

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 6172 CNRS -- Université de Limoges
123 avenue Albert Thomas
87060 Limoges Cedex, FRANCE

Email: Damien.Sauveron@unilim.fr
Web: <http://damien.sauveron.fr/>
Phone: +33 (0) 5 87 50 67 93

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 ?

Qu'est ce que la sécurité ?

- Comme vous venez de le voir définir la sécurité n'est pas aussi simple qu'on le pense
- L'**approche la plus courante** concernant la sécurité informatique se résume sous le terme **CIA**
Confidentialité (Confidentiality)
Intégrité (Integrity)
Disponibilité (Availability)
- Pour d'autres types de sécurité (des personnes par exemple), nous devons la définir en relation avec les risques

Confidentialité

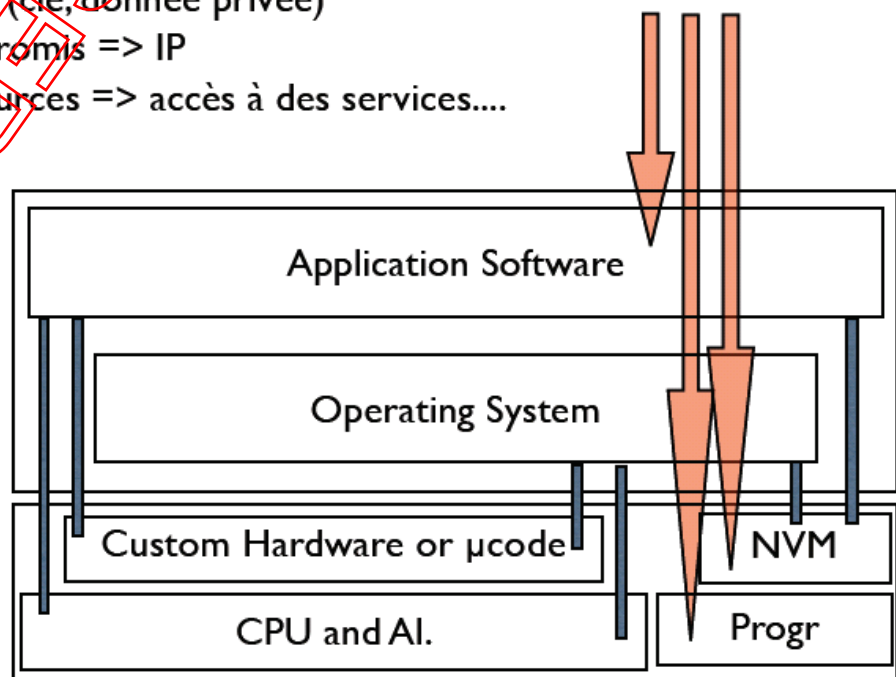
- La confidentialité consiste à empêcher **des utilisateurs non autorisés de lire** des informations pour lesquelles ils n'ont pas le droit.
- C'est en quelque sorte la propriété de « secret » attachée aux informations
- Traditionnellement, pour la plupart des gens la sécurité est assimilé à la confidentialité

Confidentialité

- Comment peut on assurer cette propriété ?
 - par **chiffrement** (mécanisme cryptographique) pour assurer la confidentialité lors de transmission d'information, i.e. pour les communications, mais aussi pour le stockage
 - par **l'utilisation de contrôle d'accès**
 - Pour un SEM, on peut utiliser des contrôles d'accès aux informations ou aux ressources (problème de granularité des droits d'accès)
 - Contrôle d'accès au SEM
 - Contrôle d'accès aux ressources internes au SEM
 - Contrôle d'accès logique à l'intérieur du SEM
- Attention : Il existe une propriété proche de la confidentialité qui est **l'anonymat**. Elle consiste à assurer la confidentialité d'une donnée bien particulière : l'**identité** (on peut la voir comme un sous ensemble)

La confidentialité

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



Intégrité

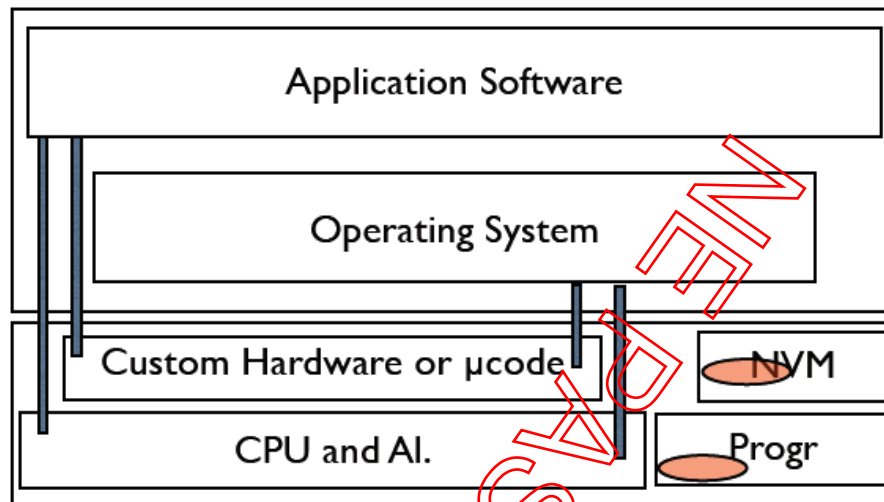
- L'intégrité consiste à s'assurer que les choses seront faites comme elles devraient l'être
- Dans le *contexte de l'informatique*, l'intégrité consiste à empêcher des utilisateurs **non autorisés d'écrire** des informations pour lesquelles ils n'ont pas le droit.
- Dans un *contexte général*, l'intégrité consiste à s'assurer que l'état d'un système n'a pas été modifié par des personnes qui n'ont pas le droit de le faire.

Intégrité

- Dans le ~~contexte des communications de données~~ l'intégrité se restreint souvent à détecter les modifications de ces informations.
Une propriété proche consiste à identifier de qui l'information provient.
C'est l'**authentification** des données (peut être vu comme une généralisation de l'authentification d'entité qui porte sur l'authentification d'une donnée bien particulière : l'identité)
- Comment peut on assurer cette propriété ?
 - Par du contrôle d'accès
 - Par des mécanismes de MAC ou de signature numérique (cryptographie asymétrique)
 - Par des mécanismes de CRC ou Checksum (somme de contrôle) ou de redondance
 - Mécanismes assurés par du matériel ou du logiciel

L'intégrité

- Données et programmes changés



11

Intégrité

- Informations concernées par l'intégrité :
 - Les données
 - Les programmes (i.e. le code)
 - Peut avoir un impact sur les données des applications, sur les données du système lui-même (autorisation de nouveau service, modification de table d'accès, etc.)
 - L'altération peut être volontaire (e.g. une attaque) mais également le fruit d'une erreur de programmation (i.e. bug)
- L'exécution d'un programme ? **Comment garantir cela ?**

Disponibilité

- La disponibilité est la propriété d'un système d'être accessible à la demande par un utilisateur autorisé à y accéder.
- Cette notion va bien au delà de la sécurité et concerne aussi la tolérance aux fautes.
- D'un point de vue sécurité, on s'intéresse principalement à éviter les attaques par déni de service d'utilisateurs non autorisés.
 - Par exemple, dans le cas d'un serveur web, la disponibilité sera le fait que les requêtes sont satisfaites et que l'attaque par déni de service sera sans effet.
- On peut associer à la notion de disponibilité, celle de QoS (Quality of Service – Qualité de Service). Cette propriété fonctionnelle englobe plusieurs paramètres comme par exemple la capacité à répondre dans un délai prévu.

Quelles autres propriétés ?

D'autres propriétés

- Attention, il y a d'autres propriétés de sécurité en plus de CIA.

- **Responsabilité** (Accountability)

En pratique, on ne peut pas empêcher des actions malveillantes de se produire.

=> Les utilisateurs doivent être rendus **responsables** de leurs actions, y compris les mauvais usages du système

- Cela se traduit souvent par la mise en place d'un mécanisme d'authentification puis un traçage et un enregistrement des actions ayant trait à la sécurité dans un log d'audit.

Cette notion permet de faire de l'**imputation** et de la **non répudiation**

D'autres propriétés

- En lien avec la sécurité :

Fiabilité (Reliability)

- Pour les systèmes qui doivent fonctionner correctement dans des conditions adverses, la sécurité est clairement proche de la fiabilité (reliability) et de la sûreté (safety)

Dépendabilité (Dependability)

- Terme parfois utilisé pour englober la sûreté et la fiabilité.

- Si les objectifs de la sécurité et de la dépendabilité sont proches, les méthodes utilisées pour évaluer les systèmes sont souvent similaires

Les Systèmes Embarqués et Mobiles

- Particularités des SEM

Le dispositif est entre toutes les mains

- Porte ouverte aux intrusions, ...
- En opposition à un data center qui est une unité de lieu bien délimité
Toutefois les grilles de calculs distribués ouvertes connaissent un peu la même problématique
- Dispose souvent d'une connectivité
Porte d'entrée d'une possible attaque
- Plate-forme parfois ouverte (type Java)
Facilite le time-to-market et l'écosystème mais aussi les attaques de l'intérieur

- Les menaces sont celles des systèmes informatiques classiques

Mais :

- Le **contexte d'utilisation** de l'objet peut être **spécifique**
PayTV
- Les **aspects système** peuvent être **spécifiques**
Attaques par déclenchement des chauffages en forçant la température sur les capteurs de chauffage
- Les **enjeux**
Carte bancaire = argent

Qu'est-ce
qu'on veut
sécuriser ?

RAPPEL

- Sécurité
- Dépendabilité : Fiabilité & Sureté
- Confidentialité et Anonymat
- Intégrité et « authentification »
- Disponibilité
- Responsabilité
=> Imputation/Non Répudiation

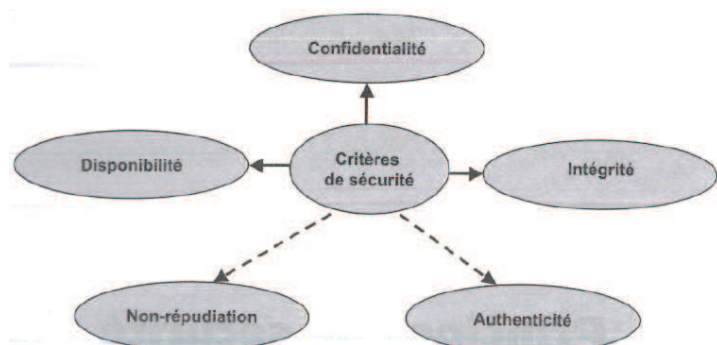
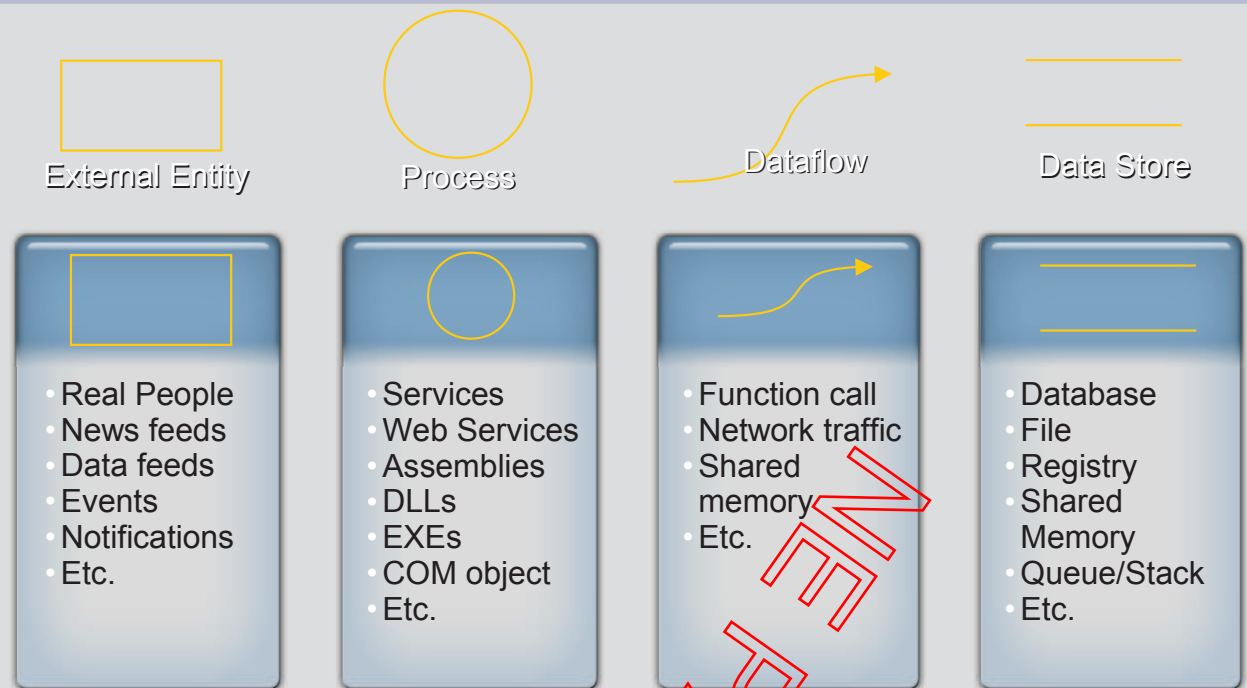


Figure 1.1 – Critères de sécurité.



Une autre définition de la sécurité

- Une autre façon de définir la sécurité, en particulier dans le cas de système non informatique, consiste à faire tout d'abord une **analyse des menaces**. La sécurité est alors définie comme la lutte contre les menaces perçues.
- Toutes les menaces ne sont pas toujours toutes intéressantes à contrer.
Il faut donc faire une analyse coût/bénéfice.
- L'**analyse de risques** consiste à évaluer l'importance de chaque menace pour décider si elle doit ou non être combattue.
En effet, il peut être moins coûteux de vivre avec certaines menaces que de les empêcher.

Intégration de la sécurité

- De façon générale, on peut se demander comment la sécurité peut être intégrée dans un système ?
- Quels sont les grands types de contrôles de sécurité et où sont-ils intégrés ?
- La sécurité intégrée dans une application peut être contournée par une attaque sur le système d'exploitation !
- La sécurité intégrée dans le système d'exploitation peut quand à elle être contournée par une attaque au niveau du matériel !
- Aussi penser l'intégration de la sécurité dans un système **depuis sa conception** est bien meilleure que l'ajouter après coup.

Quels grands types de contrôles ?

- Lorsque l'on protège des données dans un système informatique, on utilise souvent des règles sur le comportement du système :
Ces **règles** peuvent être :
 - Limiter les façons pour manipuler une donnée
 - Limiter les opérations qui peuvent être réalisées sur des données
 - Limiter les utilisateurs qui peuvent réaliser certains types d'actionsLes contrôles de sécurité peuvent cibler les données, les opérations ou les utilisateurs (ou des combinaisons).
- Les règles ne sont pas les seuls types de contrôles de sécurité
Il ne faut pas oublier la **sécurité physique**.

Localisation des contrôles

- Un système IT classique peut se modéliser comme 5 couches :
Applications/Programmes
Services : e.g. fourni par un SGBD ou un système de fichier distribué
Le système d'exploitation : gestion des fichiers, des impressions, etc.
Le noyau de l'OS (Kernel) : intermédiaire pour l'accès au processeur et à la mémoire
Le matériel : le processeur et la mémoire
- **Les contrôles de sécurité peuvent être localisés dans n'importe laquelle de ces couches.**
- Les mécanismes bas niveaux (près du matériel) seront plus génériques et orienté vers la sécurité du système alors que plus les mécanismes haut niveaux (près des applications) seront plus orientés utilisateur.

Remarque : Identification/Authentification

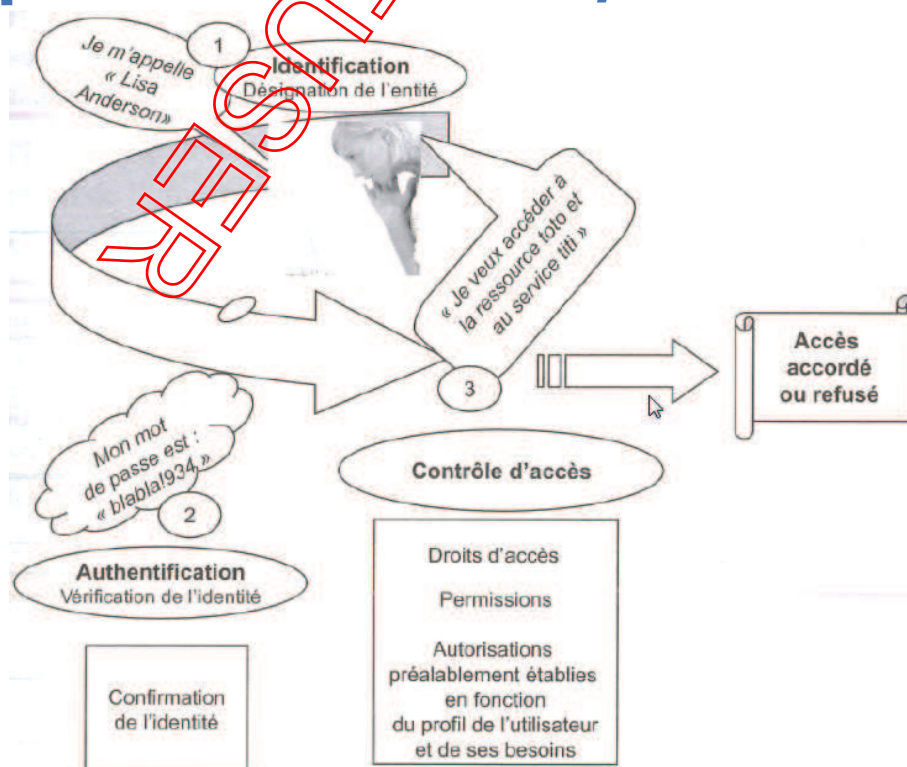
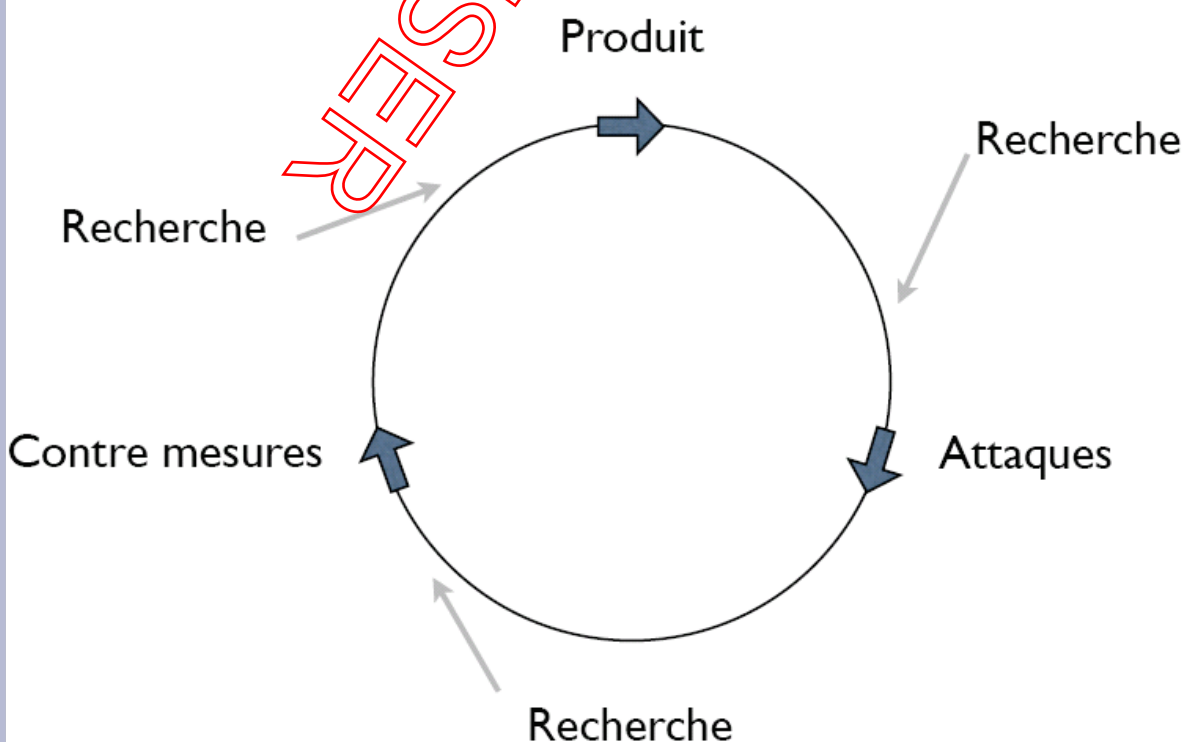


Figure 1.2 – Identification et authentification.

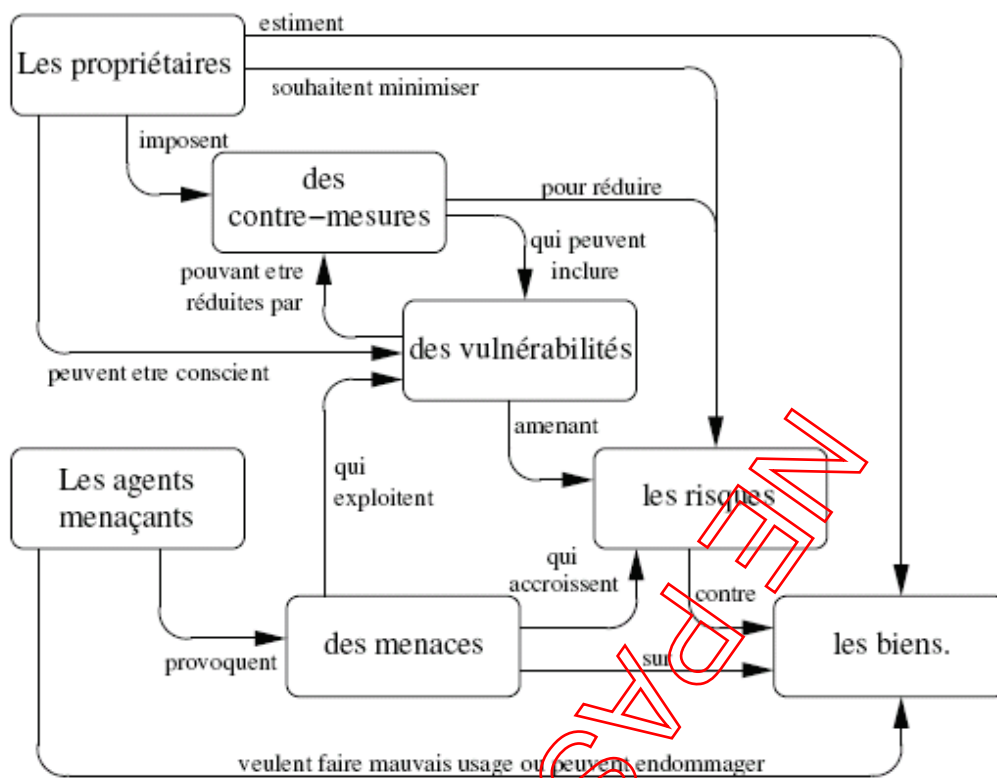
Quelques remarques

- Pour la sécurité des communications, le principal outil est la cryptographie
- Cette différence technologique est à la base du développement séparé de :
 - Comsec : Communication Security
 - Compusec : Computer Security

Un cycle infernal!

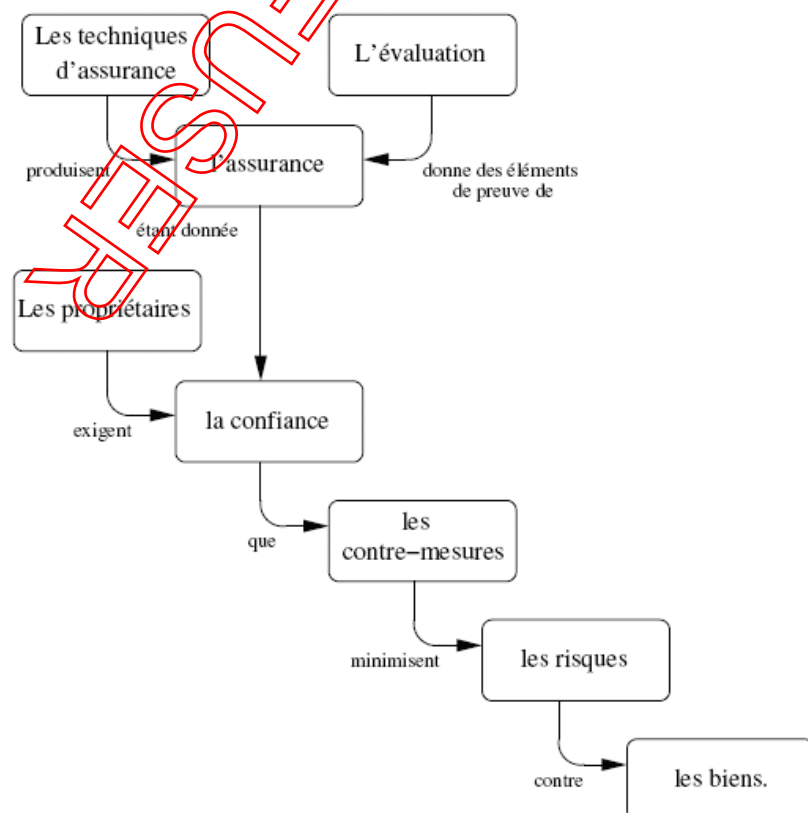


Concepts de sécurité et relations



27

Concepts de l'évaluation et relations



28

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.

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.

Normes pour l'évaluation

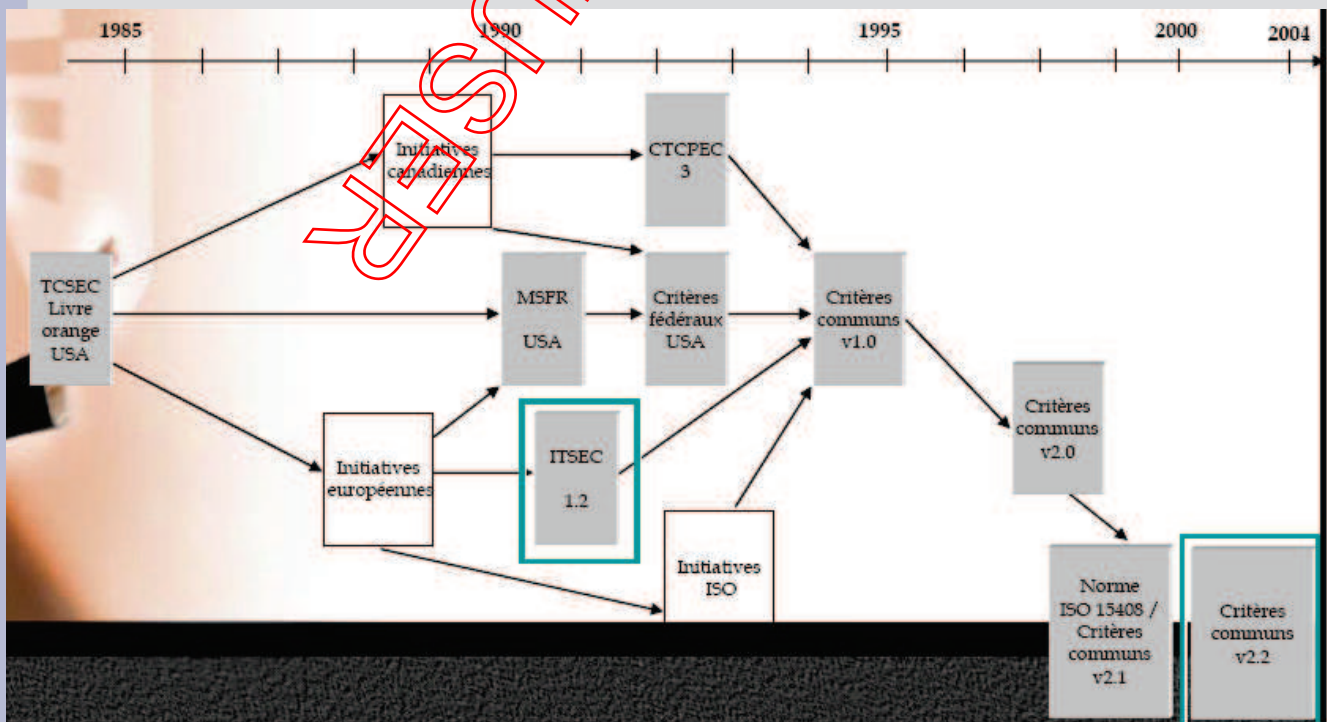
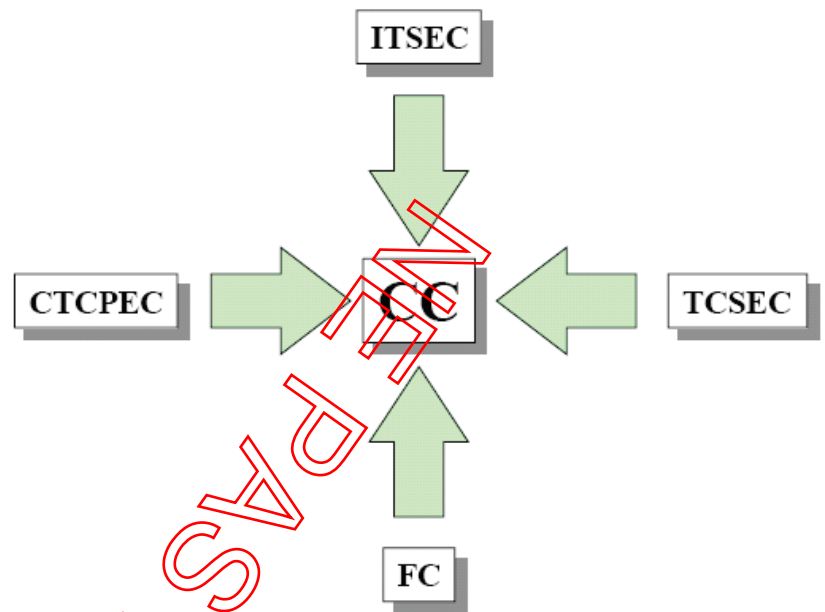
Avant l'apparition des CC, les pays utilisaient des critères d'évaluation différents :

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



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

33

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

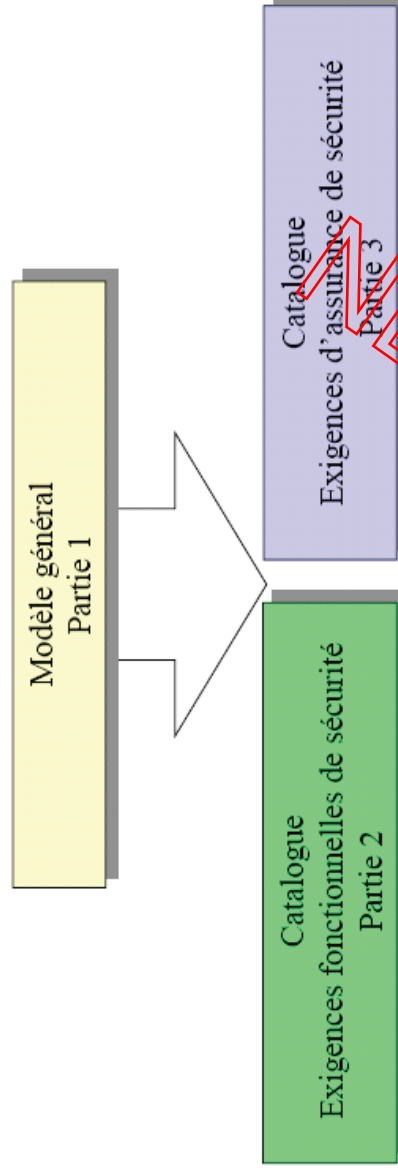
Partie 2 Exigences de sécurité fonctionnelles

ISO/IEC IS 15408-3

Partie 3 Exigences de sécurité d'assurance

34

Expression des exigences



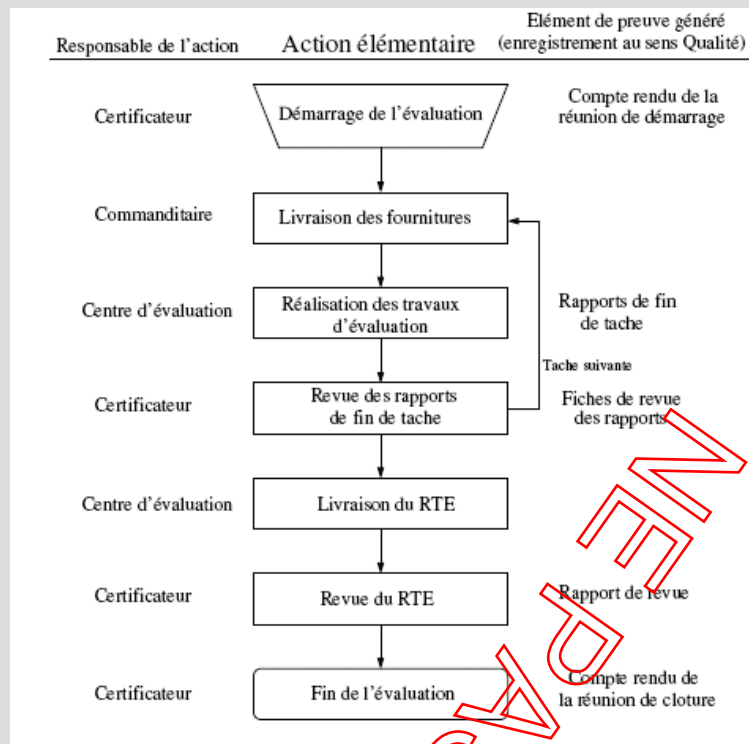
35

Public

	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.

36

Déroulement de l'évaluation



37

Evaluation Process : main steps



38

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 PPs pour l'évaluation de puce nue – i.e. sans applicatif –, pour le domaine des applications bancaires)

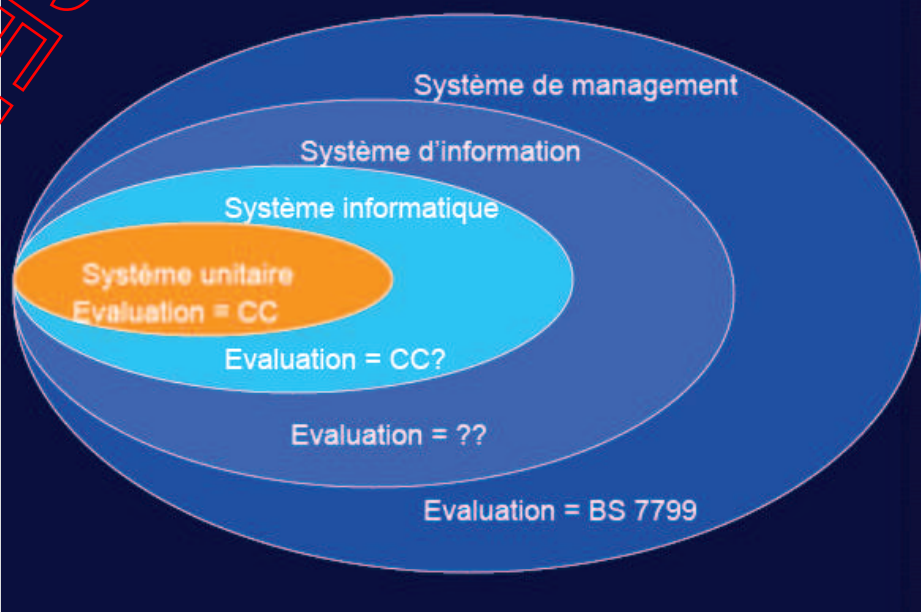
- Target of evaluation (TOE) : an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation. It defines assets to protect.
- TOE Security Functions (TSF) : A set consisting of all hardware, software, and firmware of the TOE that must be 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.

39

Périmètre

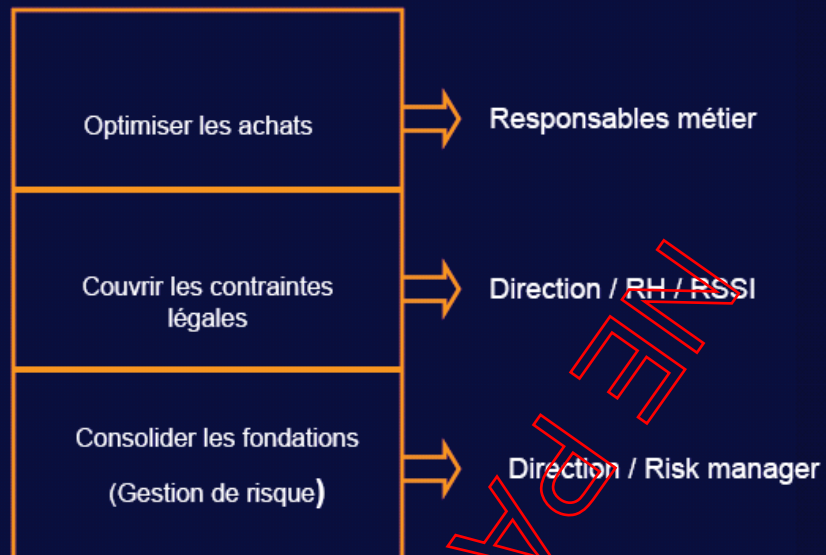
Et même un sous ensemble

Que cherche t'on à évaluer ?



40

Pourquoi une évaluation des systèmes d'information?



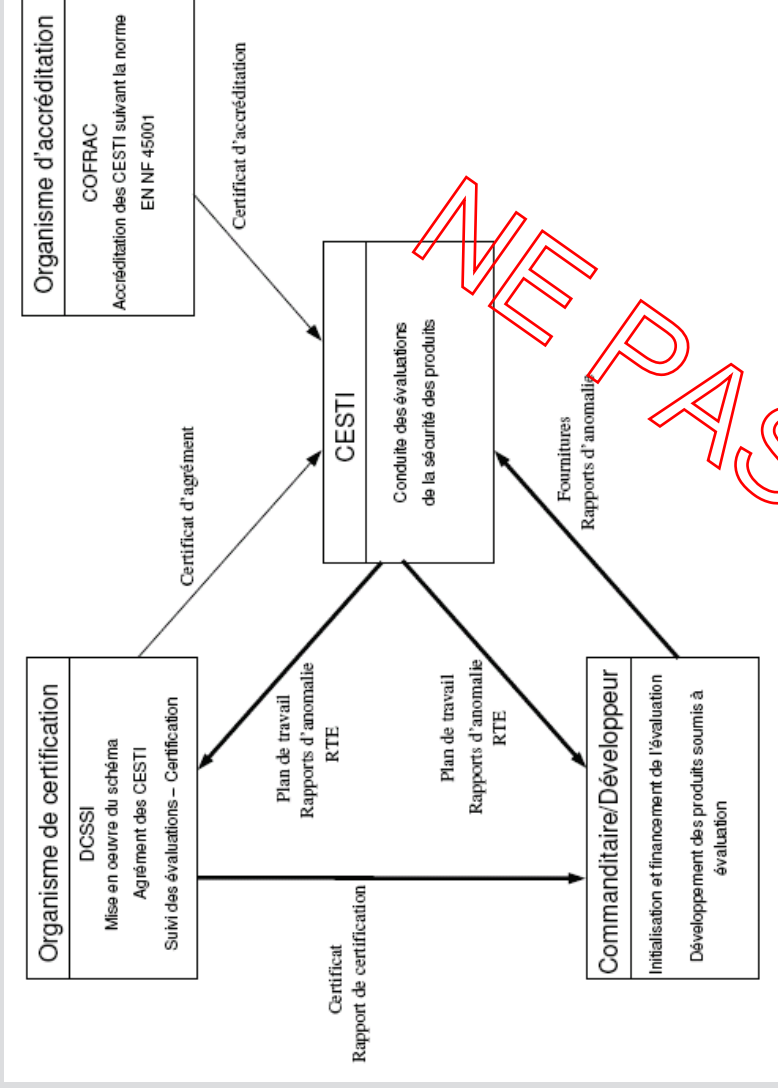
41

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)

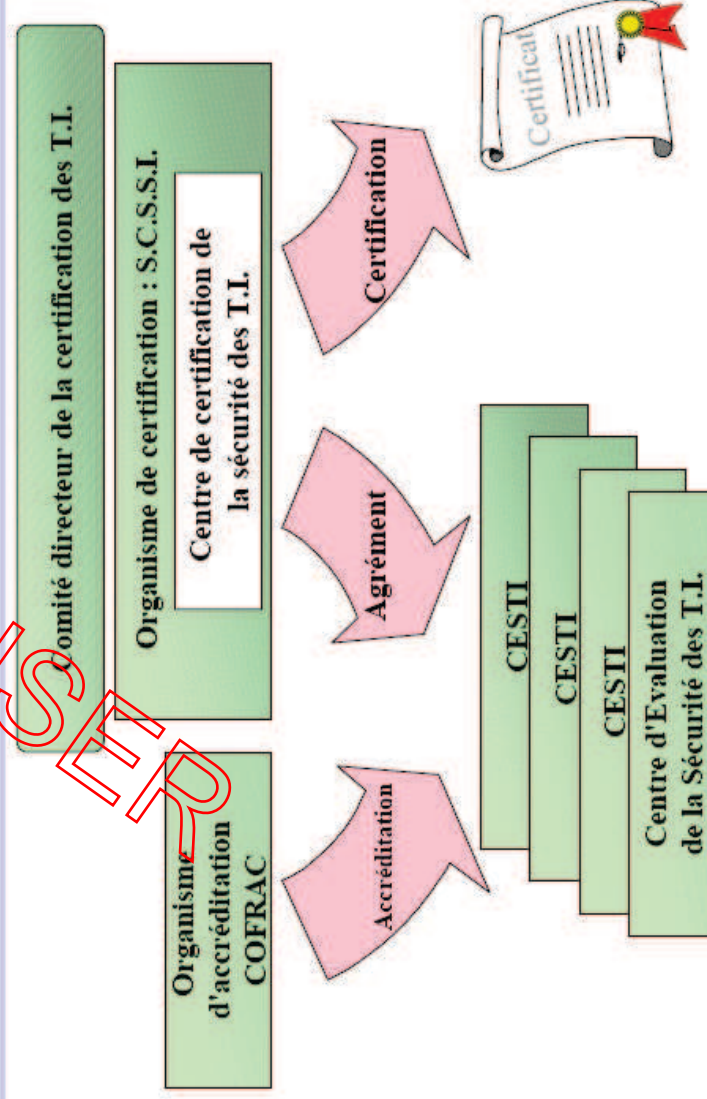
42

Le schéma Français



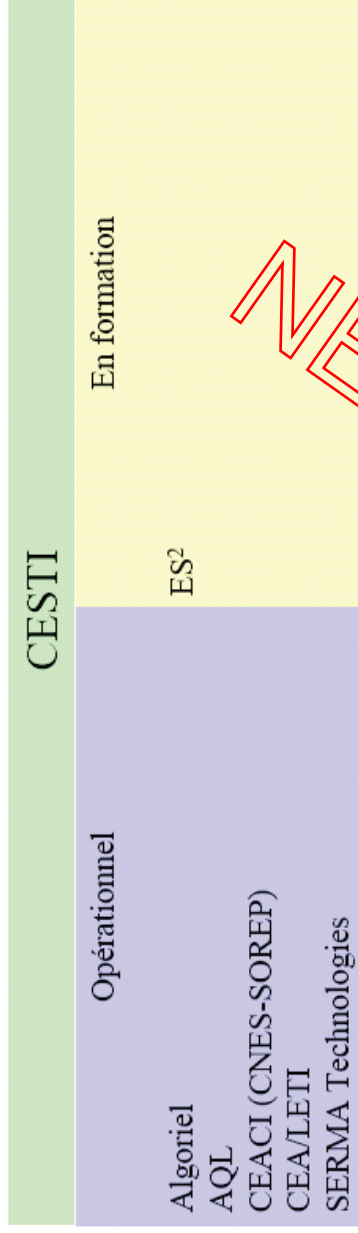
43

Organisme de certification



44

Centres d'évaluation



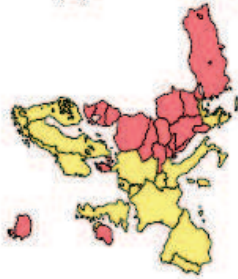
Agréés pour le domaine de la carte à puce :
 CEACI,
 CEA/LETI,
 SERMA Technologies.

Un environnement international...

Organismes de certification:

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

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



47

Reconnaissance mutuelle



Mai 2000

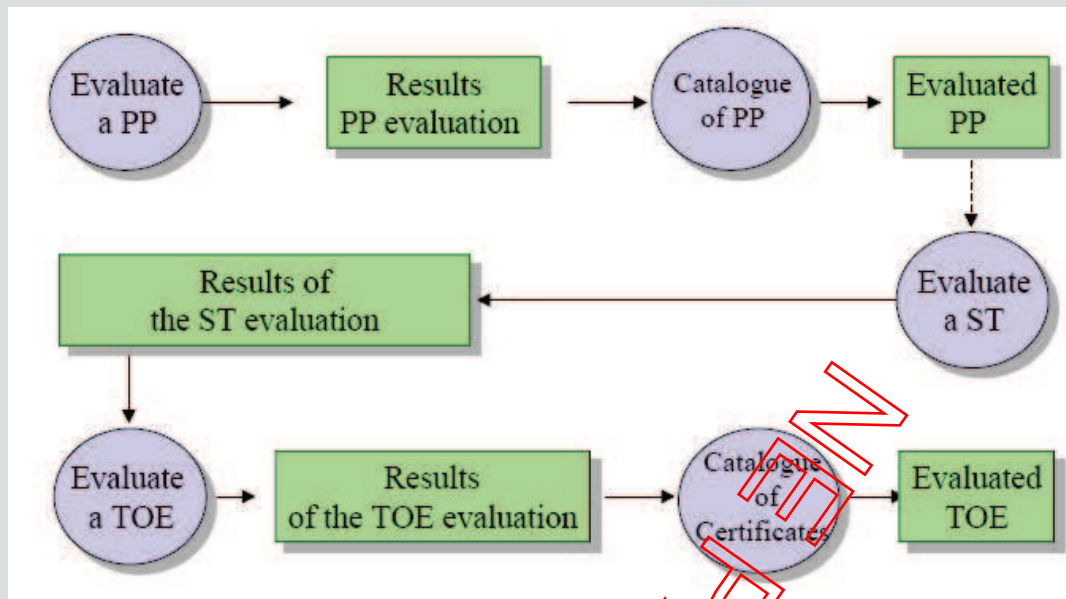
Arrangement harmonisé

- 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 CESC (Royaume Uni)
- Organismes de certification commerciaux
- Certificat CC EAL1 à EAL4



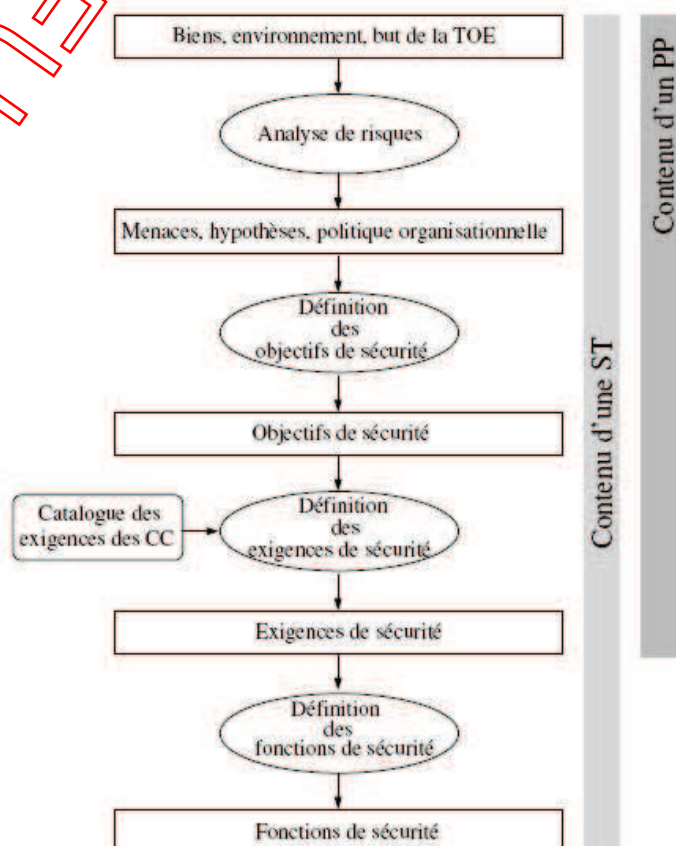
48

CC evaluations and their results

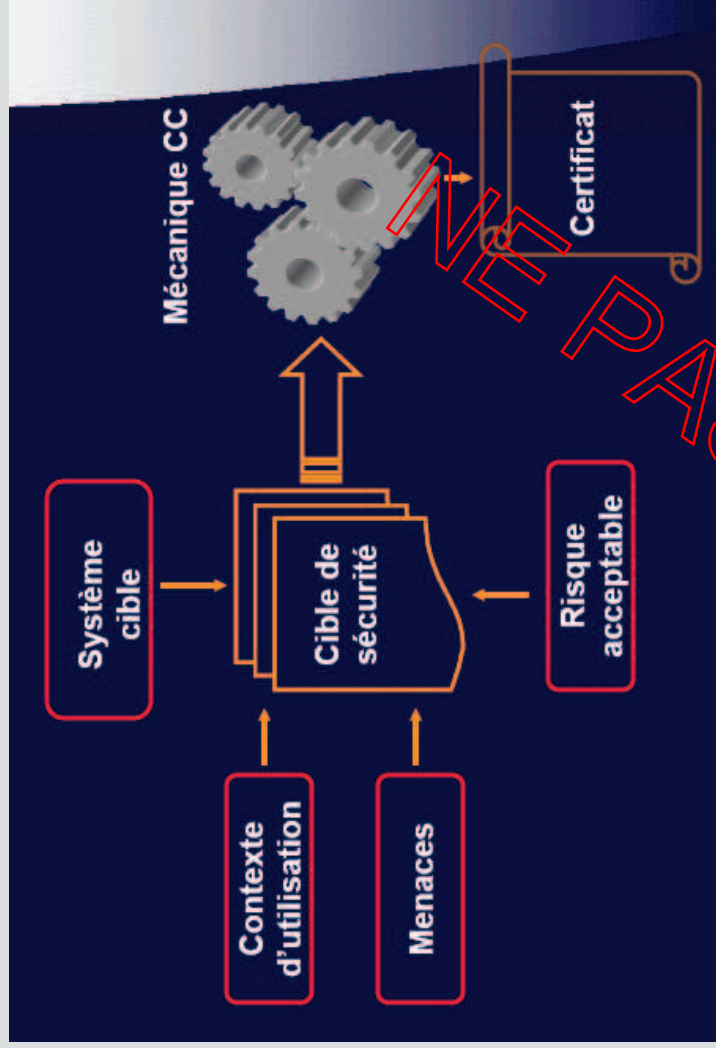


49

Contenu d'une ST et d'un PP



50



51

Un certificat

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



52

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

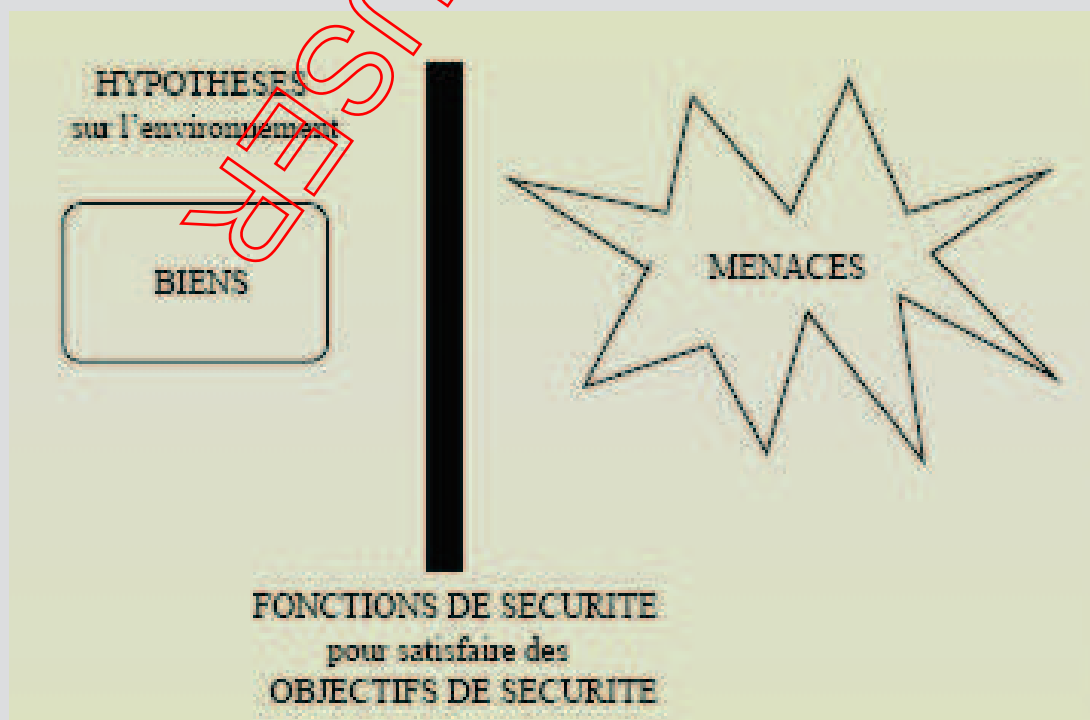
⊕ Caractéristiques du projet

- Durée : 7 mois
- Coût : 200K€

53

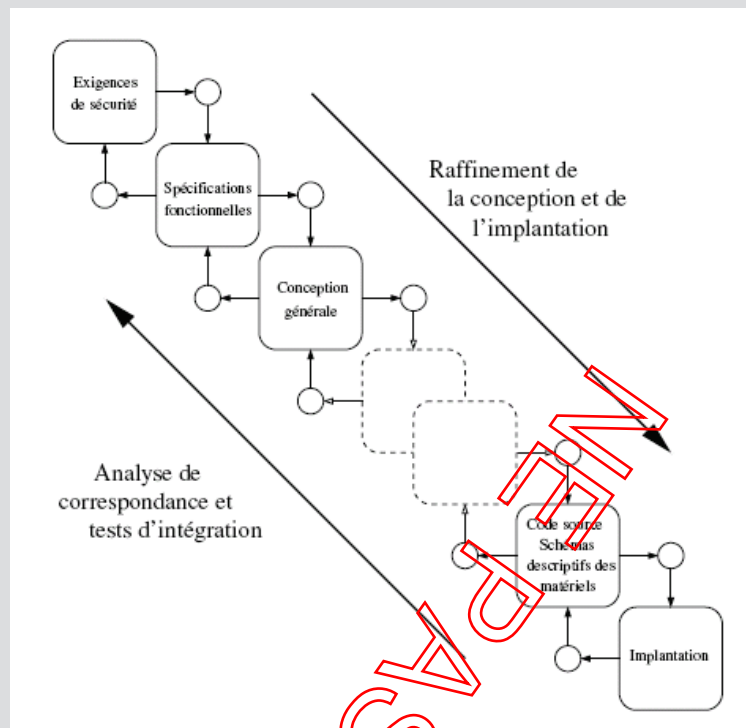
Les bases des critères communs

Critères Communs (ISO15408)



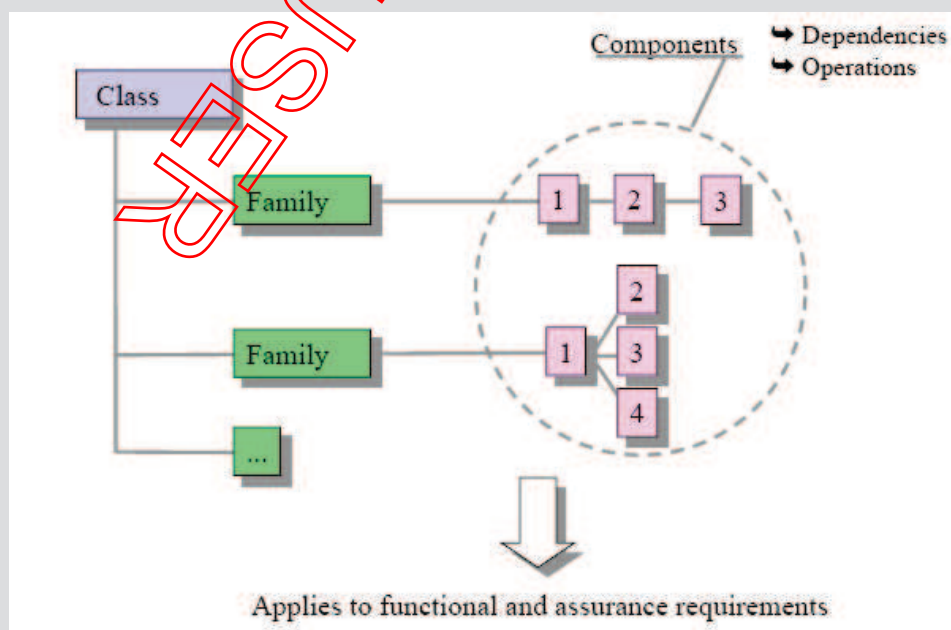
54

Modèle de développement d'une TOE



55

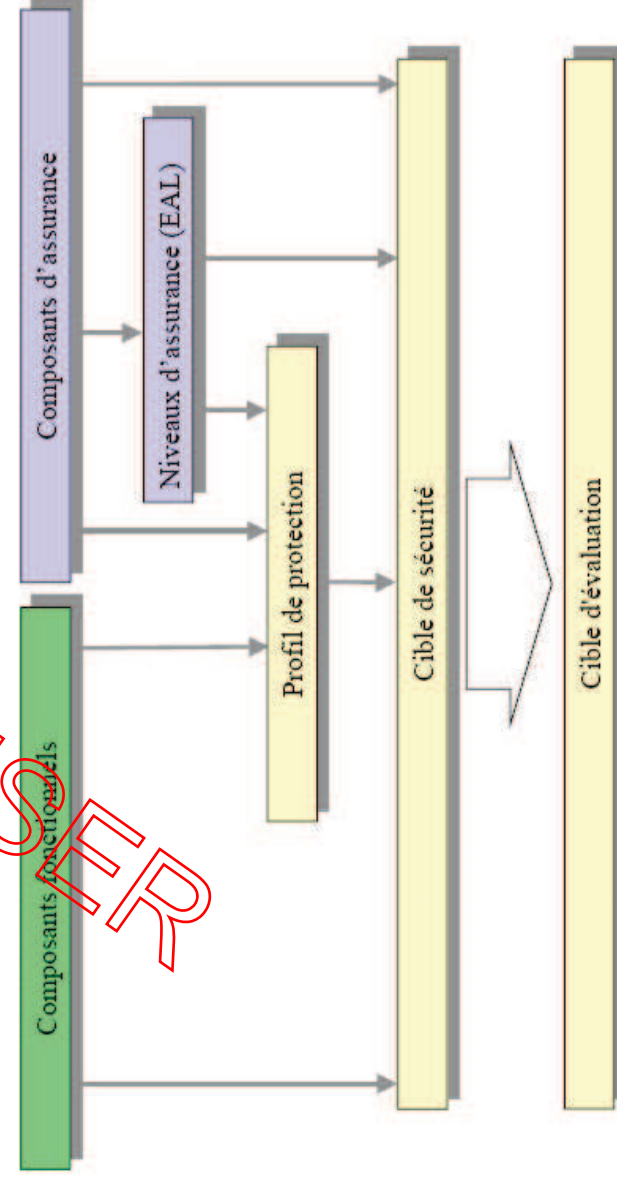
Requirements : hierarchical structure

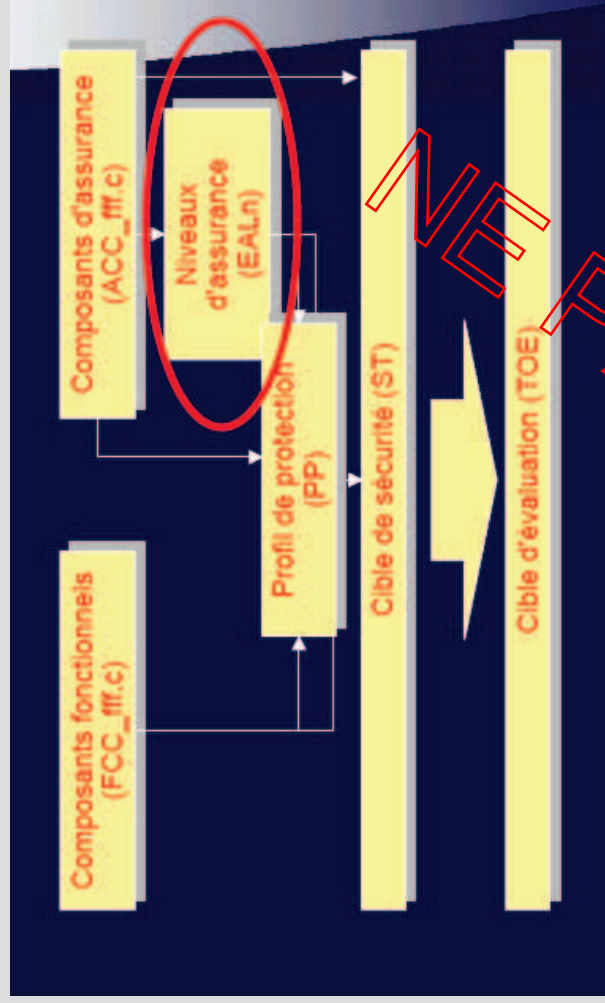


56

- **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.

Utilisation des catalogues





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 sécurités : doivent couvrir tous les objectifs
 - Référence à une cible type : le Profil de Protection (PP)