

Certification et Développement Sécurisé

Damien Sauveron
damien.sauveron@unilim.fr
<http://damien.sauveron.fr/>

(et tous les auteurs cités en bibliographie)

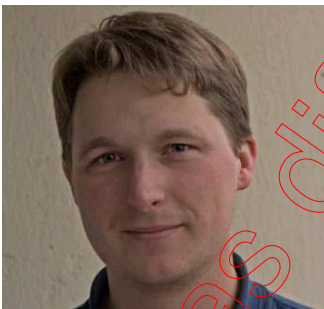
1

Intervenants dans le module

Damien Sauveron (Cours, TD et TP) :

- Membre de l'équipe « Sécurité de l'Information »
- Thème de recherche : sécurité des cartes à puce et des réseaux ad hoc

Pour me contacter :



Damien Sauveron
XLIM UMR CNRS 6172 -- Université de Limoges
Site Jide
83 rue d'Isle
87000 Limoges, FRANCE

Email: Damien.Sauveron@unilim.fr
Web: <http://damien.sauveron.fr/>
Phone: +33 (0) 5 55 43 69 83
Fax: +33 (0) 5 55 43 69 77

2004-2006 :

Visiteur/Postdoctorant dans le Smart Card Centre de l'Information Security Group du Royal Holloway, University of London (6 mois)

ATER à l'université de Limoges

2001-2004 :

Thèse au LaBRI – Université Bordeaux 1 sur la *Sécurité de la Technologie Java Card*

Ingénieur R&D dans le CESTI de SERMA Technologies (Pessac) spécialisé sur *les évaluations sécuritaires puces*

2

Plan

La sécurité ?

- Quelques définitions
- Quoi protéger ?
- Comment ?
- Vérifier la sécurité ?
- UML
- Méthodes formelles & Test
- Évaluation sécuritaire et certification
- Open source vs propriétaire
- Outils d'analyse logiciel
- Analyse de sécurité
- Procédures d'attaques

Les sécurités

- Au niveau physique
- Au niveau logicielle
- Au niveau de l'environnement de production

Qu'est ce que la sécurité ?

What is Security?

Defining security is not as easy as it seems.

For computer security, the most common approach is in terms of **CIA**:

- ▶ Confidentiality
- ▶ Integrity
- ▶ Availability

For other types of security, we must define security in terms dealing with risks.

5

Confidentiality

Confidentiality is about preventing **unauthorised** users **reading** information to which they are not entitled.

Traditionally, security and confidentiality are often identified.

We shall see how confidentiality is provided by **encryption**.

Warning: Privacy (anonymat)

6

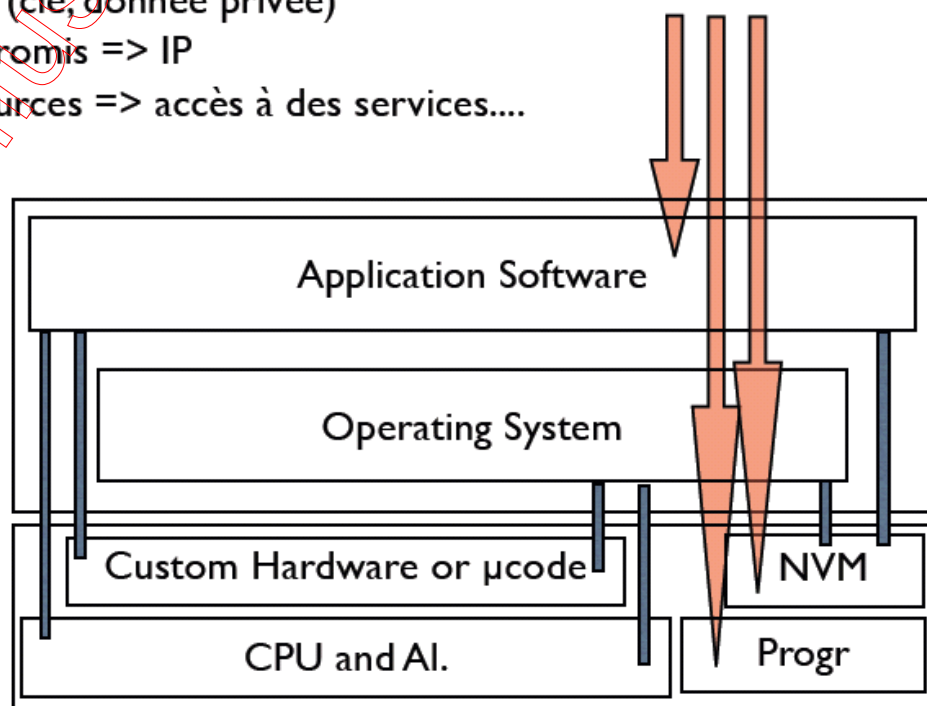
La confidentialité

- La confidentialité est la propriété de “secret” attaché aux informations. Seul les entités autorisées à accéder aux ressources le sont.
- Elle est assurée par le contrôle d'accès aux informations et ressources du SEM. De même le SEM ne peut communiquer de l'information qu'aux entités autorisées à recevoir cette information.
- Mise en oeuvre de techniques pour assurer la confidentialité
 - Contrôle d'accès au SEM
 - Contrôle d'accès aux ressources internes dans le SEM

7

La confidentialité

- Data compromise (clé, donnée privée)
- Programme compromis => IP
- Accès à des ressources => accès à des services....



Integrity

Integrity is about making sure things are as they should be.

In the context of computing, integrity is about preventing **unauthorised** users **writing** information to which they are not entitled.

In a general system, integrity is about ensuring that the system state has not been modified by those not authorised to do so.

In the context of data communications, integrity is often restricted to **detecting modifications** or knowing where information comes from

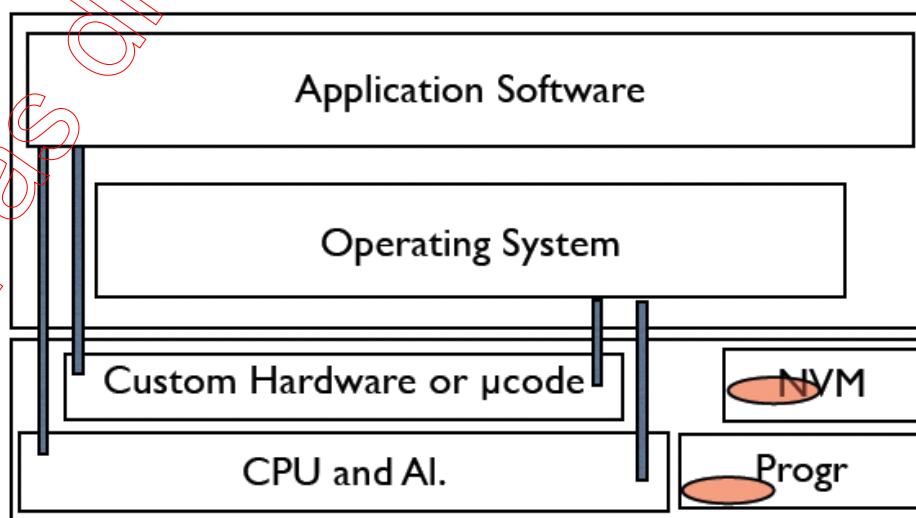
We shall see how integrity is provided by **MACs** and **digital signatures**.

Warning:
Authentication
(authentication)

9

L'intégrité

- Données et programmes changés



L'intégrité sur les données

- L'intégrité sur les données est assurée par le contrôle sur les actions d'écriture.
- De manière passive on peut vérifier que des données ne sont pas altérées en effectuant des contrôle sur les valeurs :
 - Par redondance, par CRC, par signature,...
 - Ceci peut être fait par matériel ou logiciel

11

L'intégrité sur les programmes

- Un programme ayant subi une altération peut avoir des conséquences très importantes :
 - Modification sur ses données des applications,
 - Modifications sur des données du système d'exploitation :
 - table d'autorisations, programmes,...
 - ouverture de nouveau services
 - ...
 - L'altération initiale peut être volontaire mais peut aussi être le résultat d'une erreur de programmation!

**Comment garantit-on
l'intégrité d'une exécution ?**

12

Availability

Availability is about a systems services being accessible on demand by an authorised entity.

This covers areas beyond the normal scope of security, including fault-tolerance.

For security we are primarily concerned with preventing **denial of service** attacks by unauthorised entities.

But CIA is not enough, there are other properties we need to consider.

13

La disponibilité

● La disponibilité est la propriété qui assure que les fonctions du SE&M sont utilisables pour les utilisateurs dans les délais prévus.

● Dans le cas d'un serveur Web la disponibilité sera le fait que les requêtes sont satisfaites et que l'attaque par déni de services sera sans effet.

14

Quelles autres propriétés ?

15

Accountability

Responsabilité =>

Imputation/Non Repudiation

In practice not all improper actions can be prevented.

Thus users must be held **accountable** for their actions, including system misuse.

This is typically done by securely identifying users, and keeping an **audit trail** of security related events.

16

Security is related to **reliability** and **safety**, dealing with systems which must perform properly in adverse conditions.

Dependability is sometimes used to encompass both security and reliability.

Not only are goals of security and dependability related, but similar methods are often used for system evaluation.

Particularité des SE&Ms

- Le dispositif est entre toutes les mains
 - Porte ouverte aux intrusions...
 - A la différence d'un centre de traitement qui est une unité de lieu, néanmoins les grilles de calculs "ouvertes" connaissent un peu la même problématique
- Via le réseau des attaques sont possibles (porte d'entrée),
- La plate-forme peut être ouverte (Java Architecture)

Les menaces sur les plate-formes

● Les menaces sur les SEMs (systèmes embarqués et mobiles) sont celles classiques des systèmes informatique,

● Mais :

● Le contexte d'utilisation de l'objet peut être spécifique

● PayTv

● Les aspects systèmes peuvent être spécifiques

● Attaques par déclenchement des chauffages en forçant la température sur les capteurs chauffage

● Les enjeux

● Carte bancaire = argent

3

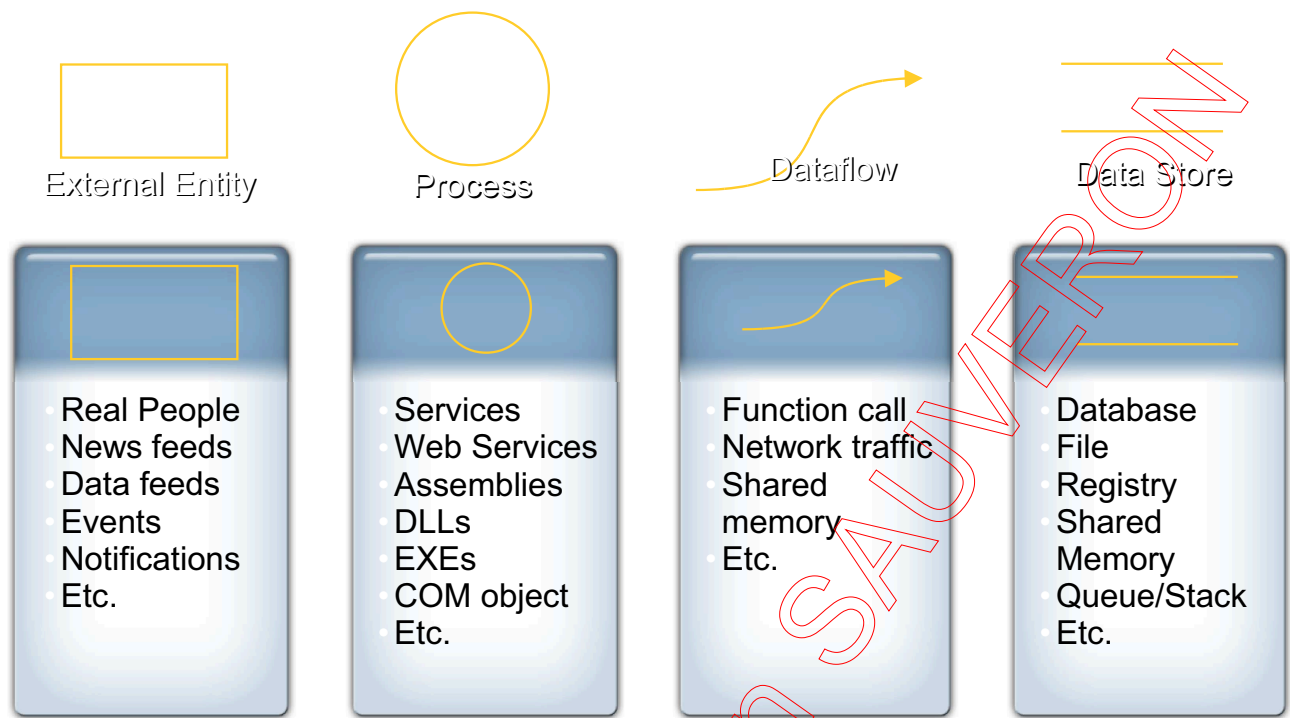
Qu'est ce qu'on veut sécuriser ?

Qu'est ce
qu'on veut
sécuriser ?

RAPPEL:

- Sécurité : Security
- Fialailité/Sûreté : Dependability
- Confidentialité : Privacy
- Intégrité : Integrity
- Disponibilité : Availability

Asset (les biens !)



21

Security Threats

Another way of defining security, particularly in the case of systems other than computers, is to first perform a threat analysis. Security can then be defined in terms of combating the perceived threats.

Not all threats are always worth defeating

- Need a Cost/Benefits Analysis

Risk Analysis This notion of assessing the importance of each threat, thereby leading to an assessment of whether it should be combated, is the essence of **risk analysis**. The cost of living with some threats (e.g. low level theft which can be quantified) may be less than the cost of prevention.

22

Providing Security

Next consider (in general terms) how security can be provided in a system.

What general types of security control exist, and where can these be located ?

Security provided in an application can be subverted by attacking the operating system.

Security provided in the OS can be subverted by attacking the hardware.

Designing security into a system from the start is much better than adding security as an afterthought.

23

Focus of Control

When protecting data in a computer system, it is often done using **rules** on system behaviour.

These rules may be...

- ▶ Limit ways in which data is handled.
- ▶ Limit which operations can be performed on which data
- ▶ Limit which users can perform certain types of actions.

i.e. security controls can focus on data, operations or users (or some combination)

e.g. Compartmentalised Operating Systems.

24

Location of Security Controls

A typical IT system can be modelled as having 5 layers

- ▶ **Application Programs**
- ▶ **Services** : eg provided by DBMS or a distributed file system
- ▶ **Operating System** : Performing file and printer management etc.
- ▶ **Kernel** (of OS) : Mediating access to processor and memory.
- ▶ **Hardware** : Processor and memory.

Security controls can be located in any of these layers.

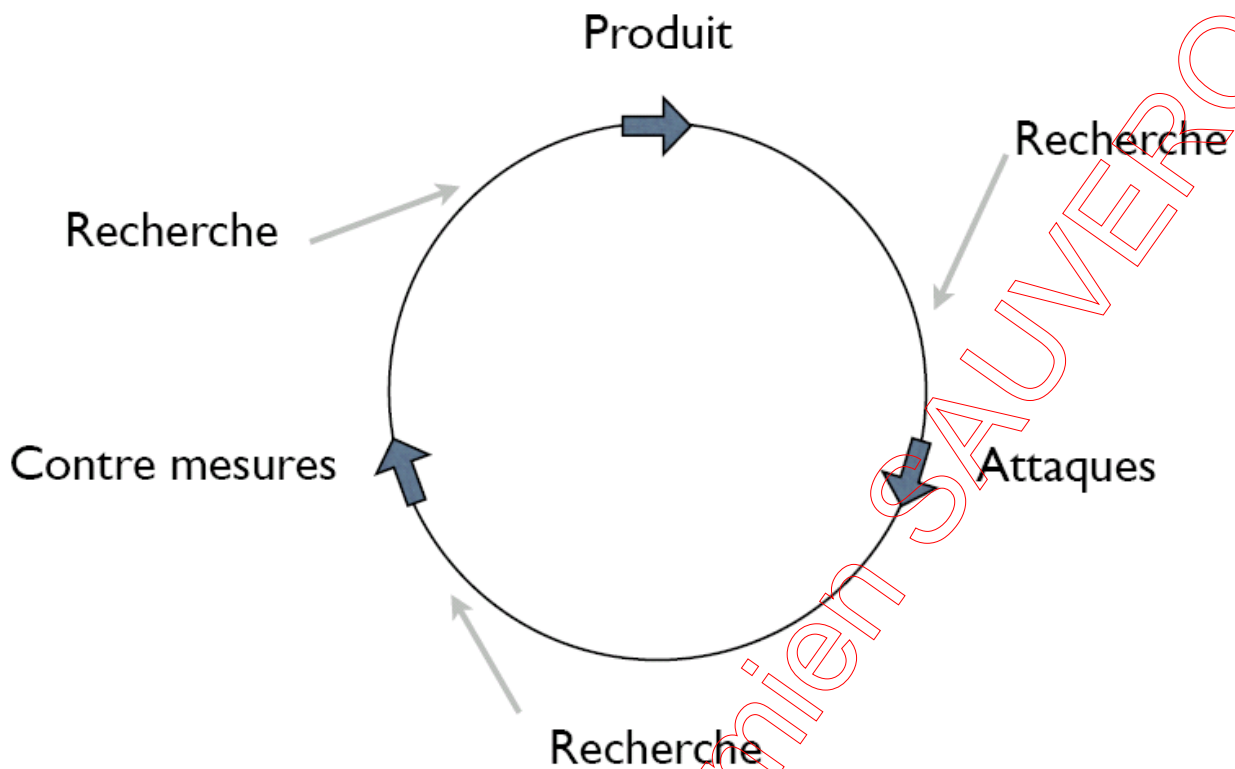
Mechanisms close to hardware are typically more generic and computer-oriented, whilst those close to the application are more user-oriented.

25

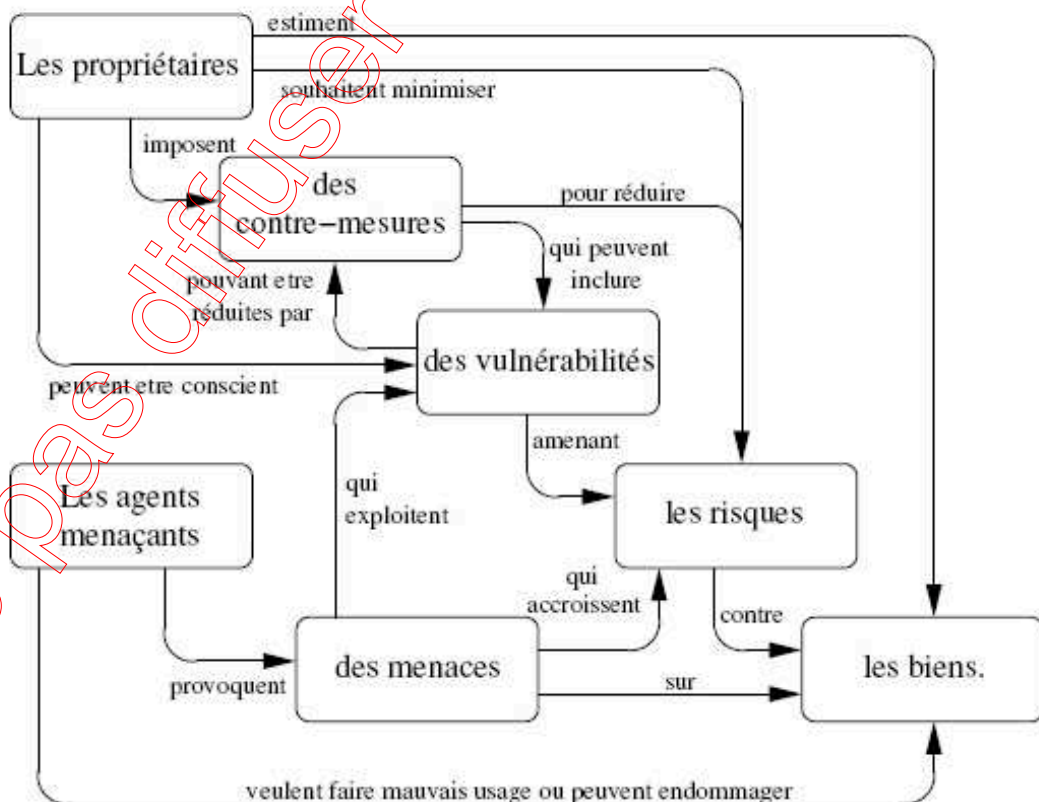
In this course we focus on Communications Security (or more generally Security of Information)

26

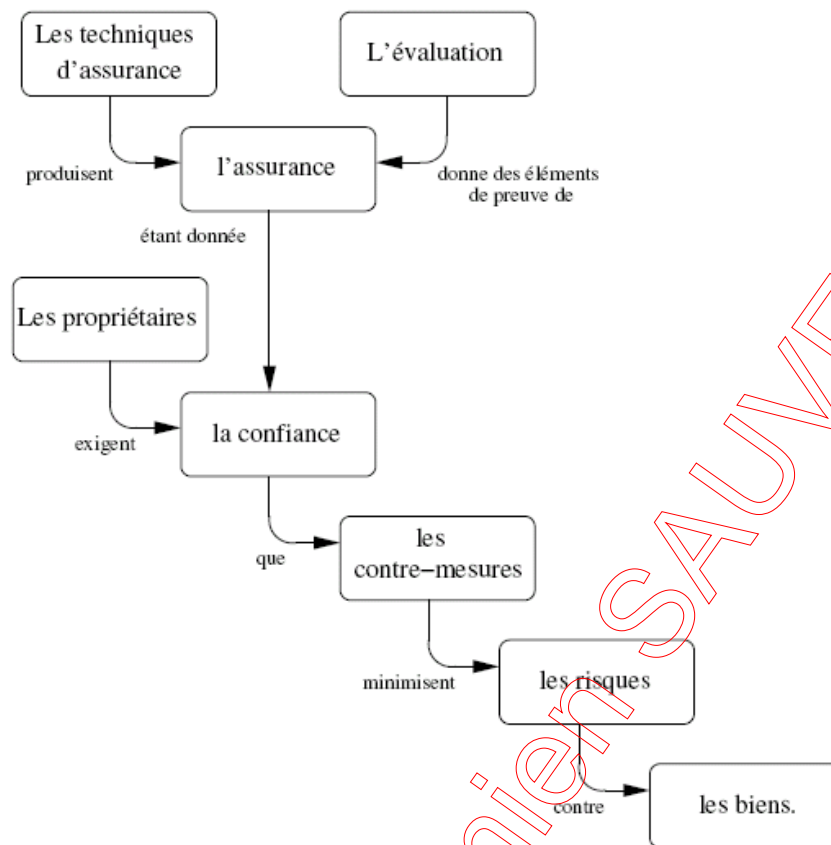
Un cycle infernal!



Concepts de sécurité et relations



Concepts de l'évaluation et relations



29

Functionality versus Assurance

In assessing secure systems, two different aspects need considering

- ▶ **Functionality**, i.e. what security facilities are provided.
- ▶ **Assurance**, i.e. what guarantees are offered that the security functionality performs as claimed.

These two aspects are often reflected in **Security Evaluation Criteria**, from the **Orange Book** onwards.

30

Assurance versus Complexity

The work involved in providing a high level of assurance in security features is proportional to the complexity of those features.

Hence, if a high level of assurance is required it makes sense to minimise complexity.

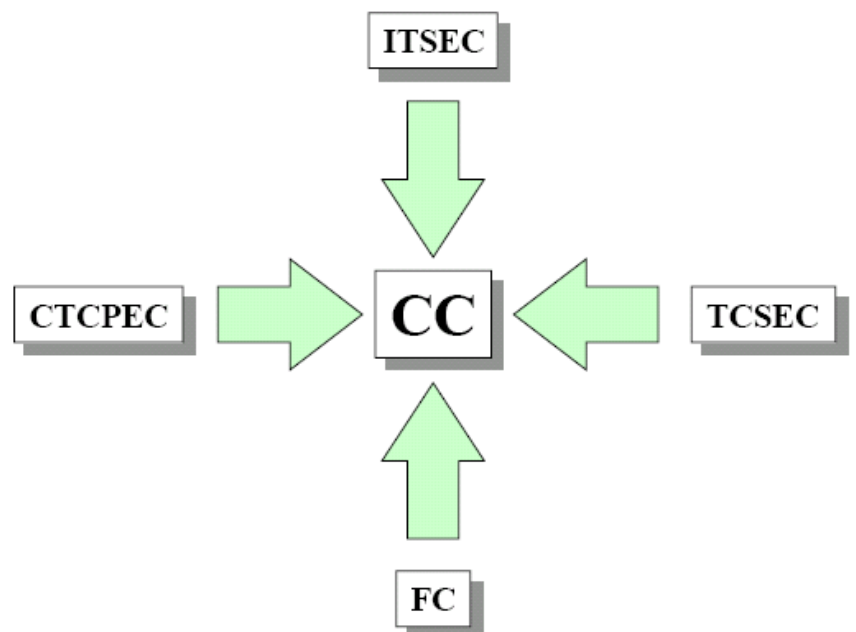
31

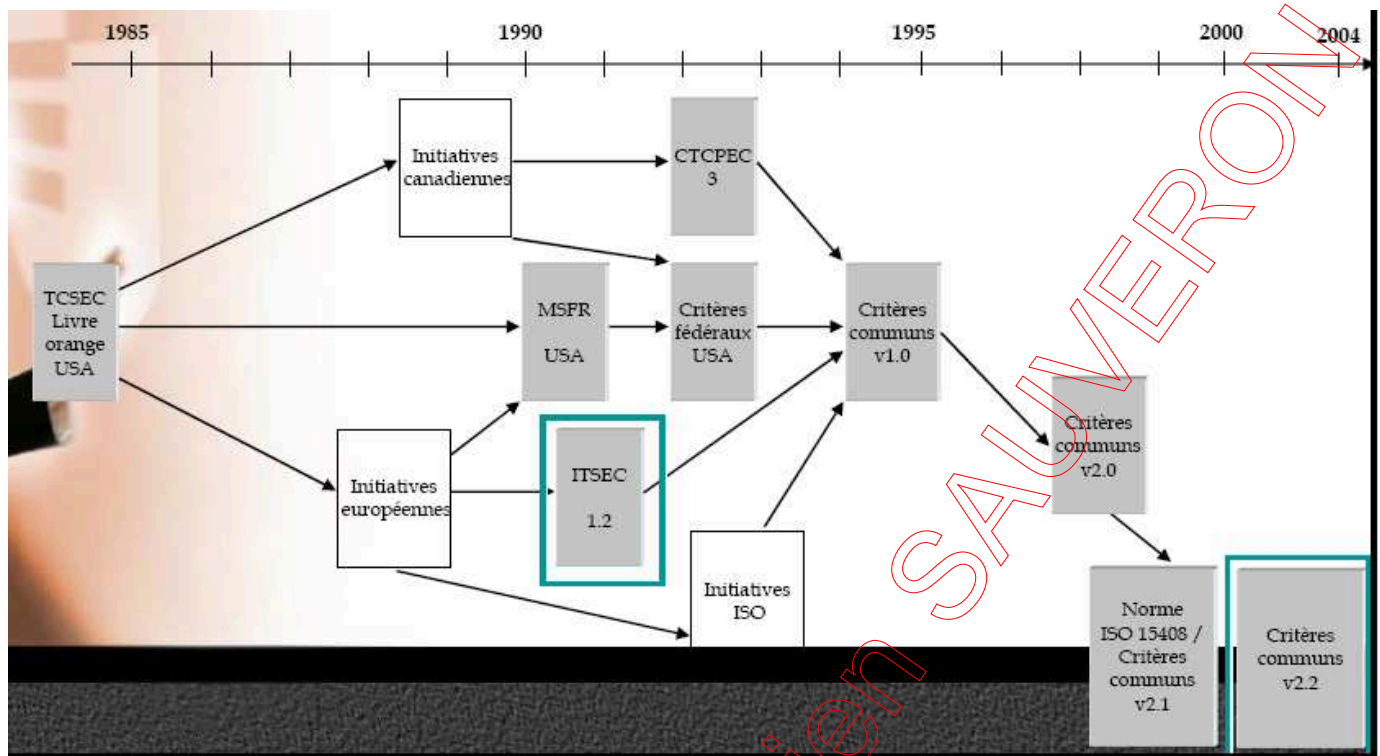
Normes pour l'évaluation

Avant l'apparition des CC, les pays utilisaient des critères d'évaluation différents :

l'Orange Book pour les États Unis ;
les ITSEC pour la France, l'Allemagne, le Royaume-Uni et les Pays-Bas ;
le CTCPEC pour le Canada.

Harmonisation des critères existants





33

Critères Communs

Les Critères Communs (CC) sont une norme qui a pour vocation d'être utilisée comme base pour l'évaluation des propriétés de sécurité des produits et systèmes des Technologies de l'Information (TI). Ils sont définis par le Common Criteria Interpretations Management Board (CCIMB) et sont depuis quelques années une norme ISO définie comme ISO/IEC 15408

- **CC : Common Criteria v2.1, August 1999**
(<http://www.scssi.gouv.fr/documents/docs/CC/cc21.html>)
 - Part 1 : Introduction and general model
August 1999 Version 2.1
 - Part 2 : Security functional requirements
August 1999 Version 2.1
 - Part 3 : Security assurance requirements
August 1999 Version 2.1
- **CEM : Common Methodology v1.0, August 1999**
(<http://www.scssi.gouv.fr/documents/docs/CEM/cem.html>)
 - Evaluation methodology for PP and ST
Version 1.0
 - Evaluation Methodology for levels EAL1 to EAL4
Version 1.0

34

Une norme internationale

ISO/IEC JTC 1/SC27
Technologies de l'information - Techniques de sécurité

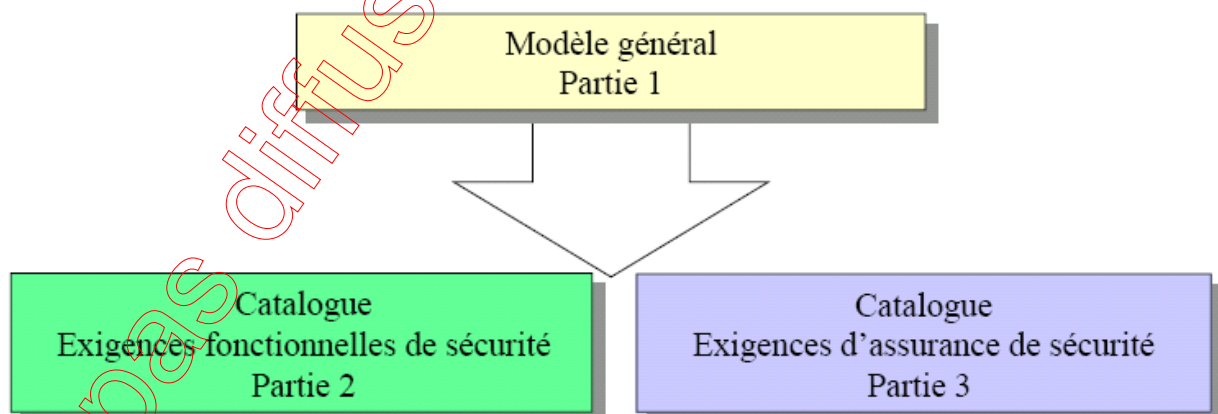


Juin 1999 Normalisation des Critères Communs

ISO/IEC IS 15408-1	Partie 1 Introduction et modèle général
ISO/IEC IS 15408-2	Partie 2 Exigences de sécurité fonctionnelles
ISO/IEC IS 15408-3	Partie 3 Exigences de sécurité d'assurance

35

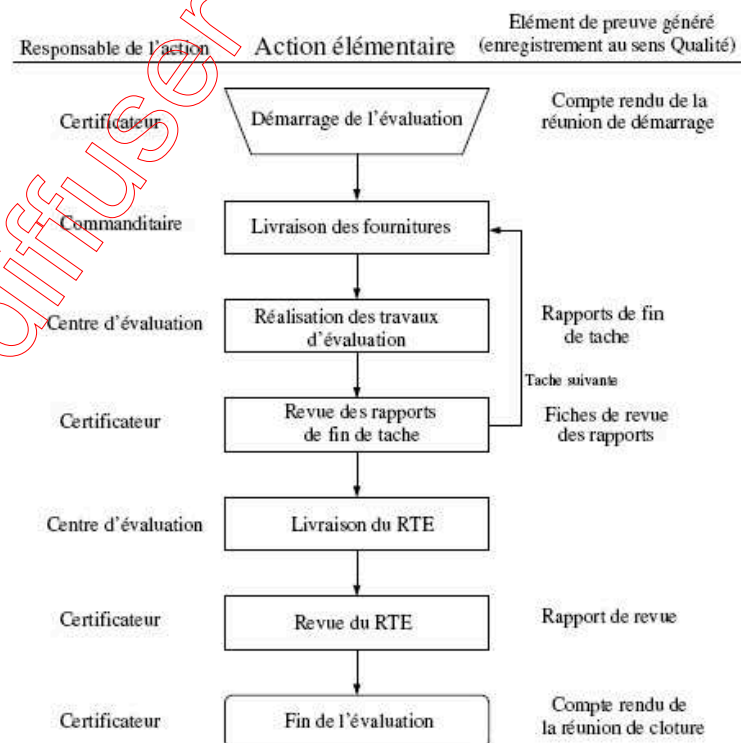
Expression des exigences



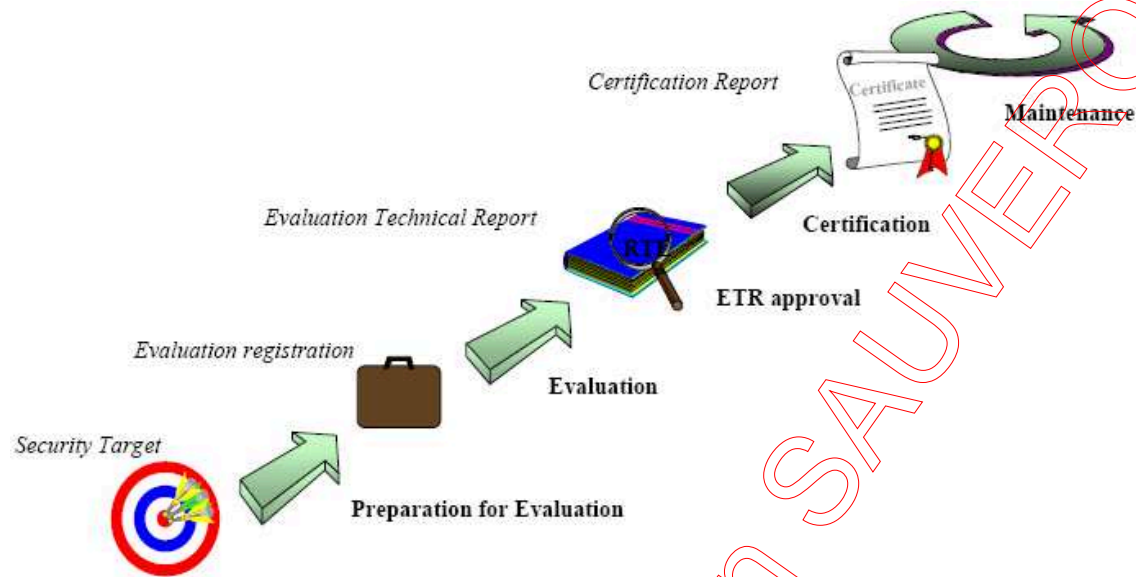
36

	Consumers	Developers	Evaluators
Part 1	Use for background information and reference purposes. Guidance structure for PPs.	Use for background information and reference for the development of requirements and formulating security specifications for TOEs.	Use for background information and reference purposes. Guidance structure for PPs and STs.
Part 2	Use for guidance and reference when formulating statements of requirements for security functions.	Use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Use as mandatory statement of evaluation criteria when determining whether a TOE effectively meets claimed security functions.
Part 3	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Use as mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

Déroulement de l'évaluation



Evaluation Process : main steps



39

Quelques définitions

TOE (Target Of Evaluation) pour définir la cible d'évaluation, i.e. le produit ou le système TI à évaluer ;

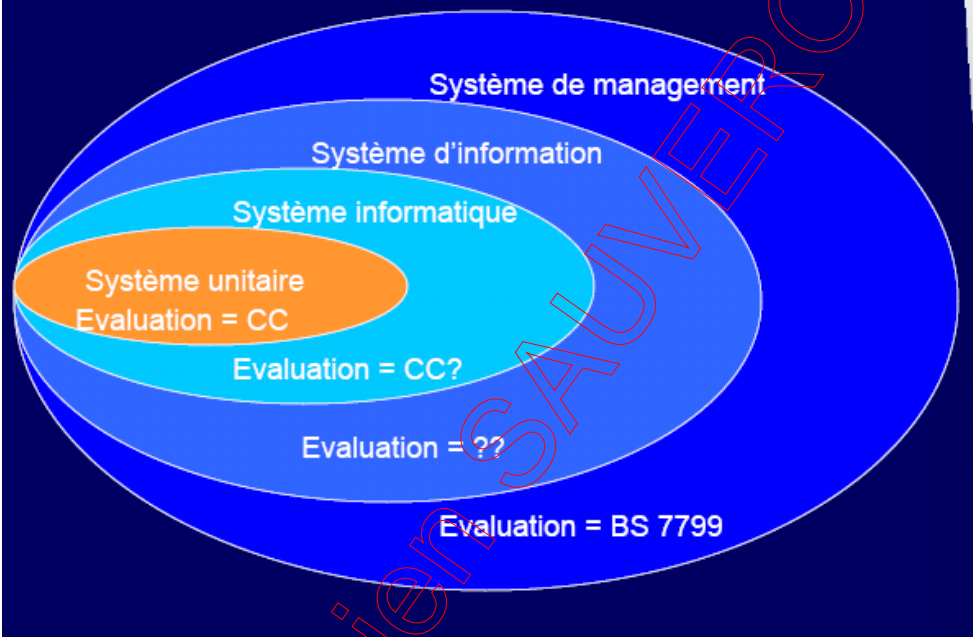
ST (Security Target) pour désigner une cible de sécurité, i.e. un document rassemblant l'ensemble des exigences de sécurité et des spécifications à utiliser comme base pour l'évaluation d'une TOE identifiée ;

PP (Protection Profil) pour désigner un profil de protection, i.e. un document rassemblant l'ensemble des exigences de sécurité valables pour une catégorie de TOE qui satisfait des besoins spécifiques d'utilisateurs, indépendamment de son implantation (e.g. il existe des PP pour l'évaluation de puce nue – i.e. sans applicatif –, pour le domaine des applications bancaires)

- **Target of evaluation (TOE)** : an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation. It defines assets to protect.
- **TOE Security Functions (TSF)** : A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
- **TOE Security Policy (TSP)** : A set of rules that regulate how assets are managed, protected, and distributed within a TOE.
- **Security Target (ST)** : Defines the target of evaluation, the environment, the threats, assets to protect, security objectives, assumptions.

40

Que cherche t'on à évaluer ?

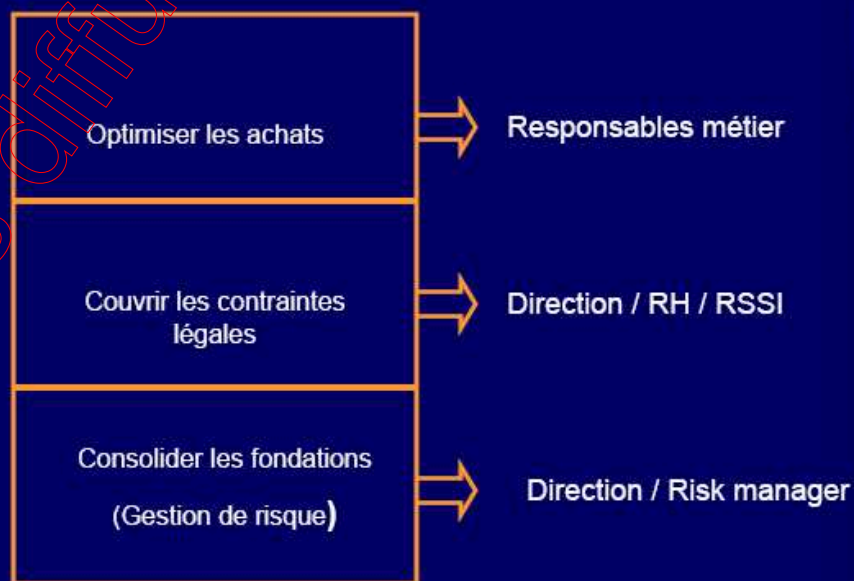


Et même un sous ensemble

41

Etablissement de la confiance !

Pourquoi une évaluation des systèmes d'information?



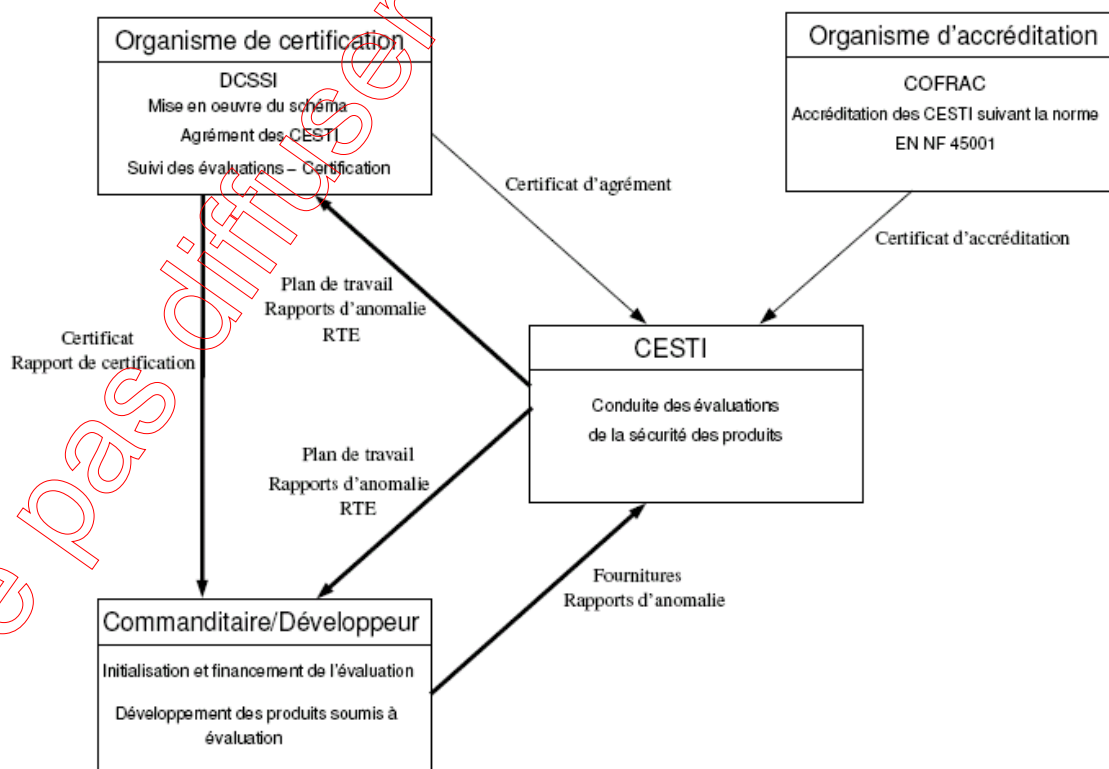
42

Usages actuels des Critères Communs

- ✚ Dans les projets, pour qualifier une technologie
 - Chronotachygraphe
 - GIE Cartes Bancaires
 - Messagerie OTAN
- ✚ Pour la fourniture de matériels de sécurité
 - Cartes bancaires
 - Firewalls
 - Modules cryptographiques
- ✚ Dans le domaine de la Défense
 - Évaluation produits de haute sécurité
 - Évaluation de systèmes complexes (ex SINAPSE)

43

Le schéma Français



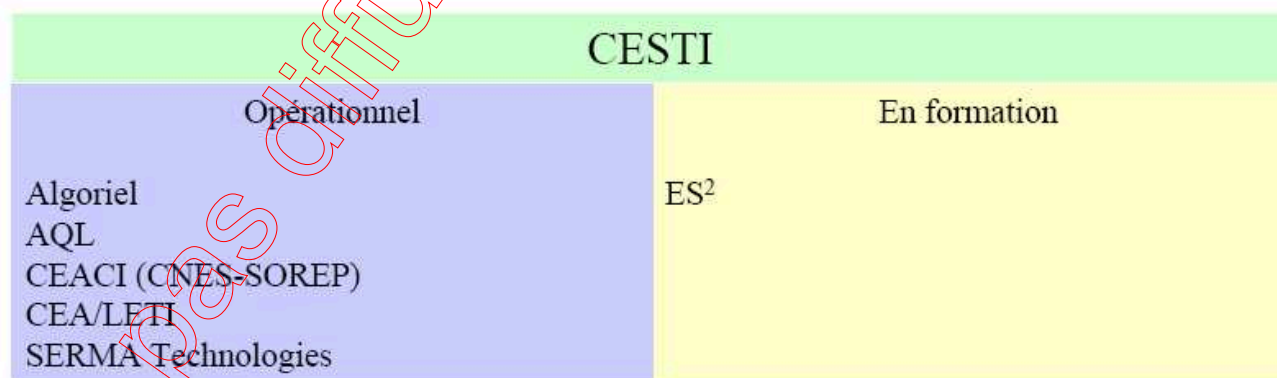
44

Organisme de certification



45

Centres d'évaluation



Agréés pour le domaine de la carte à puce :
CEACI,
CEA/LETI,
SERMA Technologies.

46

Un environnement international...

Organismes de certification:

BSI	Allemagne
CESG	Royaume Uni
DSD	Australie
CSE	Canada
NIST et NSA	Etats-Unis
SCSSI	France

47

Reconnaissance mutuelle



Mars 1998

Accord SOGIS

Senior Officials Group for Information Security of the European Commission

- Accord entre 12 pays européens :

Allemagne, Espagne, Finlande, France, Grèce, Italie, Pays-Bas, Portugal, Norvège, Royaume Uni, Suède et Suisse

- Organismes de certification qualifiés

Allemagne, France et Royaume Uni

- Certificat ITSEC E1 à E6 et CC EAL1 à EAL7



48

Reconnaissance mutuelle



Mai 2000

Arrangement harmonisé



- Accord entre 13 pays :

Allemagne, Australie & Nouvelle Zélande, Canada, Espagne, États-Unis, Finlande, France, Grèce, Italie, Pays-Bas, Norvège, Royaume Uni et Suède

- Organismes de certification qualifiés

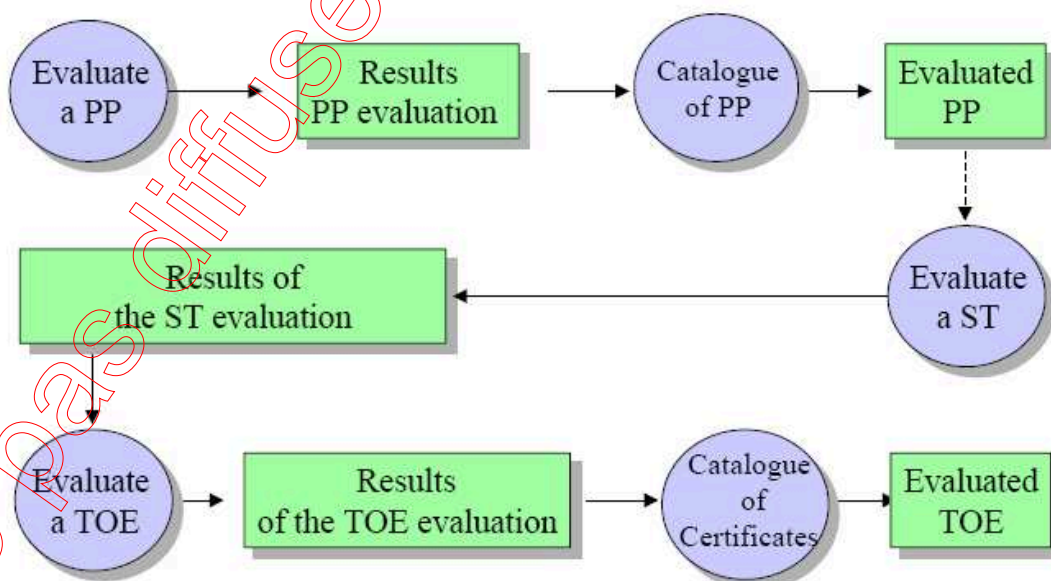
BSI (Allemagne), DSD (Australie), CSE (Canada), NIST/NSA (États-Unis), SCSSI (France) et CESG (Royaume Uni)

- Organismes de certification commerciaux

- Certificat CC EAL1 à EAL4

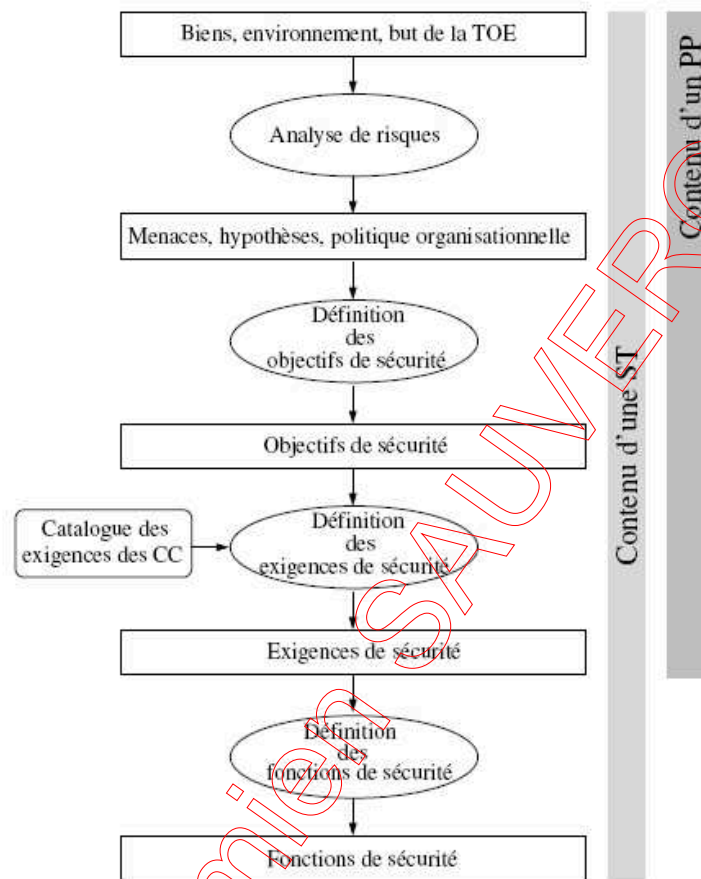
49

CC evaluations and their results

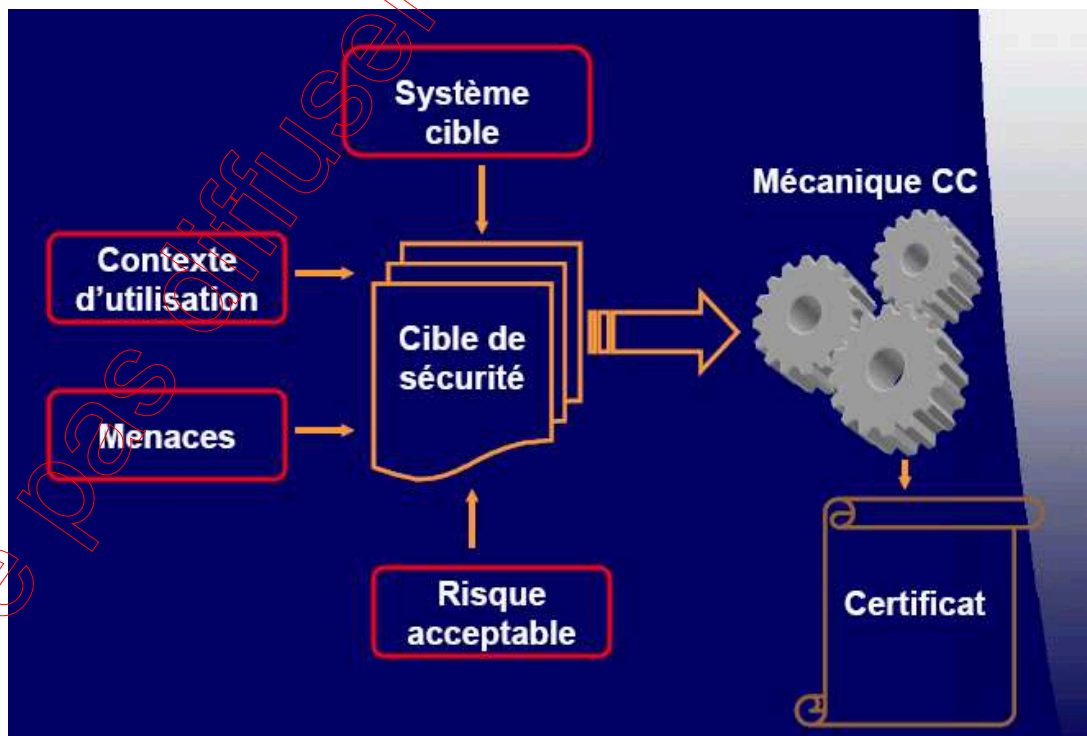


50

Contenu d'une ST et d'un PP



51



52

Retour d'expérience sur l'évaluation d'un VPN

EADS



53

Quelques chiffres !

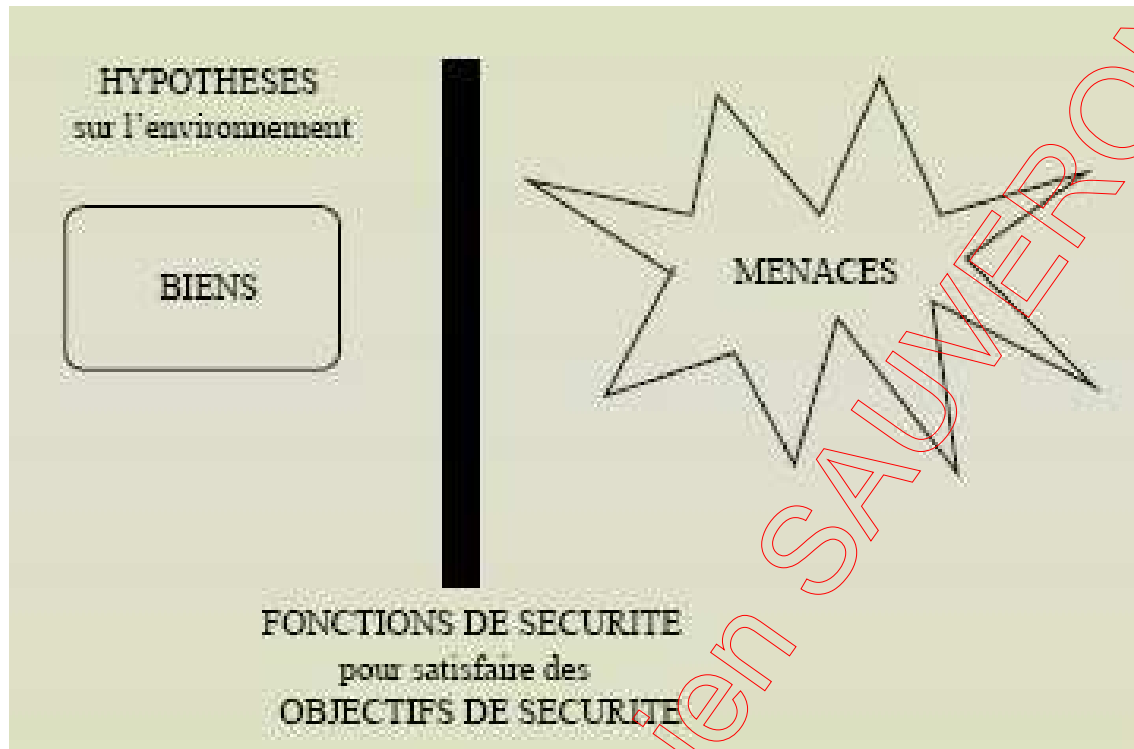
Retour d'expérience sur l'évaluation d'un VPN

- ✚ Contexte :
 - Sollicitation pour les besoins gouvernementaux
 - Évaluation CC EAL2+ (Qualification standard)
 - Périmètre le plus englobant possible
 - Certification body : DCSSI
 - Centre d'évaluation : AQL
 - Obtention du certificat en décembre 2002
- ✚ Caractéristiques du projet
 - Durée : 7 mois
 - Coût : 200KE

54

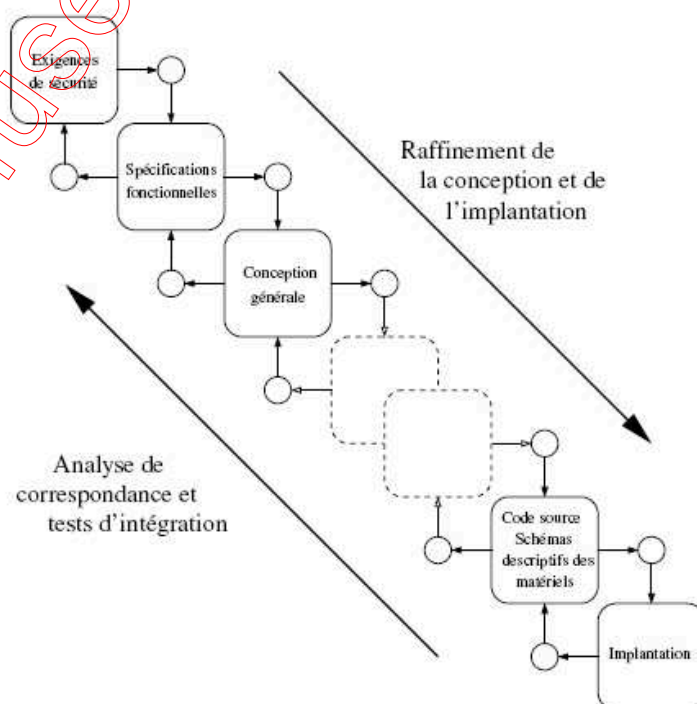
Les bases des critères communs

Critères Communs (ISO15408)



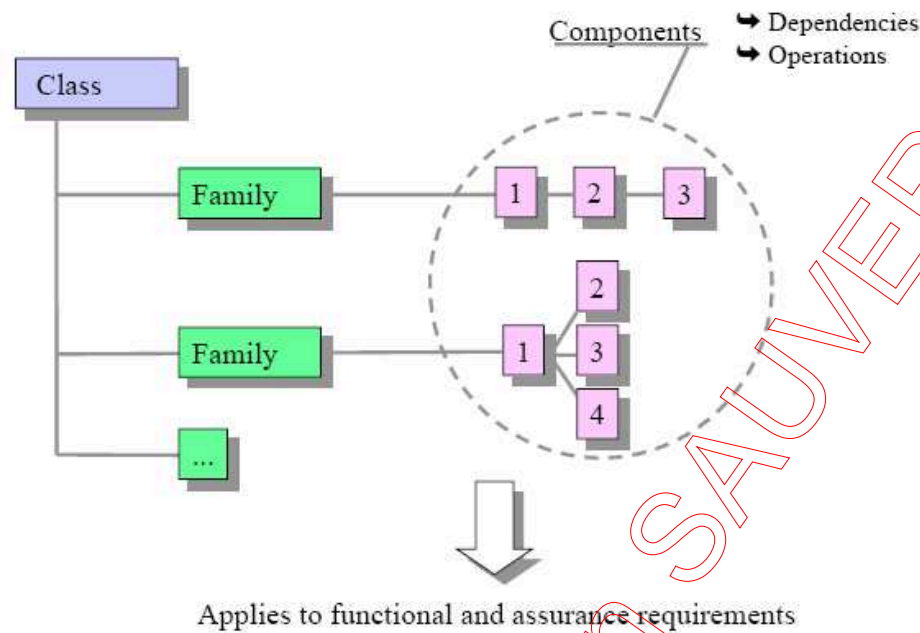
55

Modèle de développement d'une TOE



56

Requirements : hierarchical structure



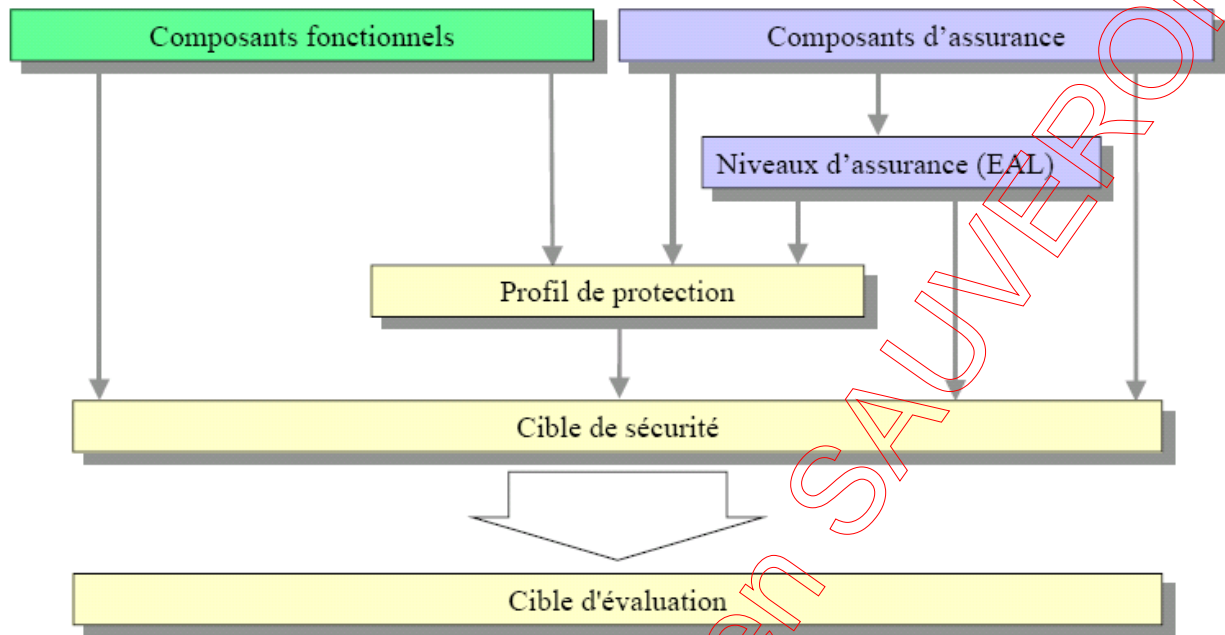
57

CC Catalogue : definitions

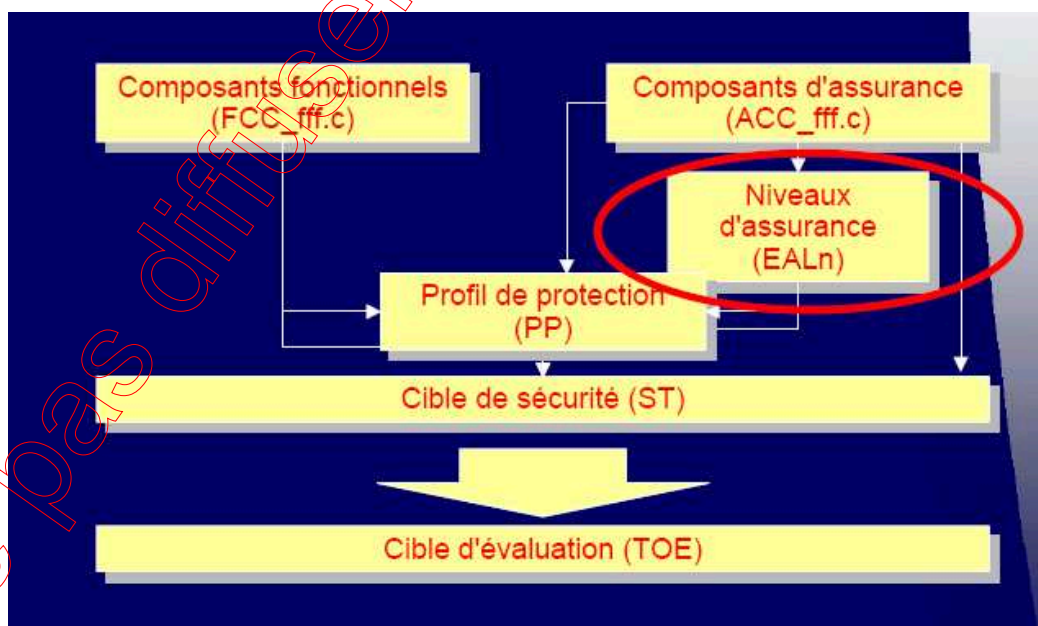
- **Class** : A grouping of families that share a common focus.
- **Family** : A grouping of components that share security objectives but may differ in emphasis or rigour.
- **Component** : The smallest selectable set of elements that may be included in a PP, an ST, or a package.
- **Package** : A reusable set of either functional or assurance components (eg. an EAL), combined together to satisfy a set of identified security objectives.

58

Utilisation des catalogues



59



60

La cible de sécurité

⊕ La clé de voûte de l'évaluation : la cible de sécurité (ST)

⊕ Architecture de la ST

- Niveau d'assurance : définit la profondeur de l'évaluation
- Périmètre du système évalué (TOE)
- Environnement de sécurité
 - Hypothèses d'utilisation
 - Menaces prises en compte
- Objectifs de sécurité : doivent couvrir toutes les menaces
- Fonctions de sécurité : doivent couvrir tous les objectifs
- Référence à une cible type : le Profil de Protection (PP)

61

Profil de protection

Introduction

Description de la TOE

Environnement de sécurité

Objectifs de sécurité

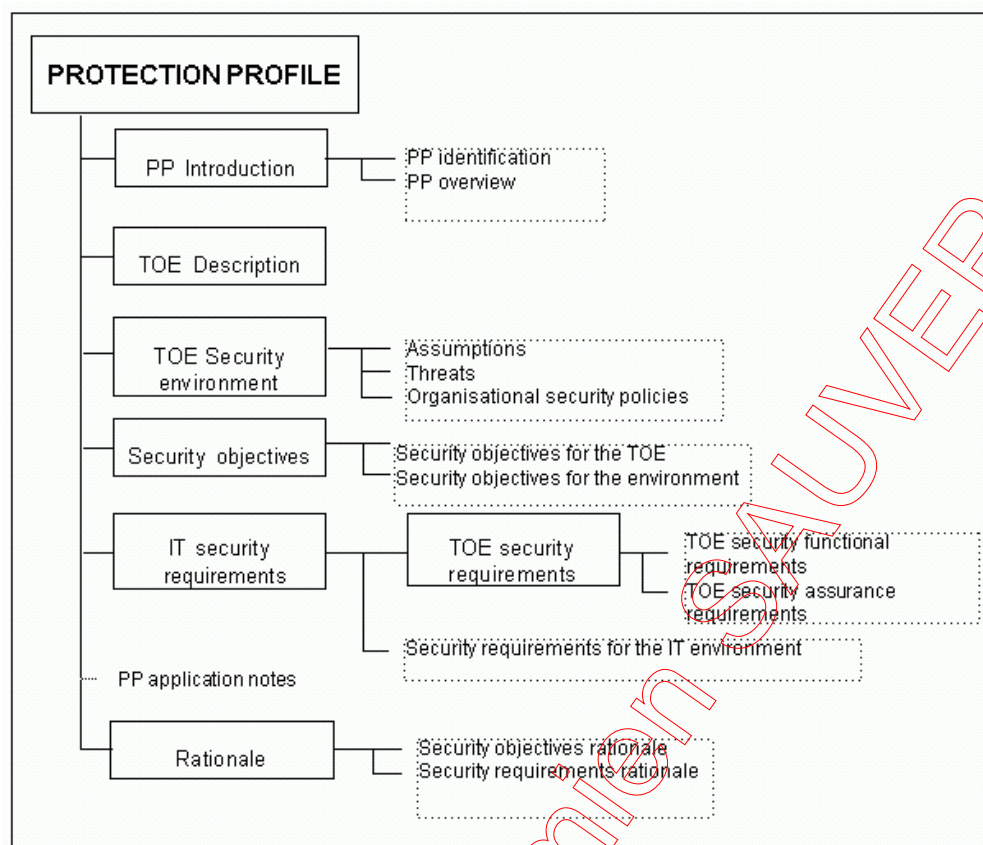
Exigences de
sécurité des TI

Exigences de
sécurité de la TOE

Justificatif

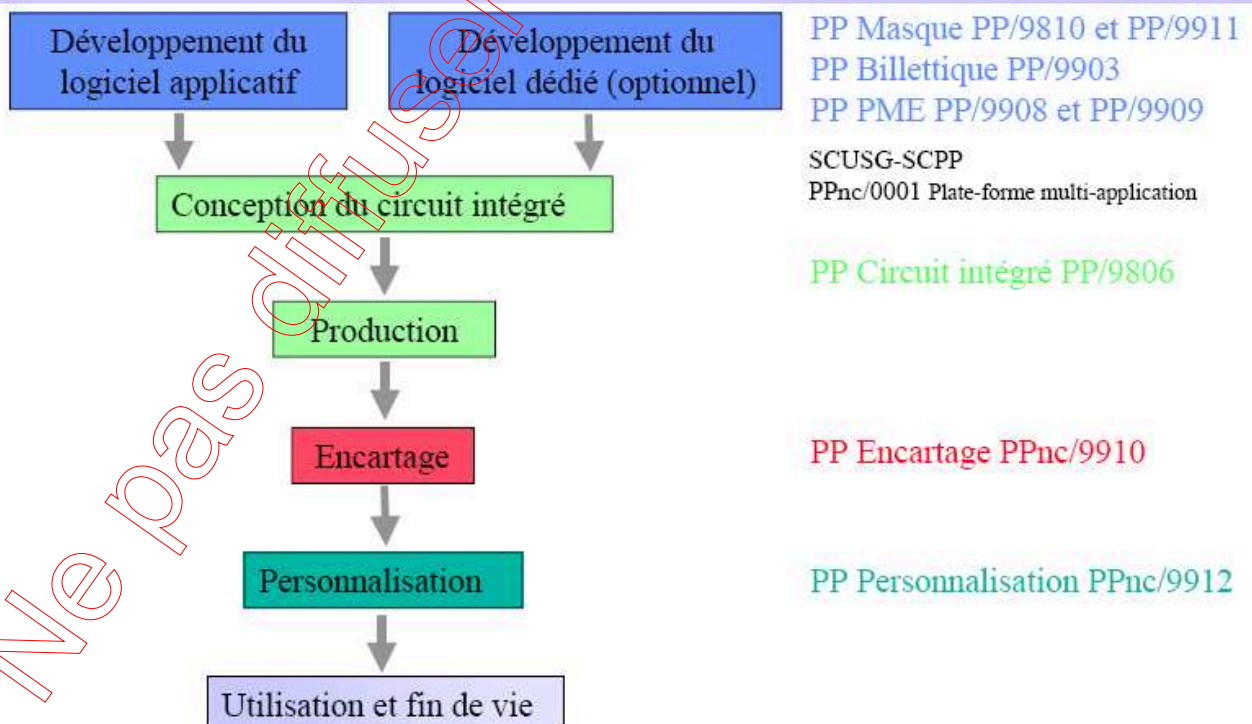
62

Protection Profile



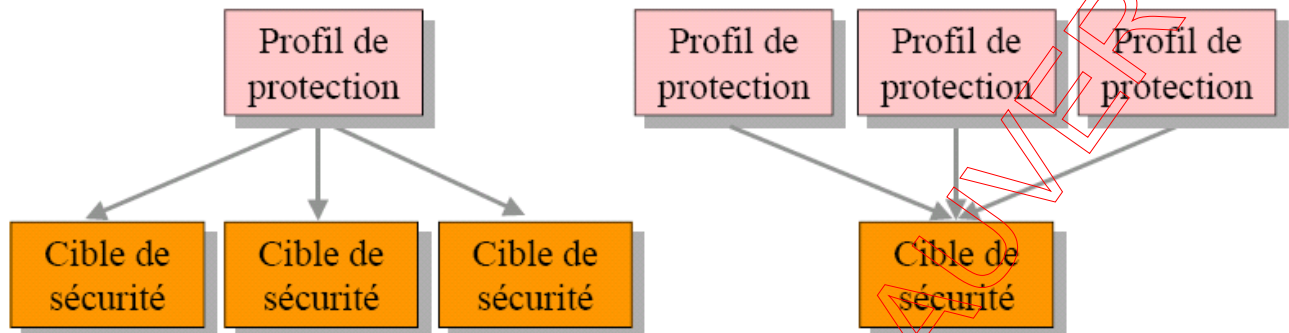
63

PP Cartes à puce



64

Utilisation des profils de protection



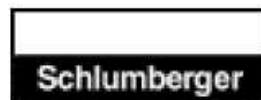
65

PP Masque

PP/9810: Smartcard embedded software

EAL4+ (ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)

Schlumberger



PP/9911: Smartcard integrated circuit with embedded software

EAL4+ (ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)

EuroSmart



66

PP Billetique

PP/9903: Carte à puce billetique avec et sans contact

EAL4+ (ADV_IMP.2, AVA_VLA.4)

SNCF, RATP



67

PP PME

PP/9908: Intersector Electronic Purse and Purchase Device

Version for Pilot Schemes only

EAL1+ (AVA_VLA.2)

Banque de France, EuroSmart, GIE Cartes Bancaires CB



PP/9909: Intersector Electronic Purse and Purchase Device

EAL4+ (ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)

Banque de France, EuroSmart, GIE Cartes Bancaires CB



68

PP Composant pour carte a puce

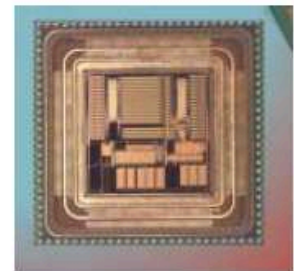
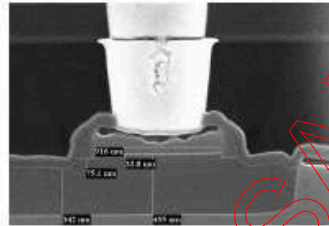
PP/9806: Smartcard integrated circuit

EAL4+ (ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)

EuroSmart,

Motorola, Philips, Siemens, STMicroelectronics,

Texas-Instruments



69

PP Encartage et personnalisation

PPnc/9910: SmartCard embelling Sites

Paquet d'assurance spécifique

AFPC (Association des Fabricants et des Personnaliseurs de Carte)



PPnc/9912: SmartCard personalization Sites

Paquet d'assurance spécifique

GIP CPS



70

PP Terminaux



PP/9907: Automates bancaires

EAL4+ (AVA_VLA.3)

Bull

Dassault A.T.

IBM

NCR

Siemens Nixdorf

Wang Global

PP/0002: Lecteur transactionnel de cartes à puce

EAL4+ (ADV_IMP.2, AVA_VLA.3)

Cyber-COMM

71

PP Echanges de données informatisées

PP/9802: Transactions portant sur des données non confidentielles

EAL3+ (ADV_IMP.1, ADV_LLD.1, ALC.TAT.1)

Ministère de l'Economie, des Finances et de l'Industrie

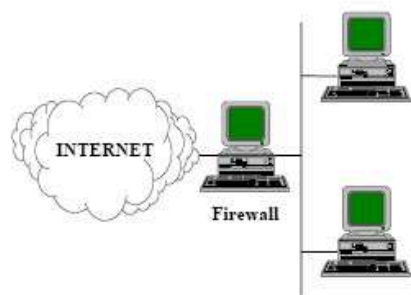
PP/9803: Transactions portant sur des données confidentielles

EAL3+ (ADV_IMP.1, ADV_LLD.1, ALC.TAT.1)

Ministère de l'Economie, des Finances et de l'Industrie

72

PP Firewalls



PP/9904: Firewall à exigences réduites

EAL4+ (ADV_IMP.2, AVA_CCA.1, AVA_VLA.3)
DGA

PP/9905: Firewall à exigences élevées

EAL5+ (ALC_FLR.2, AVA_VLA.4)
DGA

PP/9906: Passerelle filtrante de sécurité configurable

EAL5
DGA

73

PP Infrastructure de Gestion de Clés

Ressource cryptographique

PPnc/0003: Ressource cryptographique pour une infrastructure de gestion des clés

EAL 5+ (AVA_VLA.4, AVA_CCA.3)
SCSSI

Infrastructure de gestion de clés

PPnc/0004: Infrastructure de gestion de clés

EAL 3+ (ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_VLA.3)
SCSSI

Autorité d'enregistrement

PPnc/0005: Autorité d'enregistrement

EAL 3+ (AVA_VLA.3, ADV_IMP.1, ADV_LLD.1, ADV_SPM.1, ALC_TAT.1)
SCSSI

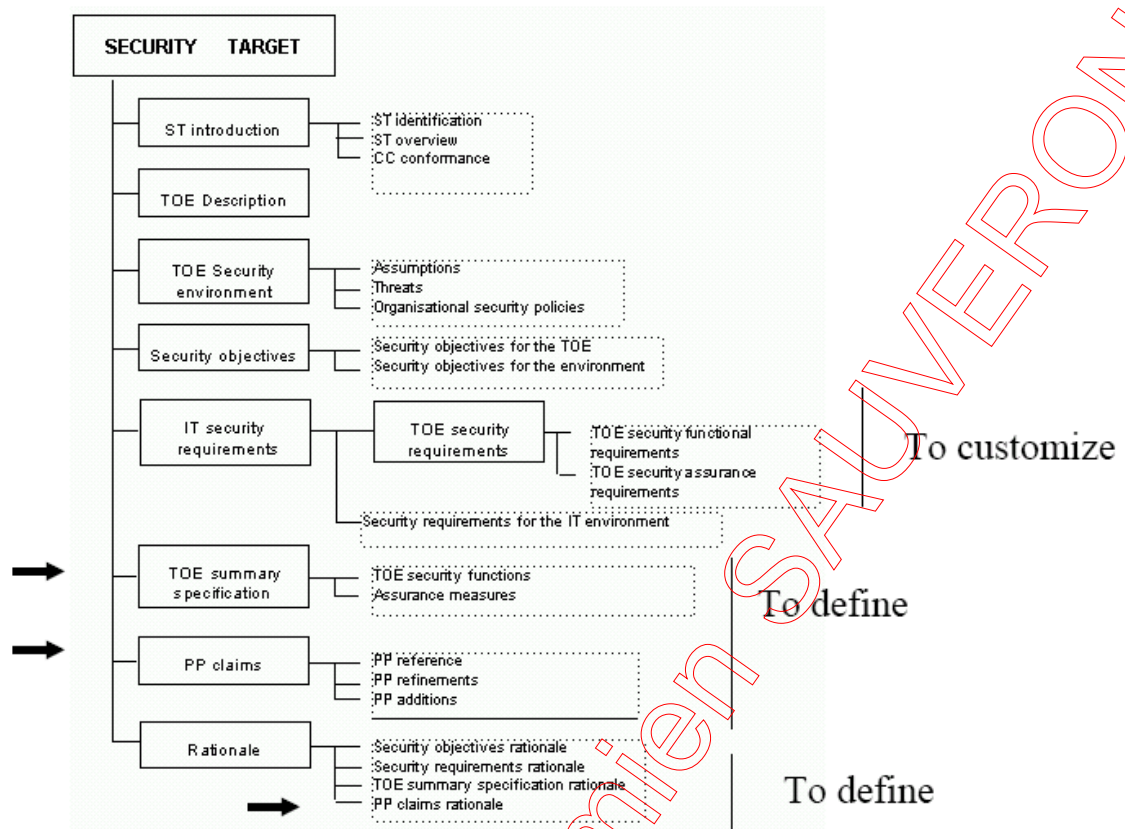
Autorité de certification

PPnc/0006: Autorité de certification

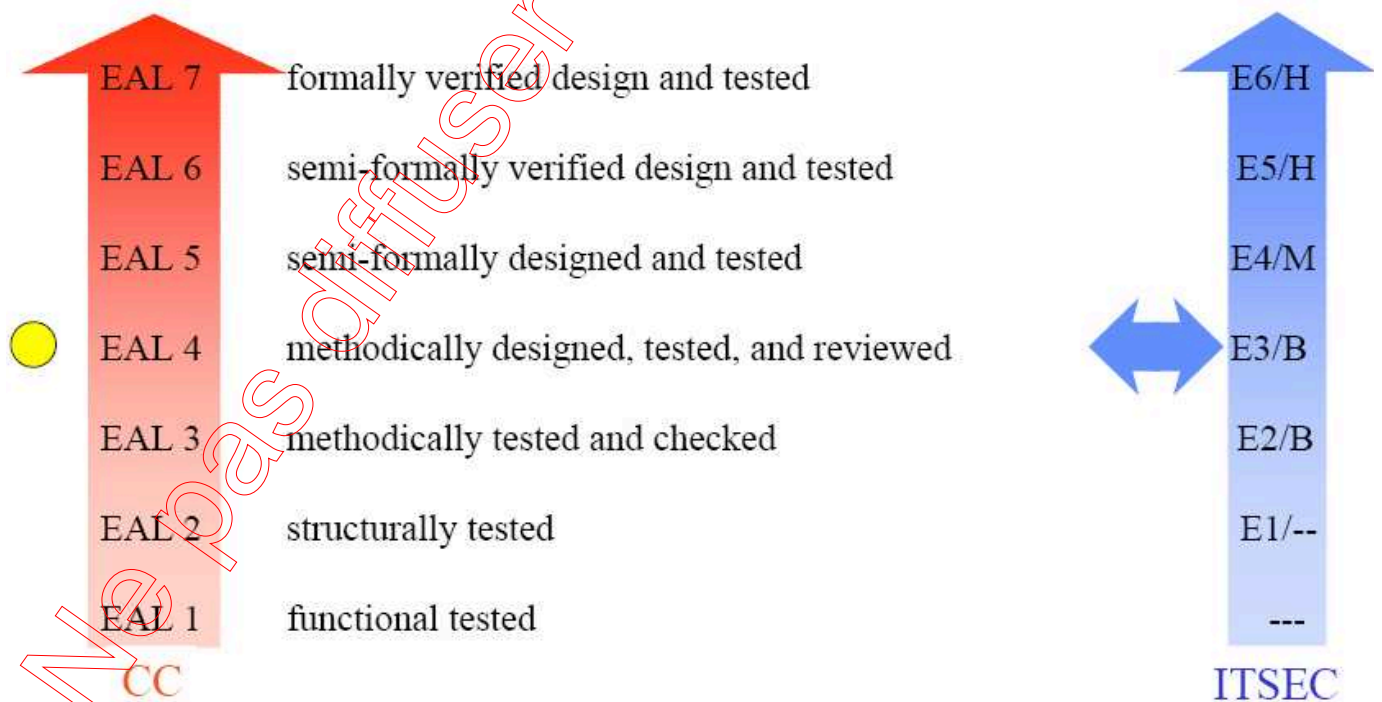
EAL 3+ (AVA_VLA.3, ADV_IMP.1, ADV_LLD.1, ADV_SPM.1, ALC_TAT.1)
SCSSI

74

Security Target

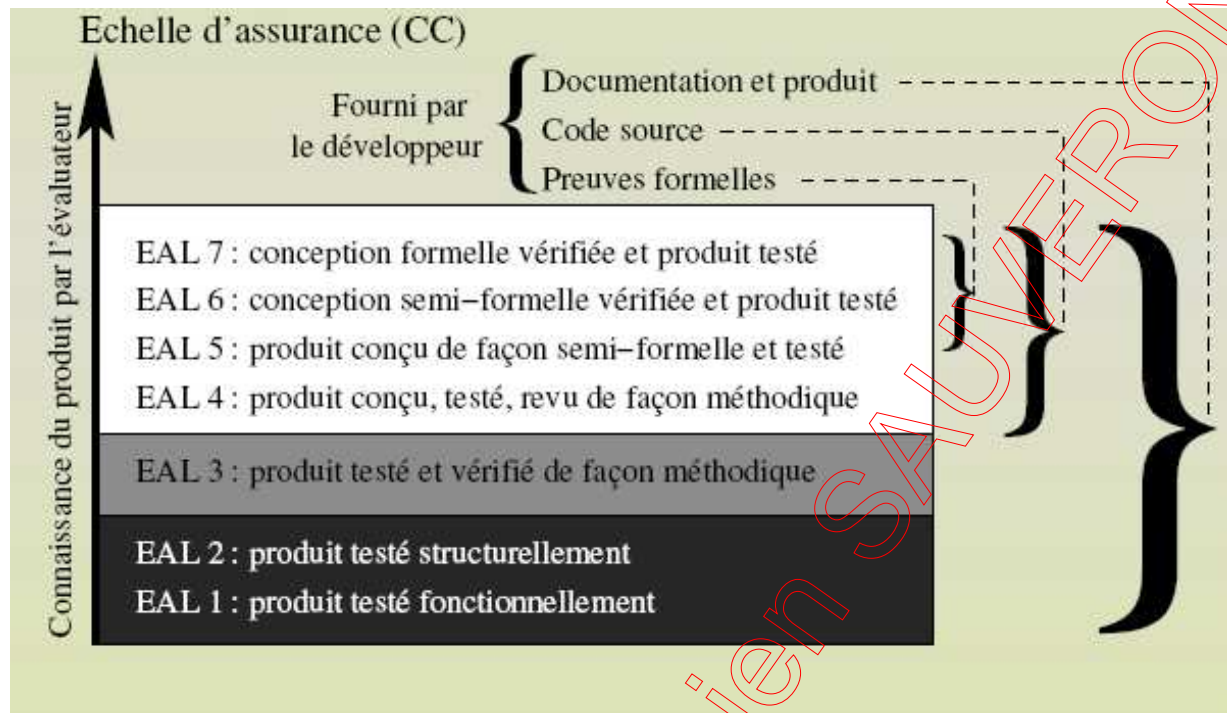


75



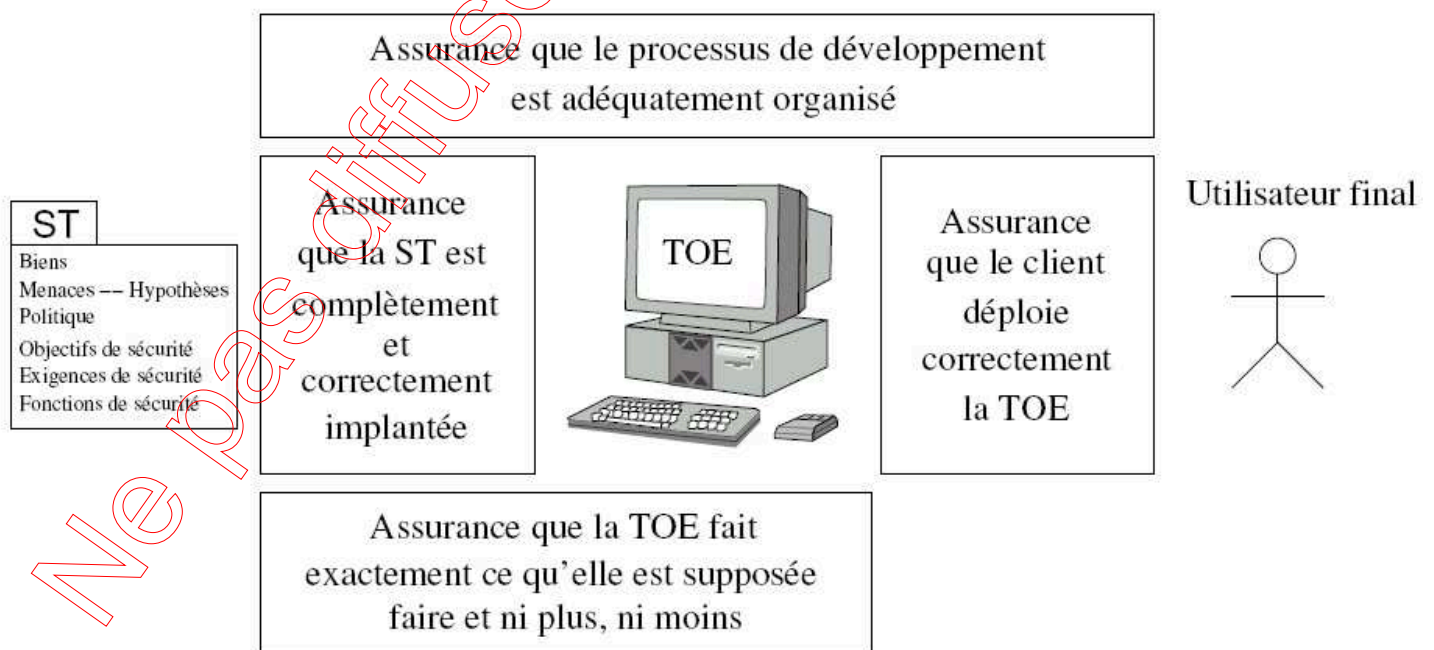
76

L'échelle d'assurance



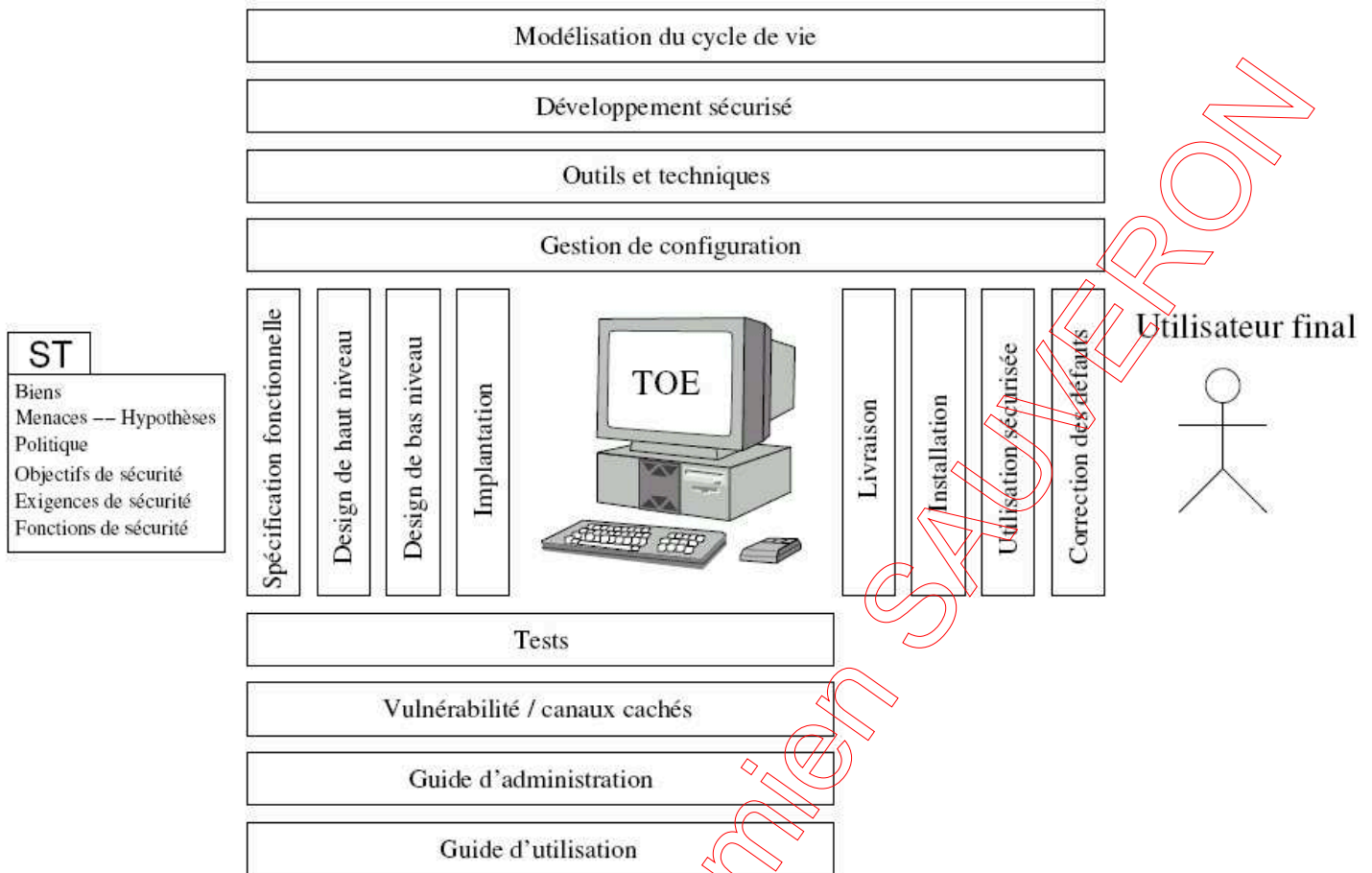
77

L'assurance des Critères Communs



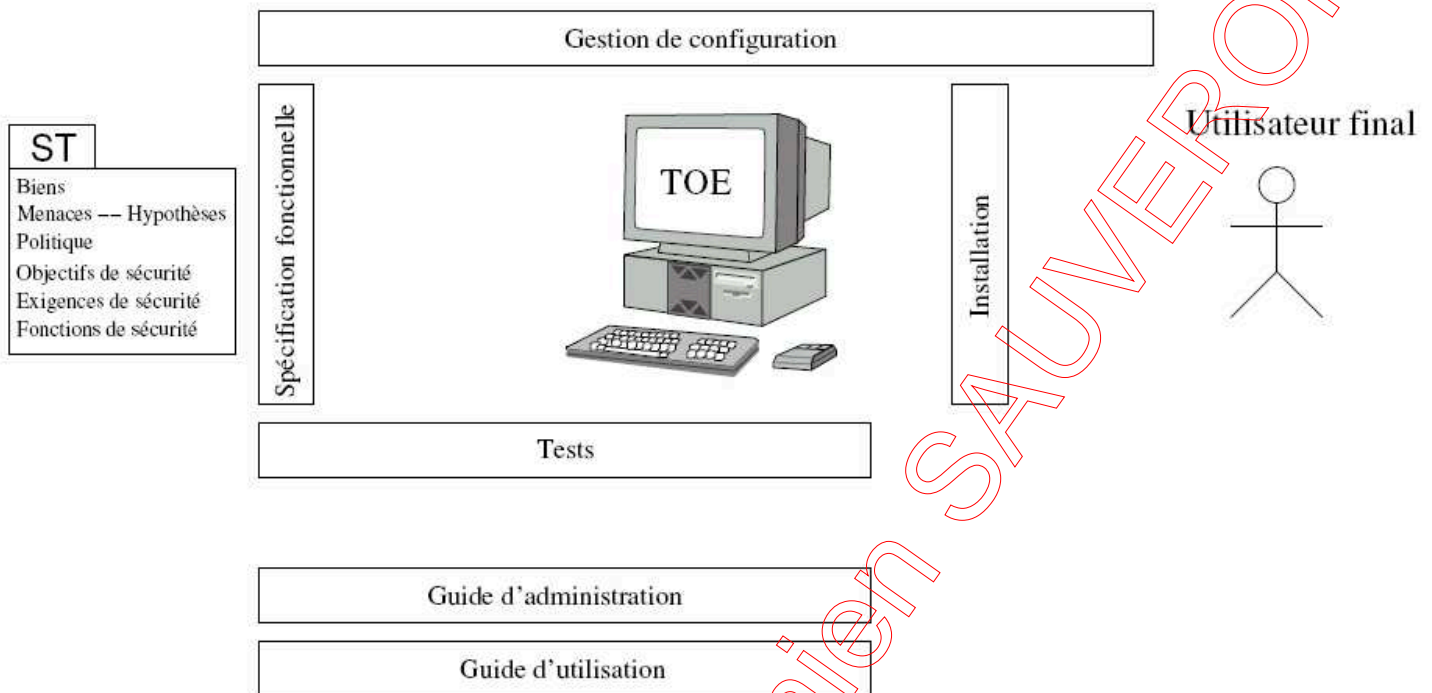
78

Les exigences d'assurance des Critères Communs



Evaluation Assurance level summary

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT	1	2	3	4	5	6	7
	ACM_CAP	1	2	3	4	5	6	7
	ACM_SCP	1	2	3	4	5	6	7
Delivery and operations	ADO_DEL	1	2	3	4	5	6	7
	ADO_IGS	1	2	3	4	5	6	7
	ADV_FSP	1	2	3	4	5	6	7
Development	ADV_HLD	1	2	3	4	5	6	7
	ADV_IMP	1	2	3	4	5	6	7
	ADV_INT	1	2	3	4	5	6	7
	ADV_LLD	1	2	3	4	5	6	7
	ADV_RCR	1	2	3	4	5	6	7
Guidance documents	AGD_ADM	1	2	3	4	5	6	7
	AGD_USR	1	2	3	4	5	6	7
	ALC_DVS	1	2	3	4	5	6	7
Life cycle support	ALC_FLR	1	2	3	4	5	6	7
	ALC_LCD	1	2	3	4	5	6	7
	ALC_TAT	1	2	3	4	5	6	7
Tests	ATE_COV	1	2	3	4	5	6	7
	ATE_DPT	1	2	3	4	5	6	7
	ATE_FUN	1	2	3	4	5	6	7
	ATE_IND	1	2	3	4	5	6	7
Vulnerability assessment	AVA_CCA	1	2	3	4	5	6	7
	AVA_MSUS	1	2	3	4	5	6	7
	AVA_SOP	1	2	3	4	5	6	7
	AVA_VLAS	1	2	3	4	5	6	7



81

EAL 1

- *Could be used for an evaluation without the developer*

- TOE security functions analysis
- TOE functional specifications and interfaces
- Security functions independent testing

EAL 2

- *Low-level independent evaluation*

- TOE security functions analysis
- TOE functional specification and interfaces
- TOE sub-systems high-level design
- Review of security functions black-box tests done by the developer
- Obvious vulnerability assessment

82

- **Moderate level evaluation**

- Grey-box testings
- Independent confirmation of a selected sample of developer tests results
- Search for vulnerabilities justified by the developer
- Development environment control
- TOE configuration management

- **Complete white-box evaluation**

- TOE modules low-level design
- Subset of implementation representation
- Independent search for vulnerabilities
- Conformance of Development process against a life-cycle model
- Tools identification
- Automated configuration management

- *High level of assurance obtained through a rigorous method of development*

- All implementation analyses
- Formal model and semi-formal presentation of functional specification and high-level design
- Semi-formal Demonstration of correspondence
- Modular design
- Search for vulnerabilities and resistance to moderate potential attacks
- Covert-channel analysis

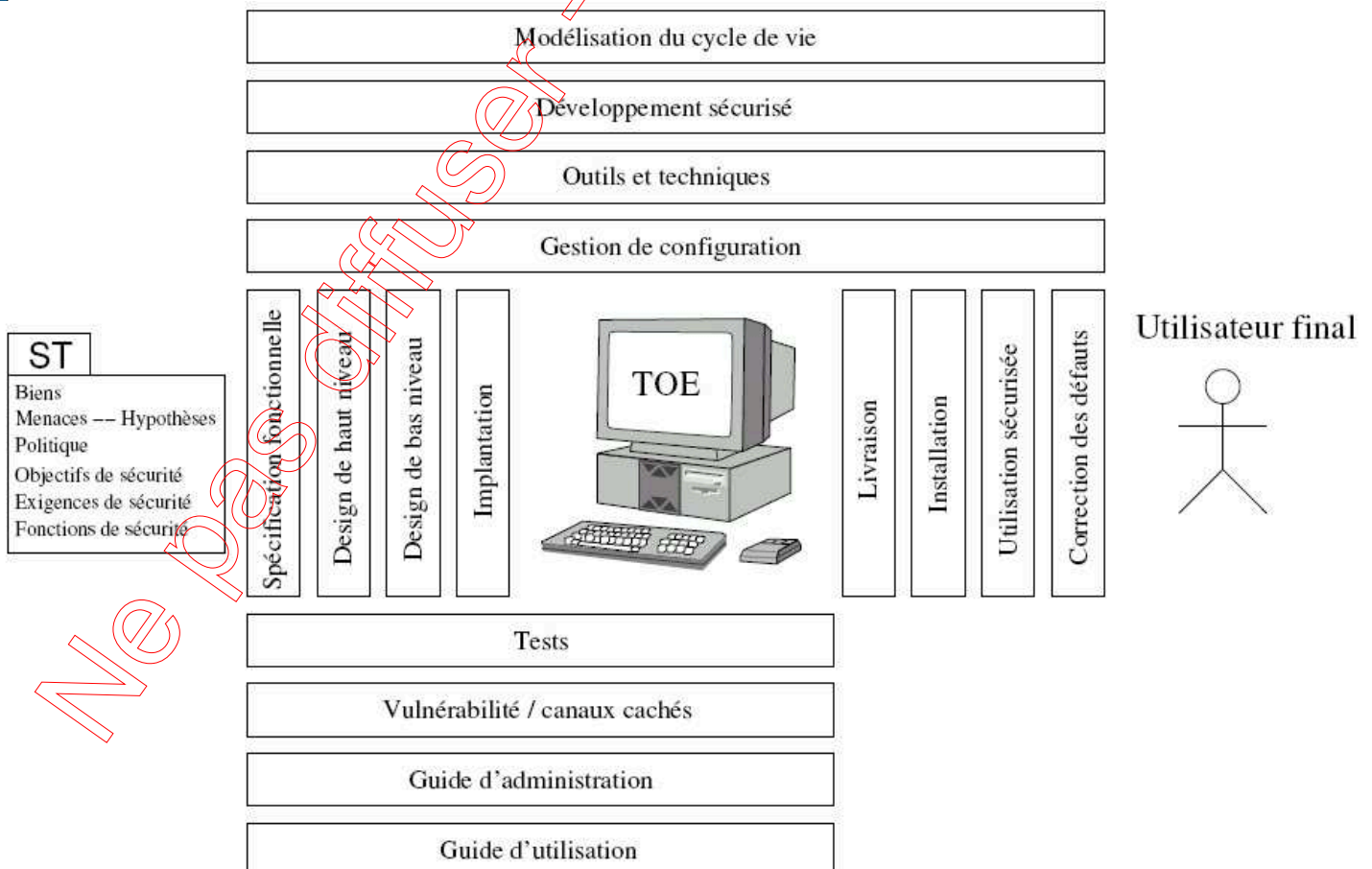
- *High-level of risks product evaluation*

- Modular design and design by successive refinements
- Structured implementation of the TSF
- High-controlled development environment and advanced configuration management
- Systematic search for vulnerabilities and resistance to high potential attacks

● **Very-high level of risks product evaluation**

- Formal presentation of functional specification and high level design
- White-box developer Comprehensive testing
- Complete and independent confirmation of developer tests results
- Minimisation of design complexity

Les exigences d'assurance des Critères Communs pour le niveau EAL7

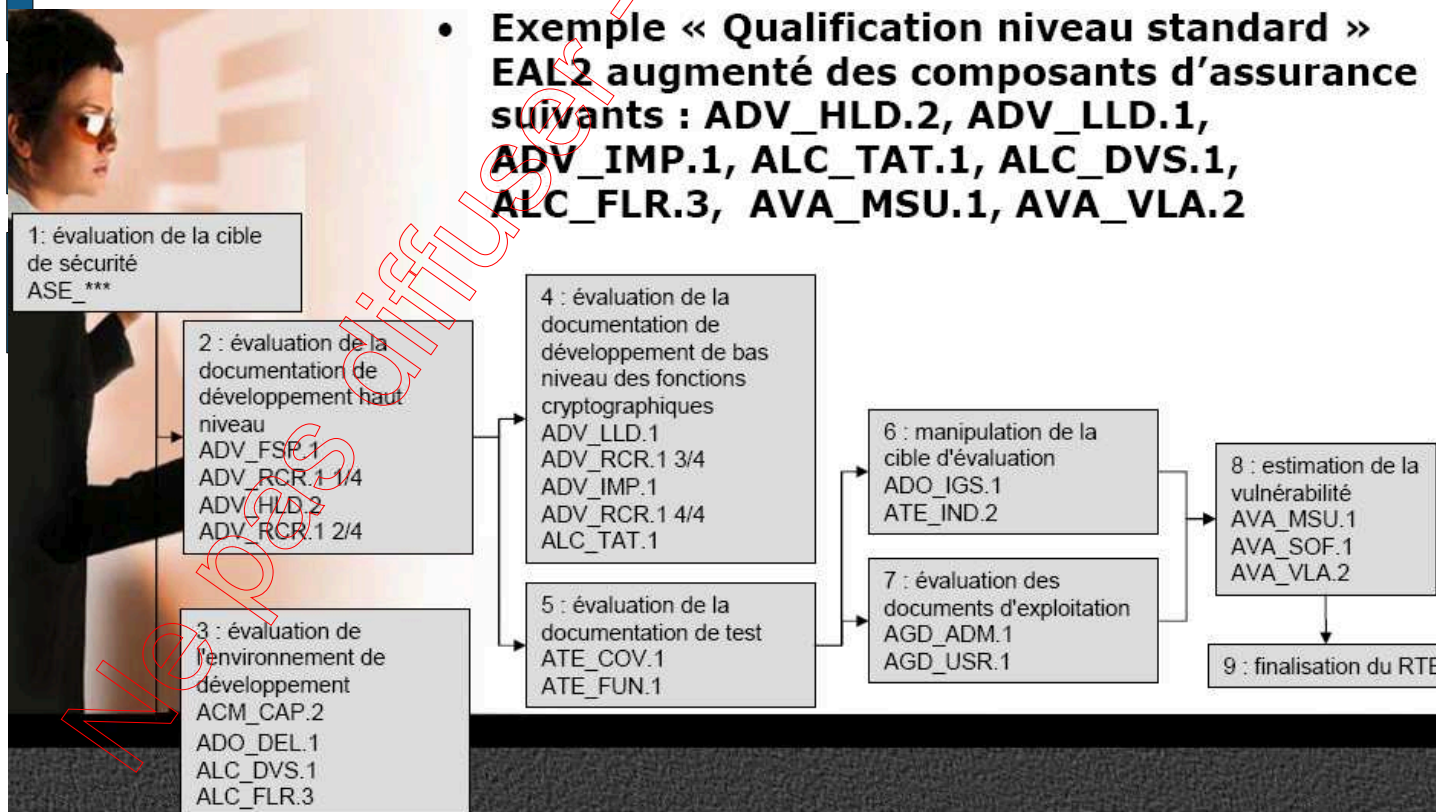


Les niveaux de confiance

Classe d'assurance	Famille d'assurance	Composants d'assurance par niveau d'assurance de l'évaluation							niveau retenu pour le paquet EAL2+ de qualification au niveau
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	
Gestion de configuration	ACM AUT				1	1	2	2	
	ACM CAP	1	2	3	4	4	5	5	2
	ACM SCP			1	2	3	3	3	
	ADO DEL		1	1	2	2	2	3	1
Livraison et exploitation	ADO_IGS	1	1	1	1	1	1	1	1
	ADV_FSP	1	1	1	2	3	3	4	1
Développement	ADV_HLD		1	2	2	3	4	5	2
	ADV_IMP				1	2	3	3	1
	ADV_INT					1	2	3	
	ADV_LLD				1	1	2	2	1
	ADV_RCR	1	1	1	1	2	2	3	1
	ADV_SPM				1	3	3	3	
	AGD_ADM	1	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2	1
	ALC_FLR								3
Support au Cycle de vie	ALC_LCD				1	2	2	3	
	ALC_TAT				1	2	3	3	1
	ATE_COV		1	2	2	2	3	3	1
	ATE_DPT			1	1	2	2	3	
Tests	ATE_FUN		1	1	1	1	2	2	1
	ATE_IND	1	2	2	2	2	2	3	2
	AVA_CCA					1	2	2	
	AVA_MSU			1	2	2	3	3	1
Estimation des vulnérabilités	AVA_SOF		1	1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4	2

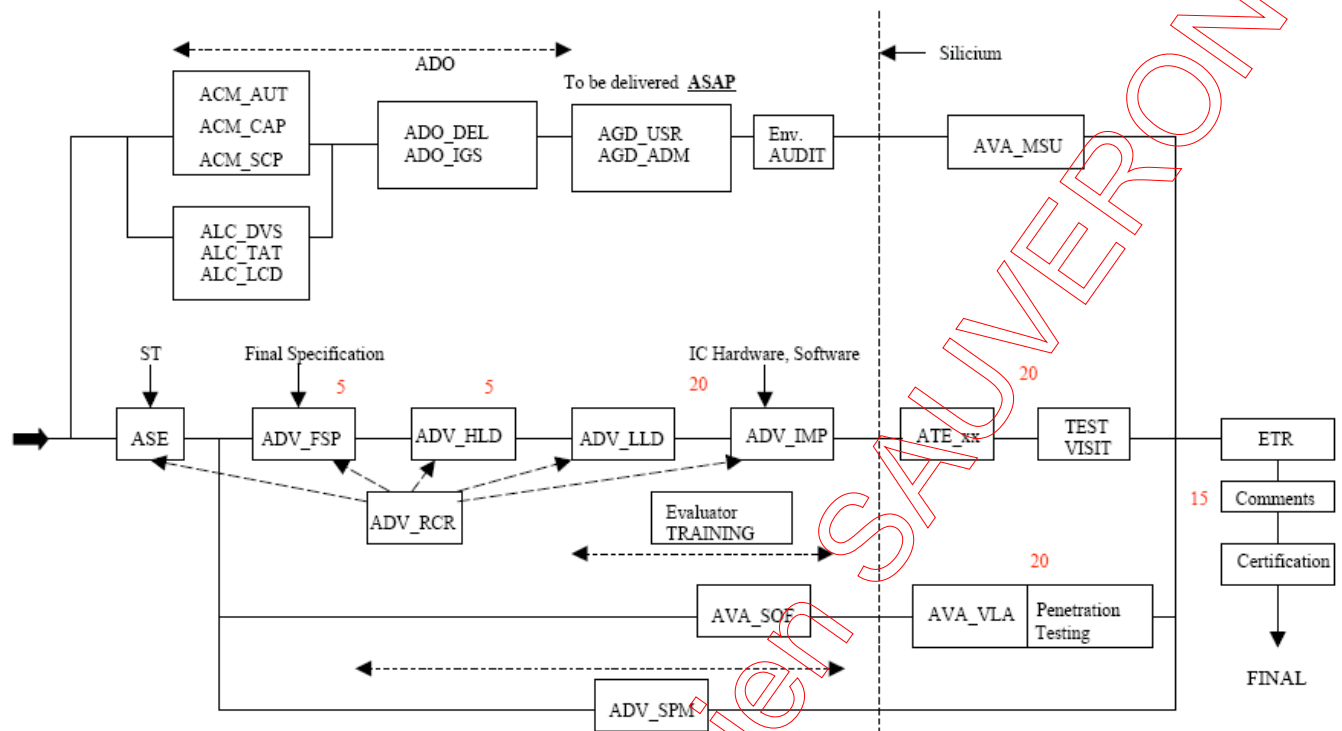
89

- Exemple « Qualification niveau standard »
EAL2 augmenté des composants d'assurance suivants : ADV_HLD.2, ADV_LLD.1, ADV_IMP.1, ALC_TAT.1, ALC_DVS.1, ALC_FLR.3, AVA_MSU.1, AVA_VLA.2



90

Evaluation Flow



91

ON SWAPPE SUR MERLE.PDF p24

92