nécessaire
    - A chaque critère une table de cotation

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?
    - 5 critères:
      - 1) Temps passé

	Identification	Exploitation
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*

Table 1: Rating for Elapsed Time

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?
    - 5 critères:
      - 2) Niveau d'expertise

	Identification	Exploitation
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6

Table 4: Rating for Expertise

- 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)

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?
    - 5 critères:
      - 3) Connaissance du produit

	Identification	Exploitation
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA

Table 5: Rating for Knowledge of TOE

- Public: information dans le domaine publique
- Restricted: information utilisé lors du développement de la puce (spécifications, guides, documents de préparation…)
- Sensitive: information HLD et LLD
- Critical: implémentation (design et code source)
- Very critical: informations et outils spécifiques et propre au produit

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?
    - 5 critères:
      - 4) Nombre d'échantillons nécessaire

	Identification	Exploitation
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*

Table 6: Rating for Access to TOE

Les critères communs

- **Le niveau AVA_VAN pour les Cartes à puce**
  - Comment coter une attaque ?
    - 5 critères:
      - 5) Equipement nécessaire

	Identification	Exploitation
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8

Table 9: Rating for Equipment

- Standard: oscilloscope de base, lecteur de carte, PC, logiciel d'analyse ou de génération de signal…
- Specialized: oscilloscope haut de gamme, microscope UV, equipement lazer, micro sonde, outils de gravure chimique…
- Bespoke: FIB (Focused Ion Beam), SEM (Scanning electron mircroscope), AFM (Atomic Force Microscope)…
- Multiple Bespoke: équipements « bespoke » sur différents niveaux de l'attaque

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

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

TOTAL

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

Les CC

- **Un exemple de cotation d'une DPA**

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

Les CC

- **Un exemple de cotation d'une DPA**

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

Les CC

- **Un exemple de cotation d'une DPA**

- 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)

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

Les CC

- **Un exemple de cotation d'une DPA**

  - Standard: oscilloscope de base, lecteur de carte, PC, logiciel d'analyse ou de génération de signal…
  - Specialized: oscilloscope haut de gamme, microscope UV, equipement lazer, micro sonde, outils de gravure chimique…
  - Bespoke: FIB (Focused Ion Beam), SEM (Scanning electron mircroscope), AFM (Atomic Force Microscope)…
  - Multiple Bespoke: équipements « bespoke » sur différents niveaux de l'attaque

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

Les CC

- **Un exemple de cotation d'une DPA**

  - Standard: oscilloscope de base, lecteur de carte, PC, logiciel d'analyse ou de génération de signal…
  - Specialized: oscilloscope haut de gamme, microscope UV, equipement lazer, micro sonde, outils de gravure chimique…
  - Bespoke: FIB (Focused Ion Beam), SEM (Scanning electron mircroscope), AFM (Atomic Force Microscope)…
  - Multiple Bespoke: équipements « bespoke » sur différents niveaux de l'attaque

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

Les CC

- **Un exemple de cotation d'une DPA**
  - Total : 15 points

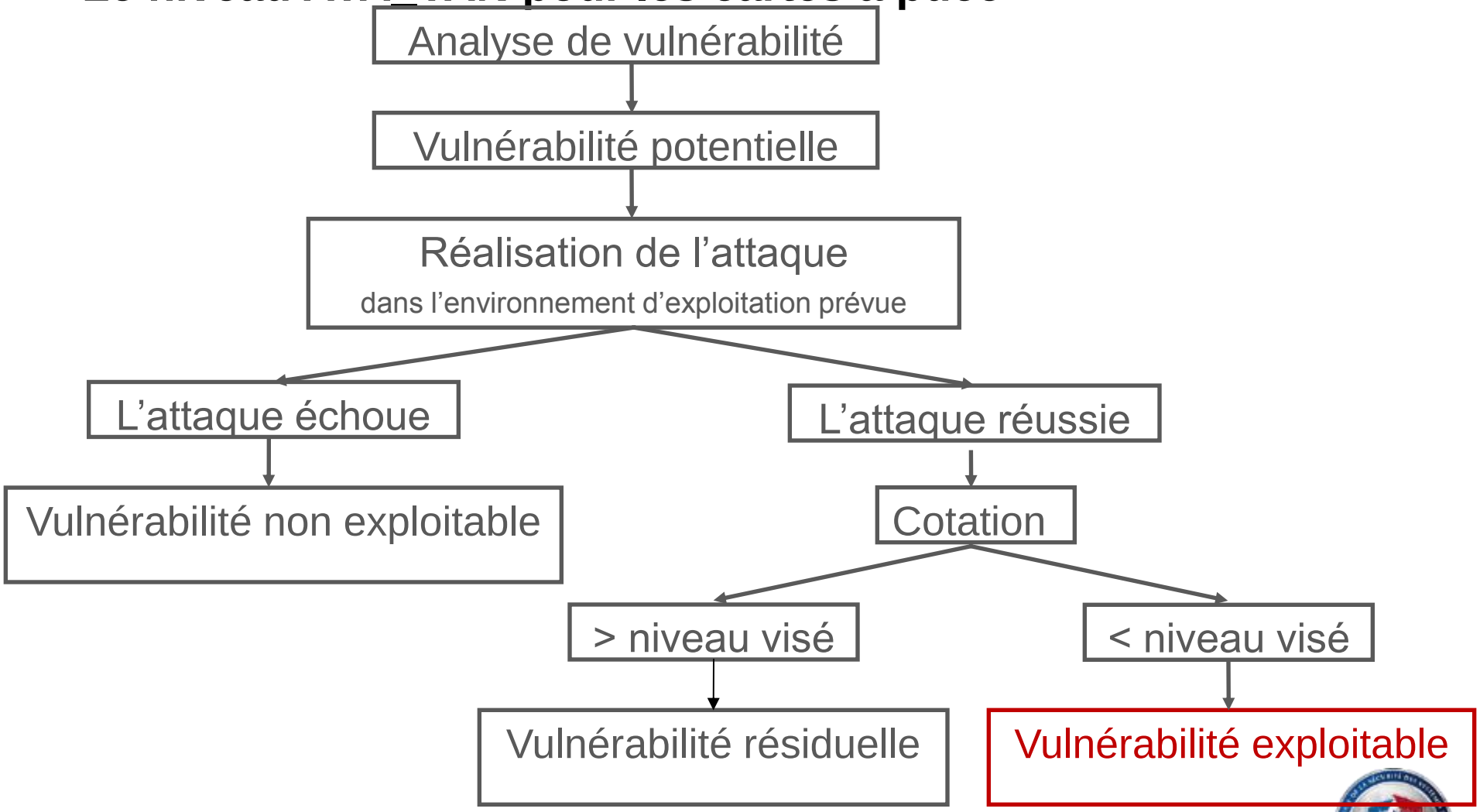
Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical 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

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

Les critères communs

- **Le niveau AVA_VAN pour les cartes à puce**



La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **CESTI : Centre d'Evaluation de la sécurité des Technologies de l'Information**
  - Ce sont les personnes qui réalisent les tests et les analyses
  - Laboratoires agrées par l'ANSSI
    - Compétence
    - Expertise dans certains domaines
  - Pour les CC, reconnu à l'international (CCRA, SOGIS)

La certification

- **CESTI : Centre d'Evaluation de la sécurité des Technologies de l'Information**
  - Seuls à pouvoir mener une évaluation CC et CSPN et à pouvoir soumettre leurs résultats d'évaluation à l'ANSSI
  - 9 laboratoires :
    - 3 CC/CSPN matériel (Leti, Serma, Thales)
    - 3 CC/CSPN logiciel (Amossys, Oppida Sogeti)
    - 3 uniquement CSPN logiciel (Lexfo, Quarkslab, Trusted Labs)

La certification

- **La validation des résultats des CESTI**
  - RTE : Rapport Technique d'Evaluation
    - Soumis à l'ANSSI en fin d'évaluation
    - Résultats d'évaluation
      - Niveau conformité ADV, AGD, ALC, ASE, ATE
      - Niveau technique AVA
    - Verdict final (le produit est-il bien résistant au niveau visé ?)
    - Confidentiel !
    - Validé (ou pas) par le CCN avec l'aide d'experts techniques internes suivants les domaines
    - Si validation, donne lieu à un certificat et un rapport de certification

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

Les spécificités françaises

La CSPN

- **Certification de Sécurité de Premier Niveau**
- **Création en 2006**
- **Début de l'expérimentation en 2008**
- **Officialisation en 2011**

La CSPN

- **Qu'est qu'une CSPN ?**
  - Méthodologie publique française
  - Expertise technique avec des méthodes d'évaluation spécifique
  - Différents domaines
    - Détection d'intrusion
    - Anti-virus
    - Pare-feu
    - Contrôle d'accès
    - Stockage sécurisé
    - Set Top Box
    - Matériel, logiciel embarqué…

La CSPN

- **Qu'est qu'une CSPN ?**
  - Charges contraintes de 25h.j. + 10h.j. si crypto
  - Si cryptographie analyse obligatoire
  - Boîte noire
  - Niveau unique
  - Pas de correction possible du produit
  - Processus mis en place en 2008
  - Beaucoup d'échecs !

La CSPN

- **Les raisons de la création de la CSPN :**
  - Les évaluations CC coûtent cher… et sont souvent longues (parfois 1 an ou 2, phénomène essentiellement lié à la maturité des développeurs et du produit)
  - L'évaluation CC est un processus mal adapté aux produits à faible retour sur investissement
  - En 2008, mise en place d'un processus d'évaluation en charges et temps contraints

La CSPN

CC	CSPN
EAL 1 à 7	Niveau unique
Boîte grise-blanche	Boîte noire
Accords de reconnaissance des certificats	Aucun accord : reconnaissance franco-française
Pas de contraintes de temps	Temps imposé: 25 h.j (+10 si crypto), adaptation si cas particulier
Mise à jour du produit possible durant l'évaluation	Version du produit figée
Connaissance des CC par le développeur pour fournir des documents conformes	Aucune connaissance spécifique nécessaire pour le développeur
Coût relativement élevé (60 à 200K€)	Coût relativement faible (25 à 35K€)

La CSPN

- **Exemple de certificats et rapports de certification CSPN (recherche sur le site)**

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La certification

- **Un peu de vocabulaire….**
  - CCN Centre de Certification National
  - SOGIS Senior Officials Group Information Systems Security
  - CCRA Common Criteria Recognition Arrangement
  - TOE Target Of Evaluation (Cible d'évaluation)
  - ST Security Target (Cible de sécurité)
  - PP Profil de Protection
  - EAL Evaluation Assurance Level
  - CC Critères Communs
  - CESTI Centre d'Évaluation de la Sécurité des Technologies de l'Information
  - RTE Rapport Technique d'Évaluation
  - CSPN Certification de Sécurité de Premier Niveau

La maintenance

- **Continuité de l'assurance d'un produit certifié**
- **Implique une analyse d'impact**
- **Génère un rapport de maintenance si impact mineur sur la sécurité**
- **Implique une réévaluation si impact majeur sur la sécurité (évaluation partielle d'un produit certifié en utilisant les résultats de l'évaluation précédente)**

La surveillance

- **Vérification périodique de l'évolution de la résistance aux attaques d'un produit donné dans le temps**
  - Le produit évalué ne change pas
  - La classe AVA_VAN est mise à jour par le CESTI
    - Même niveau que l'évaluation :
      - rapport de surveillance avec le même niveau que le certificat initial
    - Changement de niveau :
      - rapport de surveillance avec un niveau inférieur au certificat initial
      - Ou mise à jour des guides sécuritaires du produit pour augmenter la résistance du produit et donc émission d'un rapport avec le même niveau que le certificat initial

La qualification

- Se fait dans le cadre du Référentiel Général de Sécurité (RGS)
- Cible validée par l'ANSSI
- Analyse cryptographique obligatoire
- Trois niveaux :
  - Elémentaire (CSPN)
  - Standard (CC EAL3+FLR.3+VAN.3) + expertise crypto selon le RGS
  - Renforcé (CC EAL4+FLR.3+VAN.5) + expertise crypto selon le RGS

Motivations et retour d’expérience

Les motivations

- **Approche sécuritaire**
- **Approche marketing**
- **Approche réglementaire**

Les motivations

- **Approche sécuritaire**
  - Se convaincre que la solution utilisée est sûre
    - En visant un haut niveau de confiance
    - En ne publiant pas forcément les certificats
    - Et en faisant parfois réaliser des expertises complémentaires
    - En centrant l'évaluation sur l'analyse de vulnérabilités
  - Donneurs d'ordre : banques, opérateurs de télécommunications, défense…

Les motivations

- **Approche marketing**
  - Syndrome du contrôle technique automobile:
    - Peu importe ce que l'on évalue, qui fait l'évaluation, où elle se déroule: l'important est d'avoir le certificat…
  - Le prix est prépondérant
  - Les CC ont mis un peu d'ordre dans la définition des TOE
  - Généralement conduite par les développeurs (exemples: éditeurs de produits de sécurité)

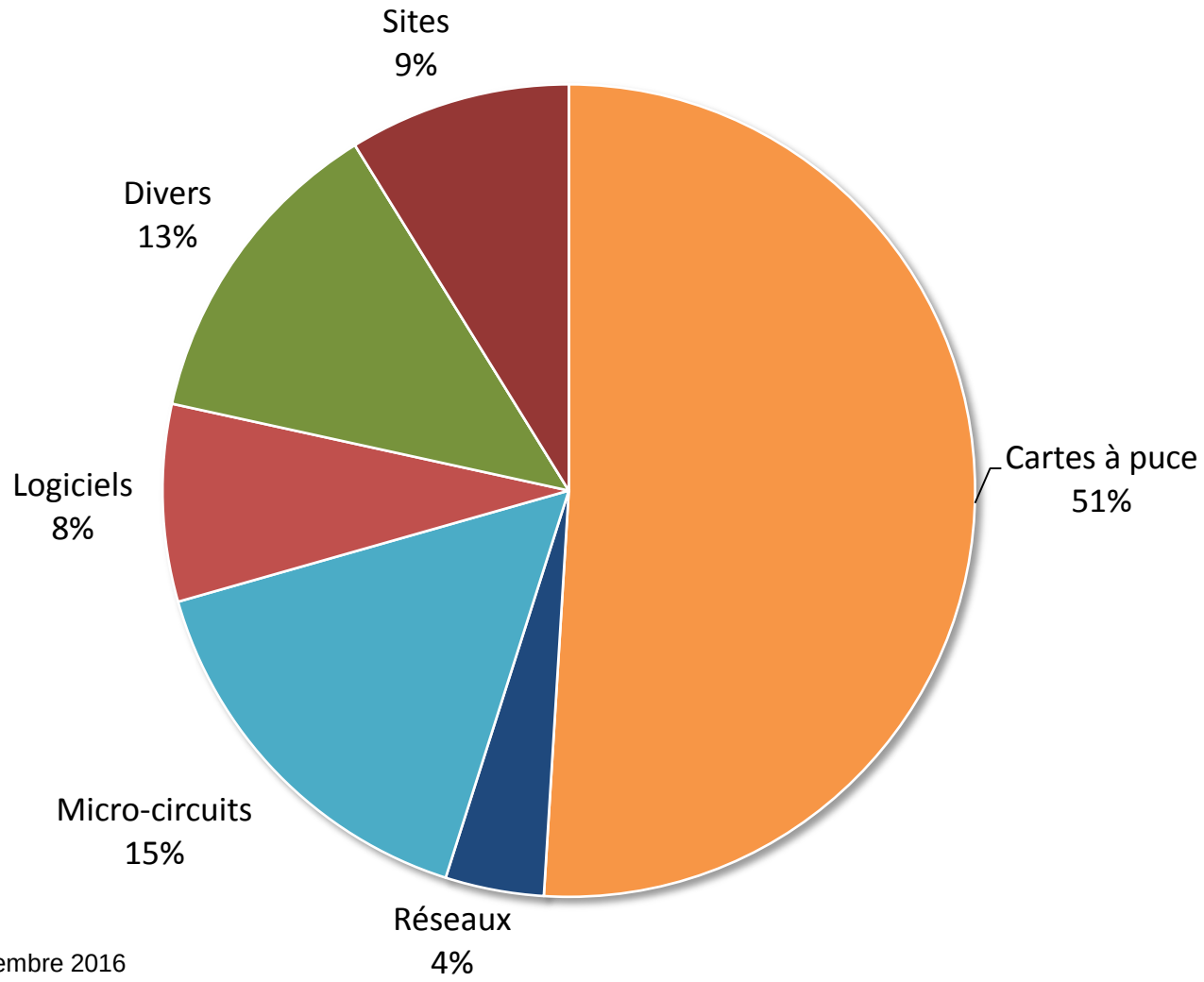
Les motivations

- **Approche réglementaire**
  - Tout est imposé (la cible de sécurité ou le PP, le niveau visé, etc.)
  - En fort développement aujourd'hui
  - Exemples: CEE pour chronotachygraphe, BdF pour porte-monnaie électronique, CEE pour signature électronique, labellisation pour les administrations…

Retour d'expérience

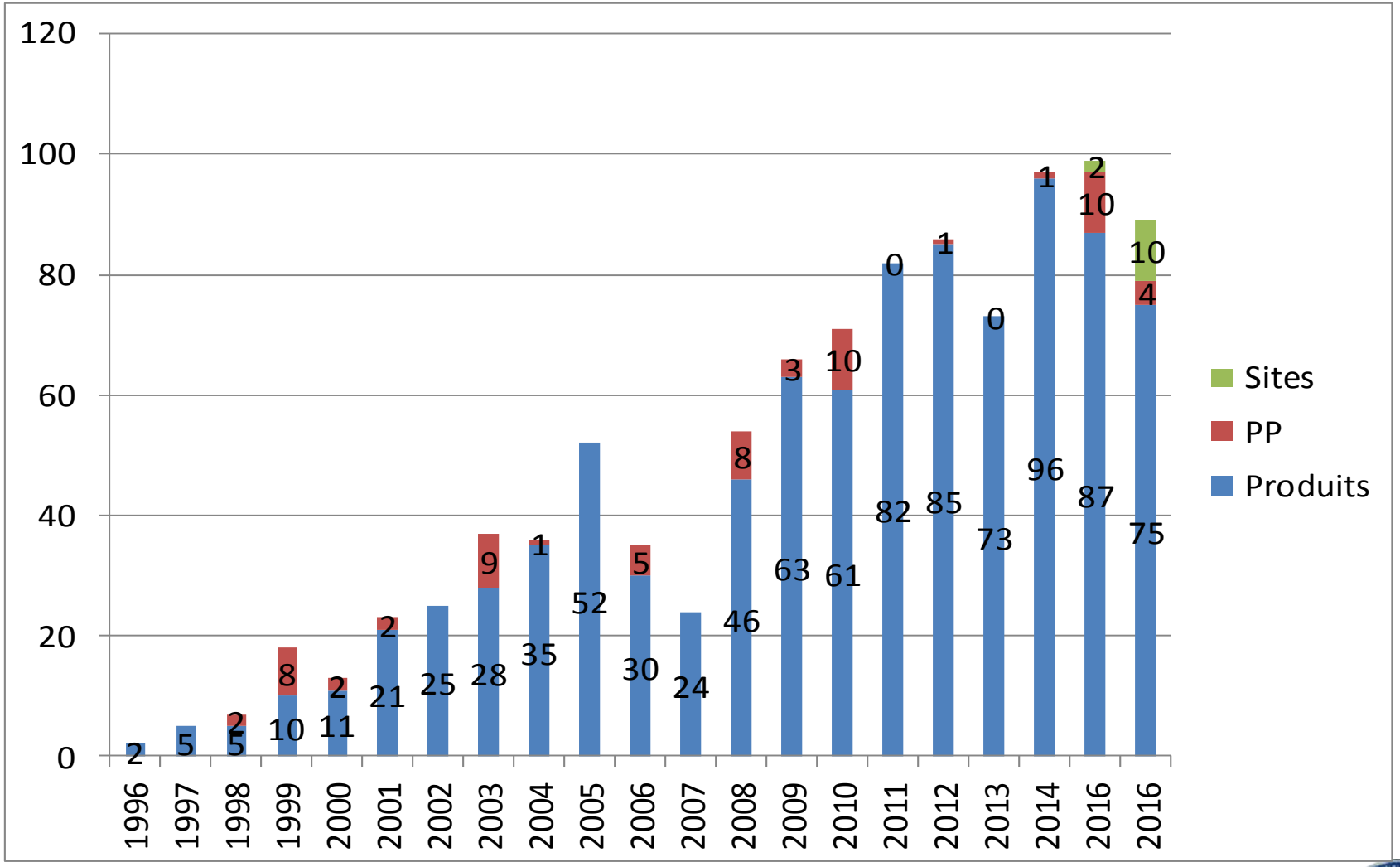
- 972 évaluations CC-ITSEC (terminées ou en cours)
- 751 certificats CC-ITSEC émis
- 52 PPs
- Environ 80% des certificats émis concernant des cartes à puce et micro-contrôleurs
- Environ 100 évaluations CC en cours
- Environ 100 surveillances en cours
- CSPN (2009 à 2015) : 109 évaluations, 53 certificats émis

Retours d'expériences : les certifications CC en 2016



Statistiques ANSSI-CCN 18 novembre 2016

Retours d'expériences : les certifications CC



Statistiques ANSSI-CCN 18 novembre 2016

Retours d'expériences

- **Parmi les leaders dans le monde**

Certified Products by Scheme and Assurance Level																		
Scheme	**EAL1**	**EAL1+**	**EAL2**	**EAL2+**	**EAL3**	**EAL3+**	**EAL4**	**EAL4+**	**EAL5**	**EAL5+**	**EAL6**	**EAL6+**	**EAL7**	**EAL7+**	**B**	**M**	**S**	**N**	**Total**
Australia	2	1	13	7	4	5	8	14	0	0	0	0	1	0	0	0	0	3	58
Canada	3	0	21	78	12	28	6	42	0	0	0	0	0	0	0	0	0	1	191
Germany	8	4	7	18	12	53	15	250	8	123	0	5	0	0	0	0	0	1	504
Spain	7	6	5	3	3	9	0	18	0	1	0	0	0	0	0	0	0	0	52
France	1	18	0	14	0	23	4	208	2	133	0	7	4	0	0	0	0	0	414
India	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Italy	1	5	0	0	2	0	1	0	0	0	0	0	0	0	0	0	0	0	9
Japan	8	2	15	5	120	51	1	2	0	0	0	0	0	0	0	0	0	0	204
Republic of Korea	0	0	1	0	9	13	24	13	0	5	0	0	0	0	0	0	0	0	65
Malaysia	6	0	3	0	0	2	1	2	0	0	0	0	0	0	0	0	0	0	14
Netherlands	0	0	0	1	0	1	1	12	0	3	0	6	0	1	0	0	0	0	25
Norway	0	0	1	9	0	4	7	6	2	3	0	0	0	0	0	0	0	0	32
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	0	0	0	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	3
Turkey	0	0	1	1	0	0	0	10	0	2	0	0	0	0	0	0	0	0	14
United Kingdom	0	0	1	10	1	3	0	7	0	0	0	0	0	0	0	0	0	0	22
United States	1	0	38	82	10	24	7	77	0	2	0	2	0	0	0	0	0	2	245
Totals:	**37**	**36**	**106**	**228**	**174**	**216**	**75**	**663**	**12**	**272**	**0**	**20**	**5**	**1**	**0**	**0**	**0**	**7**	**1852**

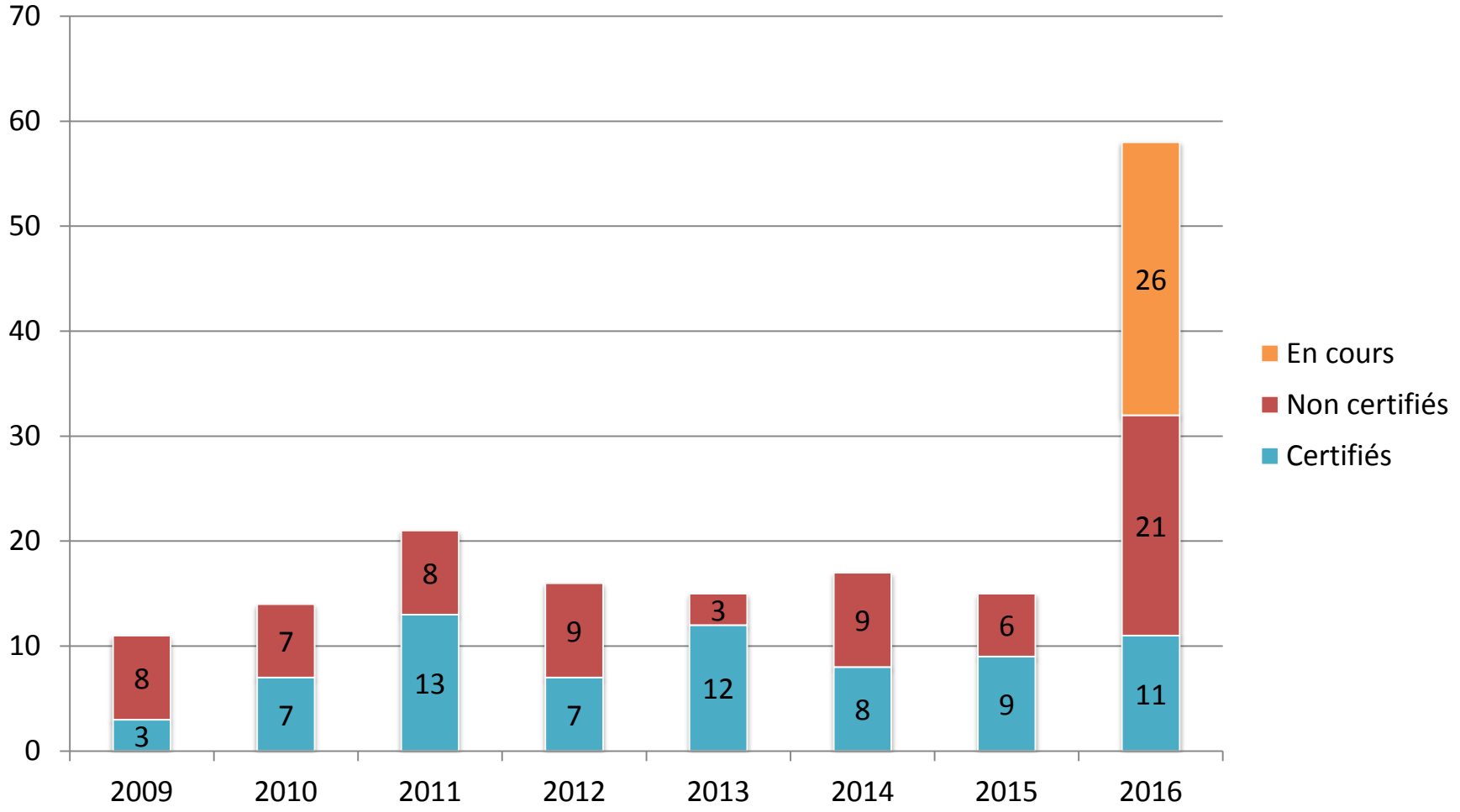
Retours d'expériences

- **Le domaine majoritaire : la carte à puce**

1852 Certified Products by Category *	
Category	**Products**
Access Control Devices and Systems	78
Biometric Systems and Devices	3
Boundary Protection Devices and Systems	111
Data Protection	77
Databases	45
Detection Devices and Systems	45
ICs, Smart Cards and Smart Card-Related Devices and Systems	702
Key Management Systems	36
Multi-Function Devices	193
Network and Network-Related Devices and Systems	176
Operating Systems	102
Other Devices and Systems	203
Products for Digital Signatures	78
Trusted Computing	3
Totals:	**1852**

Statistiques CCRA Novembre 2013

Retours d'expériences : certificats et projets CSPN



*Statistiques ANSSI-CCN 18 novembre 2016

Retours d'expériences

- **La certification, de la conformité… mais pas que !**
  - Schéma français très réputé
  - Choix d'un schéma technique
  - Importance des experts ANSSI
  - Malgré le cadre, les sigles (!), la théorie…: c'est du concret !
    - Utilisé au quotidien par de nombreux industriels
    - Assure une cohérence indispensable pour certains type de produits

Retours d'expériences

- **Limites de l'exercice**
  - Lire les cibles (au moins objectifs de sécurité, TOE != produit et hypothèses !)
  - Ne pas oublier les guides du produit
  - Vérifier les versions certifiées
  - Lire aussi le rapport de certification…
- **Lecture des niveaux EAL**
  - le niveau VAN est le plus important de la cible !

Retours d'expériences

- **L'évaluation améliore la qualité et l'efficacité des produits, même… pour un faible niveau de confiance visé !**
  - Par exemple au niveau étatique : un produit certifié sera préféré à un produit non certifié (même si les besoins de sécurité ne correspondent pas tout à fait à ceux de la cible de sécurité)

Liens utiles

CCRA

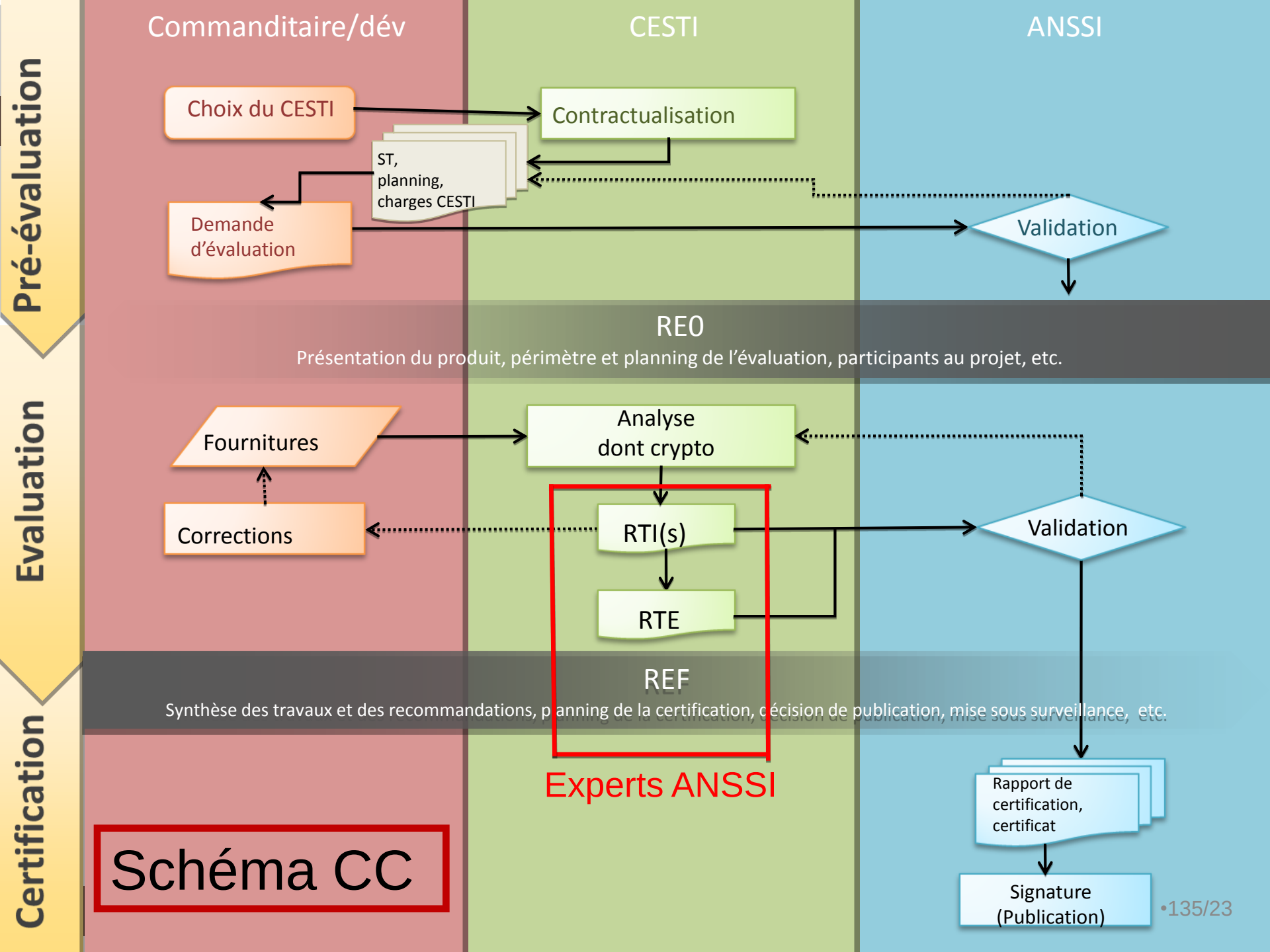
https://www.commoncriteriaportal.org/

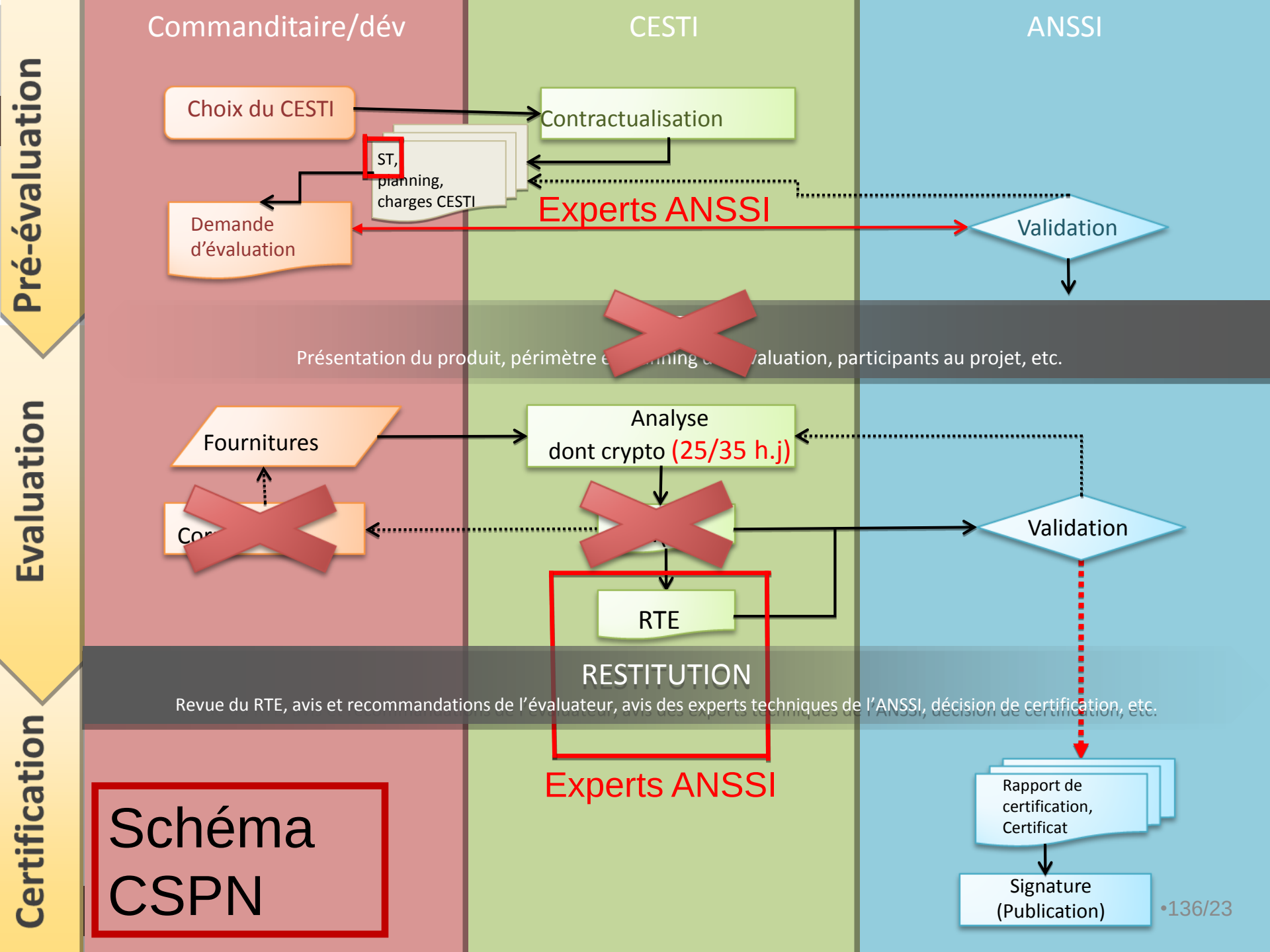
SOGIS

http://sogis.org/index_en.html

ANSSI

http://www.ssi.gouv.fr/fr/certification-qualification/


Commanditaire/dév
CESTI
ANSSI
Pré-évaluation
Evaluation
Certification
Choix du CESTI
Contractualisation
ST,
planning,
charges CESTI
Demande
d'évaluation
Validation
REO
Présentation du produit, périmètre et planning de l'évaluation, participants au projet, etc.
Fournitures
Analyse
dont crypto
Corrections
RTI(s)
RTE
Validation
REF
Synthèse des travaux et des recommandations, planning de la certification, décision de publication, mise sous surveillance, etc.
Experts ANSSI
Rapport de
certification,
certificat
Signature
(Publication)
Schéma CC


Commanditaire/dév
CESTI
ANSSI
Pré-évaluation
Evaluation
Certification
Choix du CESTI
Contractualisation
ST,
planning,
charges CESTI
Demande
d'évaluation
Experts ANSSI
Validation
Présentation du produit, périmètre
valuation, participants au projet, etc.
Fournitures
Analyse
dont crypto (25/35 h.j)
Validation
RTE
RESTITUTION
Revue du RTE, avis et recommandations de l'évaluateur, avis des experts techniques de l'ANSSI, décision de certification, etc.
Experts ANSSI
Rapport de
certification,
Certificat
Signature
(Publication)
Schéma
CSPN