

Standards et acteurs de la certification

Alexandre Gavriloff (ANSSI/CCN)



Master Cryptis

Plan

- **L'ANSSI**
- **La Certification**
 - Généralités
 - Accords de reconnaissance
- **Les Critères Communs**
- **CESTIs**
- **Les spécificités françaises**
 - CSPN
 - Maintenance
 - Surveillance
 - Motivations et retours d'expérience





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)**



■ Objectifs

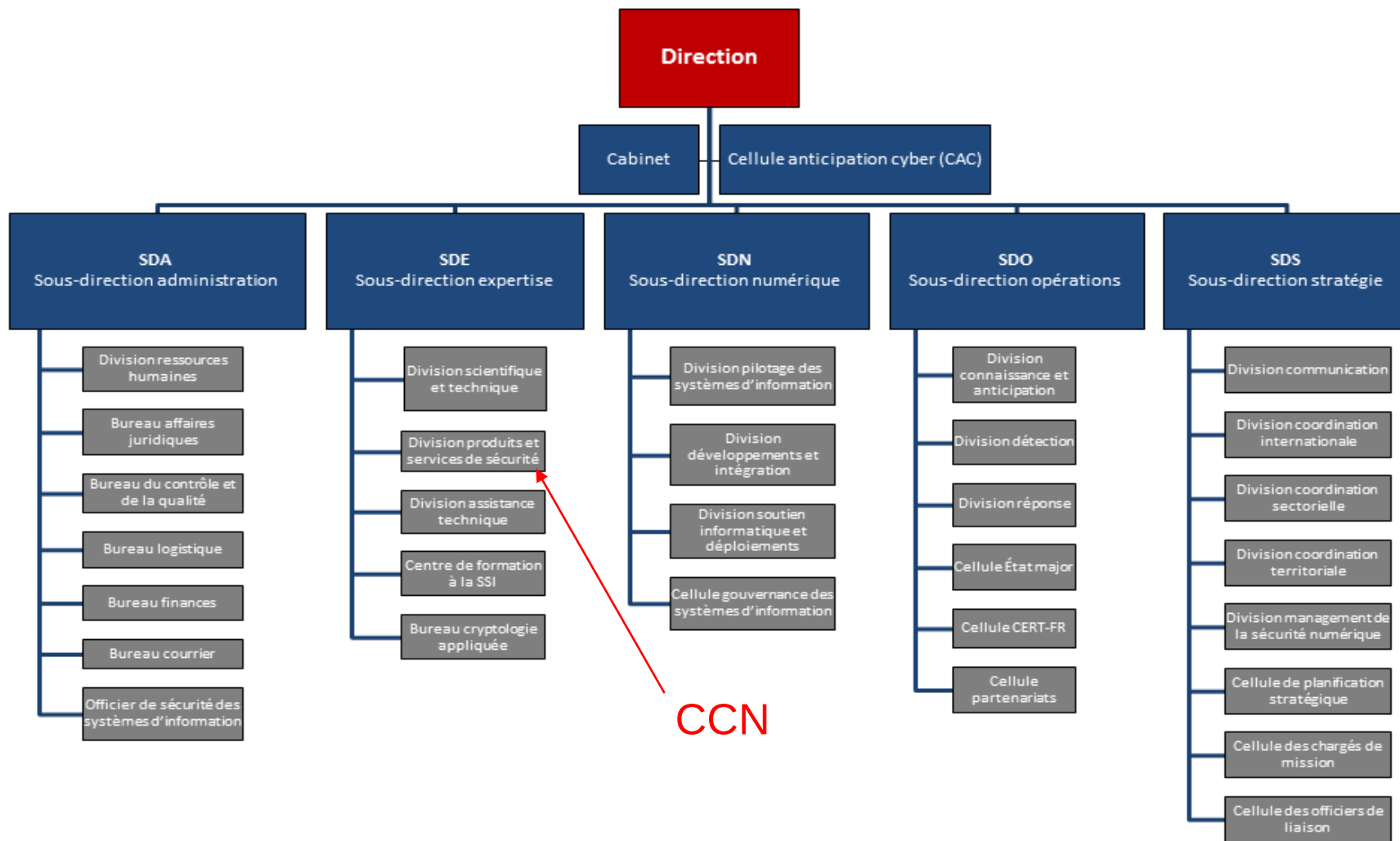
- Doter la France de véritables capacités en SSI
 - Stratégie, Livre Blanc, LPM*
- Être une puissance mondiale de Cyberdéfense

■ Moyens

- Prévention
 - Réglementation, labellisation, conseil, formation...
- Défense
 - Gestion d'incident, réponses aux crises...



L'ANSSI





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



leti

SERMA
SAFETY & SECURITY



AMOSSYS



THALES

Quarkslab
SECURING EVERY BIT OF YOUR DATA

Trusted Labs
Creating trust in a connected world

SYNACKTIV
DIGITAL SECURITY



La certification

- Des industriels utilisant le schéma français



SONY



THALES



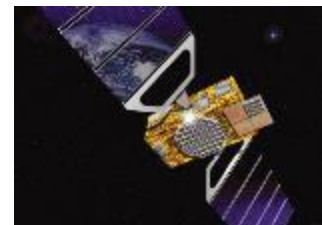
La certification

- Des industriels du « domaine public »



La certification

- Des produits connus ?



Qu'est ce que c'est ?



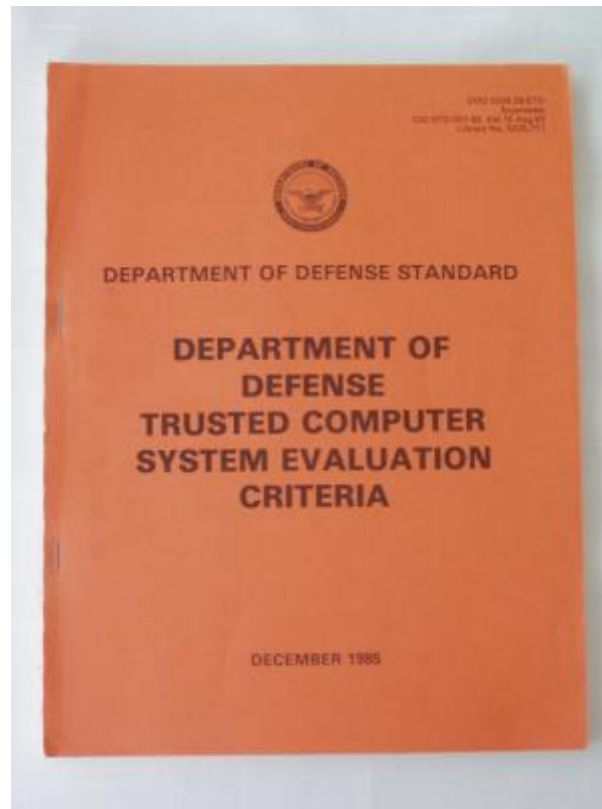
La certification

■ 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
 - Evalueur
 - Certificateur



- **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 : 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



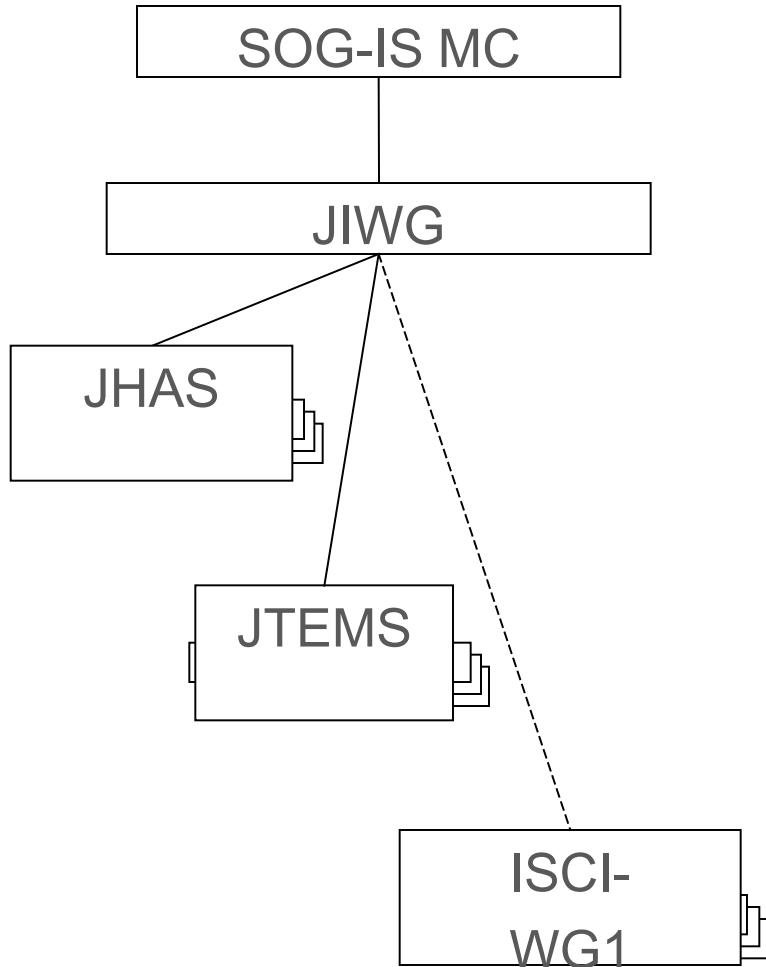
■ Reconnaissance des certificats CC

- Jusqu'à EAL 7 (niveau d'éval. max.)
 - Cartes à puce
 - Security Boxes
- EAL4 (niveau moyen)
- 4 pays qualifiés pour la carte à puce
 - France, Allemagne, Hollande, Espagne

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

*Association Européenne de Libre Echange



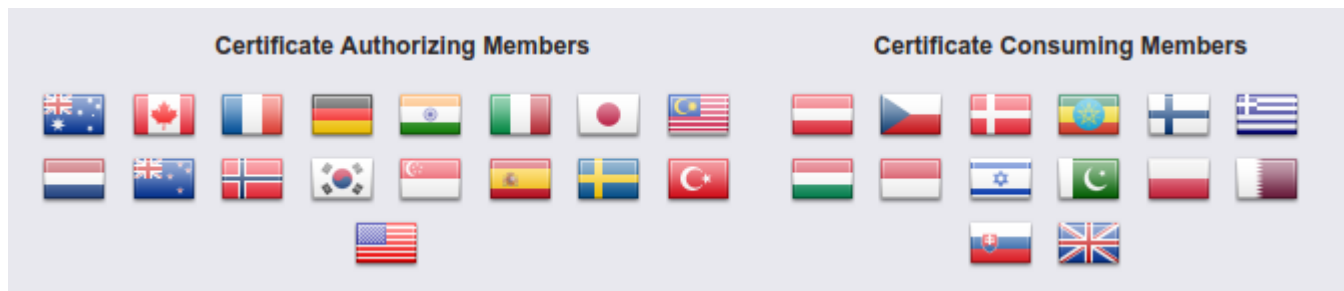


- **Managment Comitee**
 - Accepte les nouveaux membres
 - Décisions sur politique de certification
- **Joint Interpretations Working Group**
 - Développement de critères et de leurs interprétations et orientation des WGs
- **JIL Hardware related Attacks Subgroup**
 - Groupe de travail sur les aspects « 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 : 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)
- 31 pays



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



- **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**



L'avenir

■ Cybersecurity Act (CSA)

- Mandat permanent pour l'ENISA (European Union Agency for Cybersecurity)
 - Facilitateur d'échange entre les Etats membres
- Définit le cadre européen de certification de cybersécurité :
 - Harmoniser à l'échelle européenne les méthodes d'évaluation et les différents niveaux d'assurance
 - Les certificats délivrés auront une **reconnaissance mutuelle au sein de l'Union Européenne**



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



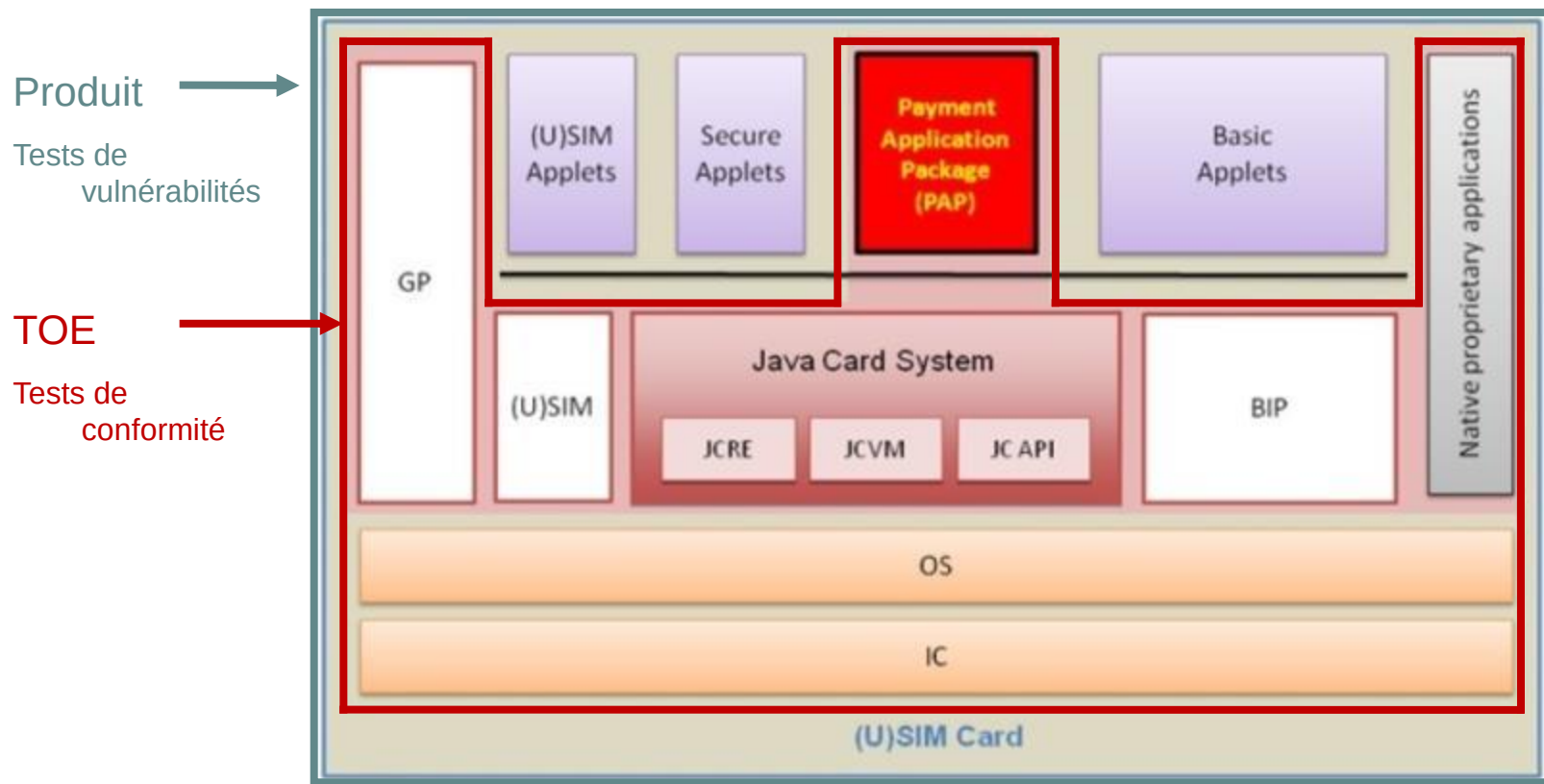


Les critères communs



Les critères communs

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



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)

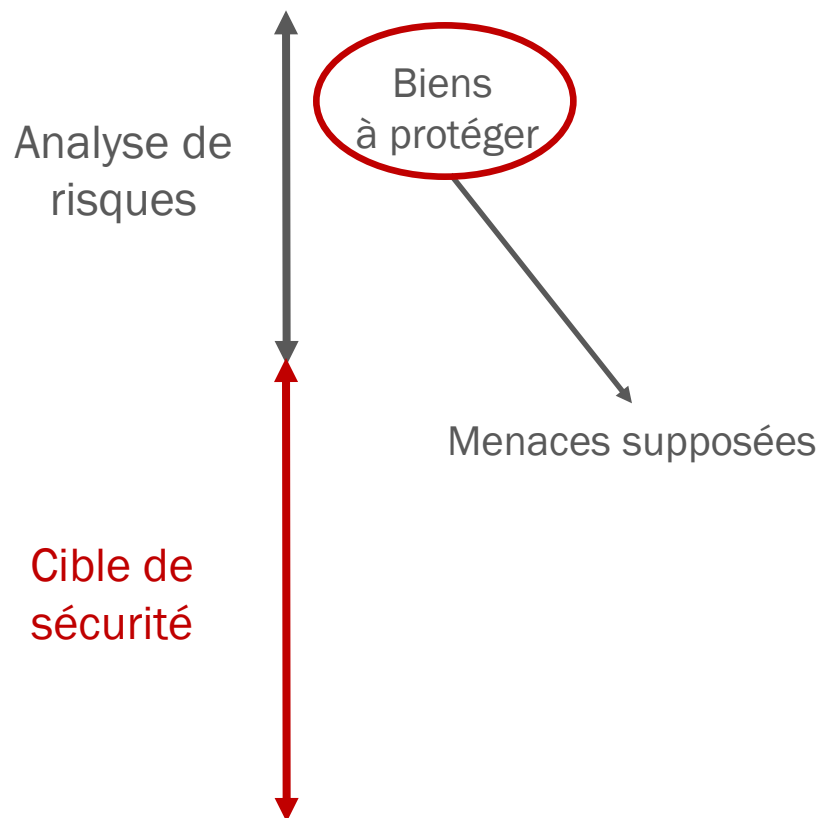
Les critères communs

■ 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



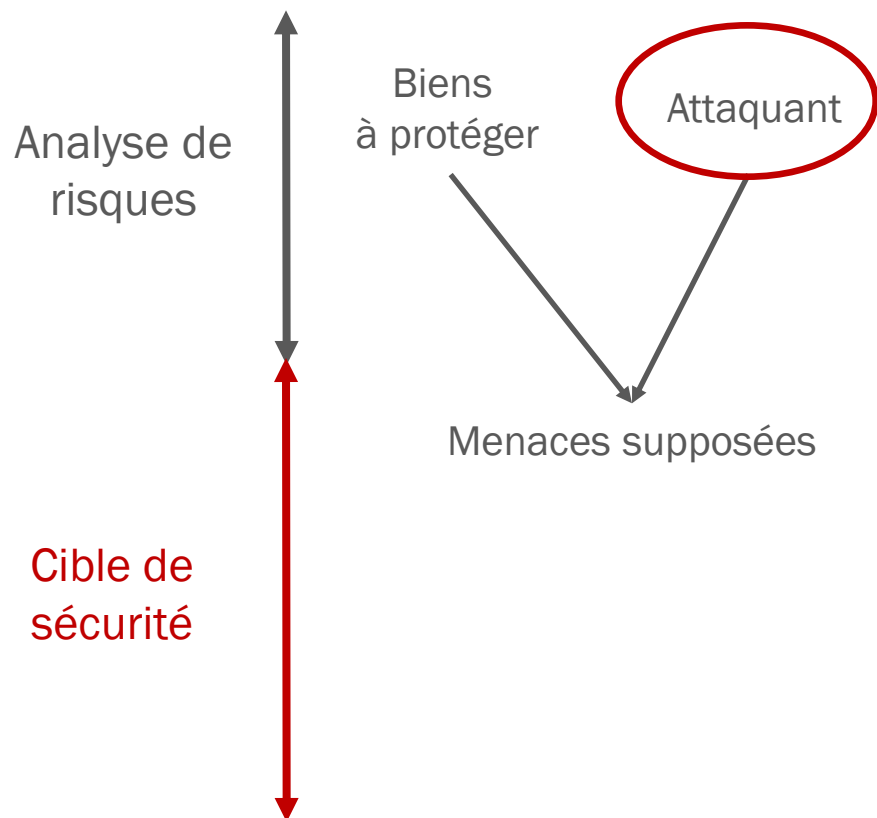
Les critères communs

- Quelques notions indispensables !
 - ST Exemple du passeport



Les critères communs

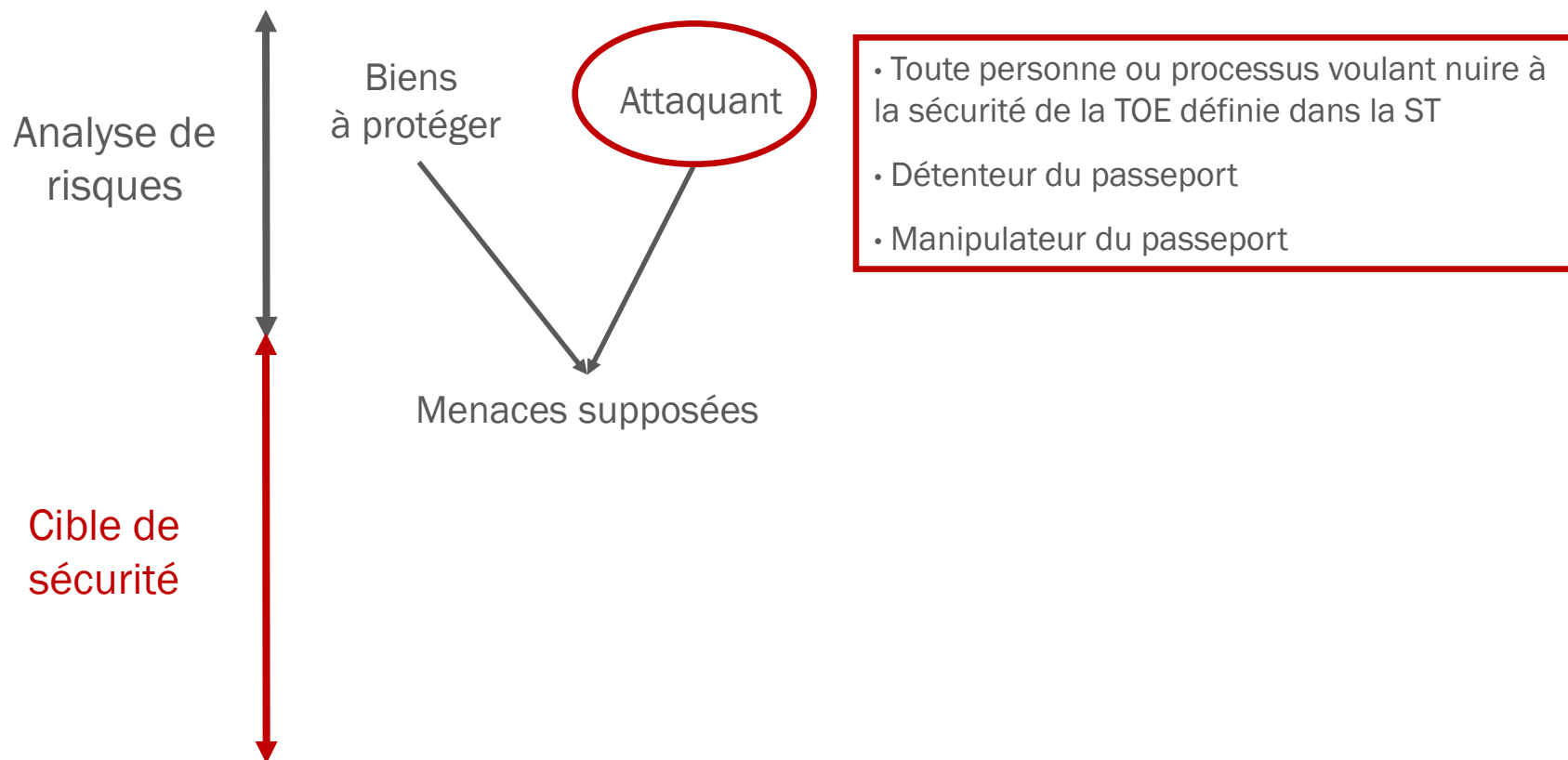
- Quelques notions indispensables !
 - ST Exemple du passeport



Les critères communs

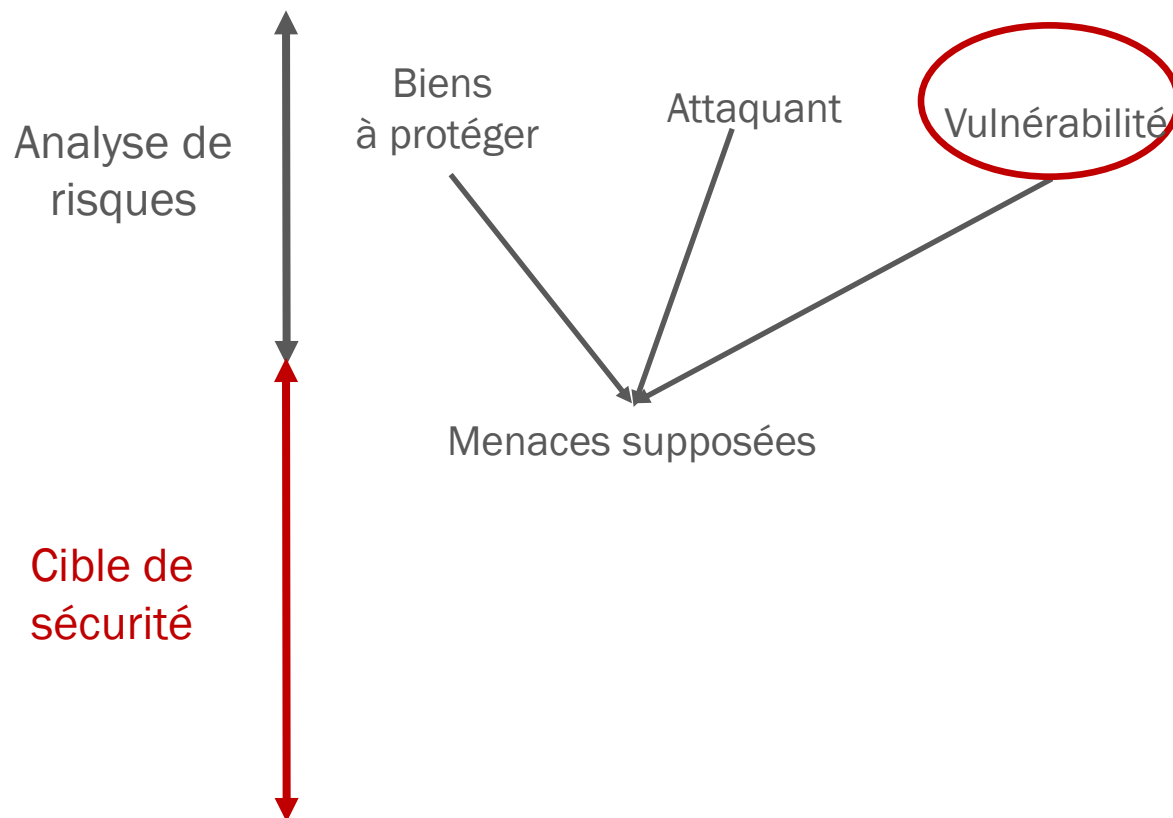
▪ Quelques notions indispensables !

- ST Exemple du passeport



Les critères communs

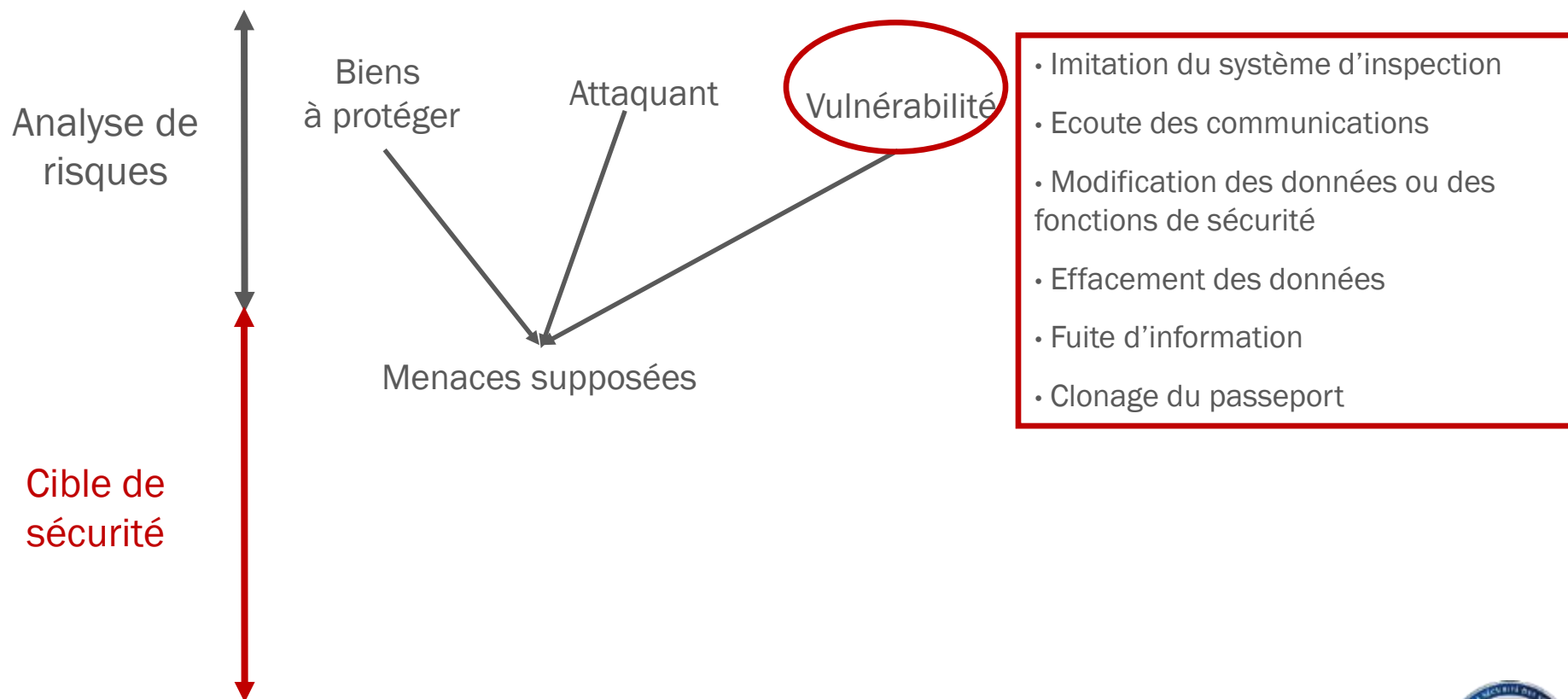
- Quelques notions indispensables !
 - ST Exemple du passeport



Les critères communs

▪ Quelques notions indispensables !

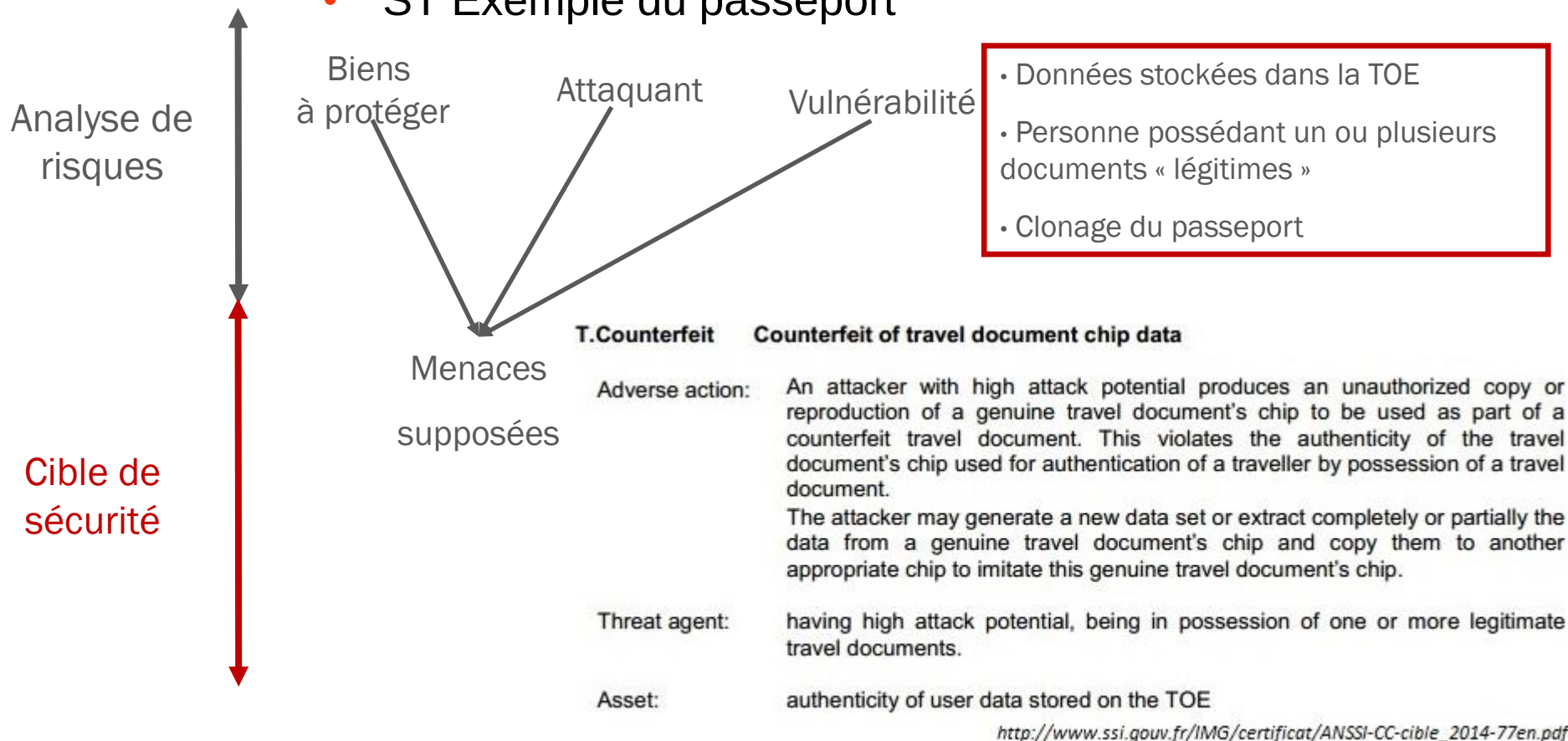
- ST Exemple du passeport



Les critères communs

▪ Quelques notions indispensables !

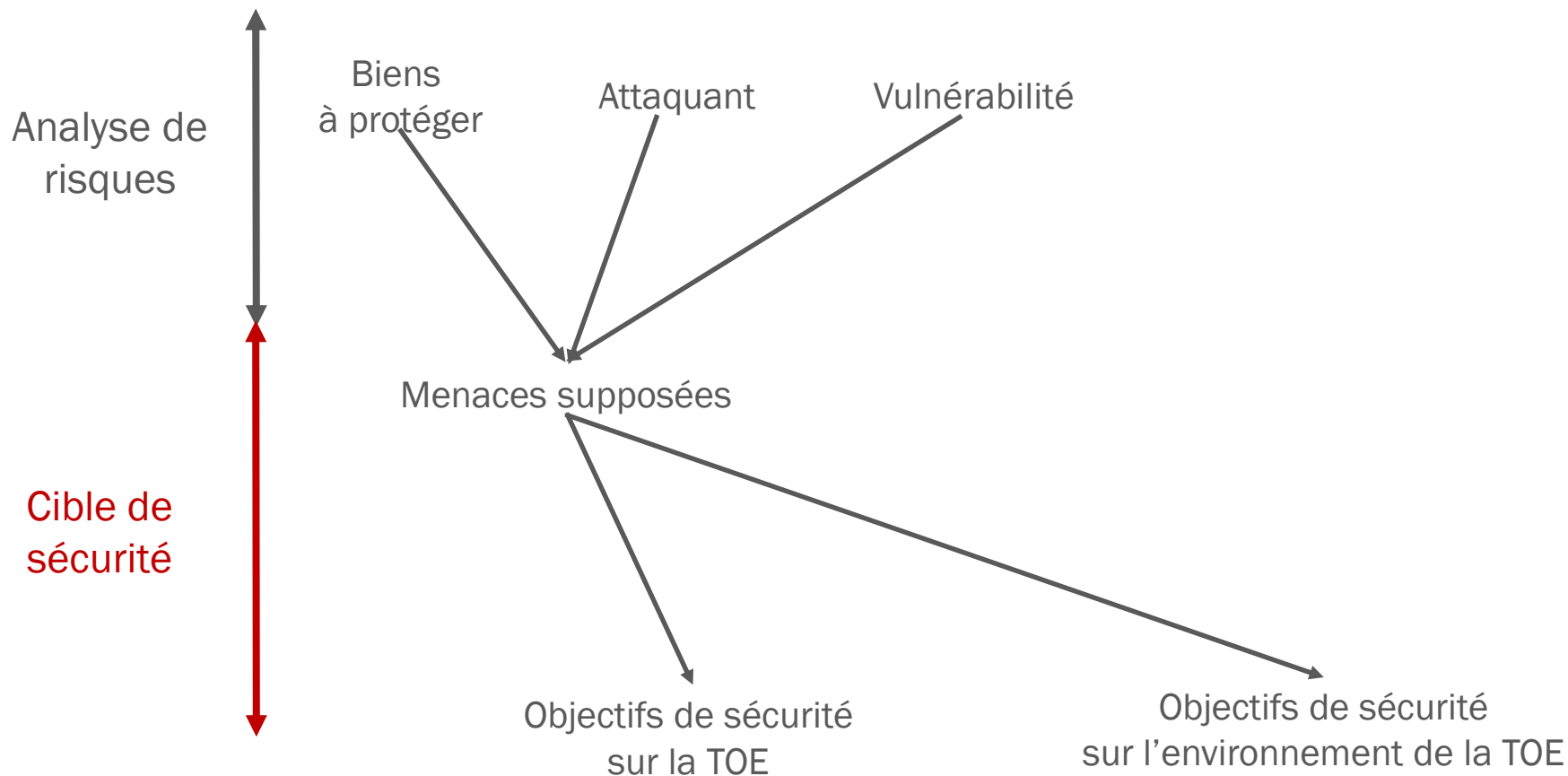
- ST Exemple du passeport



Les critères communs

▪ Quelques notions indispensables !

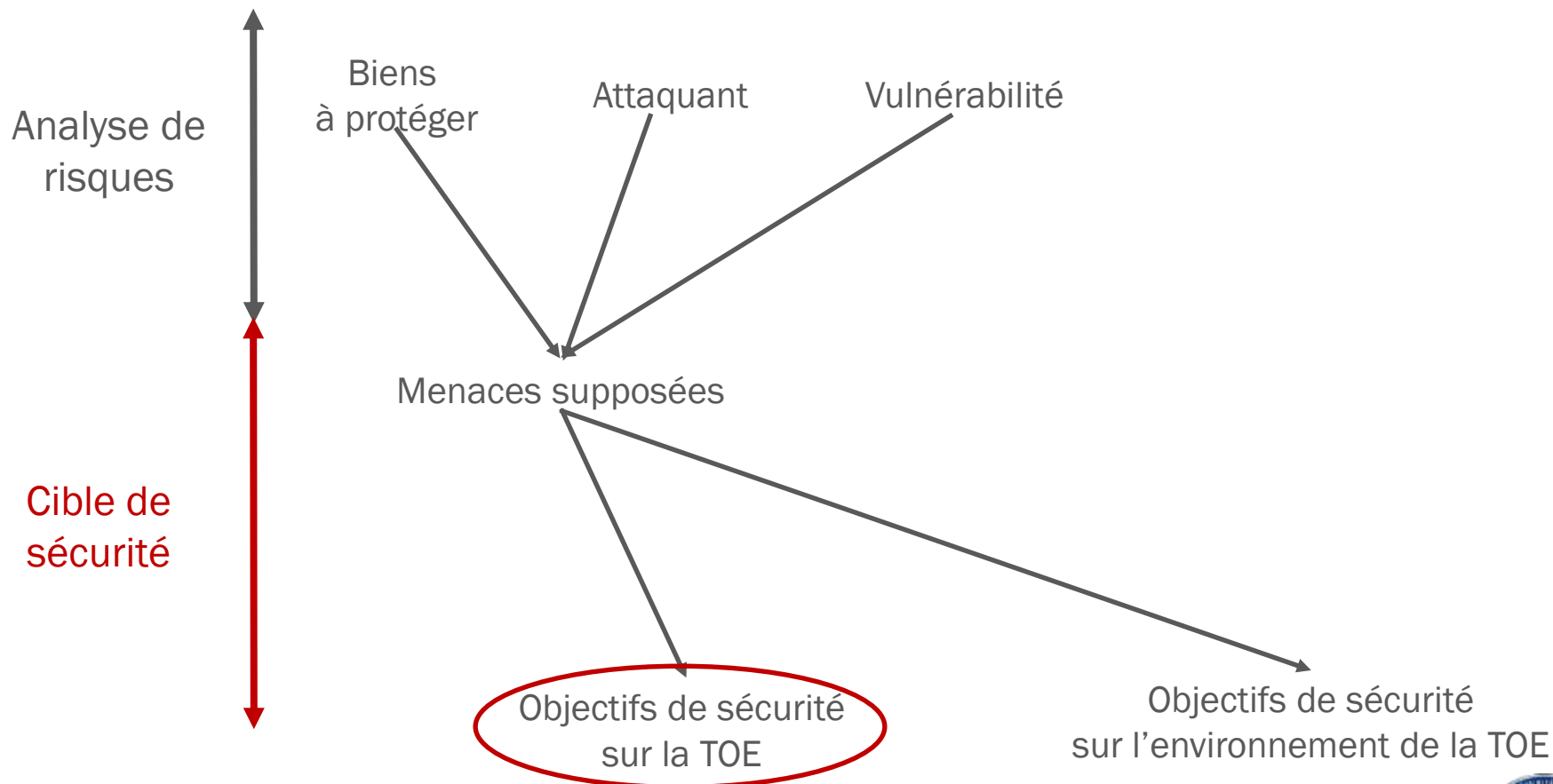
- ST Exemple du passeport



Les critères communs

▪ Quelques notions indispensables !

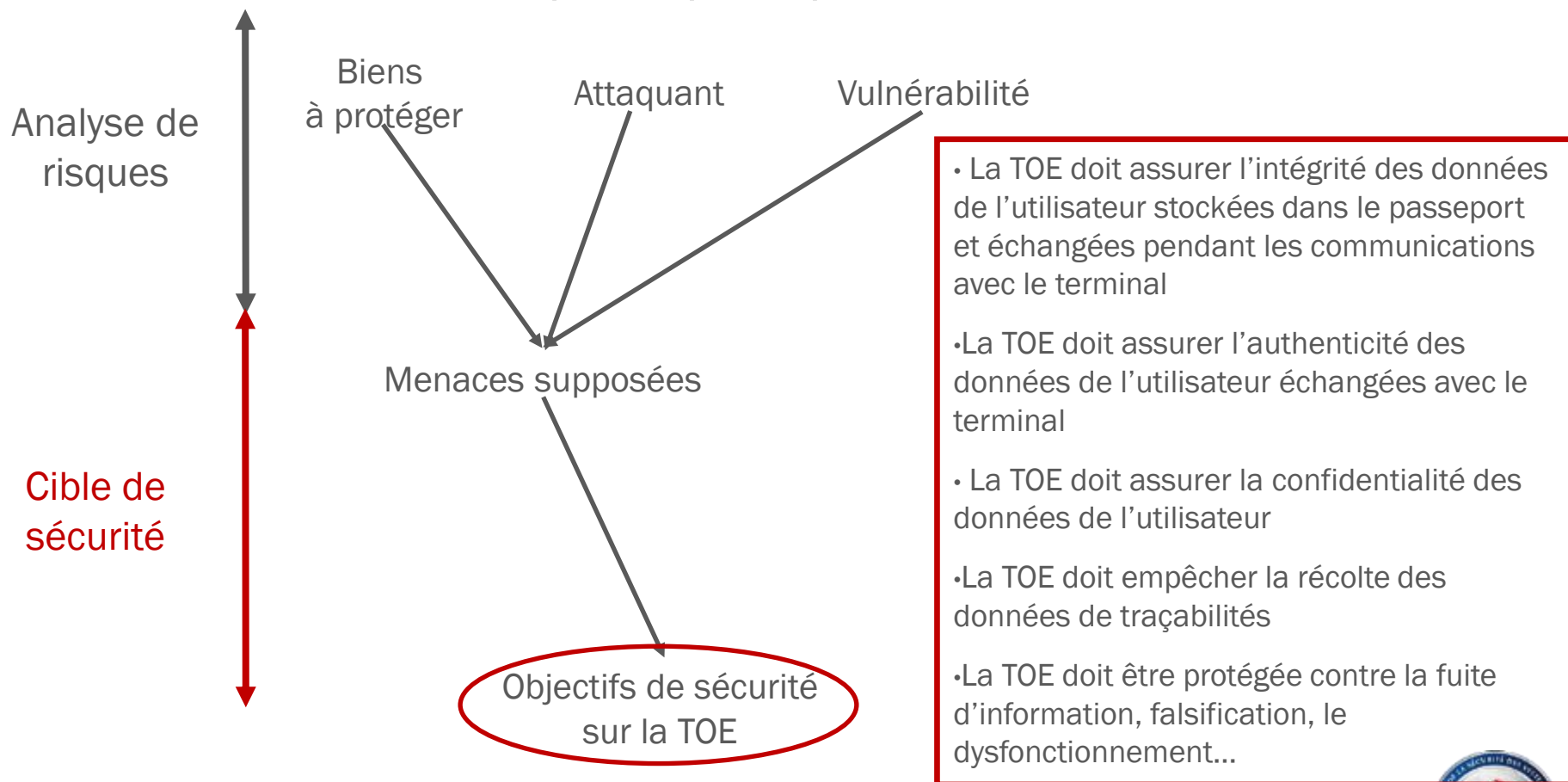
- ST Exemple du passeport



Les critères communs

▪ Quelques notions indispensables !

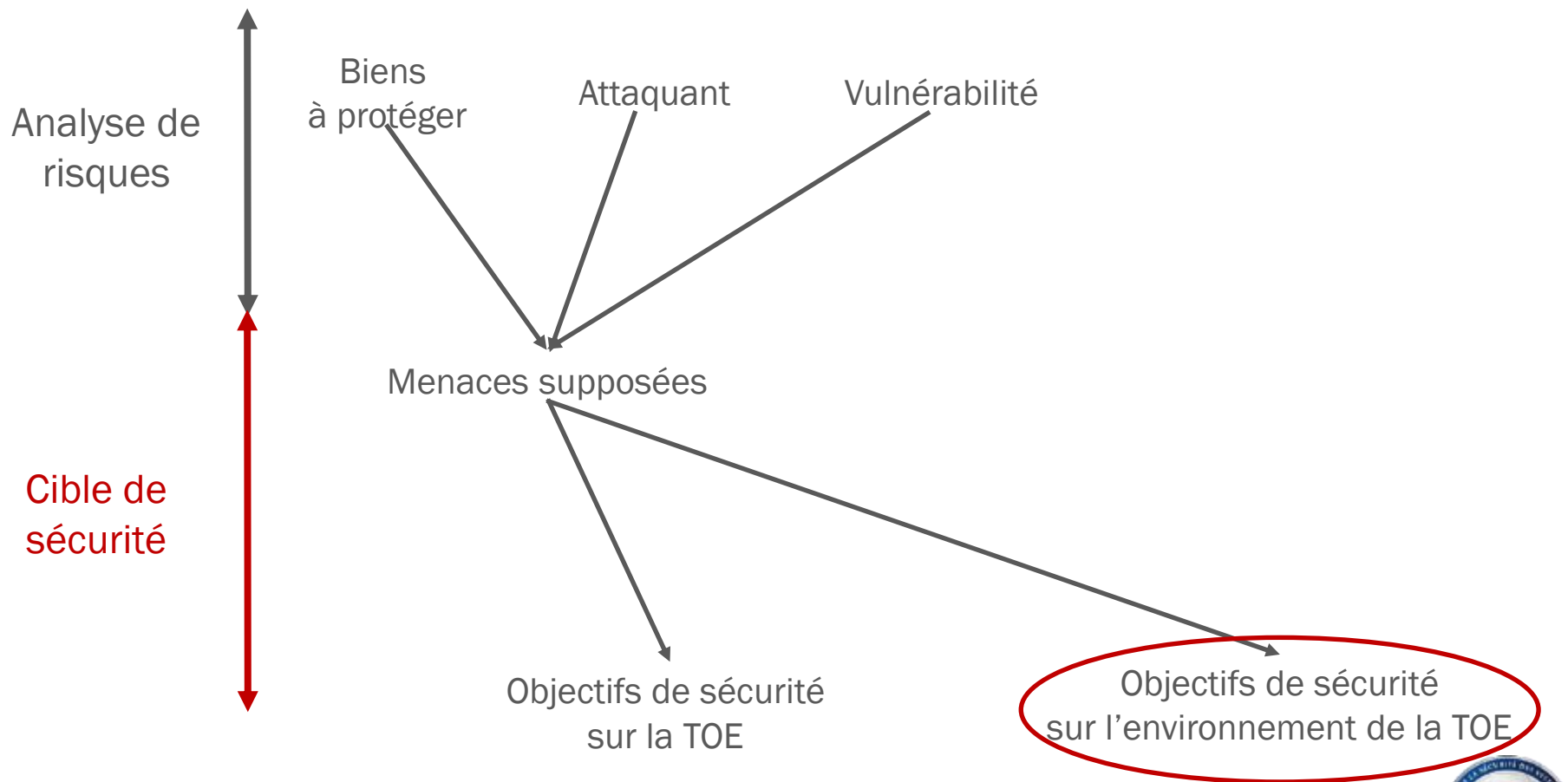
- ST Exemple du passeport



Les critères communs

▪ Quelques notions indispensables !

- ST Exemple du passeport



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 réglementations 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...)

Objectifs de sécurité
sur l'environnement de la TOE



Analyse de
risques

Cible de
sécurité

Biens
à protéger

Attaquant

Vulnérabilité

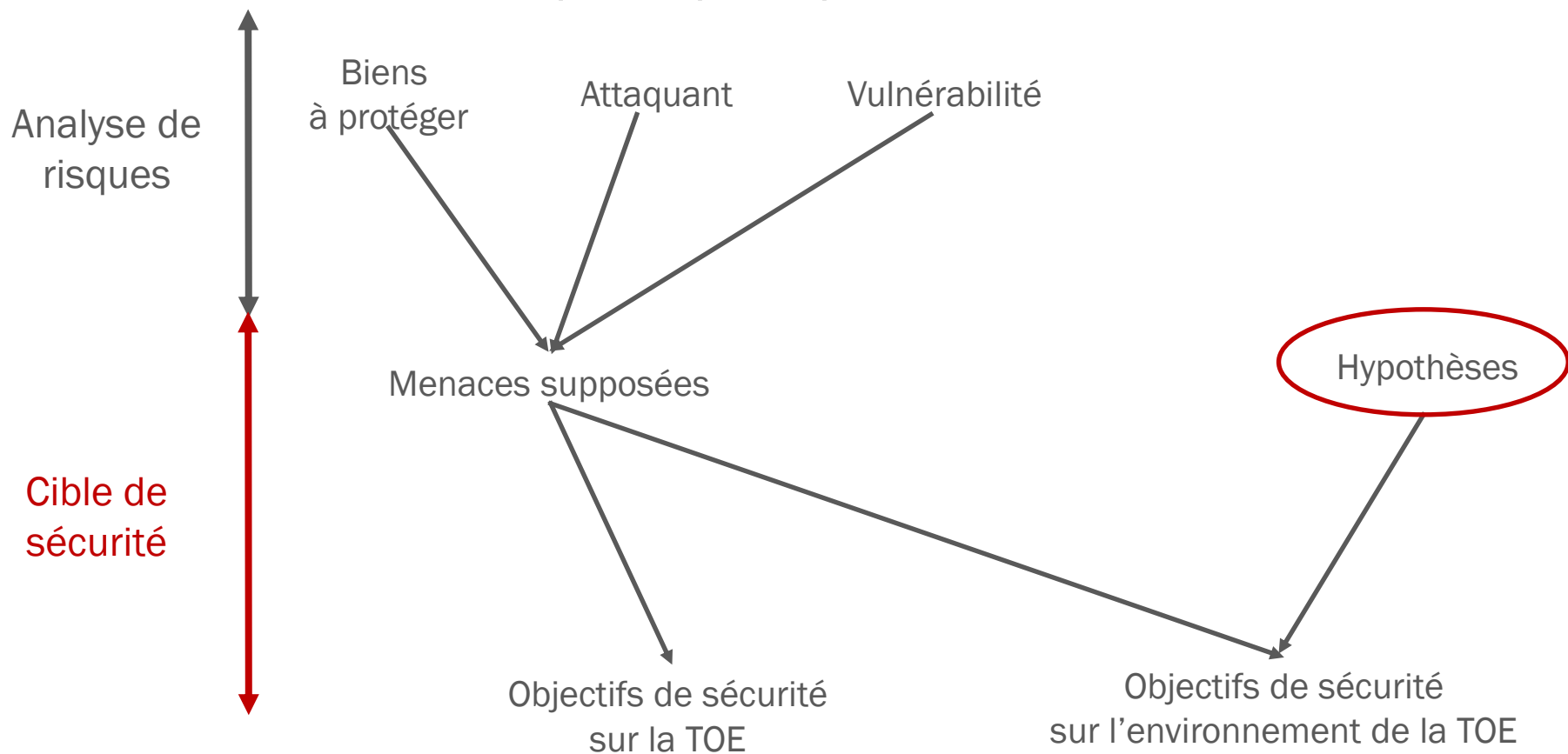
Menaces supposées

Objectifs de sécurité
sur la TOE

Les critères communs

▪ Quelques notions indispensables !

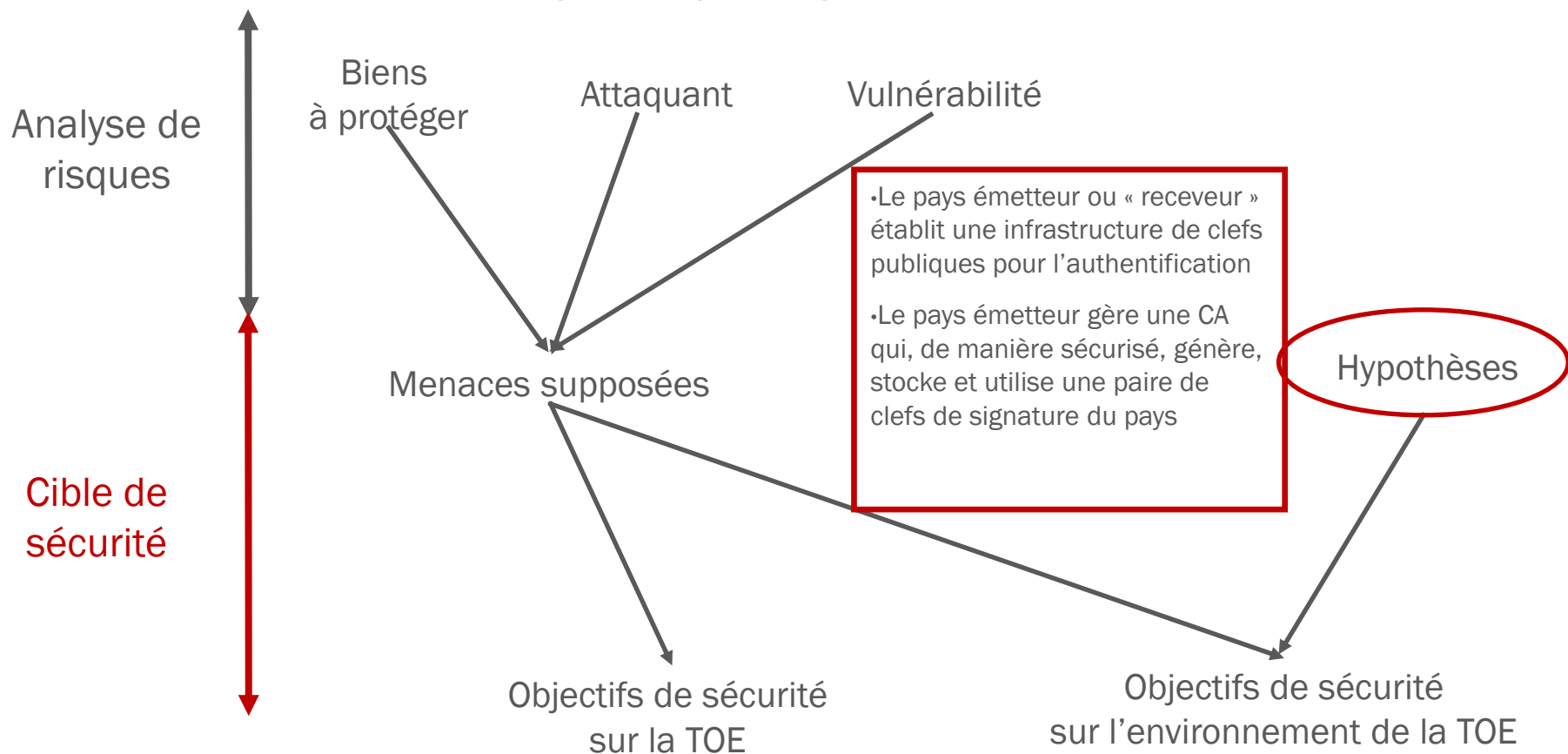
- ST Exemple du passeport



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

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	Vulnerability 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	Vulnerability Analysis

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

1. ST INTRODUCTION	4
1.1 ST IDENTIFICATION	4
1.2 ST OVERVIEW	5
1.3 REFERENCES	6
1.3.1 External References	6
1.3.2 Internal References	7
1.4 TOE OVERVIEW	8
1.4.1 TOE definition	8
1.4.2 TOE boundaries	8
1.4.3 TOE usage and security features for operational use	9
1.4.4 Toe Life-cycle	11
1.4.4.1 Four phases	11
1.4.4.2 Actors	12
1.4.4.3 Init on module at Gemalto site	13
1.4.4.4 Init on inlay at Gemalto site	14
1.4.5 Non-TOE hardware/software/firmware required by the TOE	14
2. CONFORMANCE CLAIMS	15
2.1 CC CONFORMANCE CLAIM	15
2.2 PP CLAIM	15
2.3 PACKAGE CLAIM	15
2.4 CONFORMANCE STATEMENT	15
3. SECURITY PROBLEM DEFINITION	16
3.1 INTRODUCTION	16
3.1.1 Assets	16
3.1.2 Subjects	16
3.2 ASSUMPTIONS	17
3.3 THREATS	18
3.4 ORGANIZATIONAL SECURITY POLICIES	20
3.5 COMPATIBILITY BETWEEN SECURITY ENVIRONMENTS OF [ST-BAC] AND [ST-IC]	21
3.5.1 Compatibility between threats of [ST-BAC] and [ST-IC]	21
3.5.2 Compatibility between OSP of [ST-BAC] and [ST-IC]	21
3.5.3 Compatibility between assumptions of [ST-BAC] and [ST-IC]	21
4. SECURITY OBJECTIVES	22
4.1 SECURITY OBJECTIVES FOR THE TOE	22
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	24
4.3 SECURITY OBJECTIVE RATIONALE	26
4.3.1 Rationale between objectives and threats, assumptions, OSP	26
4.3.2 Compatibility between objectives of [ST-BAC] and [ST-IC]	28
4.3.2.1 Compatibility between objectives for the TOE	28
4.3.2.2 Compatibility between objectives for the environment	28
5. EXTENDED COMPONENTS DEFINITION	29
5.1 DEFINITION OF THE FAMILY FAU_SAS	29
5.2 DEFINITION OF THE FAMILY FCS_RND	29
5.3 DEFINITION OF THE FAMILY FIA_API	30
5.4 DEFINITION OF THE FAMILY FMT_LIM	31
5.5 DEFINITION OF THE FAMILY FPT_EMS	32
6. SECURITY REQUIREMENTS	34
6.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE	34
6.1.1 Class FAU Security Audit	34
6.1.2 Class Cryptographic Support (FCS)	35
6.1.3 Class FIA Identification and Authentication	38
6.1.4 Class FDP User Data Protection	41
6.1.5 Class FMT Security Management	43
6.1.6 Class FPT Protection of the Security Functions	46

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

1. ST INTRODUCTION	4
1.1 ST IDENTIFICATION	4
1.2 ST OVERVIEW	5
1.3 REFERENCES	6
1.3.1 External References	6
1.3.2 Internal References	7
1.4 TOE OVERVIEW	8
1.4.1 TOE definition	8
1.4.2 TOE boundaries	8
1.4.3 TOE usage and security features for operational use	9
1.4.4 Toe Life-cycle	11
1.4.4.1 Four phases	11
1.4.4.2 Actors	12
1.4.4.3 Init on module at Gemalto site	13
1.4.4.4 Init on inlay at Gemalto site	14
1.4.5 Non-TOE hardware/software/firmware required by the TOE	14
2. CONFORMANCE CLAIMS	15
2.1 CC CONFORMANCE CLAIM	15
2.2 FT CLAIM	15
2.3 PACKAGE CLAIM	15
2.4 CONFORMANCE STATEMENT	15
3. SECURITY PROBLEM DEFINITION	16
3.1 INTRODUCTION	16
3.1.1 Assets	16
3.1.2 Subjects	16
3.2 ASSUMPTIONS	17
3.3 THREATS	18
3.4 ORGANIZATIONAL SECURITY POLICIES	20
3.5 COMPATIBILITY BETWEEN SECURITY ENVIRONMENTS OF [ST-BAC] AND [ST-IC]	21
3.5.1 Compatibility between threats of [ST-BAC] and [ST-IC]	21
3.5.2 Compatibility between OSP of [ST-BAC] and [ST-IC]	21
3.5.3 Compatibility between assumptions of [ST-BAC] and [ST-IC]	21
4. SECURITY OBJECTIVES	22
4.1 SECURITY OBJECTIVES FOR THE TOE	22
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	24
4.3 SECURITY OBJECTIVE RATIONALE	26
4.3.1 Rationale between objectives and threats, assumptions, OSP	26
4.3.2 Compatibility between objectives of [ST-BAC] and [ST-IC]	28
4.3.2.1 Compatibility between objectives for the TOE	28
4.3.2.2 Compatibility between objectives for the environment	28
5. EXTENDED COMPONENTS DEFINITION	29
5.1 DEFINITION OF THE FAMILY FAU_SAS	29
5.2 DEFINITION OF THE FAMILY FCS_RND	29
5.3 DEFINITION OF THE FAMILY FIA_API	30
5.4 DEFINITION OF THE FAMILY FMT_LIM	31
5.5 DEFINITION OF THE FAMILY FPT_EMS	32
6. SECURITY REQUIREMENTS	34
6.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE	34
6.1.1 Class FAU Security Audit	34
6.1.2 Class Cryptographic Support (FCS)	35
6.1.3 Class FIA Identification and Authentication	38
6.1.4 Class FDP User Data Protection	41
6.1.5 Class FMT Security Management	43
6.1.6 Class FPT Protection of the Security Functions	46

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].

« 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 »

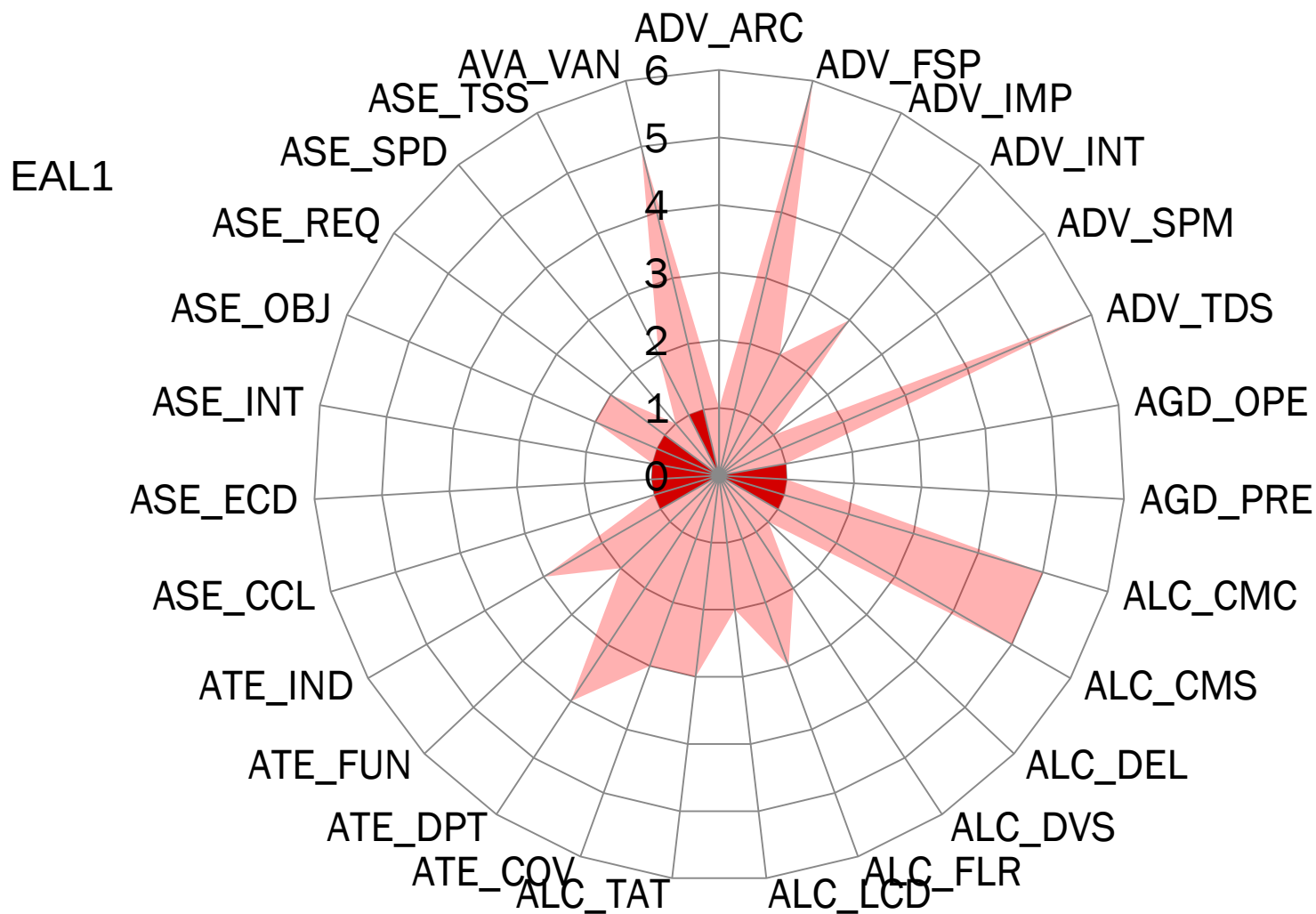


Les CC

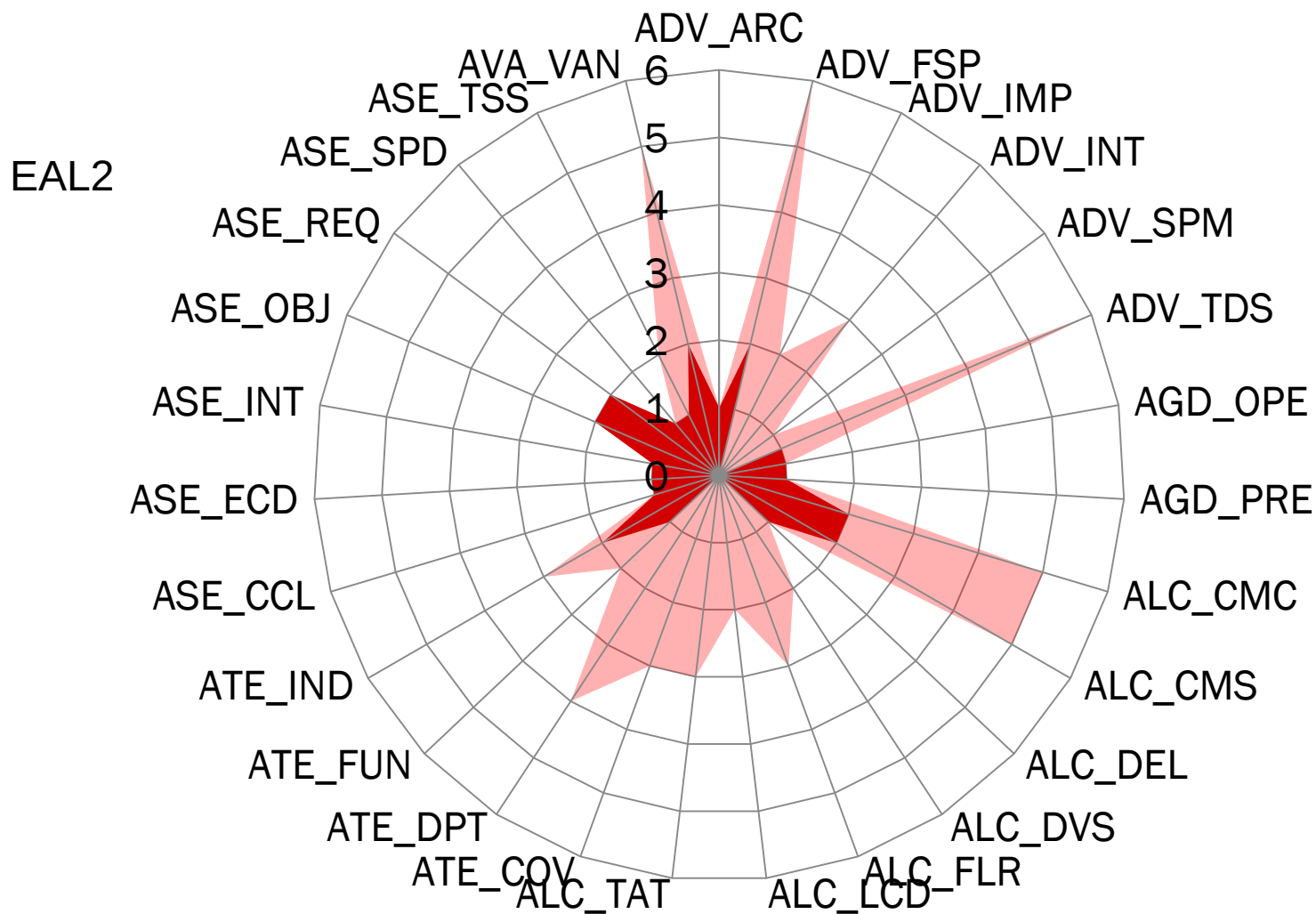
EAL

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	Vulnerability Analysis

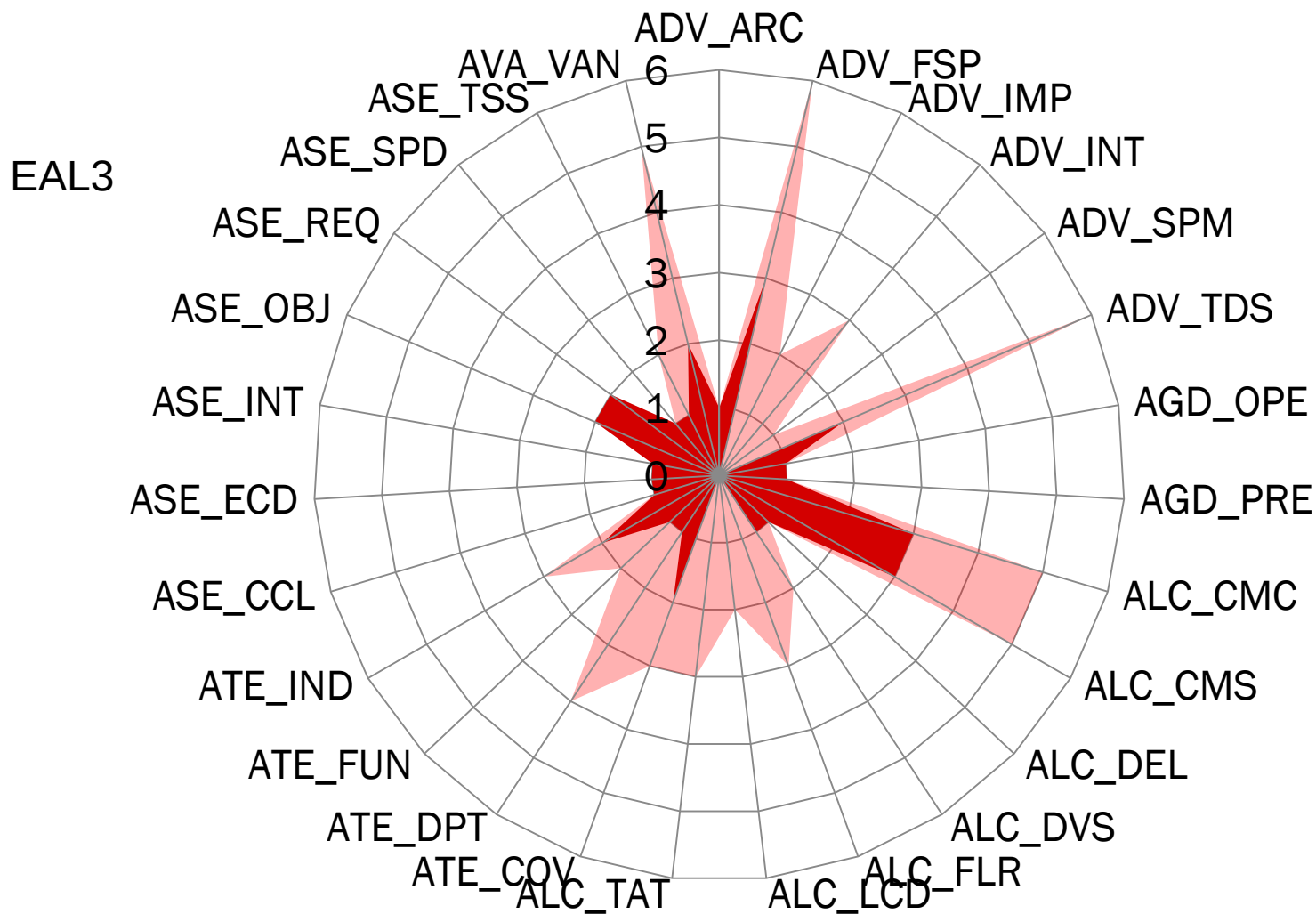
Les critères communs



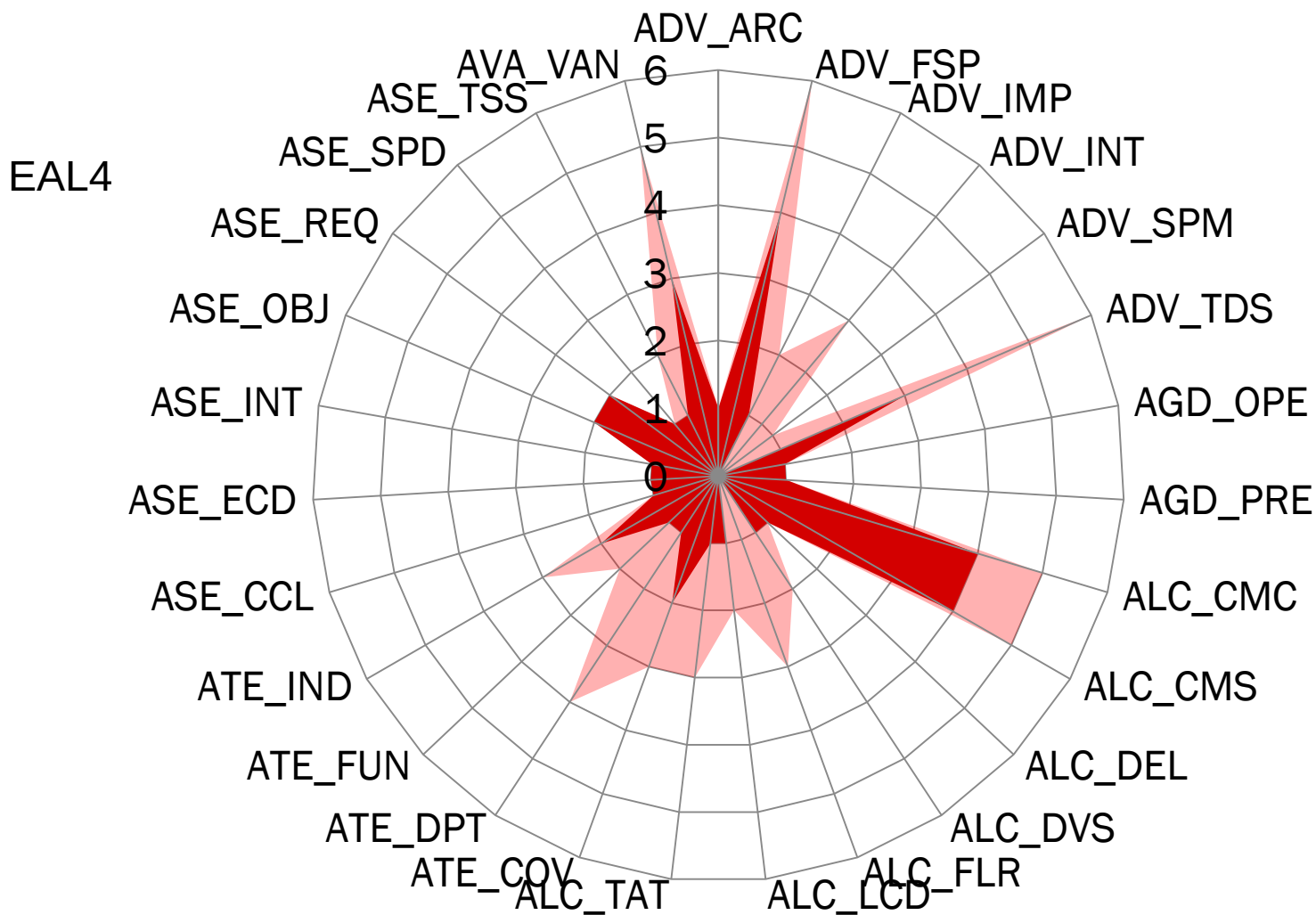
Les critères communs



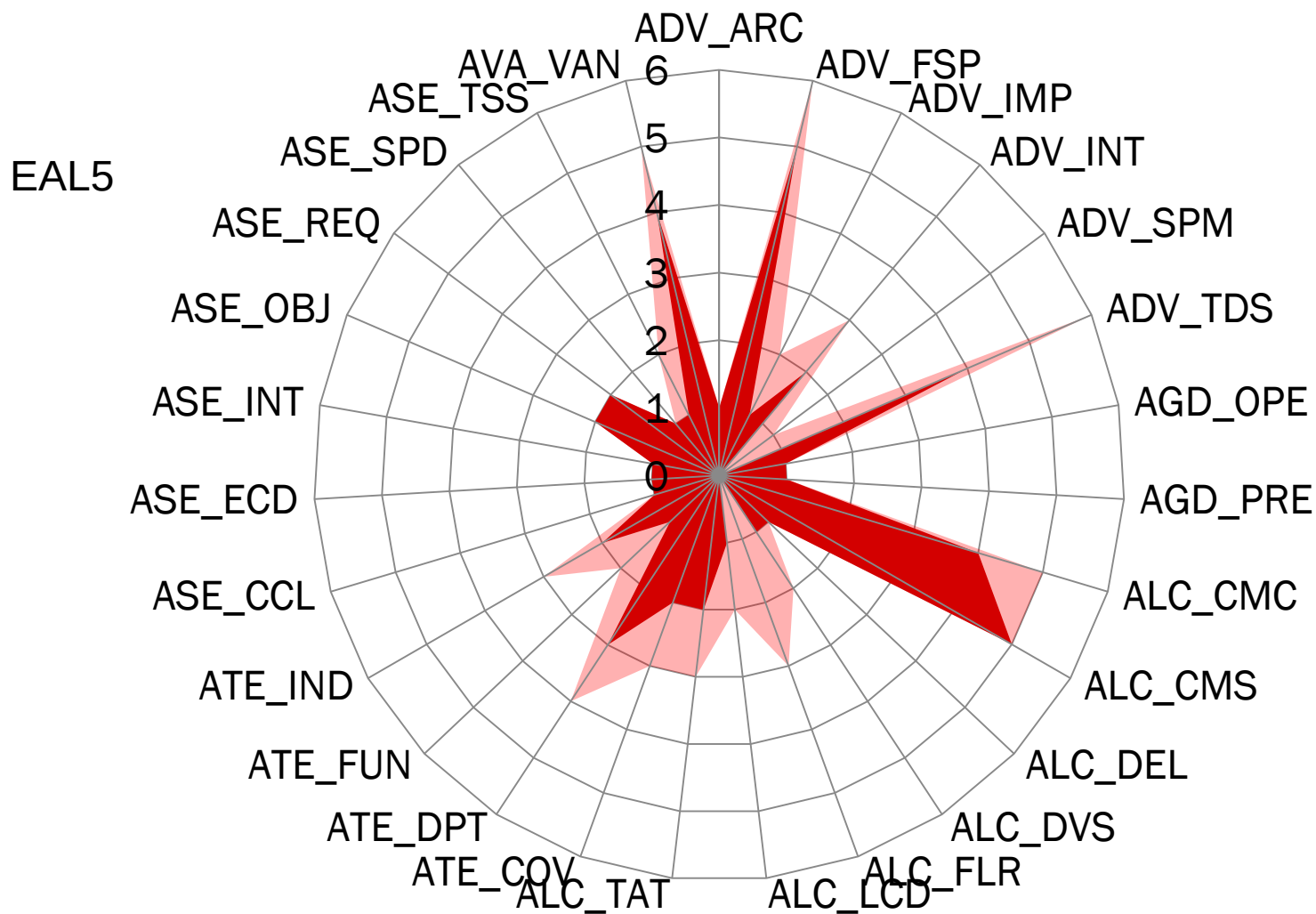
Les critères communs



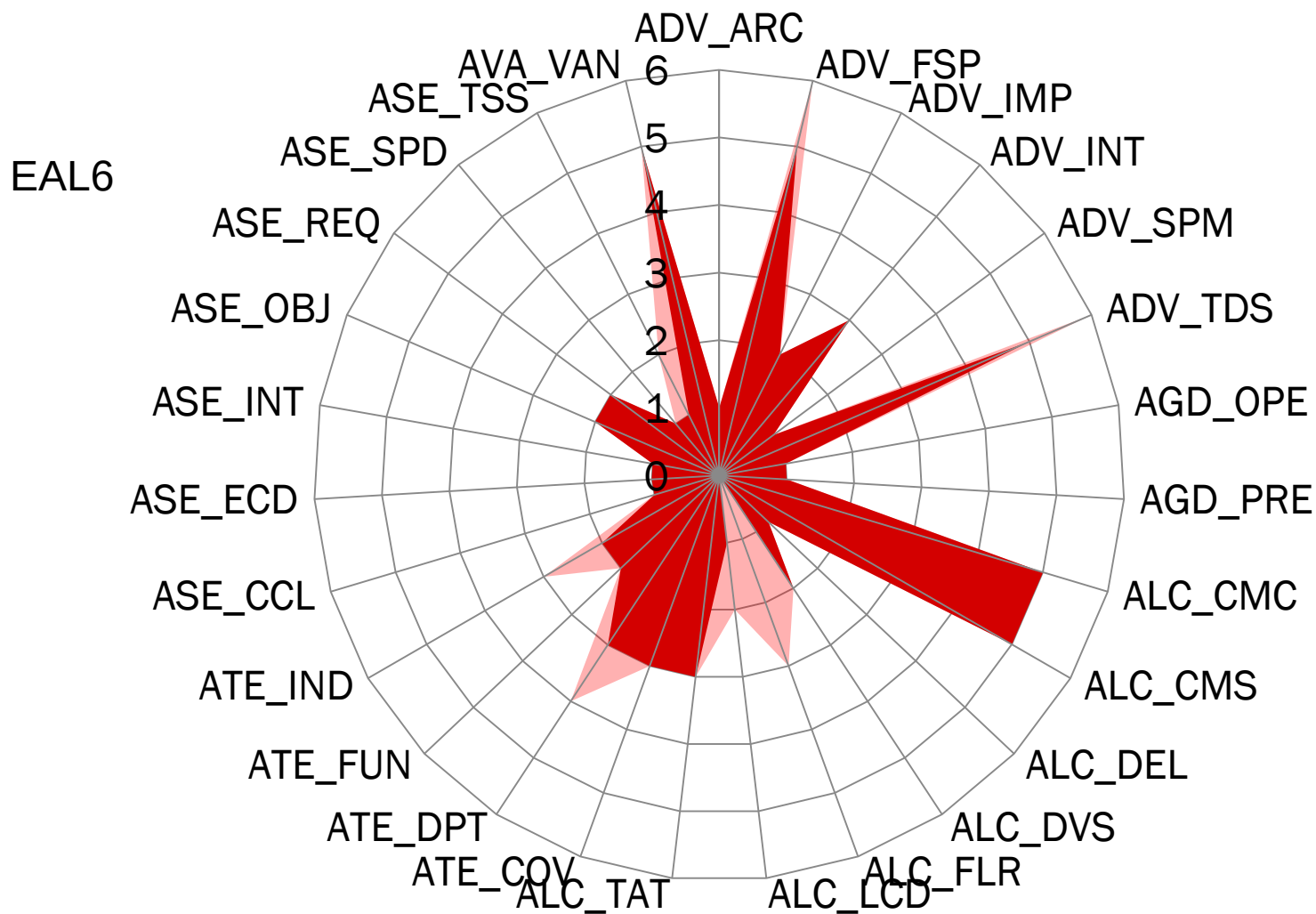
Les critères communs



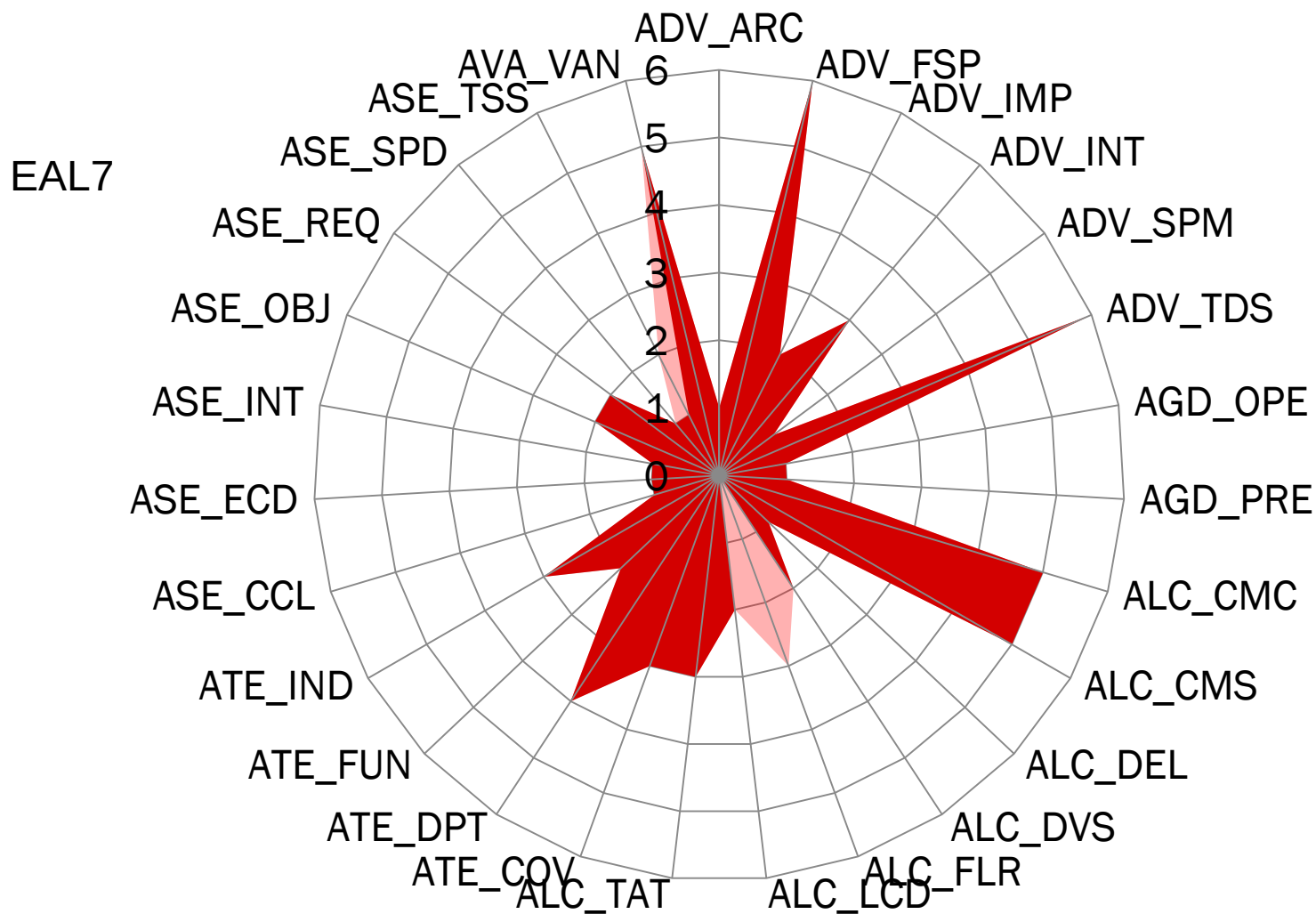
Les critères communs



Les critères communs



Les 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

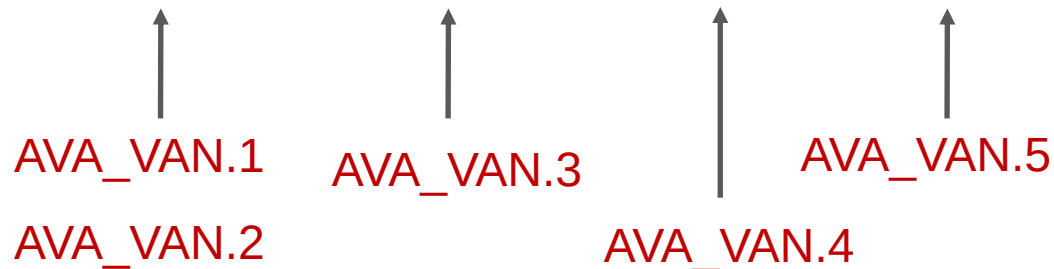
- Dans les critères*: succinct mais objectif !
 - “The developer shall provide the TOE for testing”
 - “The TOE shall be suitable for testing”
 - “The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE”
 - “The evaluator shall perform an independent,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

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

AVA_VAN.1-2 →

Table 11: Rating of vulnerabilities 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
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 vulnerabilities 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 vulnerabilities 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

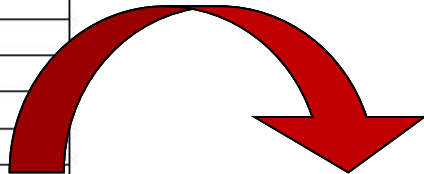
- Standard: oscilloscope de base, lecteur de carte, PC, logiciel d'analyse ou de génération de signal...
- Specialized: oscilloscope haut de gamme, microscope UV, équipement lazer, micro sonde, outils de gravure chimique...
- Bespoke: FIB (Focused Ion Beam), SEM (Scanning electron microscope), AFM (Atomic 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)	TOTAL	
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 vulnerabilities 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

- 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

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

- **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, équipement lazer, micro sonde, outils de gravure chimique...
 - Bespoke: FIB (Focused Ion Beam), SEM (Scanning electron microscope), 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

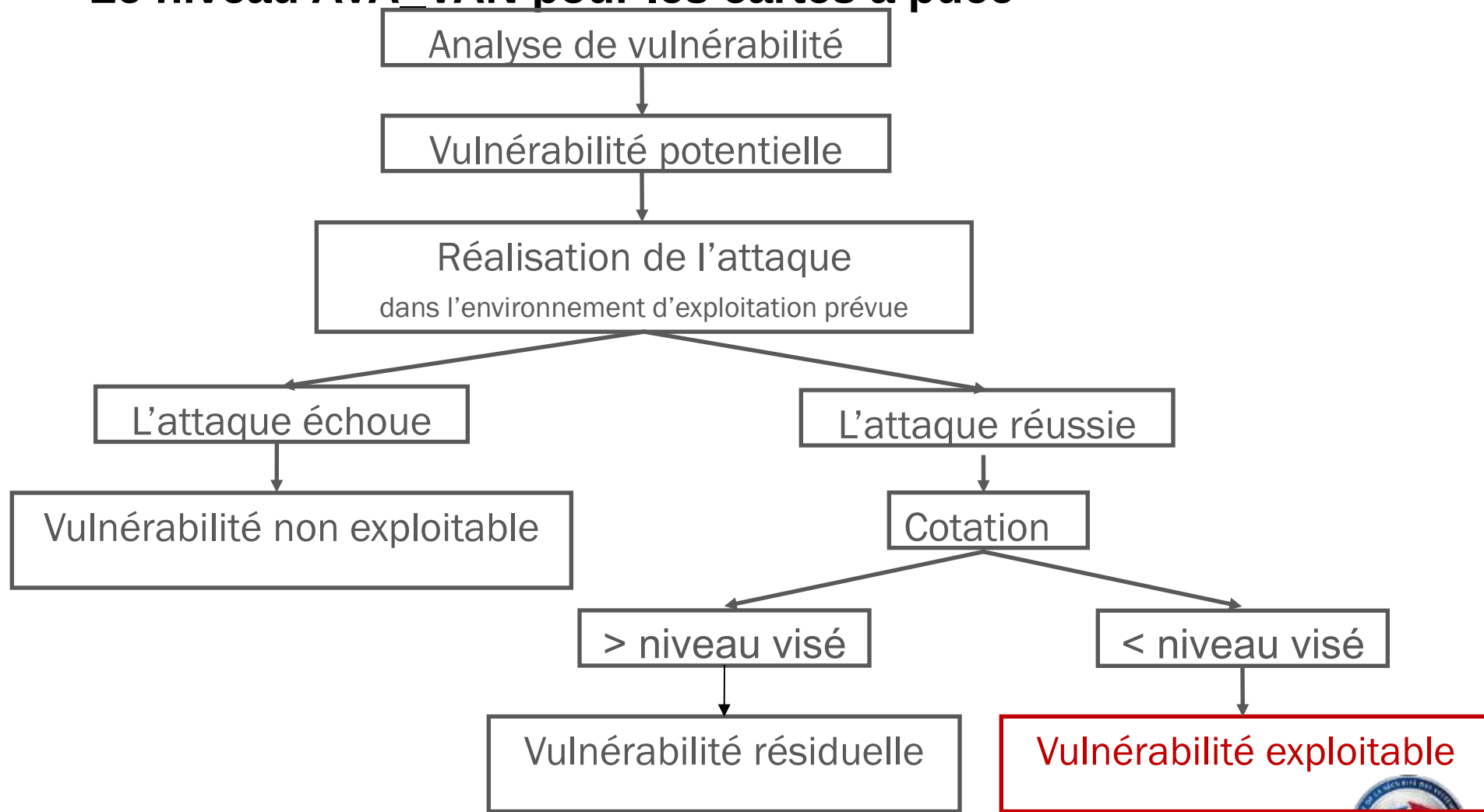
Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Table 11: Rating of vulnerabilities for CC v3

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 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





CESTI



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

- **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
 - 10 laboratoires :
 - 3 CC/CSPN matériel (Leti, Serma, Thales)
 - 2 CC/CSPN logiciel (Amossys, Oppida)
 - 5 uniquement CSPN logiciel (EDSI, Lexfo, Quarkslab, Synacktiv, Trusted Labs)

- **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 invalidé) 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**



Exemples

- Exemples de certificats et rapports de certification CC (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 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**



■ 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...



■ 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 !



■ 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€)



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



La CSPN à l'international

- **BSZ en Allemagne**
- **Lince en Espagne**
- **BSPA aux Pays-Bas**



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





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

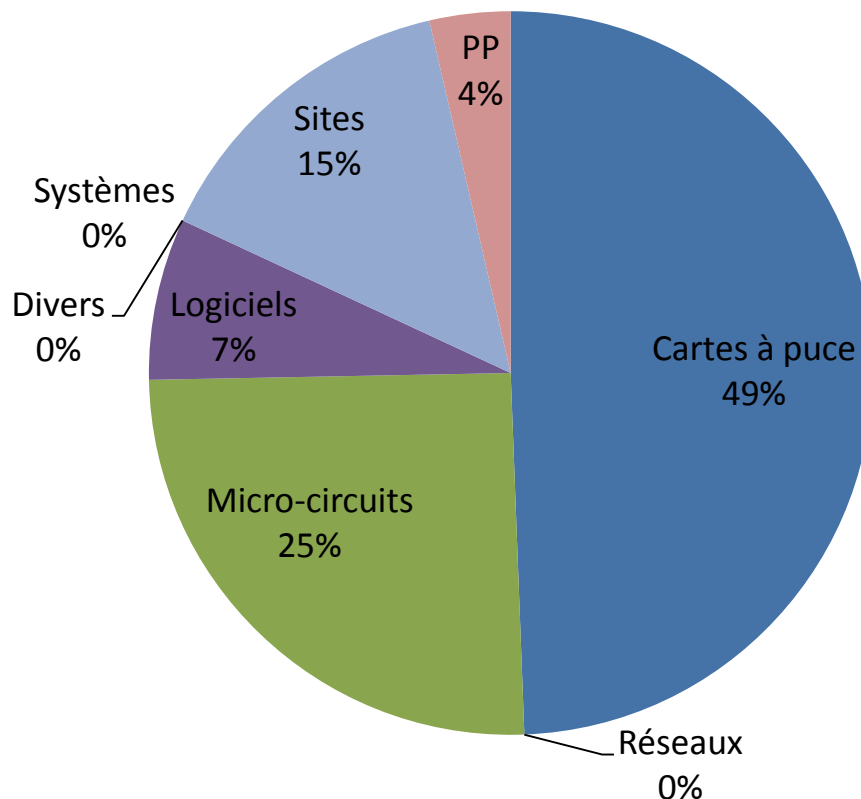
■ Approche réglementaire

- 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...



Retours d'expériences

- En France: 1009 produits certifiés Critères Communs depuis 1995 !

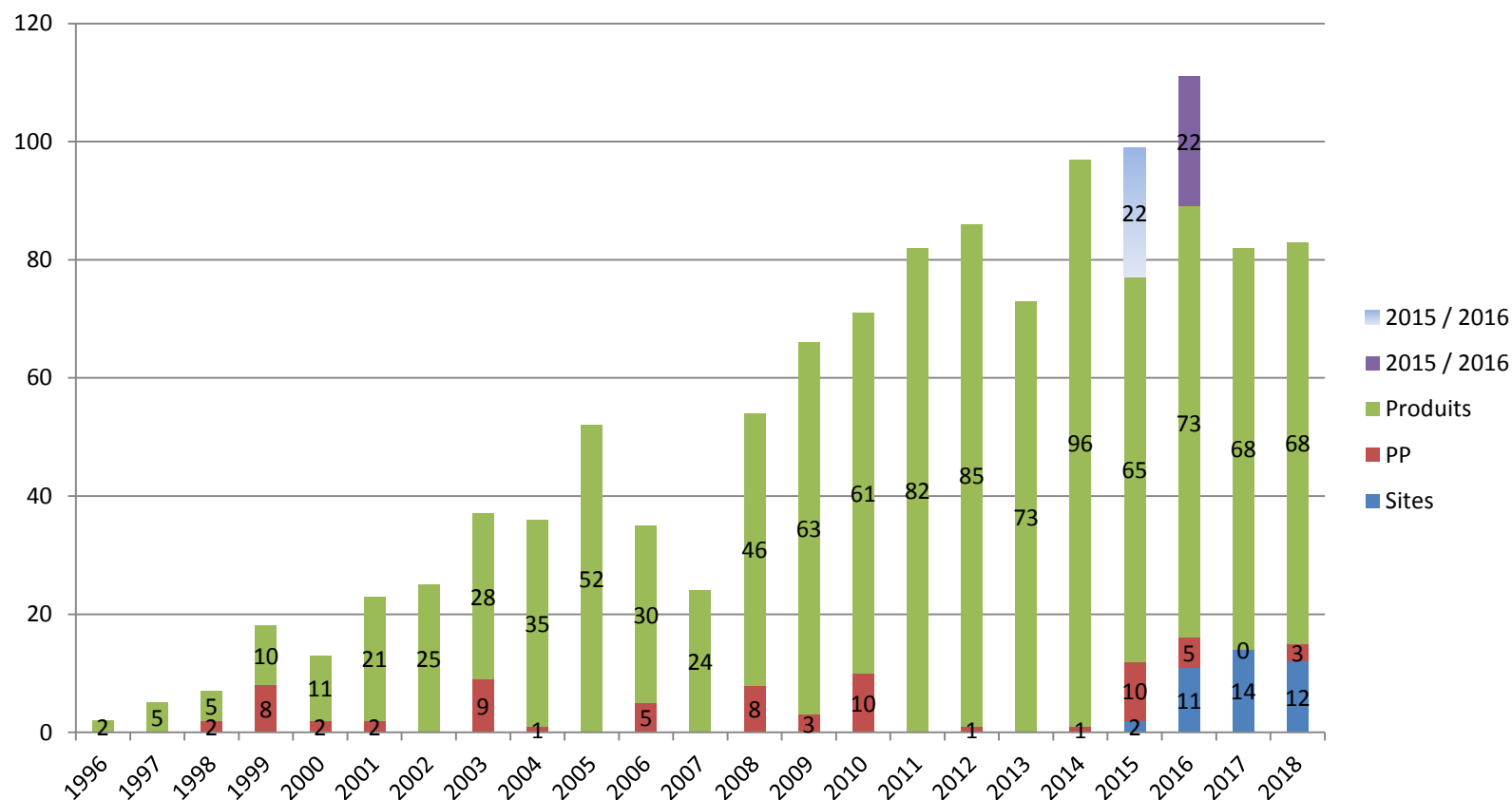


Statistiques ANSSI-CCN février 2019



Retours d'expériences

■ Evolution des certification CC en France :



*Statistiques ANSSI-CCN octobre 2018



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	10	9	2	3	5	12	0	0	0	0	1	0	0	0	0	22	67
Canada	3	0	11	117	0	0	0	0	0	0	0	0	0	0	0	0	0	51	182
Germany	10	4	14	27	16	63	18	340	8	187	0	41	0	0	0	0	0	9	737
Spain	9	8	9	16	5	13	0	37	0	9	0	0	0	0	0	0	0	6	112
France	1	18	1	15	0	41	5	295	5	313	0	18	4	0	0	0	0	0	716
India	1	0	3	0	2	0	0	1	0	0	0	0	0	0	0	0	0	0	7
Italy	5	7	1	1	2	0	1	21	0	0	0	0	0	0	0	0	0	0	38
Japan	0	0	4	90	17	30	0	0	0	0	0	0	0	0	0	0	0	11	152
Republic of Korea	7	0	5	9	8	14	24	15	0	15	0	0	0	0	0	0	0	9	106
Malaysia	6	0	24	10	0	4	1	3	0	0	0	0	0	0	0	0	0	0	48
Netherlands	0	0	5	1	1	1	2	23	0	17	0	13	0	2	0	0	0	1	66
Norway	0	0	2	25	2	12	19	21	3	11	0	0	0	0	0	0	0	0	95
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	5	0	13	2	8	4	6	5	3	0	0	0	0	0	0	0	0	6	52
Singapore	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Turkey	0	0	10	1	2	0	1	11	0	0	0	0	0	0	0	0	0	0	25
United Kingdom	0	0	4	6	1	3	0	26	0	3	0	0	0	0	0	0	0	2	45
United States	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	108	108
Totals:	49	38	116	329	66	188	82	810	19	555	0	72	5	2	0	0	0	225	2556
Standards et acteurs de la certification																			

Retours d'expériences

- Le domaine majoritaire : la carte à puce

2556 Certified Products by Category *		
Category	Products	Archived
Access Control Devices and Systems	69	64
Biometric Systems and Devices	3	0
Boundary Protection Devices and Systems	77	124
Data Protection	72	95
Databases	31	53
Detection Devices and Systems	14	57
ICs, Smart Cards and Smart Card-Related Devices and Systems	1212	33
Key Management Systems	22	28
Mobility	33	22
Multi-Function Devices	208	182
Network and Network-Related Devices and Systems	274	238
Operating Systems	108	75
Other Devices and Systems	290	331
Products for Digital Signatures	105	8
Trusted Computing	38	0
Totals:	2556	1310
Grand Total:		3866
* A Certified Product may have multiple Categories associated with it.		



Retours d'expériences

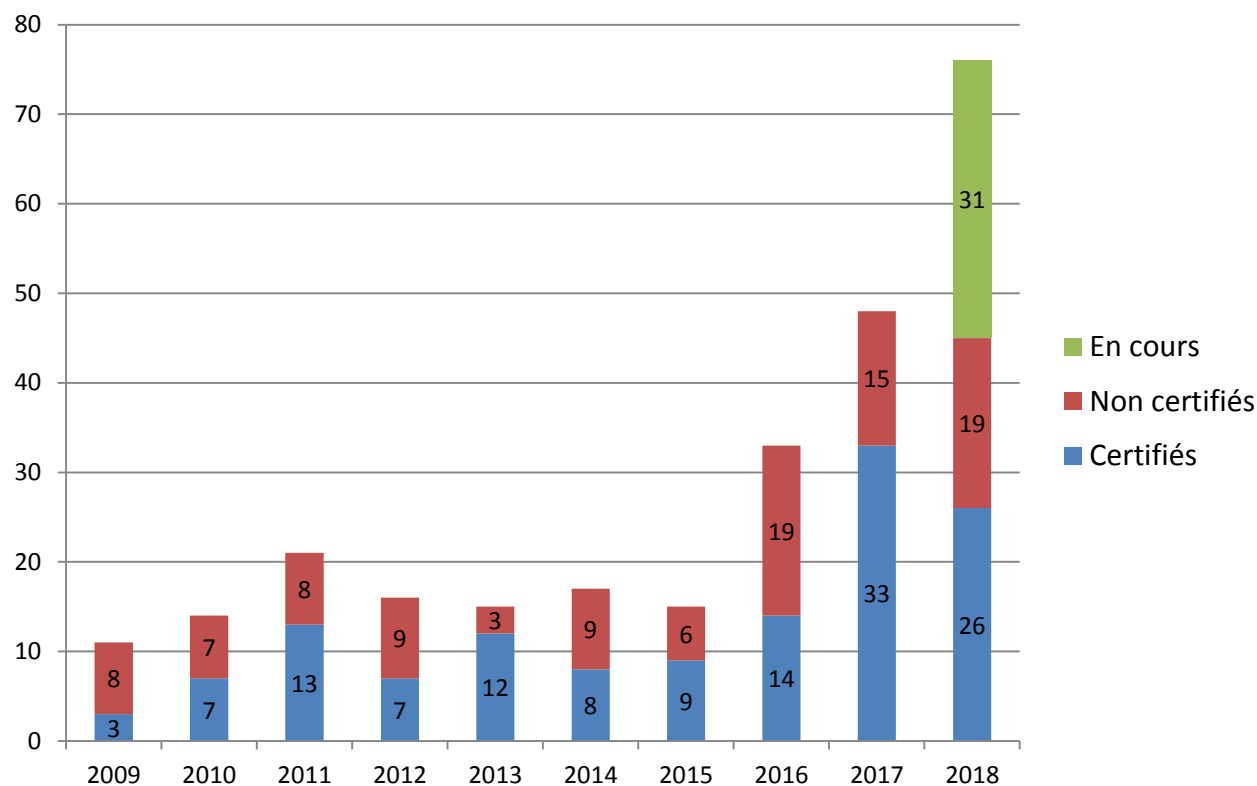
- CSPN : depuis 2009* 246 évaluations, 139 certificats
- PP: 67* certifiés

*Statistiques ANSSI-CCN décembre 2017



Retours d'expériences

■ Evolution des certification CSPN en France :

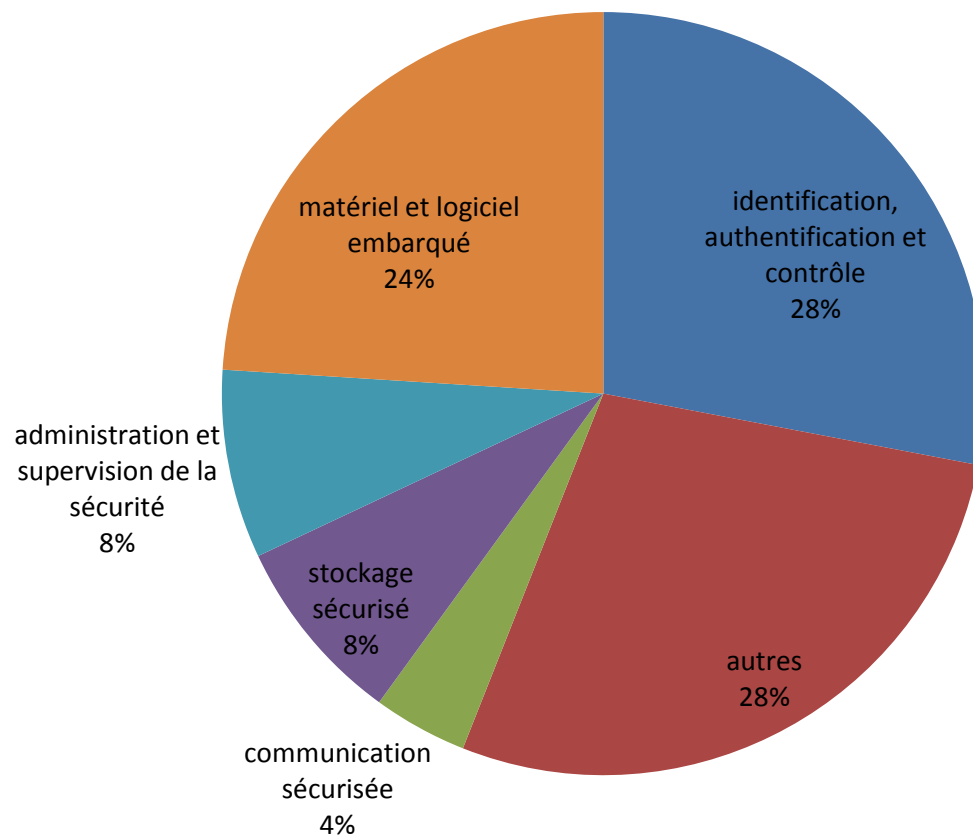


*Statistiques ANSSI-CCN novembre 2018



Retours d'expériences

■ Certificats CSPN par catégorie depuis 2008 :



*Statistiques ANSSI-CCN 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/>



Commanditaire/dév

CESTI

ANSSI

Choix du CESTI

Contractualisation

ST,
planning,
charges CESTIDemande
d'évaluation

Validation

REO

Présentation du produit, périmètre et planning de l'évaluation, participants au projet, etc.

Fournitures

Analyse
dont crypto

Corrections

RTI(s)

Validation

RTE

REF

Synthèse des travaux et des recommandations, planning de la certification, décision de publication, mise sous surveillance, etc.

Experts ANSSI

Rapport de
certification,
certificatSignature
(Publication)

Schéma CC

Standards et acteurs de la certification

Commanditaire/dév

CESTI

ANSSI

Choix du CESTI

Contractualisation

ST,
planning,
charges CESTIDemande
d'évaluation

Experts ANSSI

Validation

Présentation du produit, périmètre et planning d'évaluation, participants au projet, etc.

Fournitures

Analyse
dont crypto (25/35 h.j)

Com

Validation

RTE

RESTITUTION

Revue du RTE, avis et recommandations de l'évaluateur, avis des experts techniques de l'ANSSI, décision de certification, etc.

Schéma
CSPN

Experts ANSSI

Rapport de
certification,
Certificat

Signature

Standards et acteurs de (Publication)