

# Certification et Développement Sécurisé

Damien Sauveron  
[damien.sauveron@unilim.fr](mailto:damien.sauveron@unilim.fr)  
<http://damien.sauveron.fr/>

(et tous les auteurs cités en bibliographie)

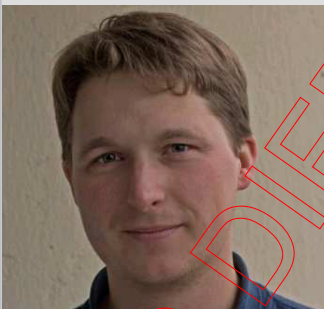
1

## 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](mailto: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.

## 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)**

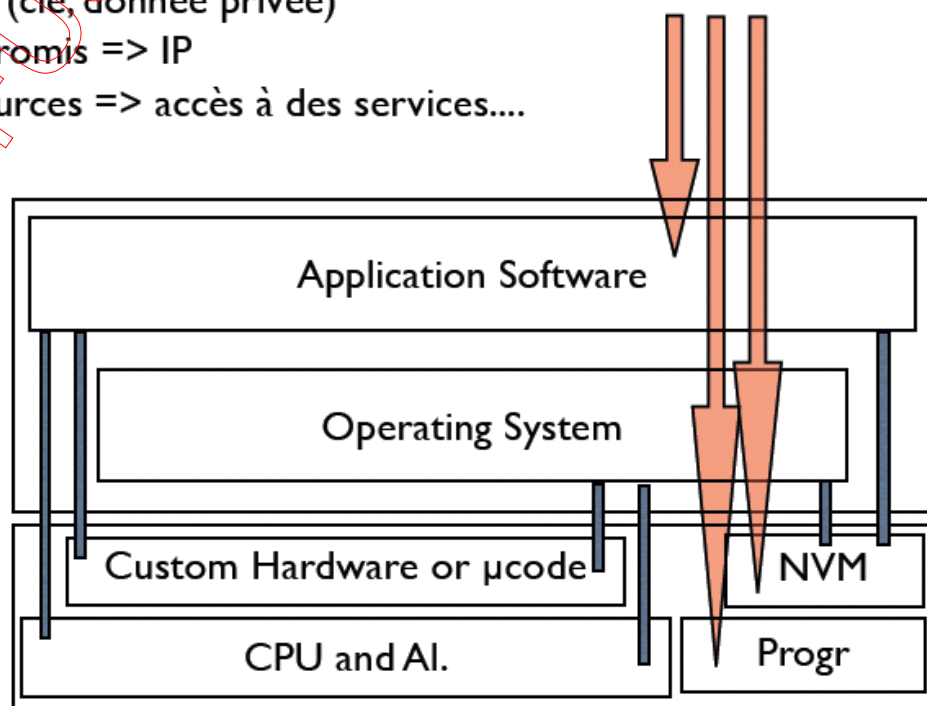
# La confidentialité

- 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

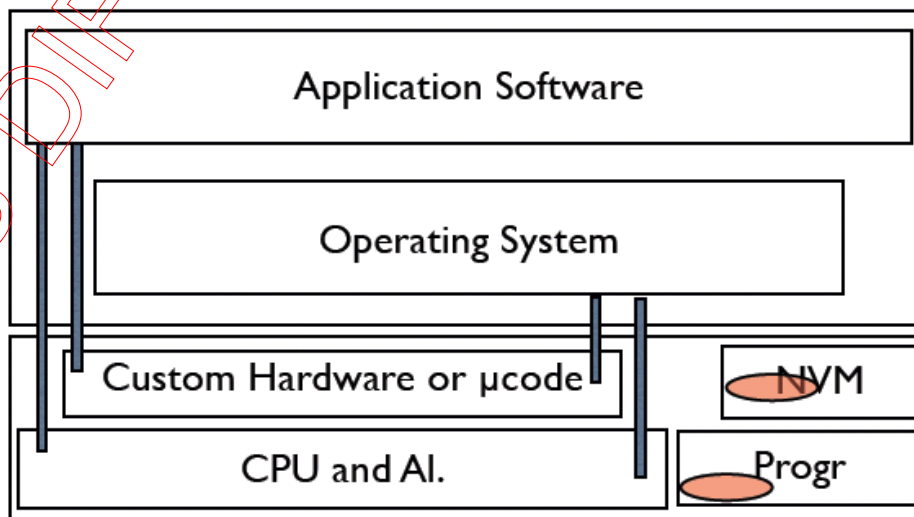
We shall see how integrity is provided by **MACs** and **digital signatures**.

**Warning:**  
**Authentication**  
**(authentication)**

9

## L'intégrité

- Données et programmes changés



10

# 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

9

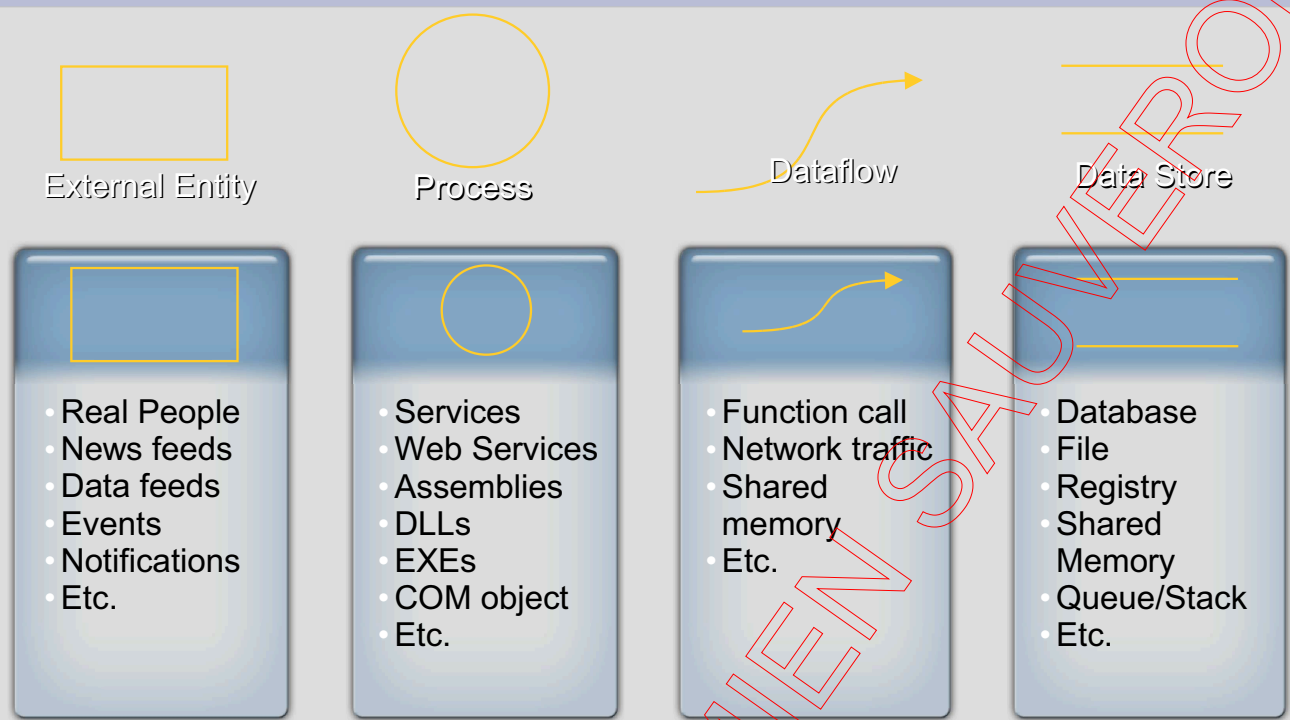
Qu'est ce qu'on veut sécuriser ?

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.

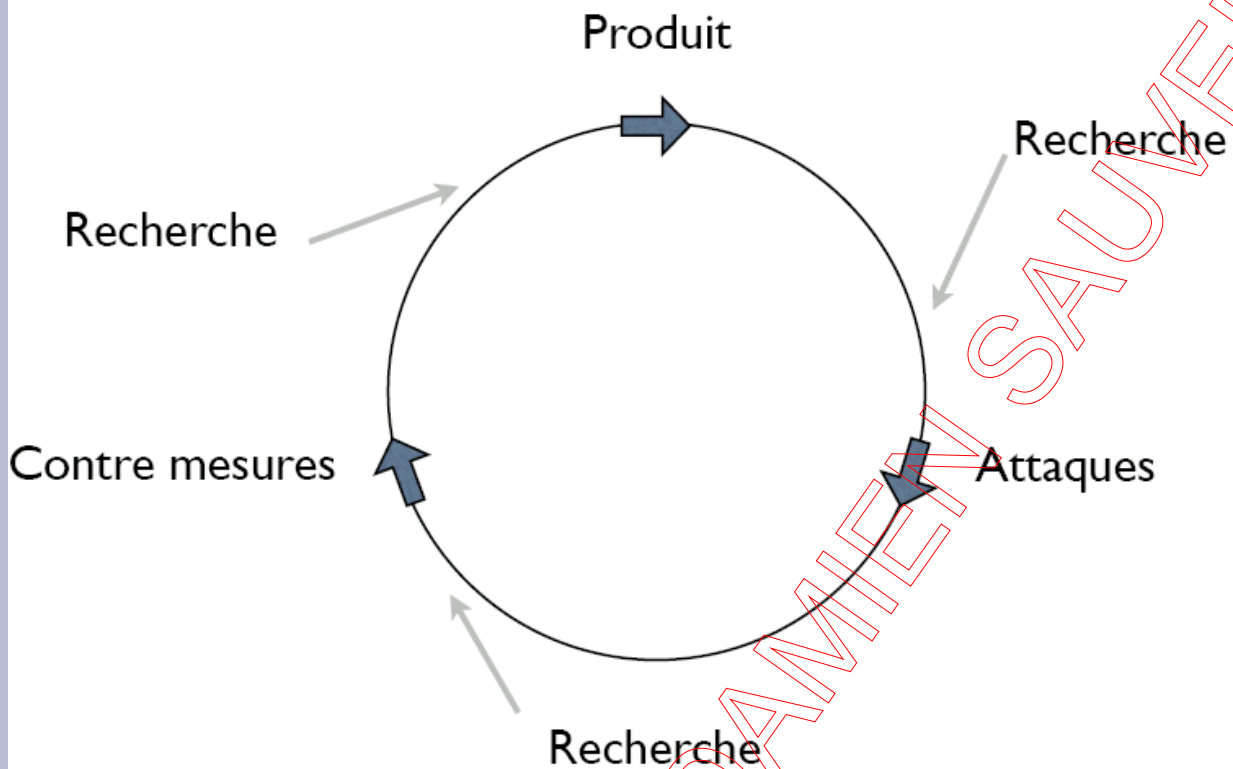
Mechanisms close to hardware are typically more generic and computer-oriented, whilst those close to the application are more user-oriented.

25

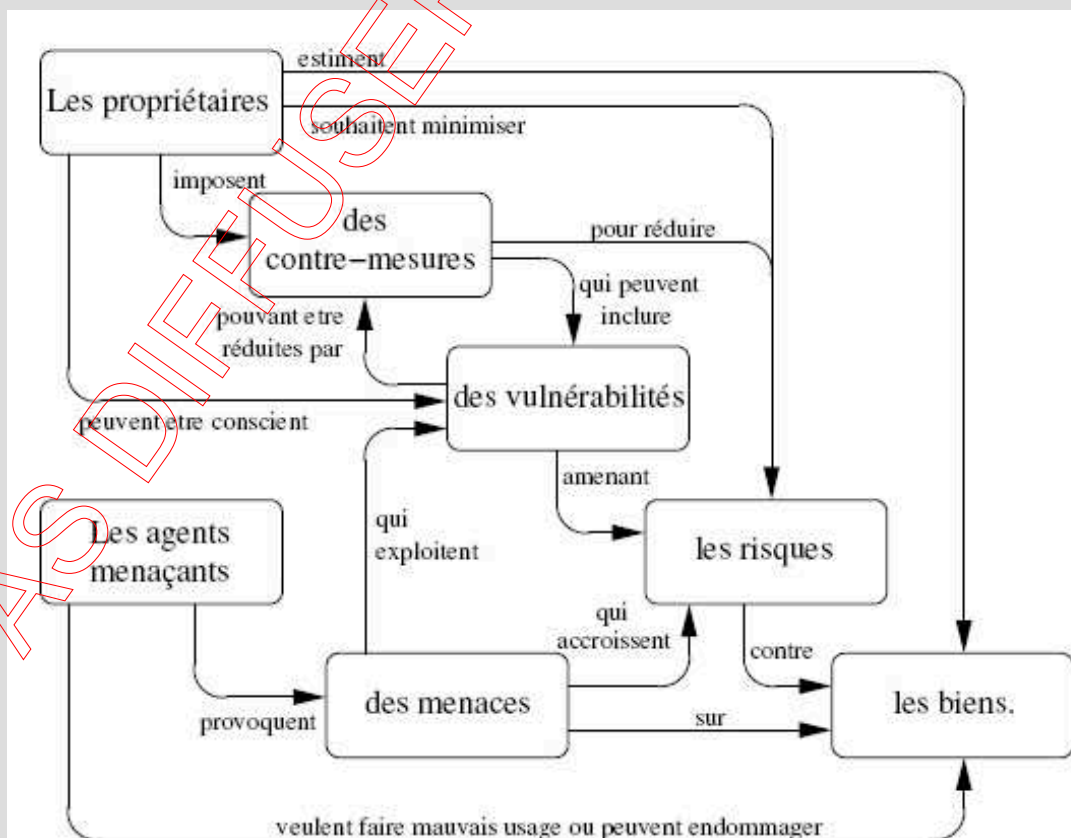
In this course we focus on Communications Security (or more generally Security of Information)

26

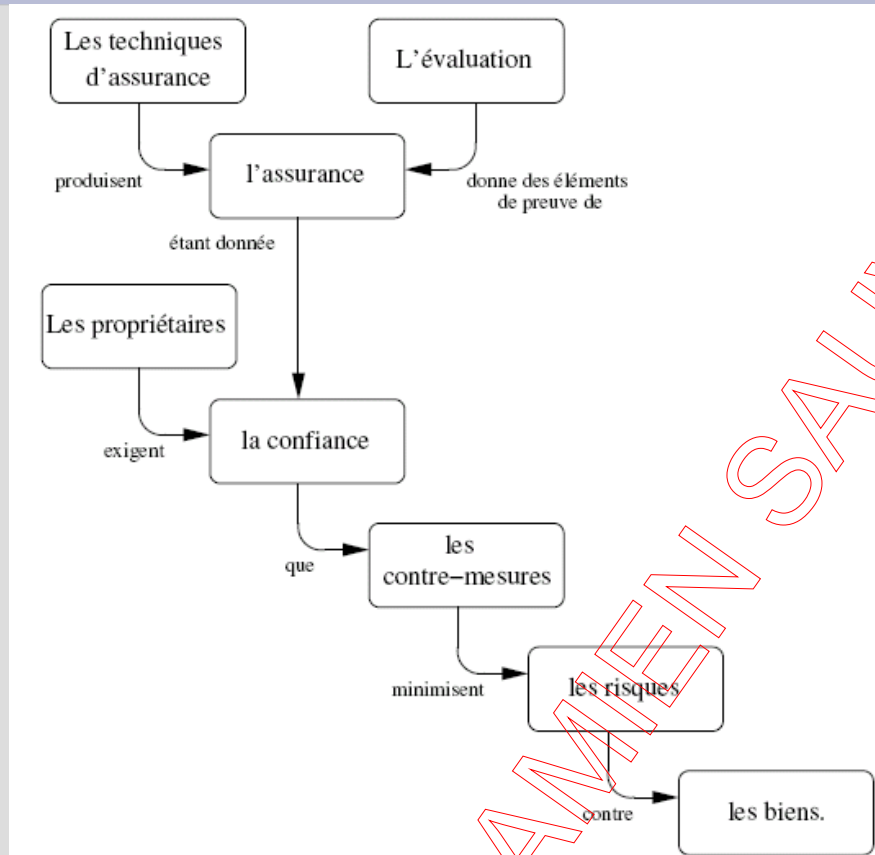
# Un cycle infernal!



## 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.

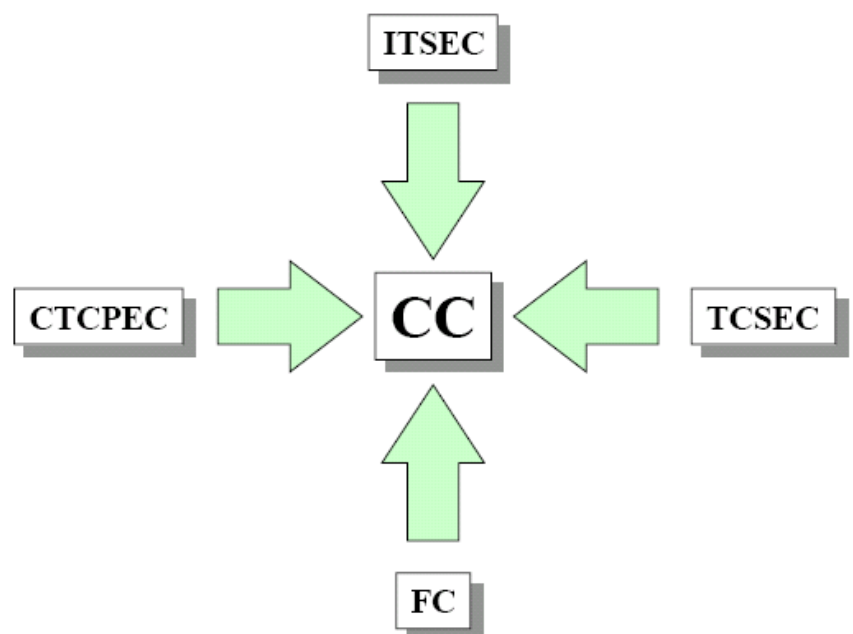
31

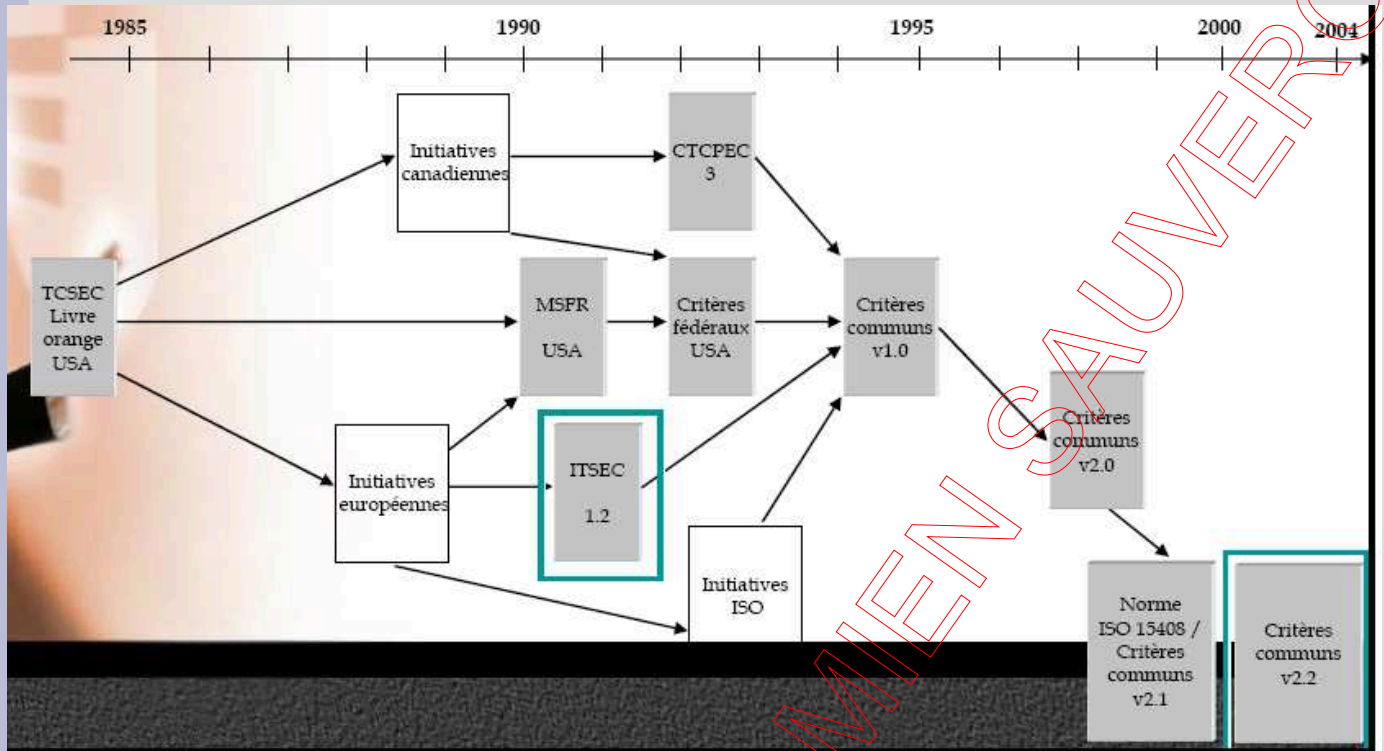
## Normes pour l'évaluation

**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

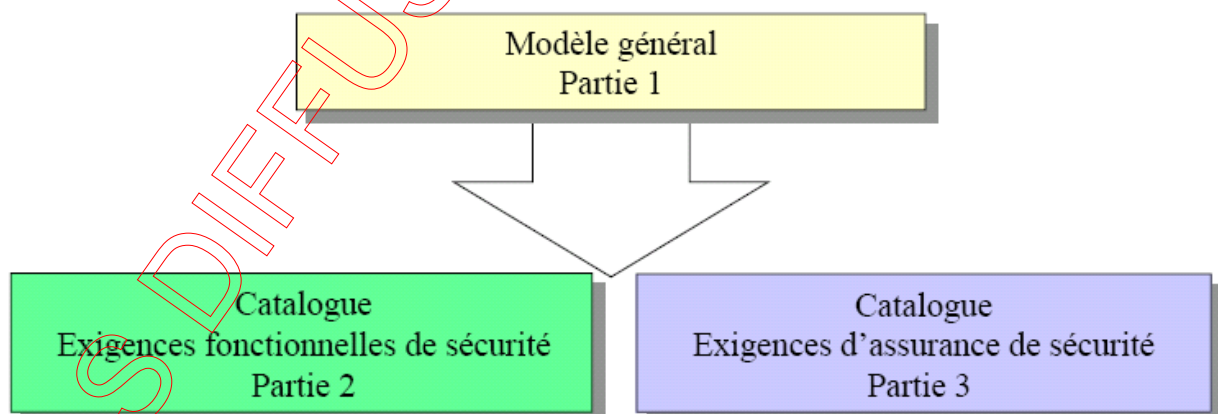


Juin 1999 Normalisation des Critères Communs

|                    |                                               |
|--------------------|-----------------------------------------------|
| 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

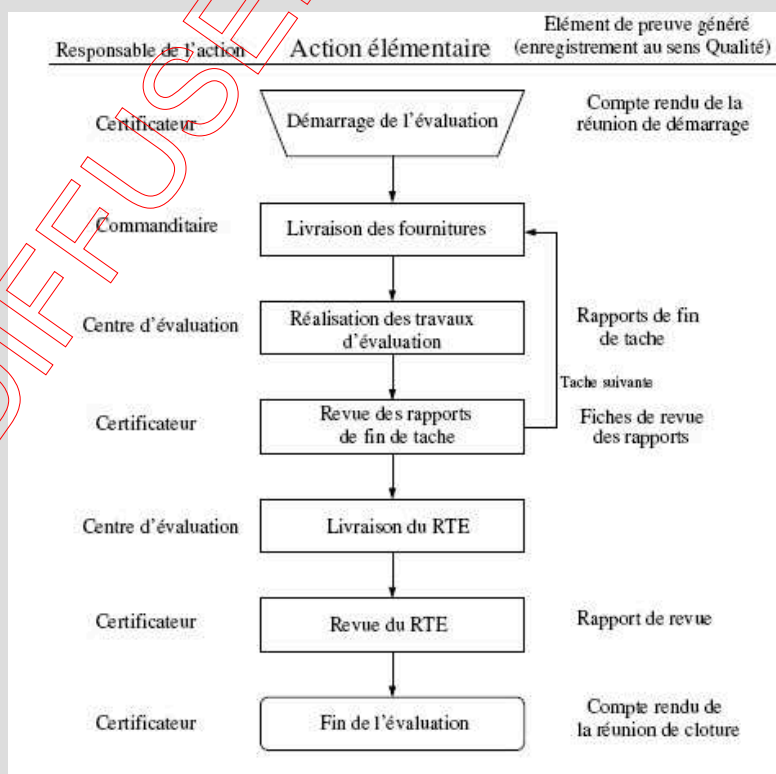
## Expression des exigences



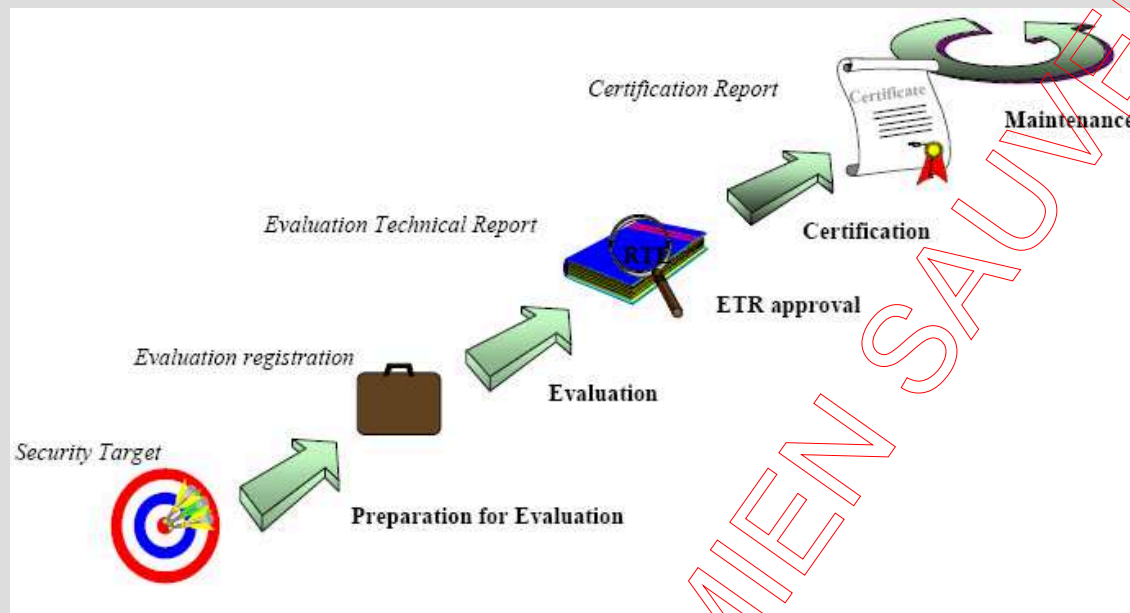
36

|               | Consumers                                                                                          | Developers                                                                                                                         | Evaluators                                                                                                                     |
|---------------|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Part 1</b> | 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.                                     |
| <b>Part 2</b> | 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. |
| <b>Part 3</b> | 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 ;

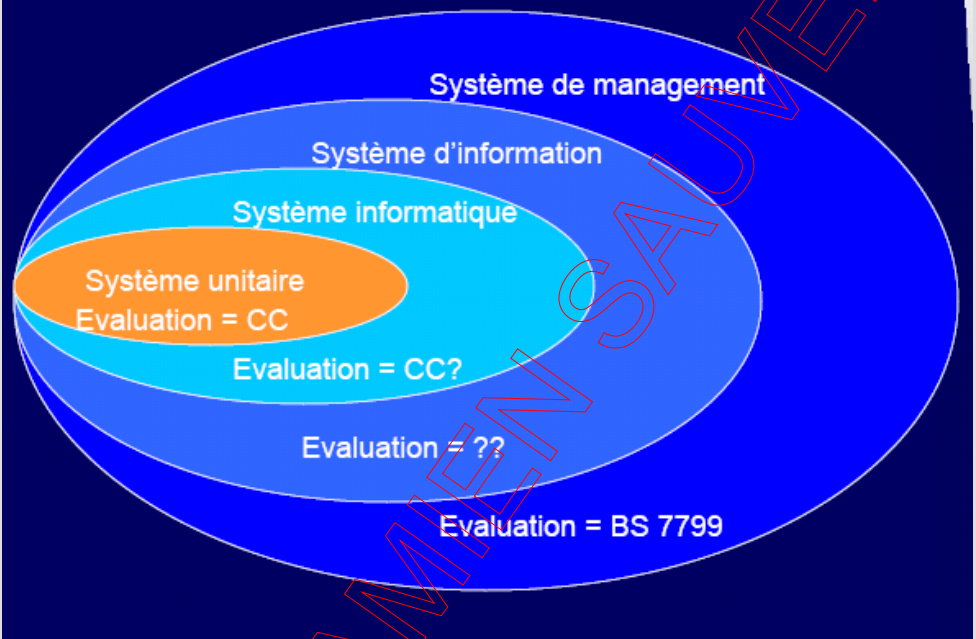
**PP (Protection Profil)** pour désigner un profil de protection, i.e. un document rassemblant l'ensemble des exigences de sécurité valables pour une catégorie de TOE qui satisfait des besoins spécifiques d'utilisateurs, indépendamment de son implantation (e.g. il existe des PP pour l'évaluation de puce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

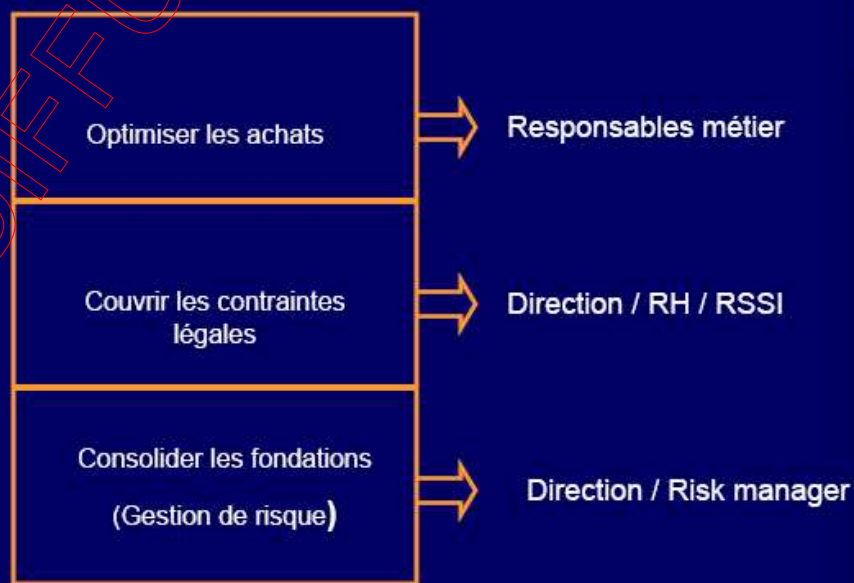
Et même un sous ensemble



41

## Etablissement de la confiance !

### Pourquoi une évaluation des systèmes d'information?



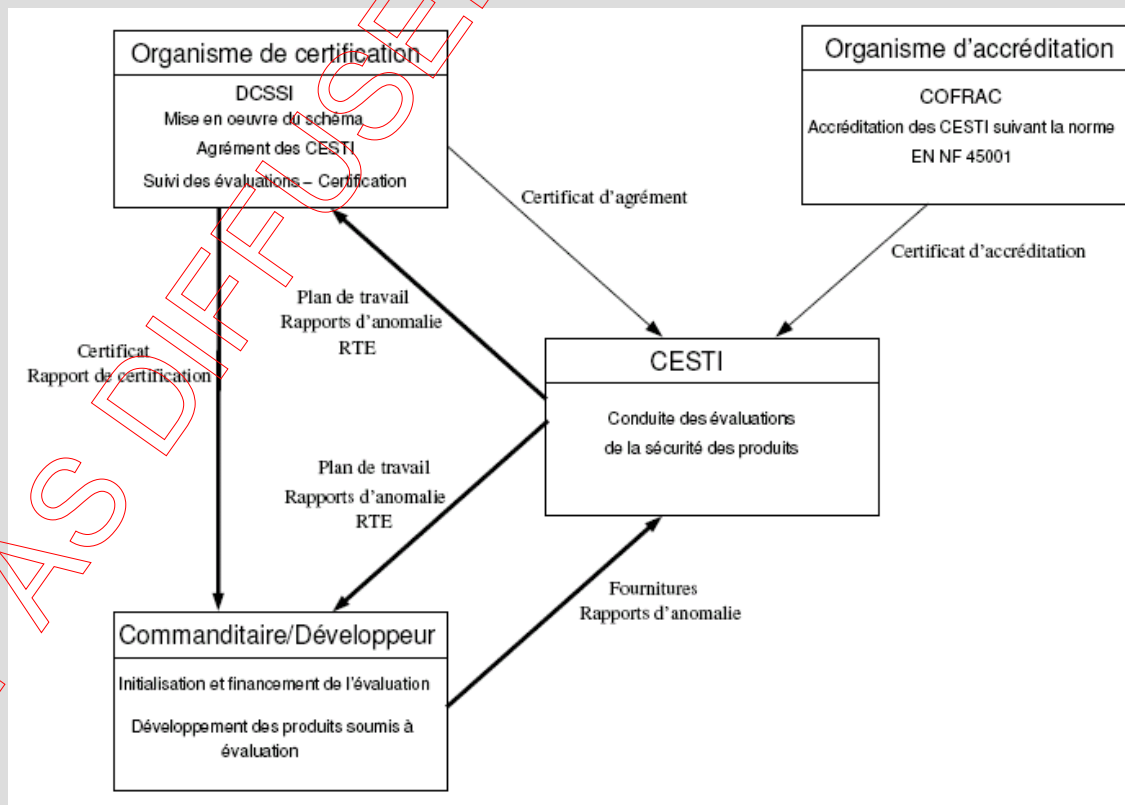
42

## 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



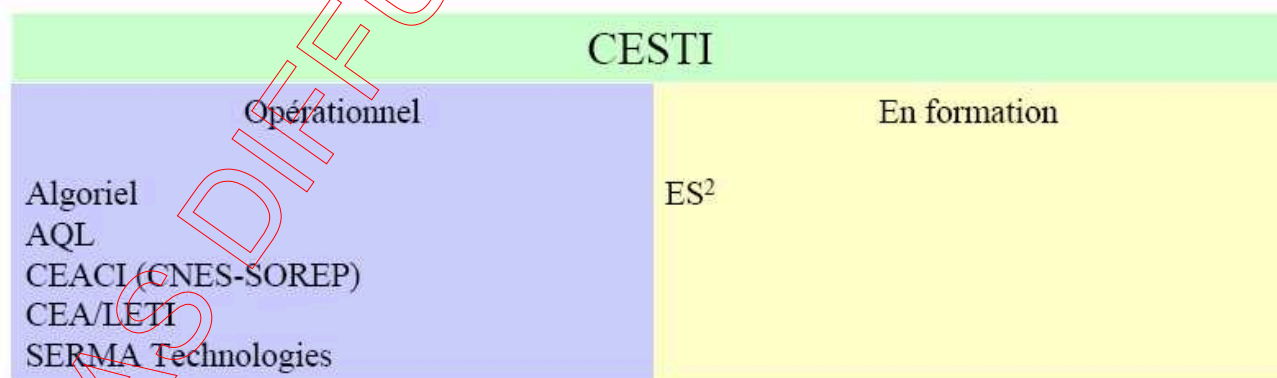
44

## Organisme de certification



45

## Centres d'évaluation



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

46

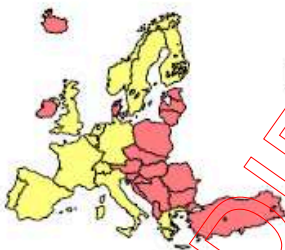
## Un environnement international...

### 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

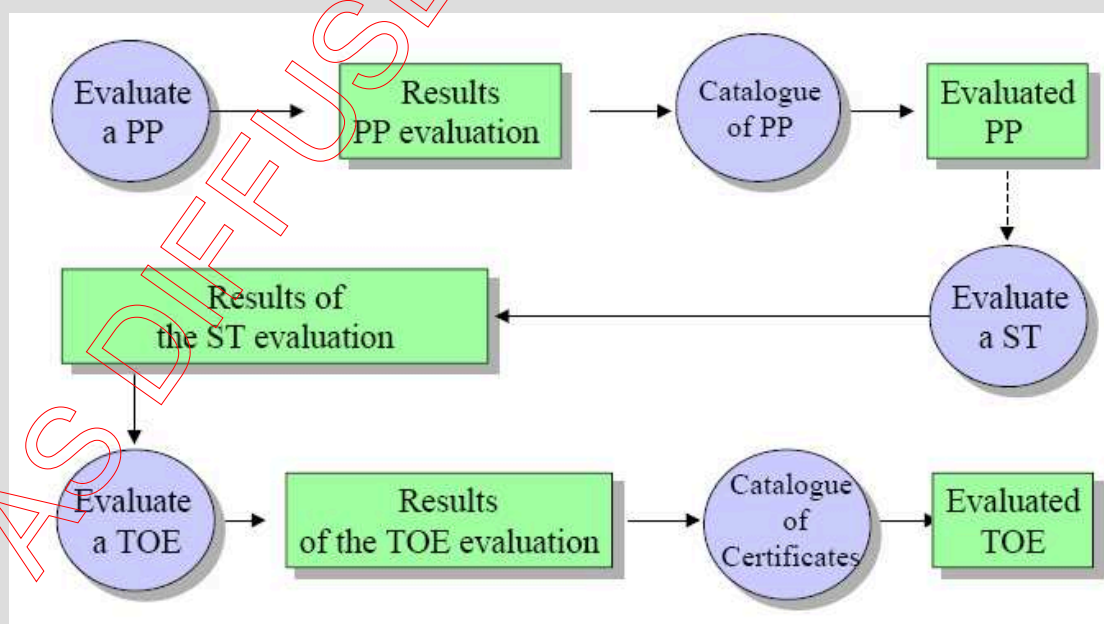
BSI (Allemagne), DSD (Australie), CSE (Canada), NIST/NSA (États-Unis), SCSSI (France) et CESG (Royaume Uni)

- Organismes de certification commerciaux

- Certificat CC EAL1 à EAL4

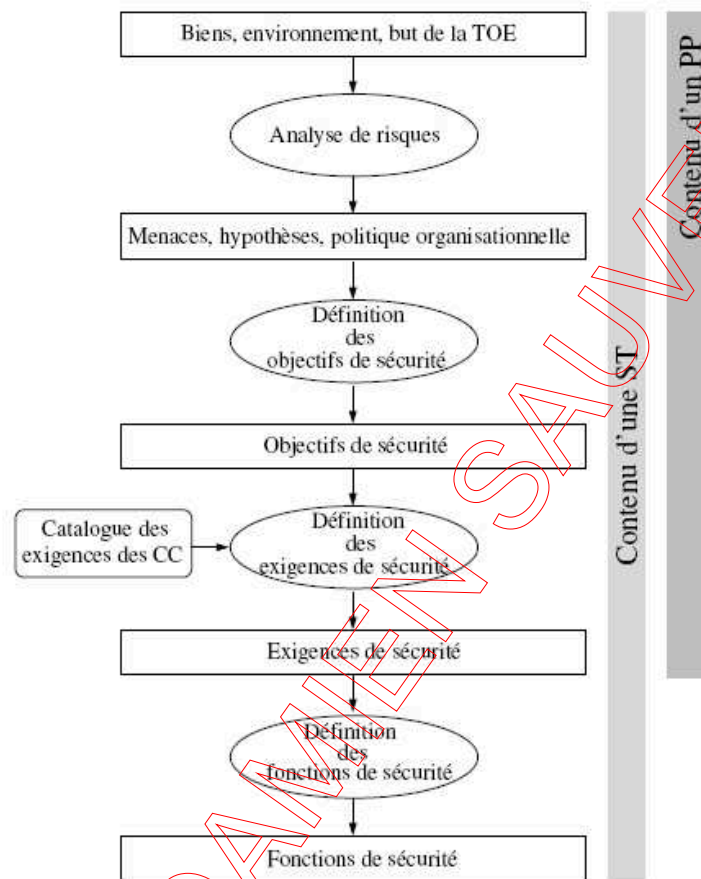
49

## CC evaluations and their results

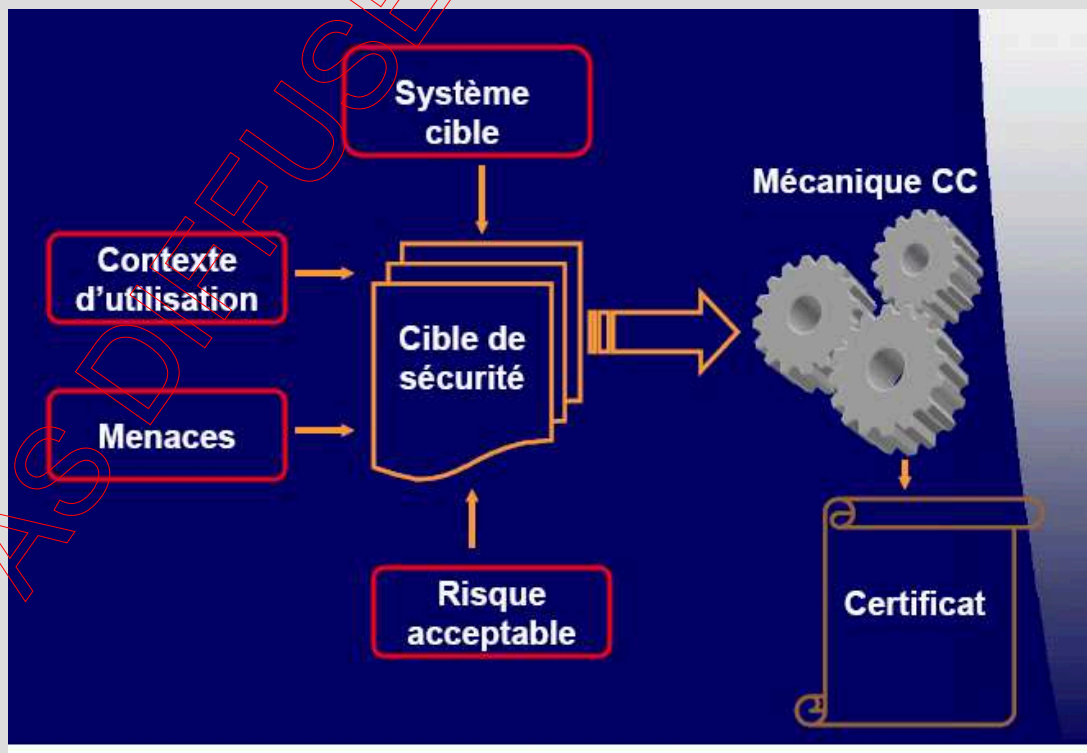


50

## Contenu d'une ST et d'un PP



51



52

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



53

## Quelques chiffres !

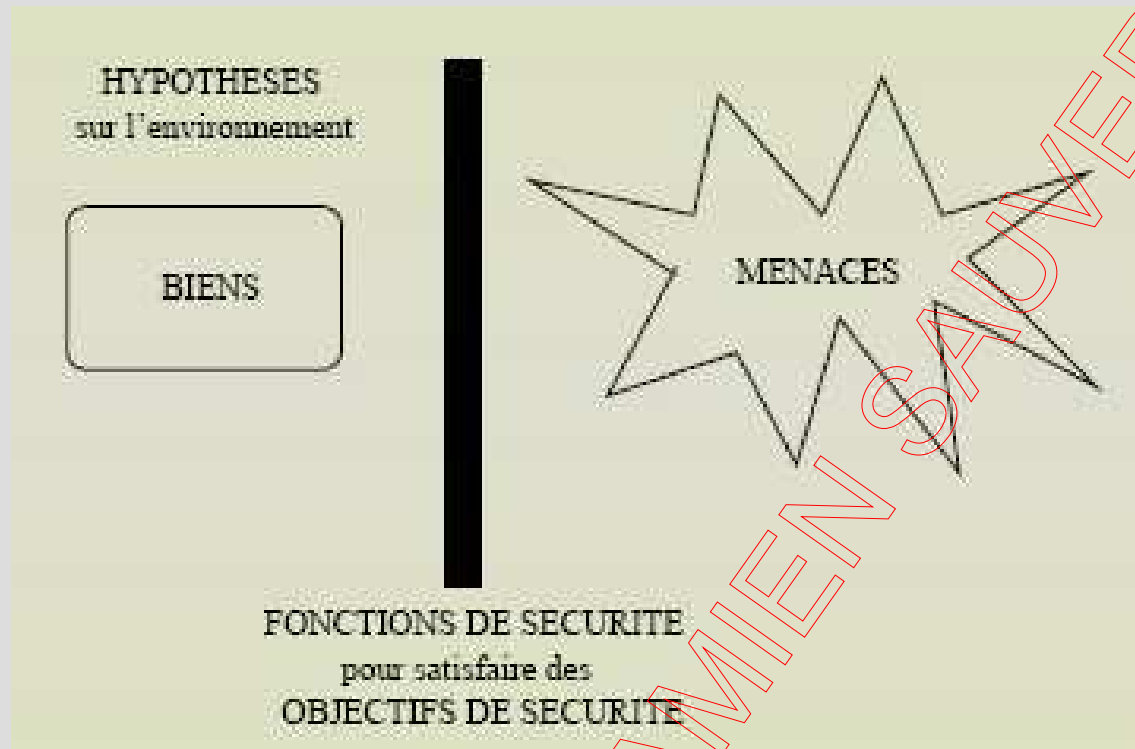
### Retour d'expérience sur l'évaluation d'un VPN

- ✚ 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

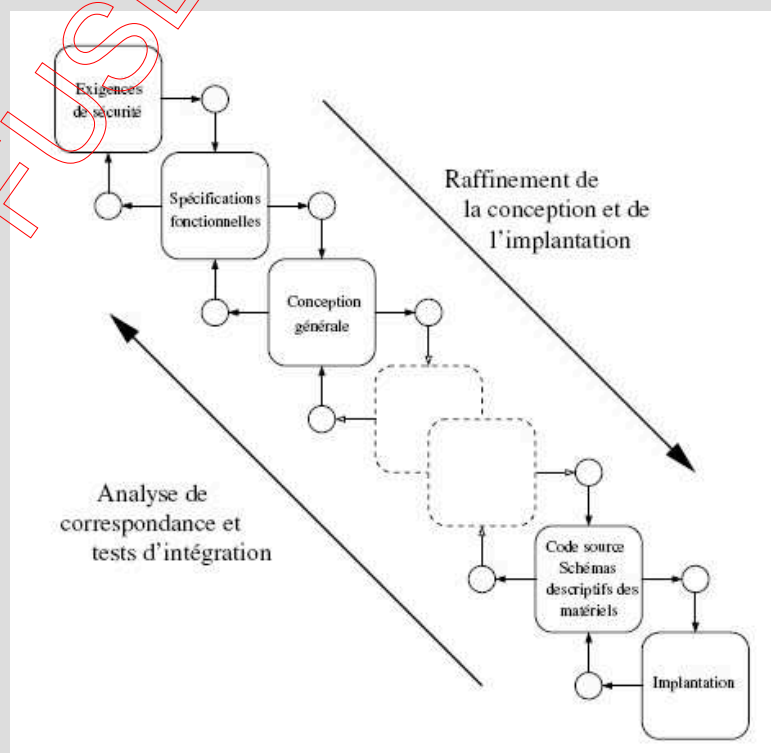
## Les bases des critères communs

### Critères Communs (ISO15408)



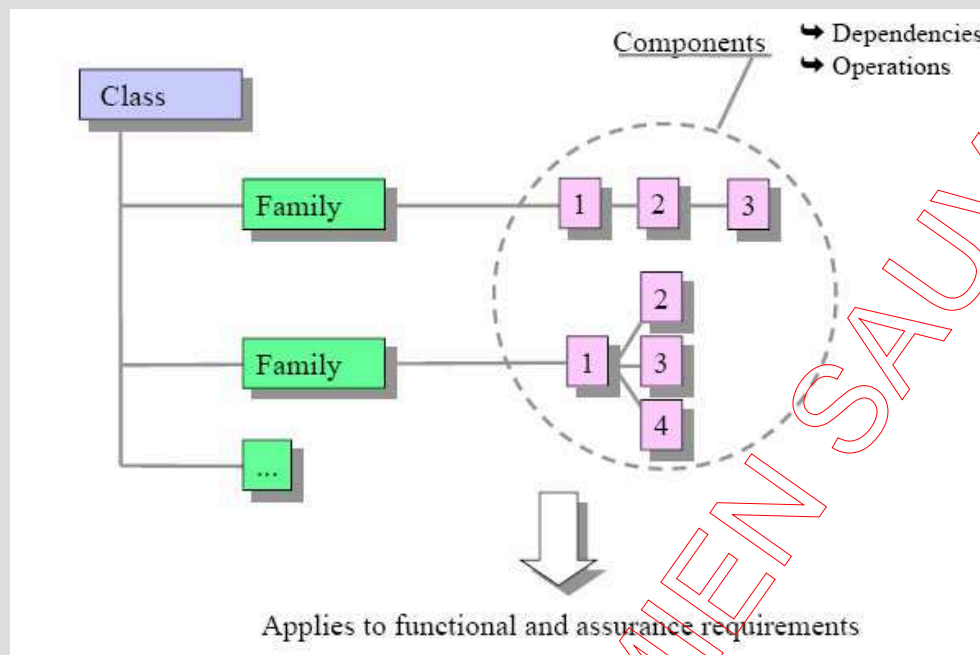
55

## Modèle de développement d'une TOE



56

## Requirements : hierarchical structure



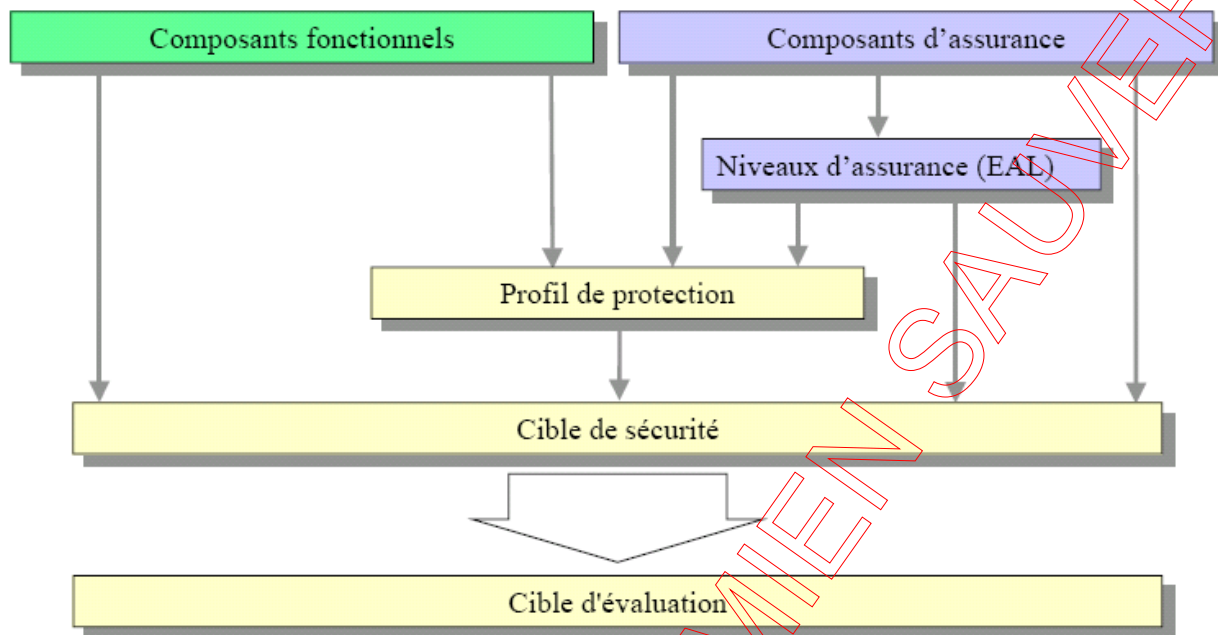
57

## CC Catalogue : definitions

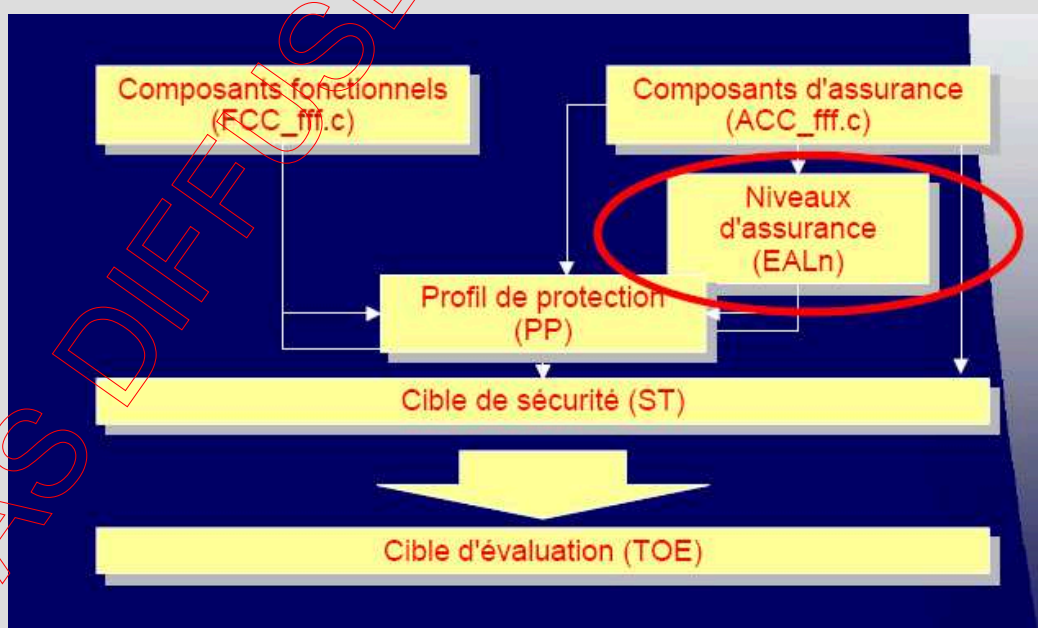
- **Class** : A grouping of families that share a common focus.
- **Family** : A grouping of components that share security objectives but may differ in emphasis or rigour.
- **Component** : The smallest selectable set of elements that may be included in a PP, an ST, or a package.
- **Package** : A reusable 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

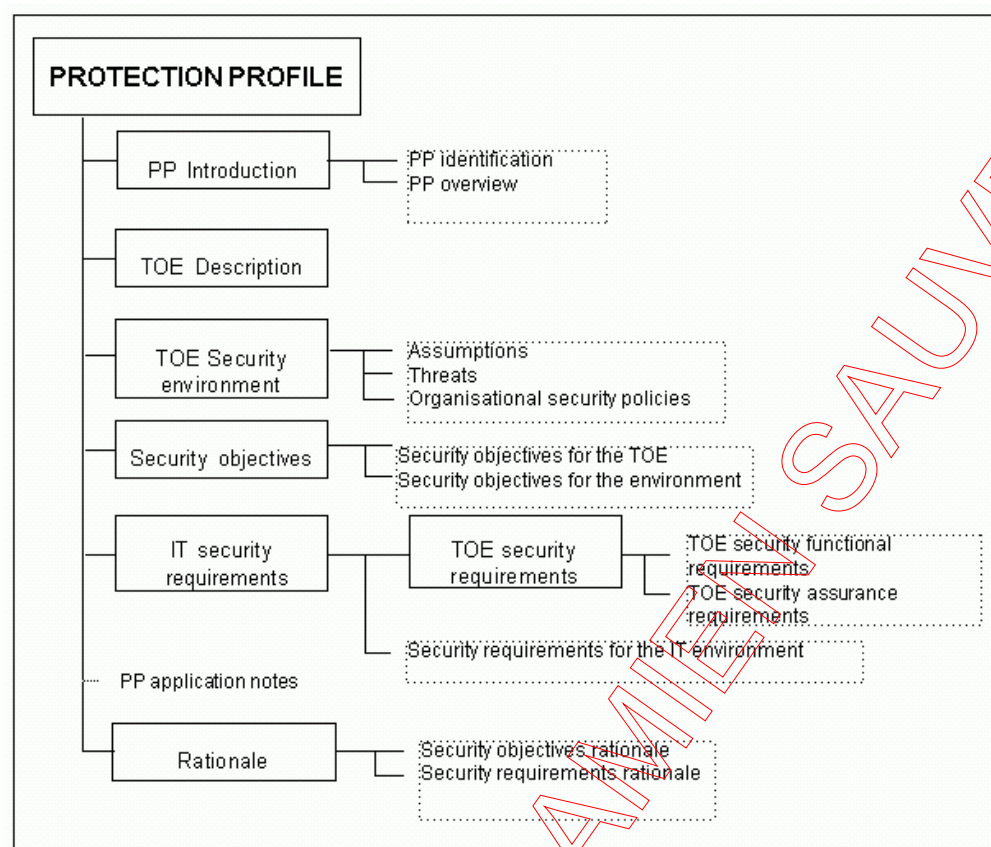
Exigences de  
sécurité des TI

Exigences de  
sécurité de la TOE

Justificatif

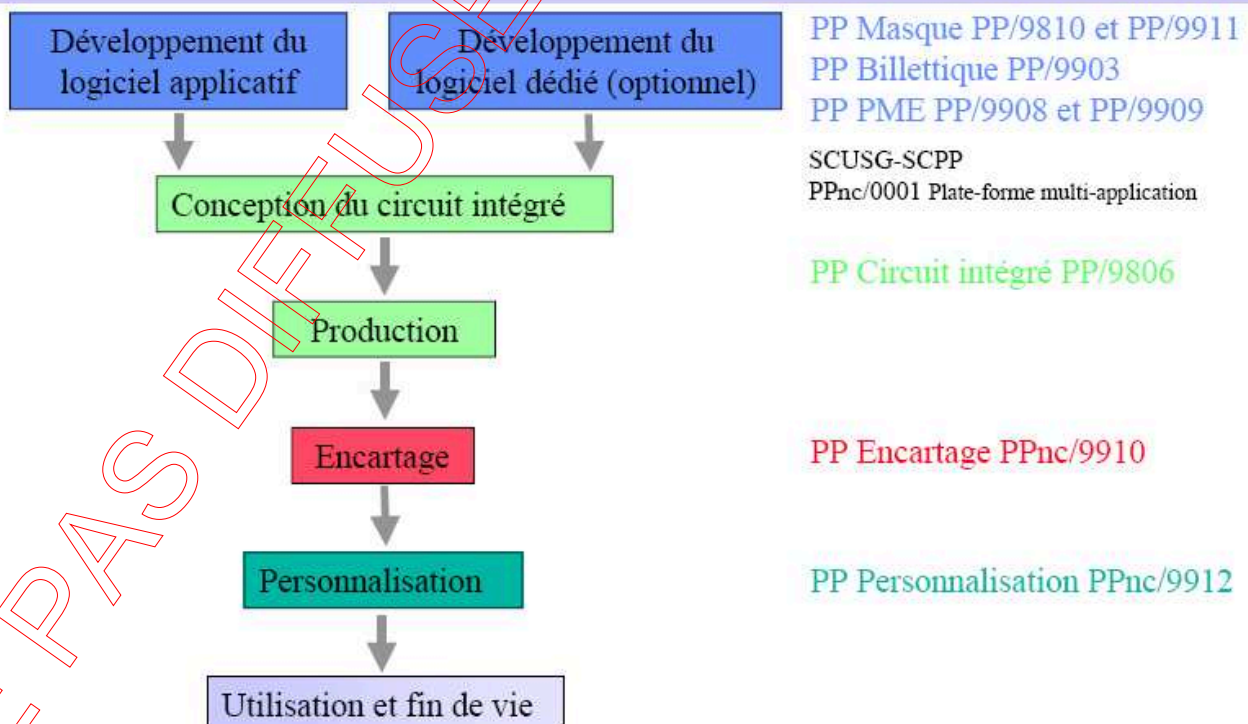
62

## Protection Profile



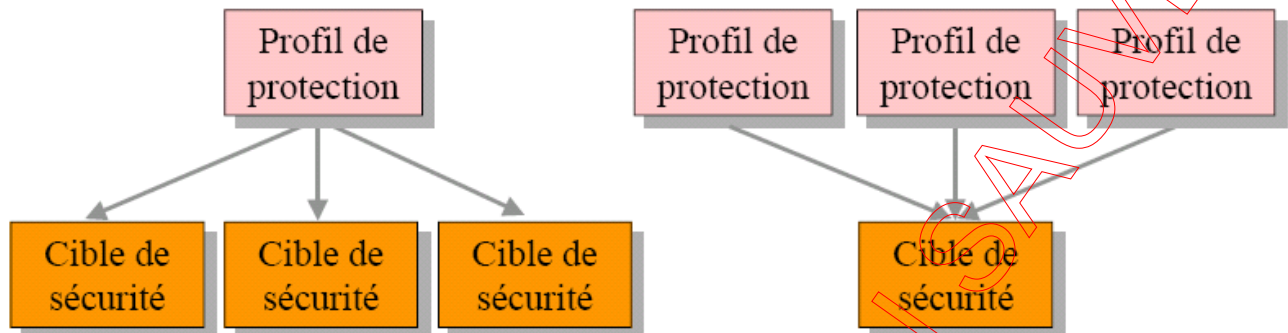
63

## PP Cartes à puce



64

## Utilisation des profils de protection



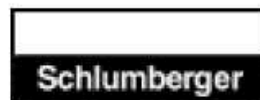
65

## 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

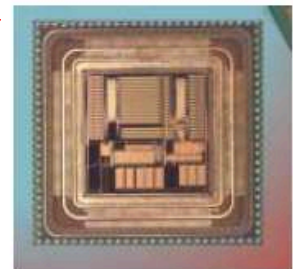
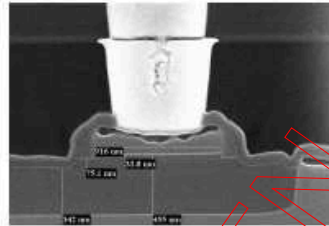
PP/9806: Smartcard integrated circuit

**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

## PP Echanges de données informatisées

### PP/9802: Transactions portant sur des données non confidentielles

EAL3+ (ADV\_IMP.1, ADV\_LLD.1, ALC.TAT.1)

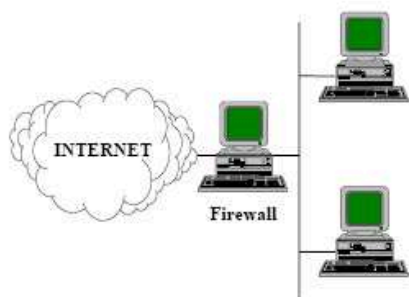
Ministère de l'Economie, des Finances et de l'Industrie

### 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

## 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

## 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

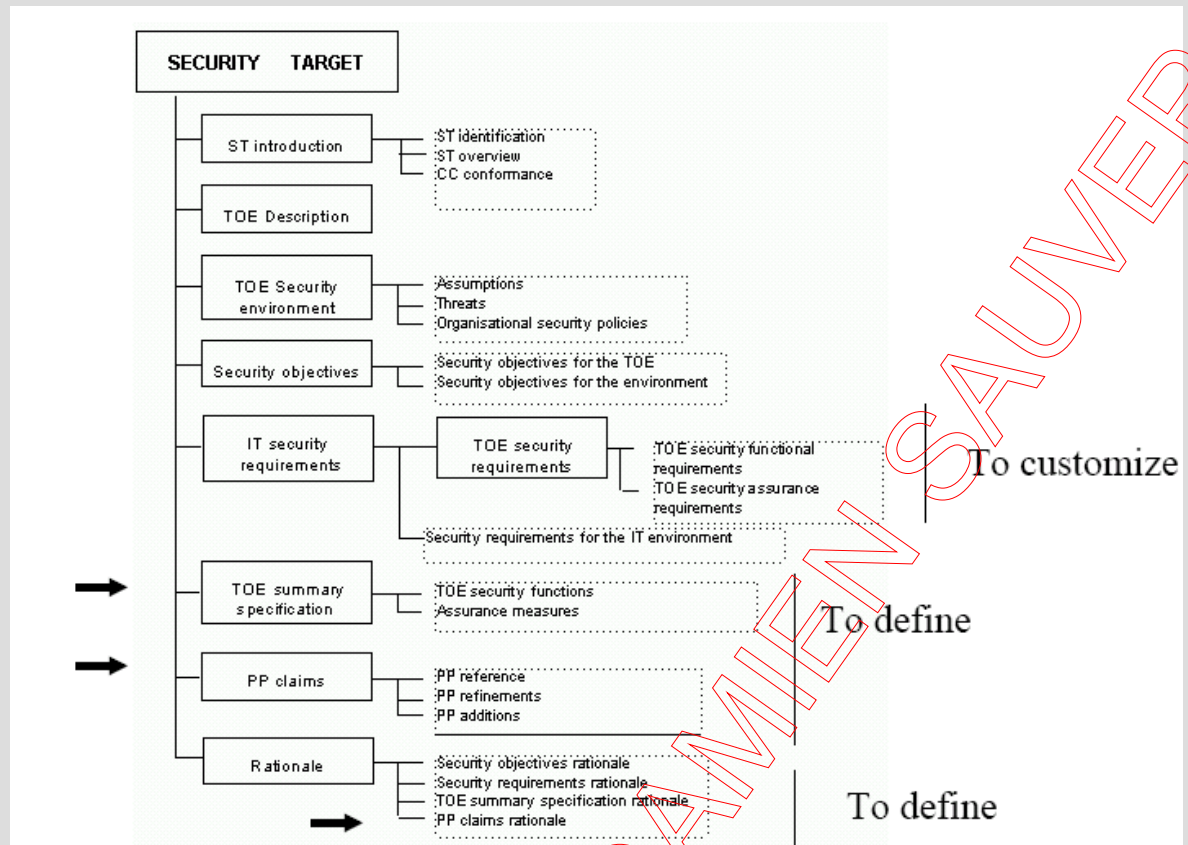
EAL 3+ (AVA\_VLA.3, ADV\_IMP.1, ADV\_LLD.1, ADV\_SPM.1, ALC\_TAT.1)  
SCSSI

Autorité de certification

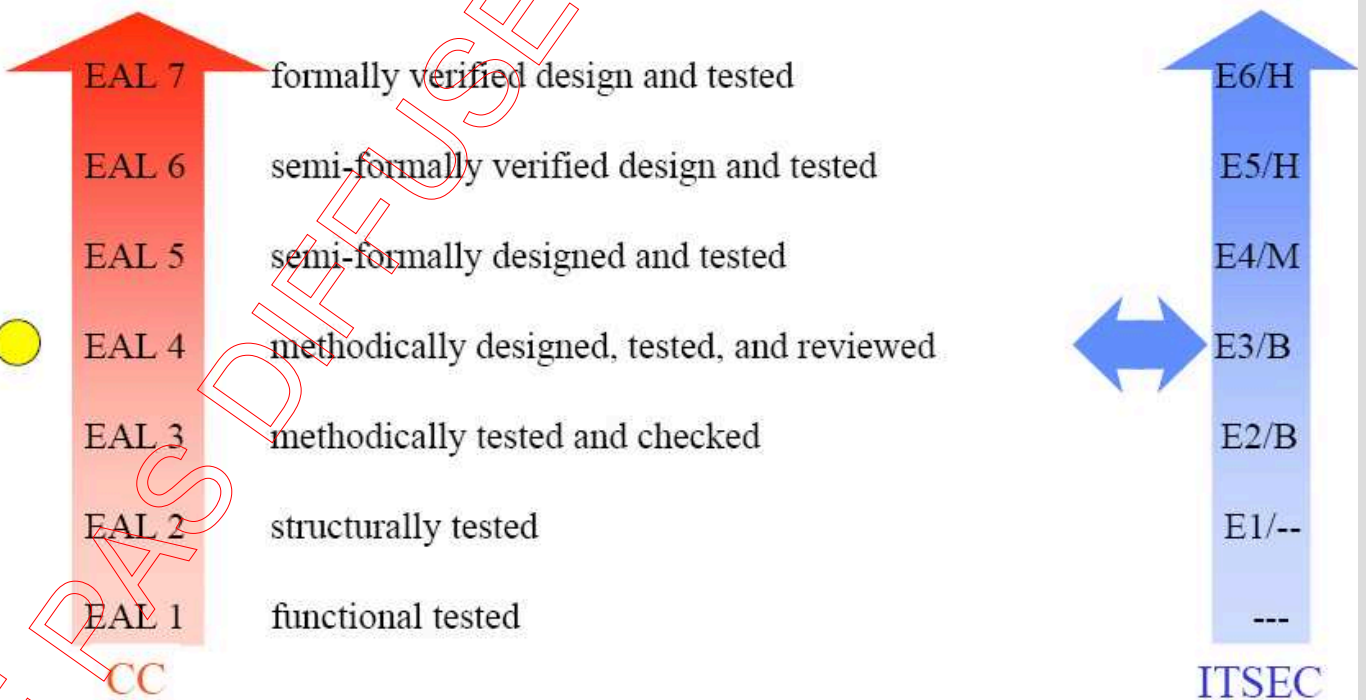
PPnc/0006: Autorité de certification

EAL 3+ (AVA\_VLA.3, ADV\_IMP.1, ADV\_LLD.1, ADV\_SPM.1, ALC\_TAT.1)  
SCSSI

## Security Target

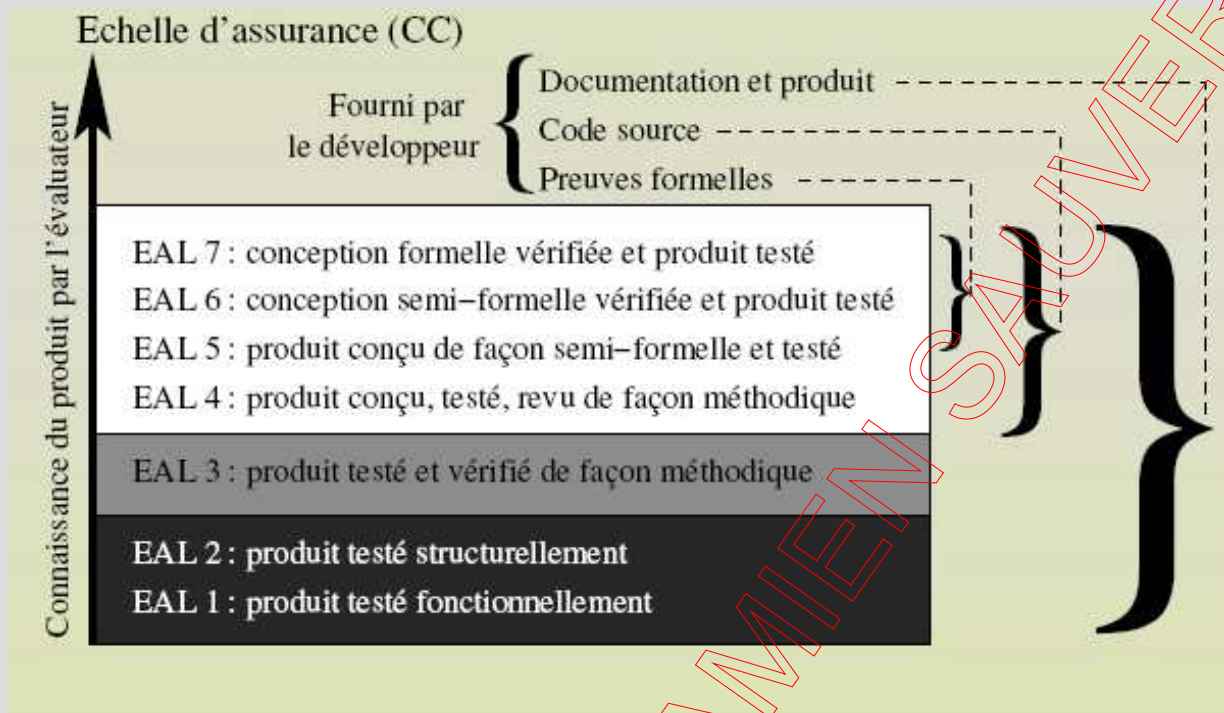


75



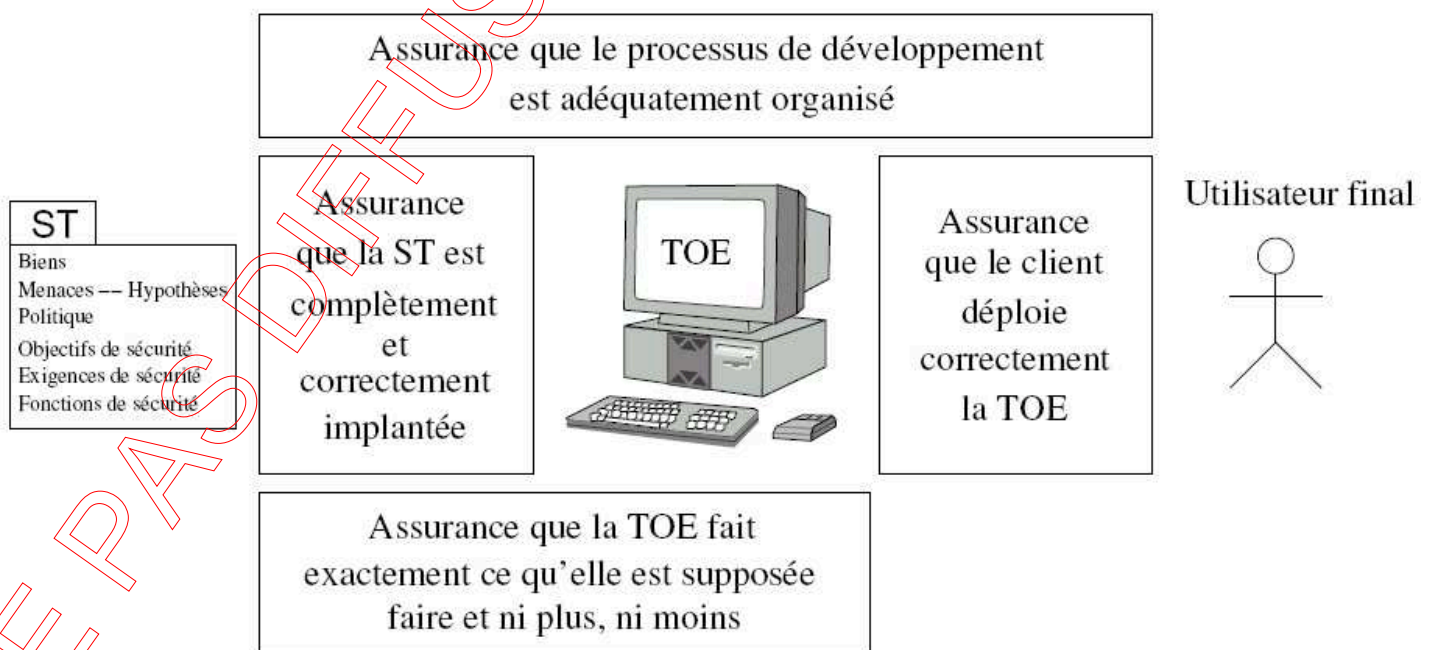
76

## L'échelle d'assurance



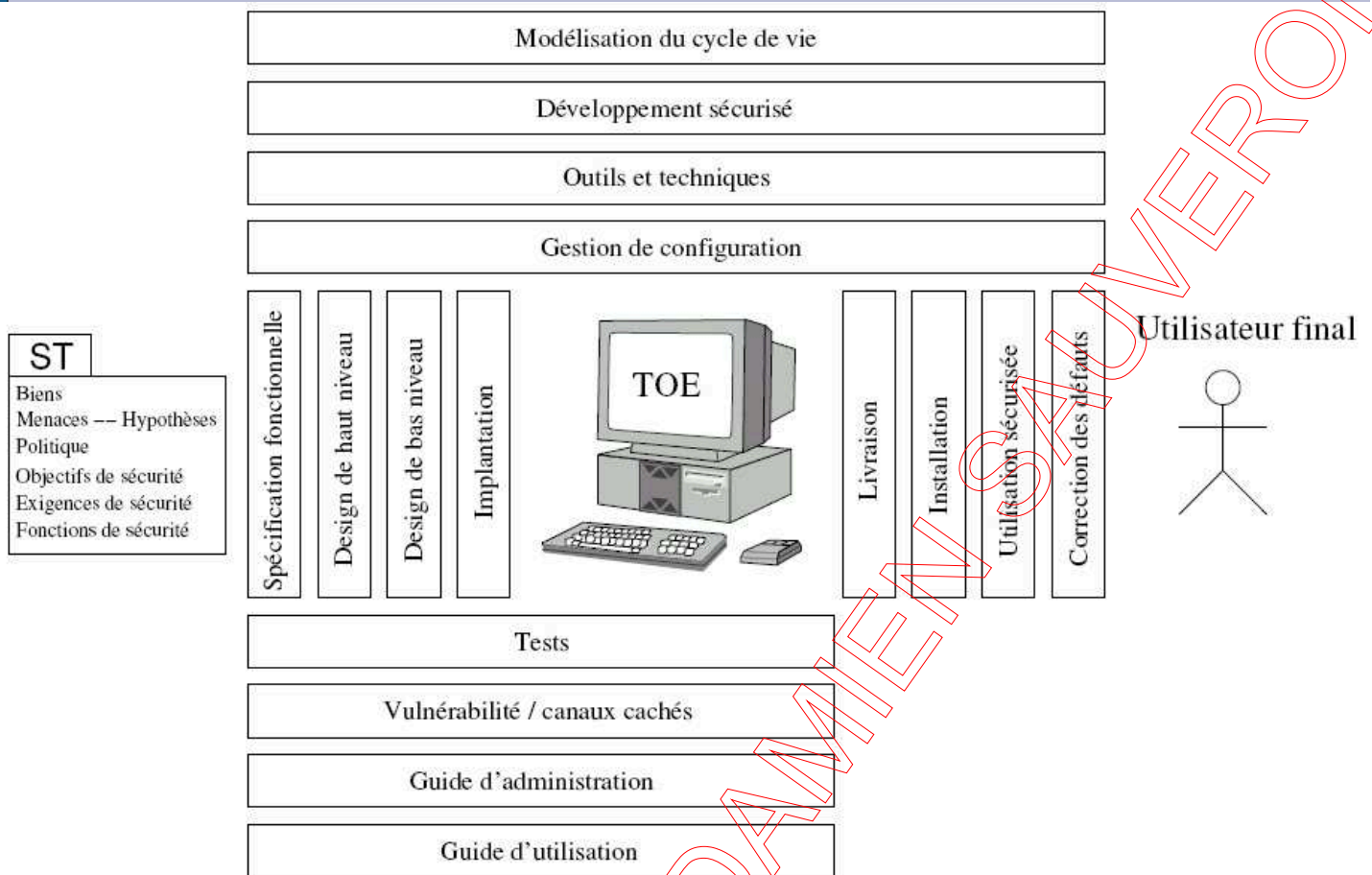
77

## L'assurance des Critères Communs



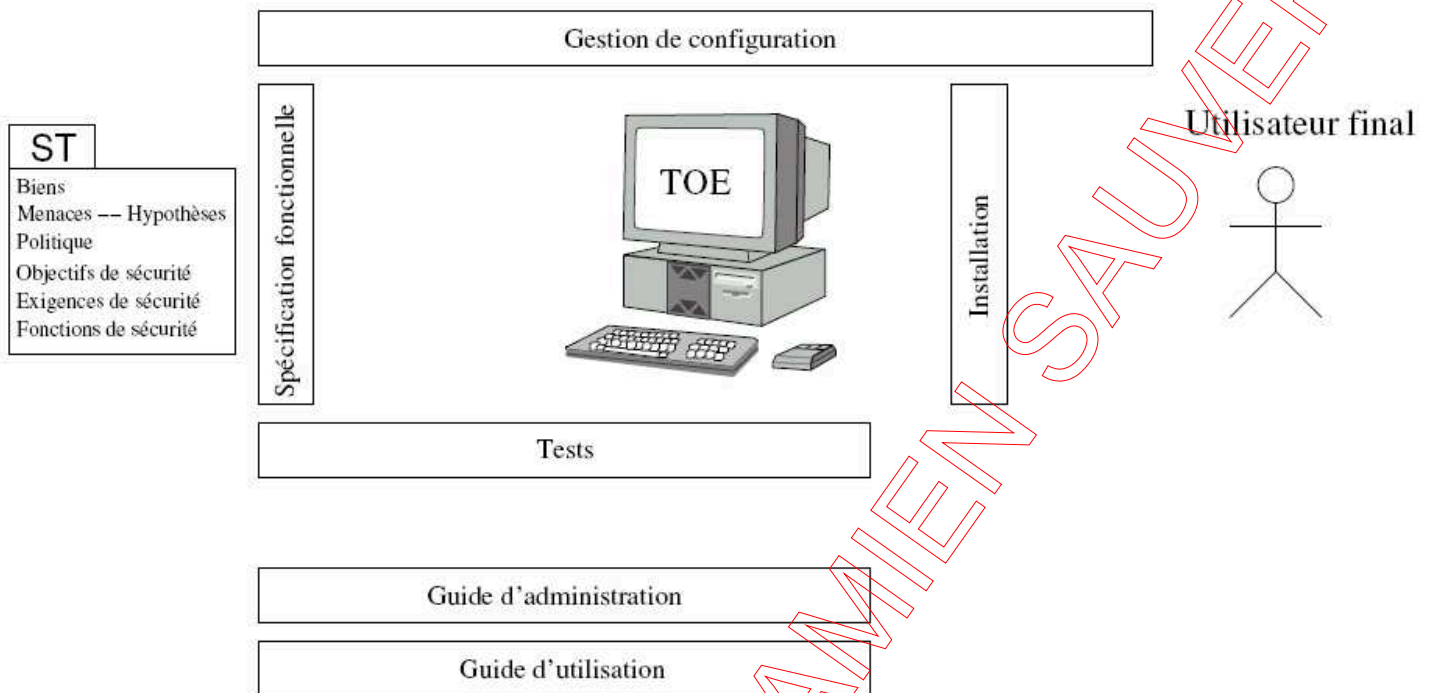
78

## 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                                                  | 1    | 1    | 1    | 1    | 2    | 2    |
|                          | ACM_CAP          | 1                                                  | 2    | 3    | 4    | 4    | 5    | 5    |
|                          | ACM_SCP          | 1                                                  | 1    | 1    | 2    | 3    | 3    | 3    |
| Delivery and operations  | ADO_DEL          | 1                                                  | 1    | 1    | 2    | 2    | 2    | 3    |
|                          | ADO_IGS          | 1                                                  | 1    | 1    | 1    | 1    | 1    | 1    |
|                          | ADV_FSP          | 1                                                  | 1    | 1    | 2    | 3    | 3    | 4    |
| Development              | ADV_HLD          | 1                                                  | 1    | 2    | 2    | 3    | 4    | 5    |
|                          | ADV_IMP          | 1                                                  | 1    | 1    | 1    | 2    | 3    | 3    |
|                          | ADV_INT          | 1                                                  | 1    | 1    | 1    | 1    | 2    | 3    |
|                          | ADV_LLD          | 1                                                  | 1    | 1    | 1    | 1    | 2    | 2    |
|                          | ADV_RCR          | 1                                                  | 1    | 1    | 1    | 2    | 2    | 3    |
| Guidance documents       | AGD_ADM          | 1                                                  | 1    | 1    | 1    | 1    | 1    | 1    |
|                          | AGD_USR          | 1                                                  | 1    | 1    | 1    | 1    | 1    | 1    |
|                          | ALC_DVS          | 1                                                  | 1    | 1    | 1    | 1    | 2    | 2    |
| Life cycle support       | ALC_FLR          | 1                                                  | 1    | 1    | 1    | 1    | 1    | 1    |
|                          | ALC_LCD          | 1                                                  | 1    | 1    | 1    | 2    | 2    | 3    |
|                          | ALC_TAT          | 1                                                  | 1    | 1    | 1    | 2    | 3    | 3    |
| Tests                    | ATE_COV          | 1                                                  | 1    | 2    | 2    | 2    | 3    | 3    |
|                          | ATE_DPT          | 1                                                  | 1    | 1    | 1    | 2    | 2    | 3    |
|                          | ATE_FUN          | 1                                                  | 1    | 1    | 1    | 1    | 2    | 2    |
|                          | ATE_IND          | 1                                                  | 2    | 2    | 2    | 2    | 2    | 3    |
| Vulnerability assessment | AVA_CCA          | 1                                                  | 1    | 1    | 1    | 1    | 2    | 2    |
|                          | AVA_MSUS         | 1                                                  | 1    | 1    | 2    | 2    | 3    | 3    |
|                          | AVA_SOP          | 1                                                  | 1    | 1    | 1    | 1    | 1    | 1    |
|                          | AVA_VLAS         | 1                                                  | 1    | 1    | 2    | 3    | 4    | 4    |



### 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

## EAL 3

### ● *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

83

## EAL 4

### ● *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

84

## EAL 5

- **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

85

## EAL 6

- **High-level of risks product evaluation**

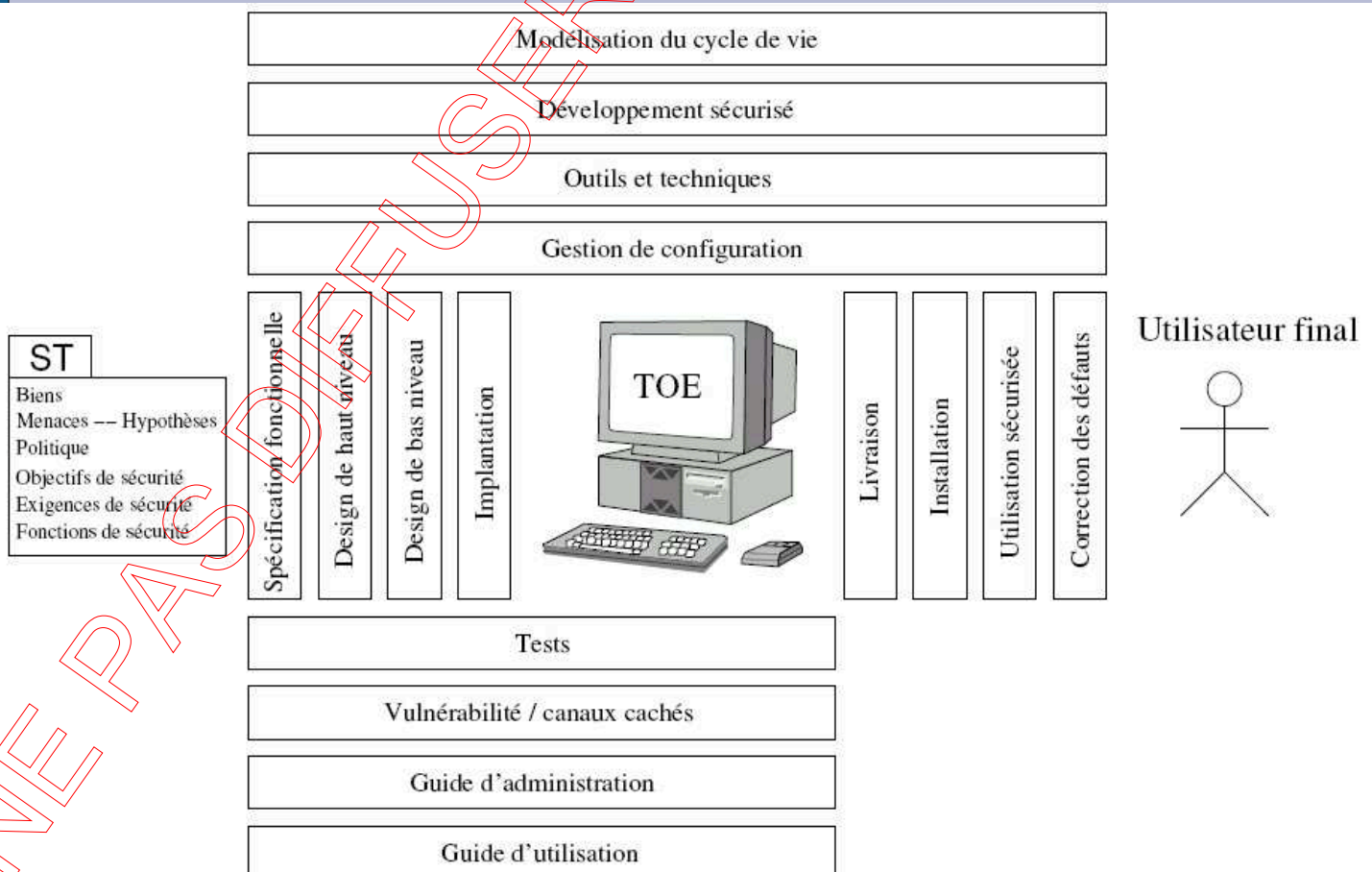
- Modular design and design by successive refinements
- Structured implementation of the TSF
- High-controlled development environment and advanced configuration management
- Systematic search for vulnerabilities and resistance to high potential attacks

86

● *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     | 2                                                             |
|                               | ACM CAP             | 1                                                             | 2     | 3     | 4     | 4     | 5     | 5     |                                                               |
|                               | ACM SCP             |                                                               |       | 1     | 2     | 3     | 3     | 3     |                                                               |
|                               | ADO DEL             |                                                               | 1     | 1     | 2     | 2     | 2     | 3     |                                                               |
| 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                                                             |
| Guides                        | ALC_DVS             |                                                               |       | 1     | 1     | 1     | 2     | 2     | 1                                                             |
|                               | ALC_FLR             |                                                               |       |       |       |       |       |       | 3                                                             |
|                               | ALC_LCD             |                                                               |       |       | 1     | 2     | 2     | 3     |                                                               |
| Support au Cycle de vie       | ALC_TAT             |                                                               |       |       | 1     | 2     | 3     | 3     | 1                                                             |
|                               | ATE_COV             |                                                               | 1     | 2     | 2     | 2     | 3     | 3     | 1                                                             |
|                               | ATE_DPT             |                                                               |       | 1     | 1     | 2     | 2     | 3     |                                                               |
|                               | ATE_FUN             |                                                               | 1     | 1     | 1     | 1     | 2     | 2     | 1                                                             |
| Tests                         | ATE_IND             | 1                                                             | 2     | 2     | 2     | 2     | 2     | 3     | 2                                                             |
|                               | AVA_CCA             |                                                               |       |       |       | 1     | 2     | 2     |                                                               |
|                               | AVA_MSU             |                                                               |       | 1     | 2     | 2     | 3     | 3     | 1                                                             |
|                               | AVA_SOF             |                                                               | 1     | 1     | 1     | 1     | 1     | 1     | 1                                                             |
| Estimation des vulnérabilités | 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

1: évaluation de la cible de sécurité ASE\_\*\*\*

2: évaluation de la documentation de développement haut niveau  
ADV\_FSP.1  
ADV\_RCR.1 1/4  
ADV\_HLD.2  
ADV\_RCR.1 2/4

3: évaluation de l'environnement de développement  
ACM\_CAP.2  
ADO\_DEL.1  
ALC\_DVS.1  
ALC\_FLR.3

4: évaluation de la documentation de développement de bas niveau des fonctions cryptographiques  
ADV\_LLD.1  
ADV\_RCR.1 3/4  
ADV\_IMP.1  
ADV\_RCR.1 4/4  
ALC\_TAT.1

5: évaluation de la documentation de test  
ATE\_COV.1  
ATE\_FUN.1

6: manipulation de la cible d'évaluation  
ADO\_IGS.1  
ATE\_IND.2

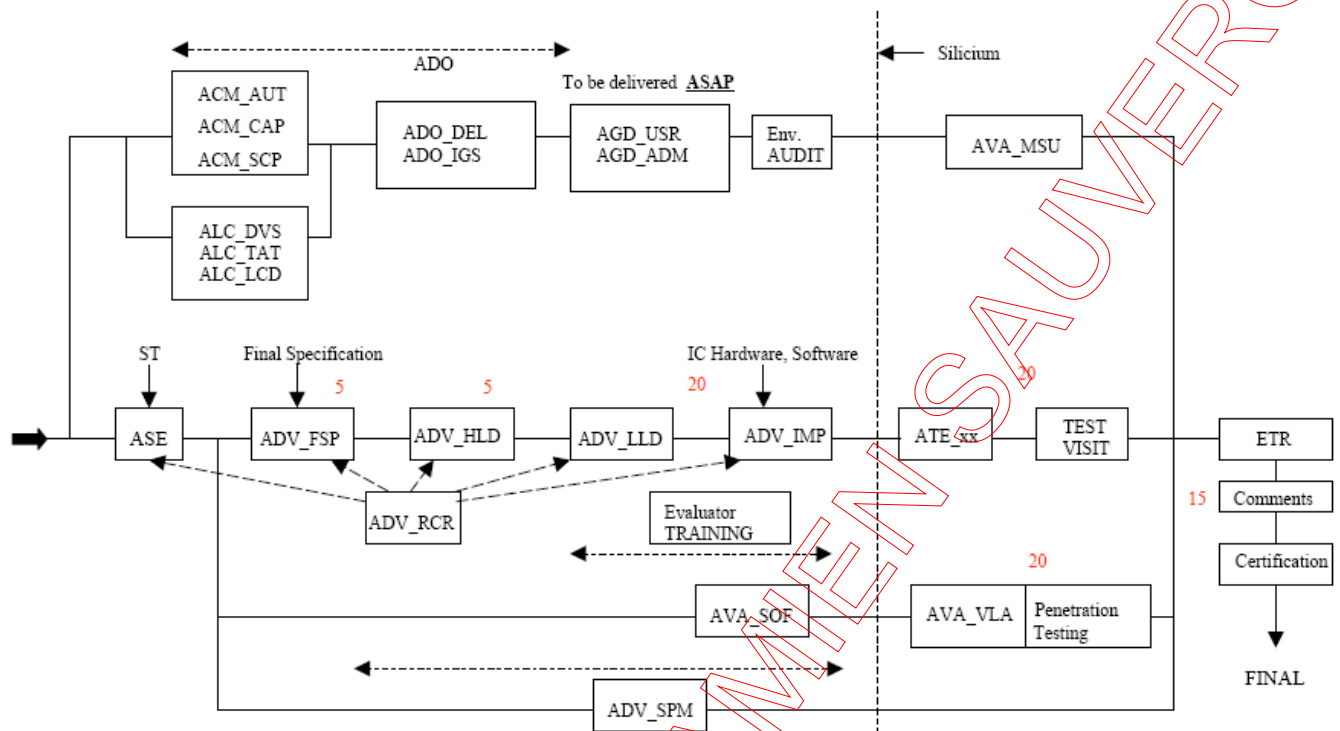
7: évaluation des documents d'exploitation  
AGD\_ADM.1  
AGD\_USR.1

8: estimation de la vulnérabilité  
AVA\_MSU.1  
AVA\_SOF.1  
AVA\_VLA.2

9: finalisation du RTE

90

# Evaluation Flow

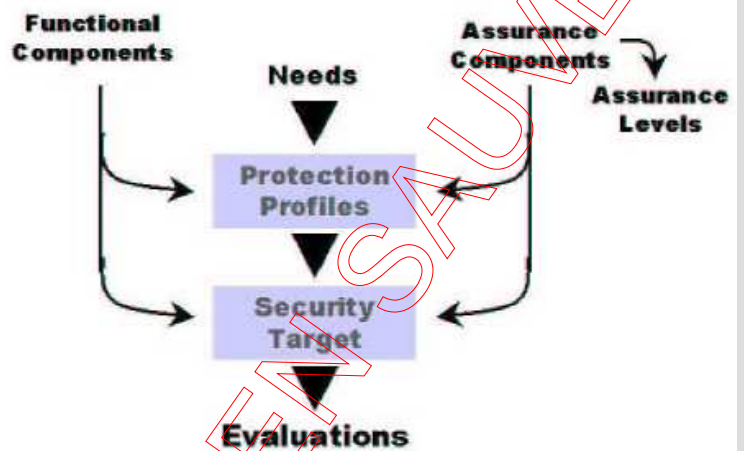
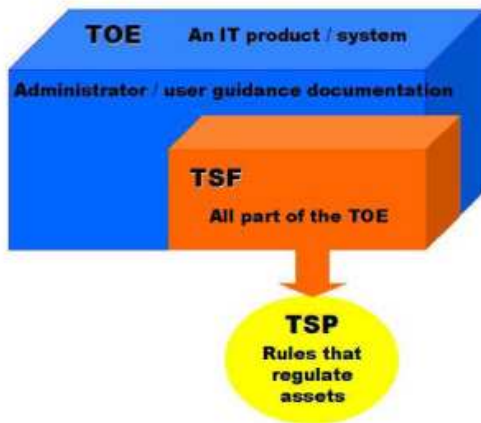


91

ON SWAPPE SUR MERLE.PDF p24

92

## Résumé



93

## Offre de produits et PP certifiés



### Offre de produits certifiés

Systèmes d'exploitation (19) : *Windows NT 4 SP3, Trusted Solaris, AIX, HP-UX, SCO, ...*

Cartes à puces (18) : *Cartes à mémoire, cartes multiapplicatives (Javacard, Multos), ...*

Lecteurs de cartes (28) : *Certification obligatoire en Allemagne*

Firewall (16) : *Netwall, Firewall-1, PLX, Gauntlet, Lucent, ...*

Bases de données (7) : *Oracle, Informix, Ingres, ...*

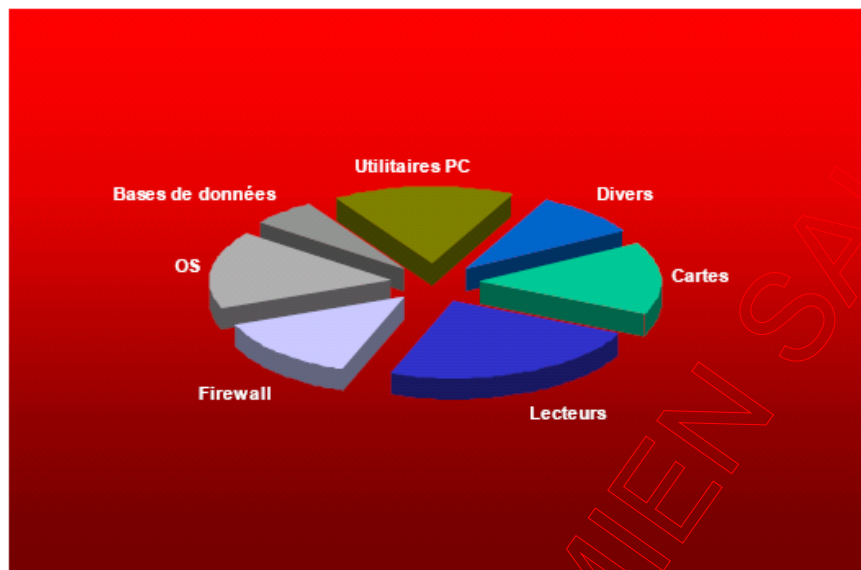
Utilitaires PC (19) : *Contrôle d'accès, utilitaires disques, ...*

Divers (11) : *Chiffrement, PKI, ...*

➔ [www.scssi.gouv.fr](http://www.scssi.gouv.fr)

Source : Certificats reconnus par le schéma français au 1er Jan. 2000

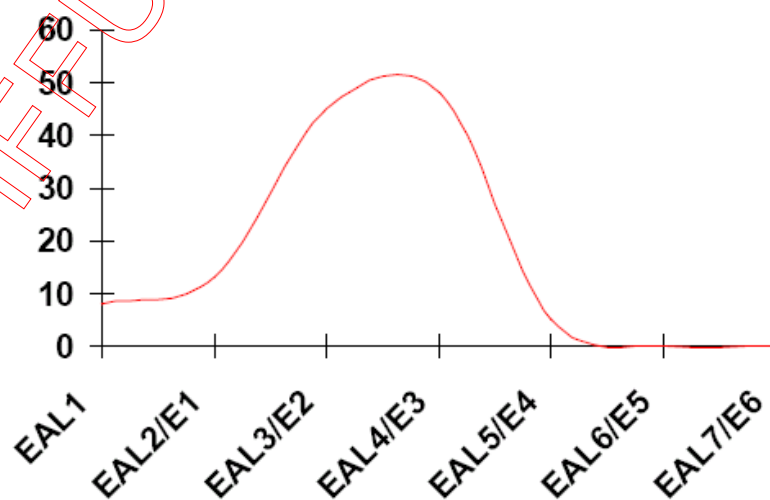
## Certificats : Domaines couverts



Source : Certificats reconnus par le schéma français au 1er Jan. 2000

95

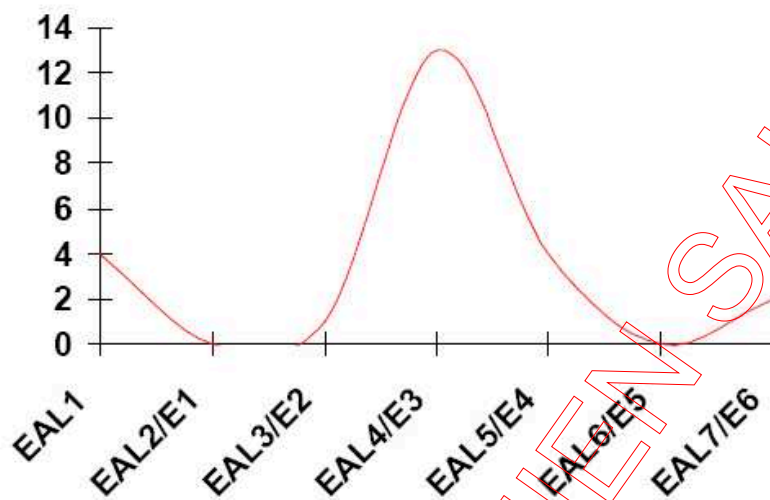
## Certificats : Répartition par niveau d'assurance



Source : Certificats reconnus par le schéma français au 1er Jan. 2000

96

## Cartes à puce certifiées



Source : Certificats reconnus par le schéma français au 1er Jan. 2000

## Offre de Profils de Protection

Cartes à puces : *Composants, applications, sites de production, ...*

Firewalls : *DGA, NIST/NSA*

Messagerie électronique : *SCSSI, MEFI*

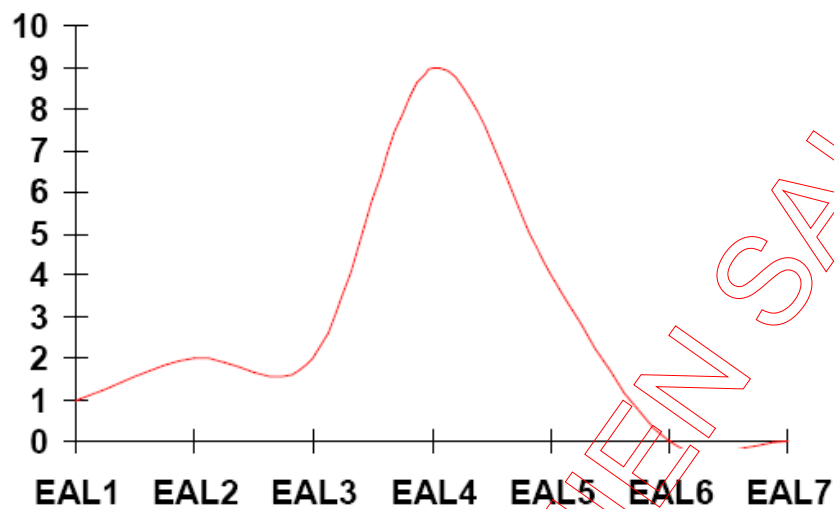
Bases de données : *Oracle*

Divers : *Contrôle d'accès, DAB, lecteurs de cartes, ...*

➔ [www.scssi.gouv.fr](http://www.scssi.gouv.fr)

Source : Certificats reconnus par le schéma français au 1er Jan. 2000

## PP : Répartition par niveau d'assurance



Source : Certificats reconnus par le schéma français au 1er Jan. 2000

99

## Un exercice de style : la rédaction de la Cible de sécurité



- ⊕ Choix du périmètre : commercial, réaliste ou rigoriste?
  - Frontière physique de la TOE
  - Hypothèses d'utilisation
    - « Les administrateurs sont de confiance et ont été formés »
    - « Les mots de passe sont aléatoires et sont formés de + de 7 caractères »
  - Menaces contrées
    - « Un individu peut effectuer une attaque en confidentialité sans connaissance des secrets »
- ⊕ Niveau d'assurance :
  - Garder en tête les fondamentaux : EAL2 = Qualité, EAL4 = Sécurité
  - Chercher ce qui se cache derrière le « + » de « EALx+ »
- ⊕ L'avenir : la conformité aux Profils de Protection (PP)

100

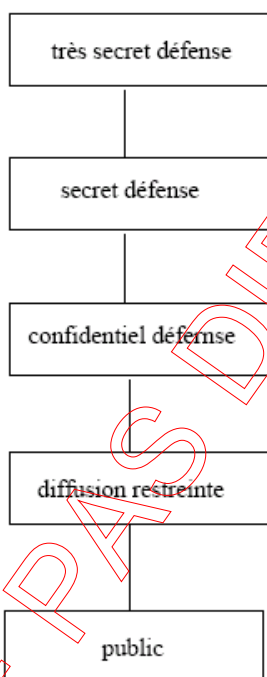
## Les limites du processus Critères Communs



- ⊕ La complexité du processus : trop long et trop coûteux
- ⊕ La difficile maintenance des certificats
  - Les procédures de surveillance sont inadaptées aux produits logiciels
  - Import de la notion américaine « assurance continuity »?
- ⊕ La complexité de l'interprétation des résultats d'une évaluation
- ⊕ L'impossibilité de composer les évaluations CC
- ⊕ L'impossibilité d'évaluer les systèmes complexes à un niveau décent

101

## Usage particulier en France des CC



- ⊕ Fondement de la PRIS (Politique de Référencement Intersectorielle de Sécurité)

- ⊕ Objectif : fournir à l'administration et au secteur privé un cadre opérationnel cohérent pour le traitement des informations sensibles et classifiées

- ⊕ Méthode : bâtir un catalogue de solutions qualifiées, sur la base de leur évaluation suivant les CC

| Sensibilité de l'information   | Niveau de qualification requis | Niveau CC requis |
|--------------------------------|--------------------------------|------------------|
| Sensible non classifié         | Niveau Standard                | EAL2+            |
| Classifié Confidentiel Défense | Niveau Renforcé                | EAL4+            |

102

## Critères Communs : les bonnes questions



Qu : Quelles parties du produit ont été analysées?

R : La TOE est décrite dans la Cible de Sécurité

Qu : Quelle confiance accorder aux vérifications effectuées?

R : Une totale confiance en terme de qualité (agrément COFRAC)

Qu : Quels sont les documents publics associés aux certifications?

R : Le rapport de certification et la cible de sécurité

Qu : Où trouve t-on ces documents?

R : Sur [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org) ou [www.ssi.gouv.fr](http://www.ssi.gouv.fr)

103

## Classification des attaques

Les attaques se font par rapport aux propriétés non fonctionnelles :

Confidentialité :

L'objectif est d'obtenir des informations.

Intégrité :

L'objectif est de changer, supprimer ou ajouter des informations.

Disponibilité :

L'objectif est de rendre le dispositif inutilisable par suite de très nombreuses requêtes.

104

# Les types d'attaques

## ● Les attaques physiques :

- Microprobing
- Electromagnétisme,...

## ● Les canaux cachés :

- Observations précises du comportement en mode en fonction du dispositif,
- Les observations peuvent porter sur le temps, la consommation,...

## ● Les attaques par injection de fautes,

## ● Les attaques logicielles :

- Virus, Chevaux de Troie,...

105

## Différentes catégories

### Non invasives

Le produit reste fonctionnel

### Invasives

Le produit est partiellement endommagé

106

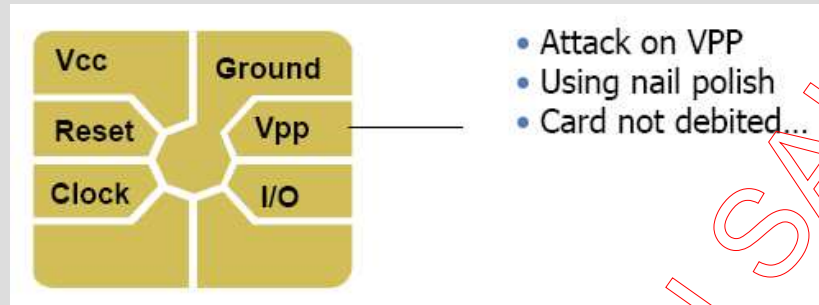
## Non invasives

modification des conditions opérationnelles (Vcc, F)

modification de la température

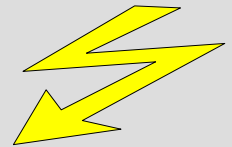
modification des rayonnements lumineux (UV, rayon X, lumière blanche, IR, ...)

injection de fautes (glitches, rayonnements lumineux)



(injection de fautes sur la JVM : <http://www.cs.princeton.edu/~sudhakar/papers/>)

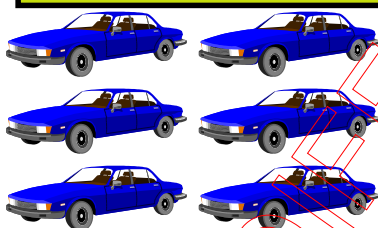
attaques sur les canaux cachés



107

## ARE WE DONE?

Broken toys are not charged to our clients



car = \$3



plane = \$5

Jack

How will you pay?

I'll send \$15  
by postal order

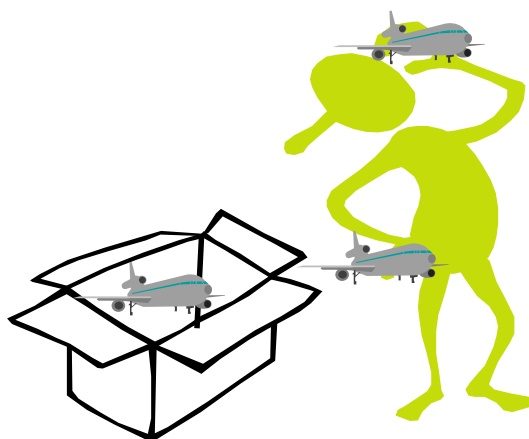
Dino

Dino buys toys from Jack

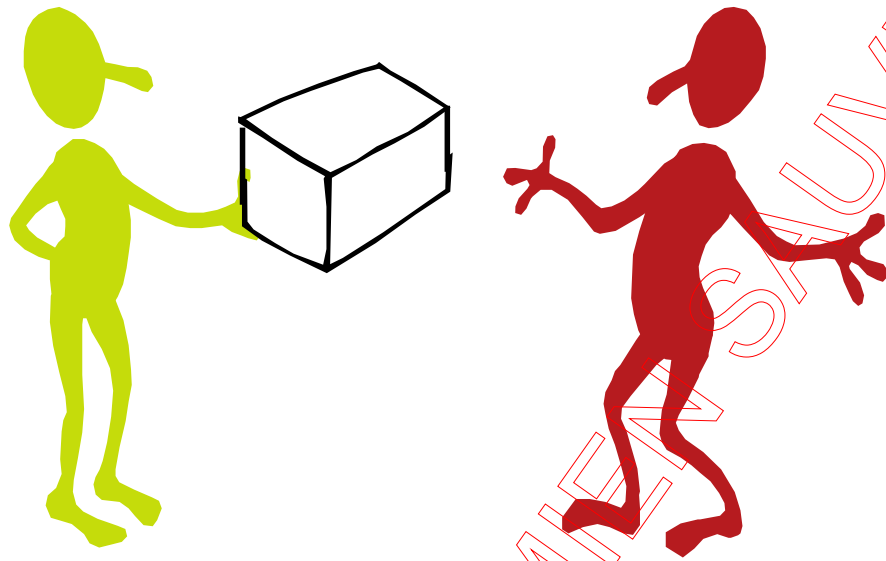
*The postman wants to know what  
Dino bought for \$15*



*In the meanwhile Jack prepares  
the DHL*



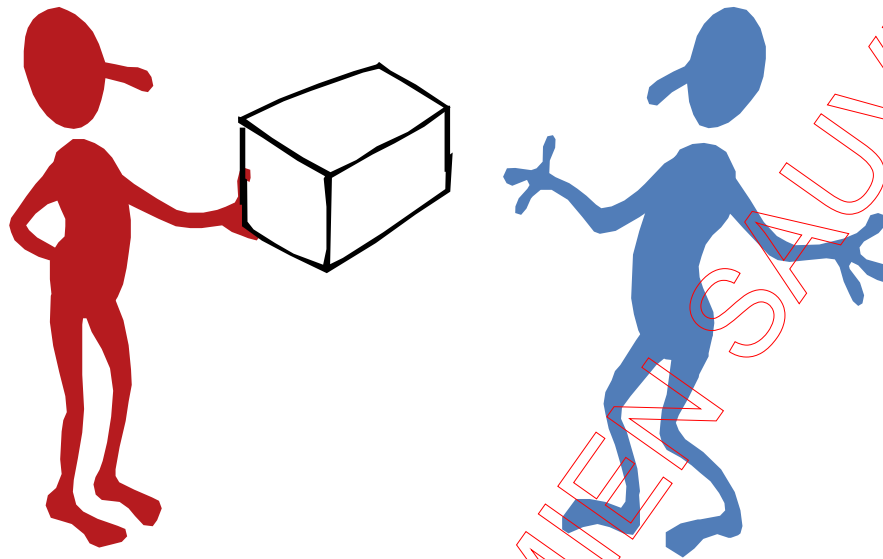
*and gives it to the postman*



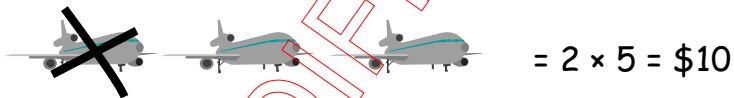
*Who kicks it strong enough to  
break one toy*



*and gives it to Dino*



*a week later he monitors Dino's  
postal order...*



**Lesson learned:** **Fault attacks** can also extract secrets from tokens!

Hardware faults can have various sources:  
voltage glitches, light beams, laser beams...

## Attaques software/hardware

Pour forger des pointeurs et ensuite ...



<http://www.cs.princeton.edu/~sudhakar/papers/memerr-slashdot-commentary.html>

115

## Les canaux cachés

### le temps d'exécution

=> nombre de cycle d'une instruction ou d'un algorithme.

### la consommation de courant

=> Les modifications rapides de la tension et de l'intensité du courant au sein du même composant sont à la base des émissions du circuit car ils conduisent des courants RF à l'intérieur et à l'extérieur du chip.

### les émissions électromagnétiques

=> Les courants RF entraînent un rayonnement électromagnétique.

116

## La “timing attack”

Cette attaque consiste à mesurer le temps d'exécution d'un algorithme.

=> Révèle des informations sur les opérations et/ou les opérandes.

Nécessite souvent :

un grand nombre d'exécution à messages choisis,  
un traitement statistique des résultats obtenus.

117

## A GAME

- You put \$28 in one of the pots and \$10 in the other:



- I ask you to multiply the contents of the blue pot by 10 and the contents of the red pot by 7, add the two results and tell me if the sum is odd or even.
- Is your answer enough to reveal what's in each pot?

# IS THIS A MEANINGFUL GAME?

- Well, normally not :

$$28 \times 7 + 10 \times 10 = 296$$

is an even number

and

$$10 \times 7 + 28 \times 10 = 350$$

is also even...

- However, just by monitoring the time it takes to give the answer (the mental calculation leading to 296 is more complicated than the one leading to 350) one can tell where each amount is!

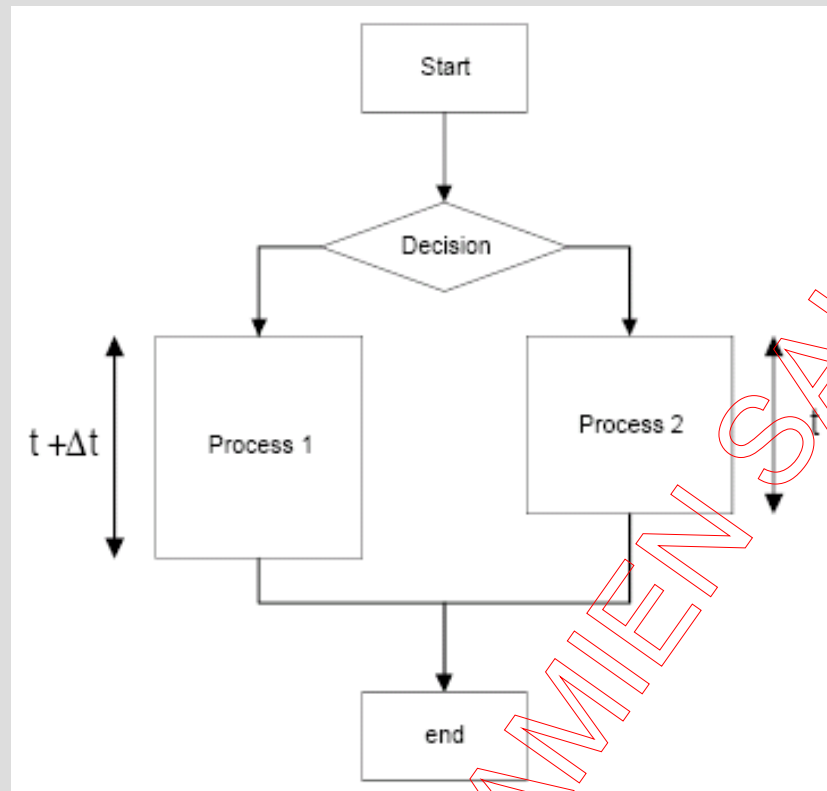
## CONCLUSION

The external monitoring of the processing time of a card may leak secrets to the external world (e.g. credit keys, PINs etc).

**Timing attacks** were exposed in the early 1990's.

Lesson learned: **Current card software runs in constant time**

## La “timing attack”



121

## La “timing attack” sur le PIN (1/2)

```
for ( i = 0 ; i <= 7; i++)  
    if ( pinCarte [ i ] != pinPresente [ i ] )  
        return false ;  
return true ;
```

**Présentons un PIN quelconque et déroulons le programme :**

cas du premier octet FAUX  
i = 0  
i <= 7 ? NON  
( pinCarte [ i ] != pinPresente [ i ] ) ? OUI  
return false

cas du premier octet VRAI  
i = 0  
i <= 7 ? NON  
( pinCarte [ i ] != pinPresente [ i ] ) ? NON  
i++  
i <= 7 ? NON  
( pinCarte [ i ] != pinPresente [ i ] ) ? OUI  
return false

122

## La “timing attack” sur le PIN (2/2)

```
for ( i = 0 ; i <= 7; i++)  
    if ( pinCarte [ i ] != pinPresente [ i ] )  
        return false ;  
return true
```

**Présenter les n valeurs possibles de pinPresente[0] (256 valeurs) (n,0,0,0,0,0,0,0).**

Mesurer la durée d'exécution de la commande T pour les n valeurs.

Calculer T[n0] le maximum des T

–  $T[n0] = \max(T[n]); n = 0; \dots; 255$

n0 est la solution pour pinCarte[0]

**Itérer sur tous les pinPresente[i]**

**Nombre d'essais :  $8 * 256 = 2048$  (contre  $256^8$  en force brute)**

123

## Exemples de protection (1/2)

```
alea = random ( 0 , 7 ) ; // alea situe dans l'intervalle [0 ; 7]  
for ( i = 0 ; i <= 7; i++) {  
    octet = ( alea + i ) mod 8 ;  
    if ( pinCarte [ octet ] != pinPresente [ octet ] )  
        return false ;  
}  
return true ;
```

**Nombre d'essais en moyenne :  $8 * 2048$  (contre  $256^8$  en force brute)**

**Possibilité d'attaque de type MasterMind.**

124

## Exemples de protection (2/2)

```
boolean test = true ;  
for ( i = 0 ; i <= 7; i++) {  
    test = test ;  
    if ( pinCarte [ i ] != pinPresente [ i ] )  
        test = test && false ;  
    else  
        test = test && true ;  
}  
return test ;
```

équivalent à :

```
boolean test = true ;  
for ( i = 0 ; i <= 7; i++)  
    test = test && ( pinCarte [ i ] == pinPresente [ i ] ) ;  
return test ;
```

125

## La consommation de courant

Elle est surtout utilisée dans le domaine de la cryptographie.

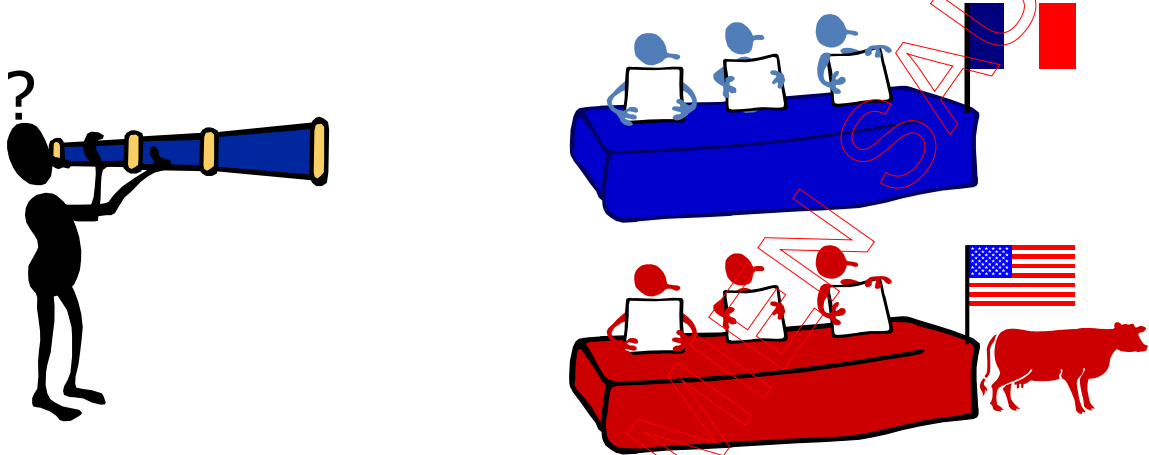
Il existe différentes attaques :

- la SPA (Simple Power Analysis)
- la DPA (Differential Power Analysis)
- la HODPA (High Order Differential Power Analysis)

126

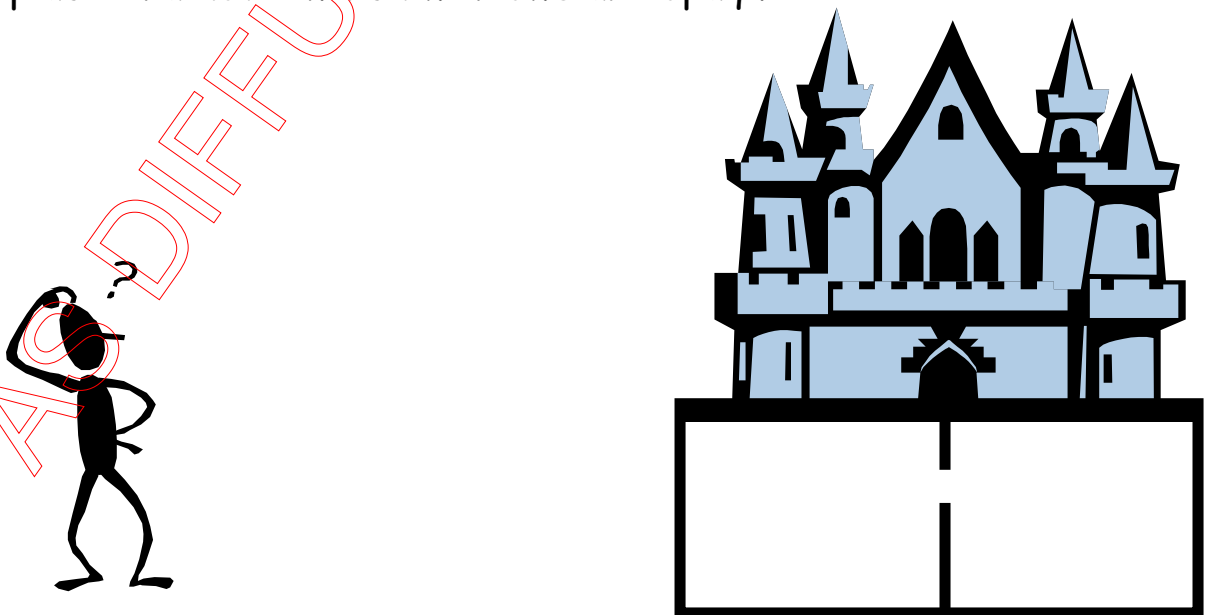
## IMPORTING THE BEEF?

- Seattle, 1999.
- US and French delegates negotiate under which conditions beef could be imported to France.
- «The Sun» sends a journalist to investigate:



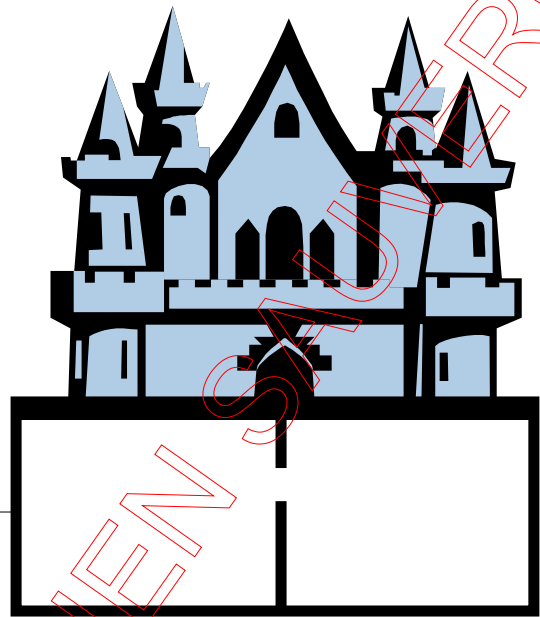
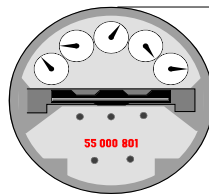
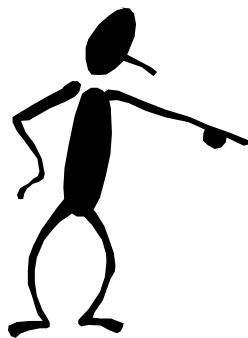
## IMPORTING THE BEEF?

- But there is a technical problem: negotiations take place in a hotel which windows are opaque



# POWER ATTACKS

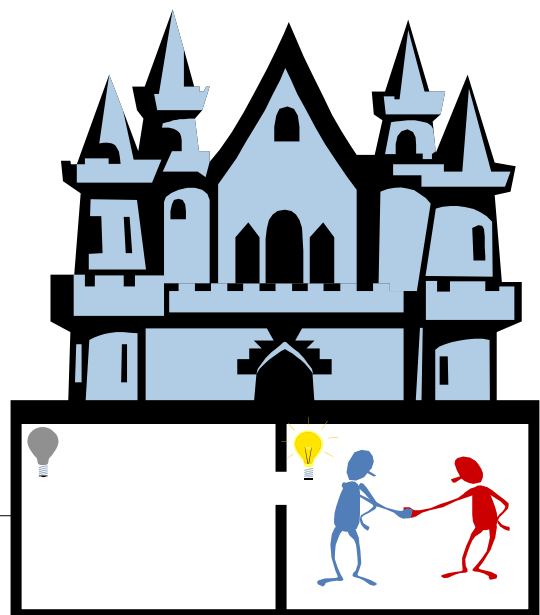
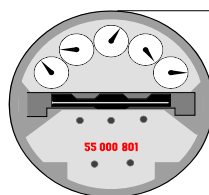
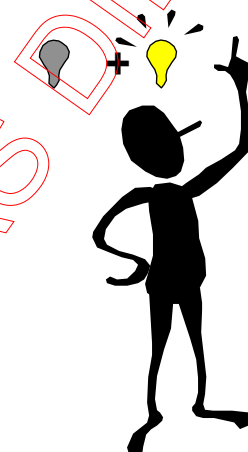
- Idea: look at the hotel's electricity meter!



# POWER ATTACKS

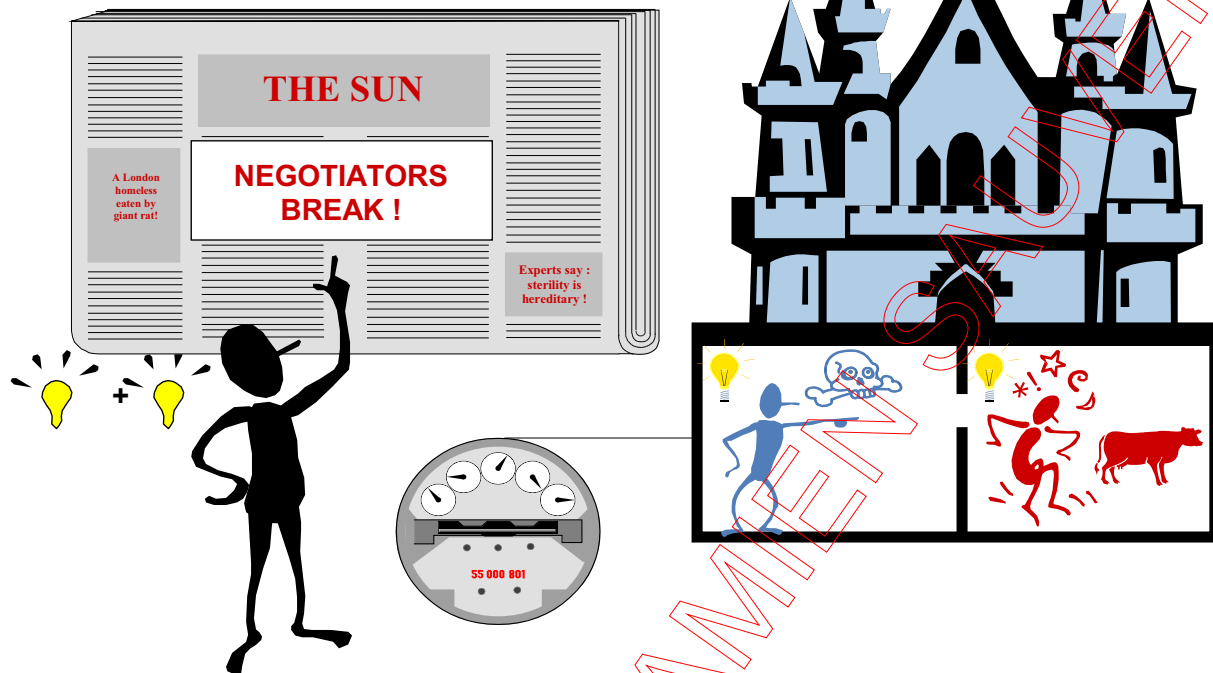
- disk is spinning slowly:

DEAL CONCLUDED



# POWER ATTACKS

- But if the disk is spinning quickly:



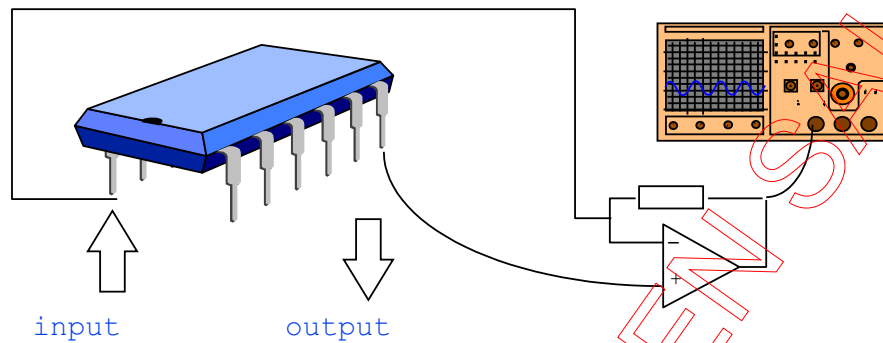
## Le matériel

- un oscilloscope numérique,
- un lecteur de carte à puce,
- un pc équipé de cartes d'acquisition et de logiciels mathématique pour le traitement des données,
- une sonde CEM si on veut étudier les émissions électromagnétiques.

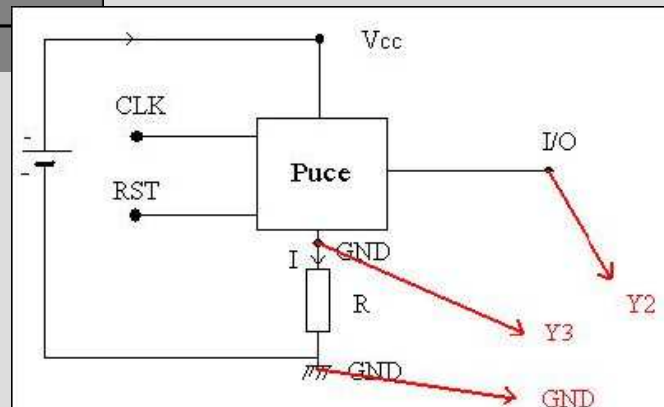
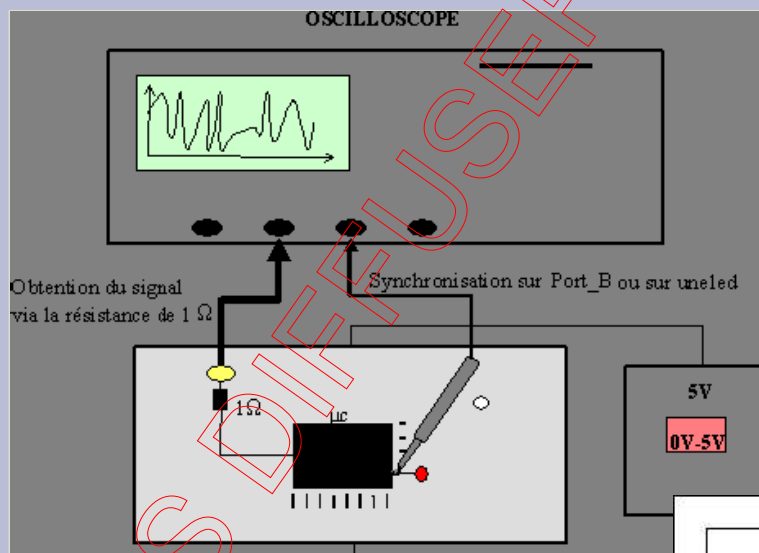


# CONCLUSION

The card's current consumption may reveal secret information.

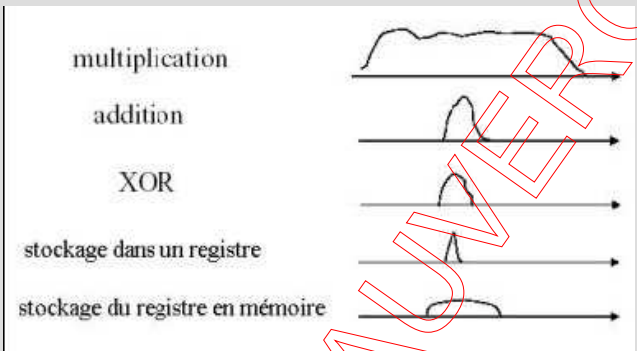


## Le montage pour suivre la consommation en courant

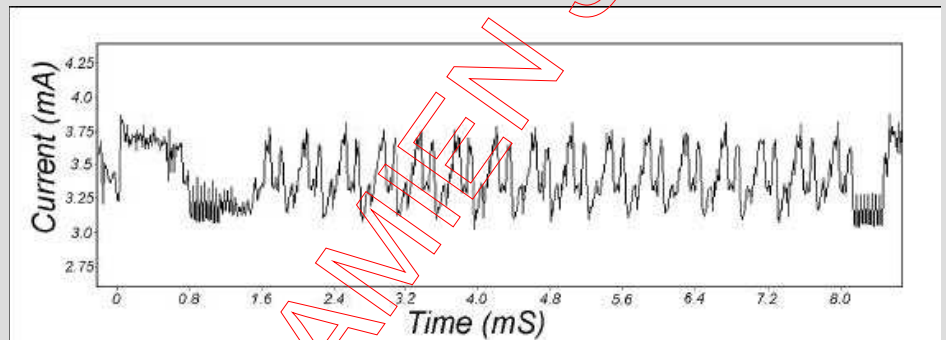


## La SPA (Simple Power Analysis)

Principe : Des instructions différentes ont une trace différente.



Consommation en courant d'un DES. On peut voir la permutation initiale, suivie des 16 tours.



135

## La SPA sur la signature RSA

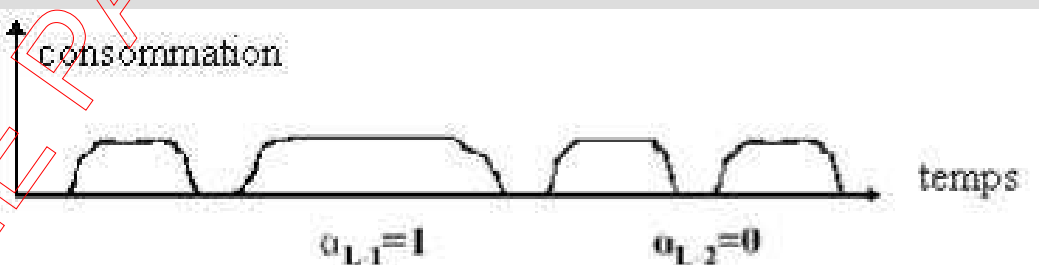
```
s = 1 ;  
for ( i = L - 1 ; i >= 0 ; i-- ) {  
    s = s*s mod n ;  
    if ( a [ i ] == 1 )  
        s = s*y mod n ;  
}
```

Signature RSA :  $y^a \bmod n$

y est le message à signer,

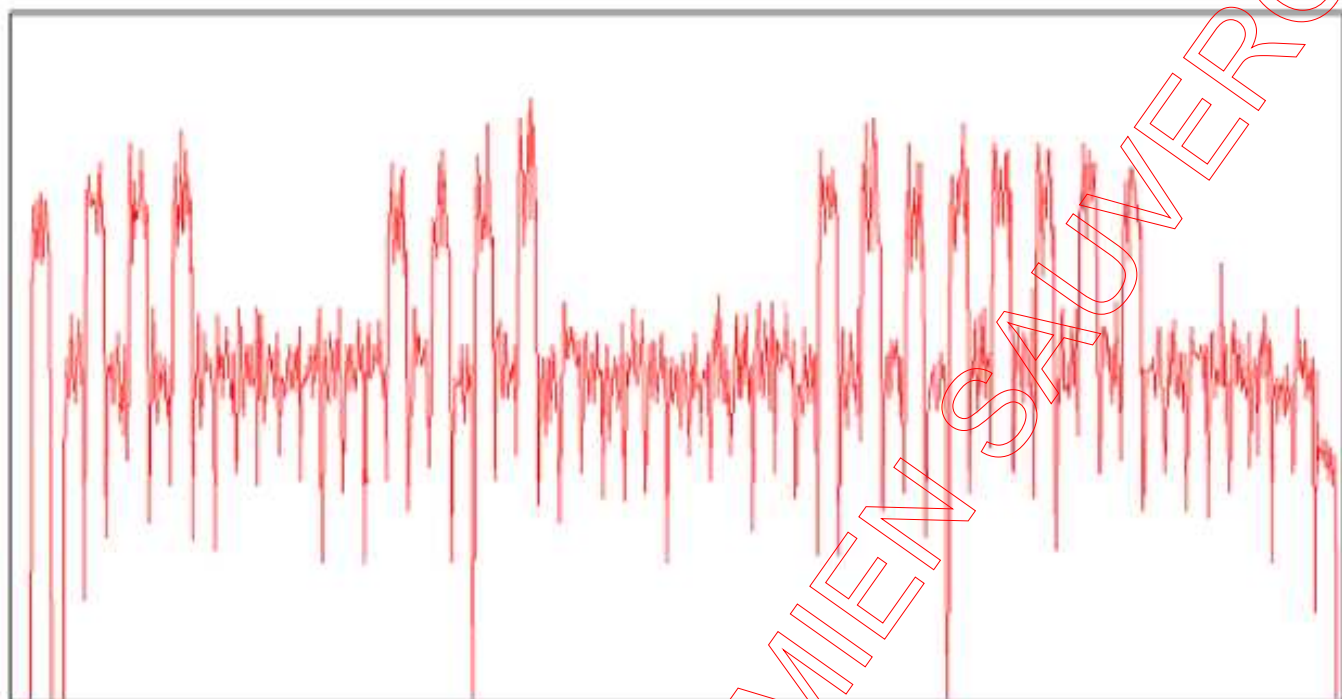
n est public,

a, l'exposant peut être considéré comme la clé secrète.



136

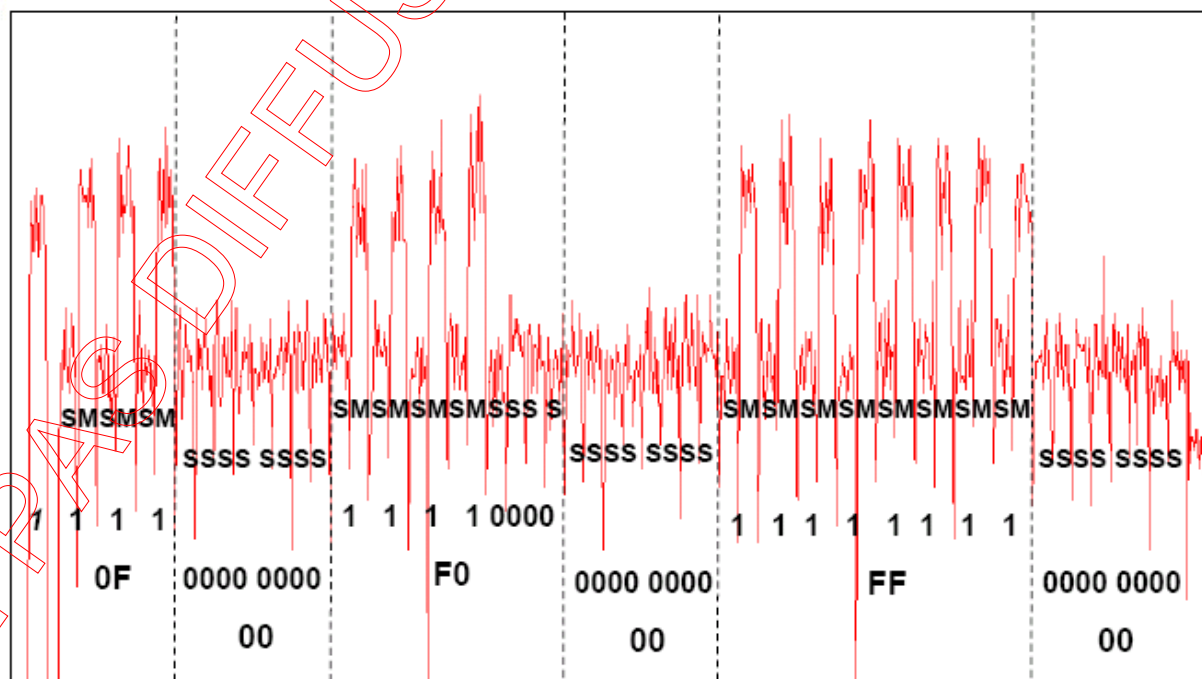
## Exemple « réel »



137

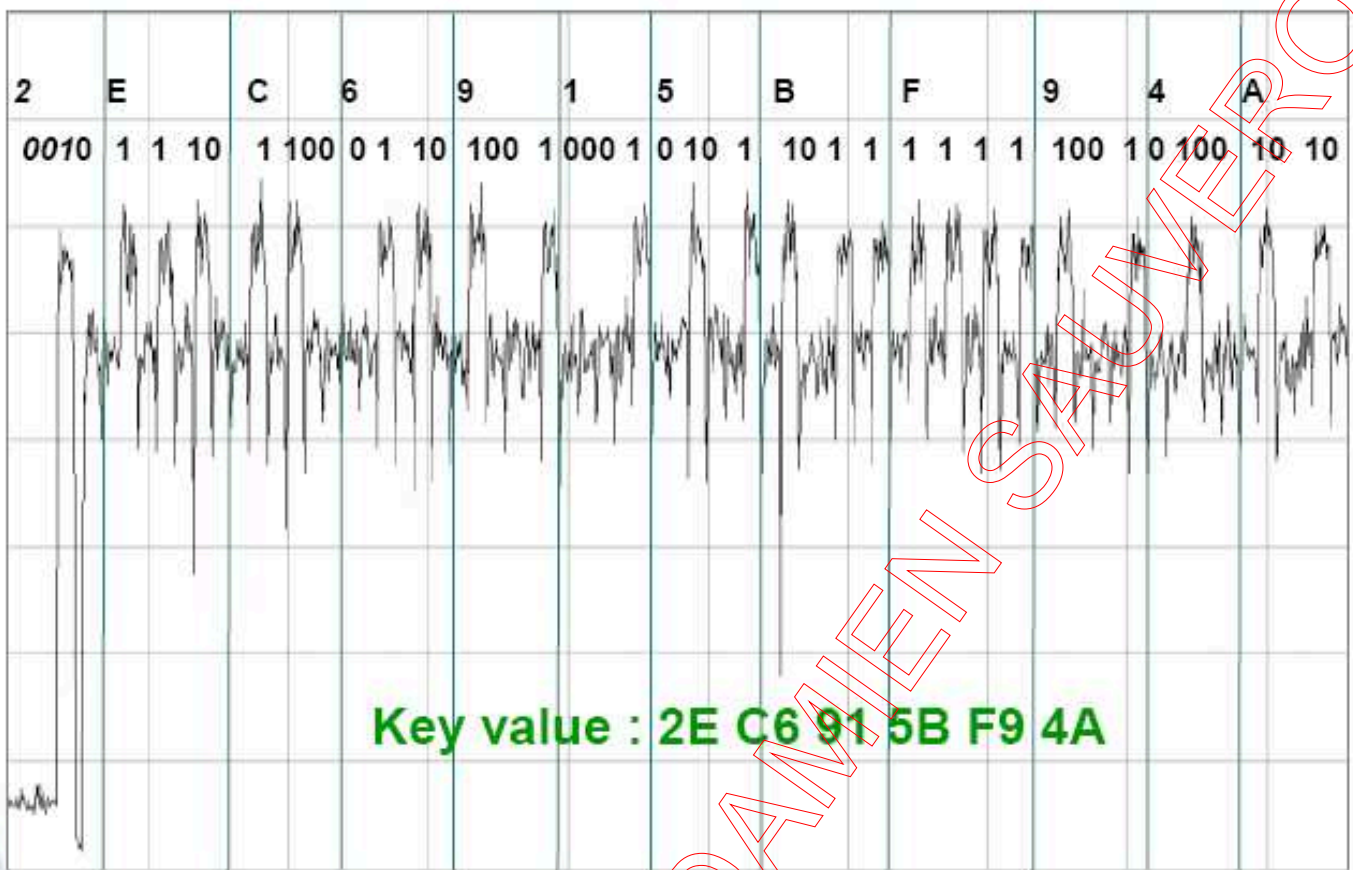
## Exemple « réel »

Test key value : 0F 00 F0 00 FF 00



138

## Exemple « réel »

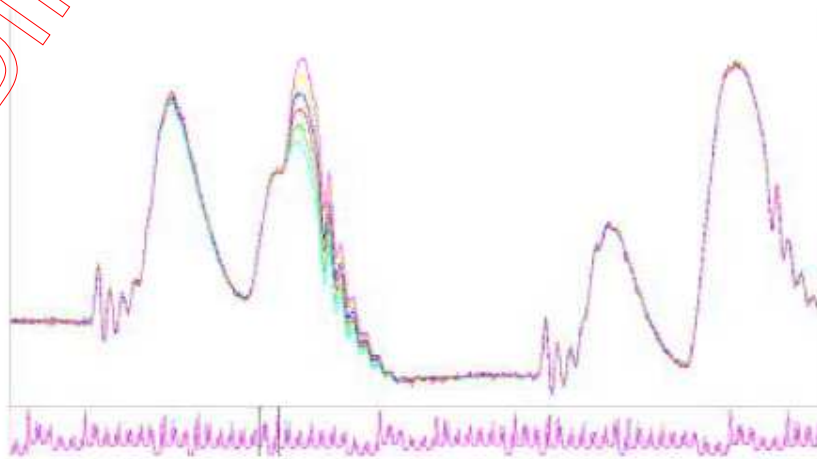


## La DPA (Differential Power Analysis)

**Principe :** La consommation dépend des opérations effectuées (les instructions) mais aussi des opérandes.

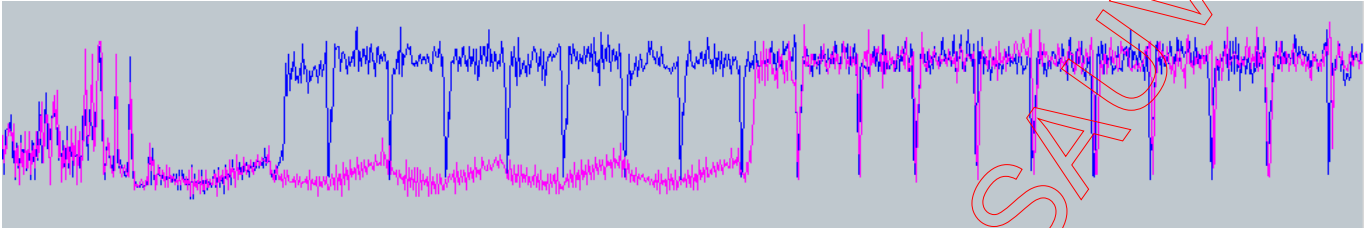
Elle utilise des fonctions statistiques adaptées à l'algorithme visé qui font ressortir des corrélations entre un bit intermédiaire  $a$  (ne dépendant que d'un fragment  $Kr$  de  $r$  bits de la clé et du message d'entrée  $M$ ) et la consommation de courant.

- Based on SPA  
Adding the power of statistics to separate signal from noise



## CONCRETE ATTACK ON CONCRETE KEYS

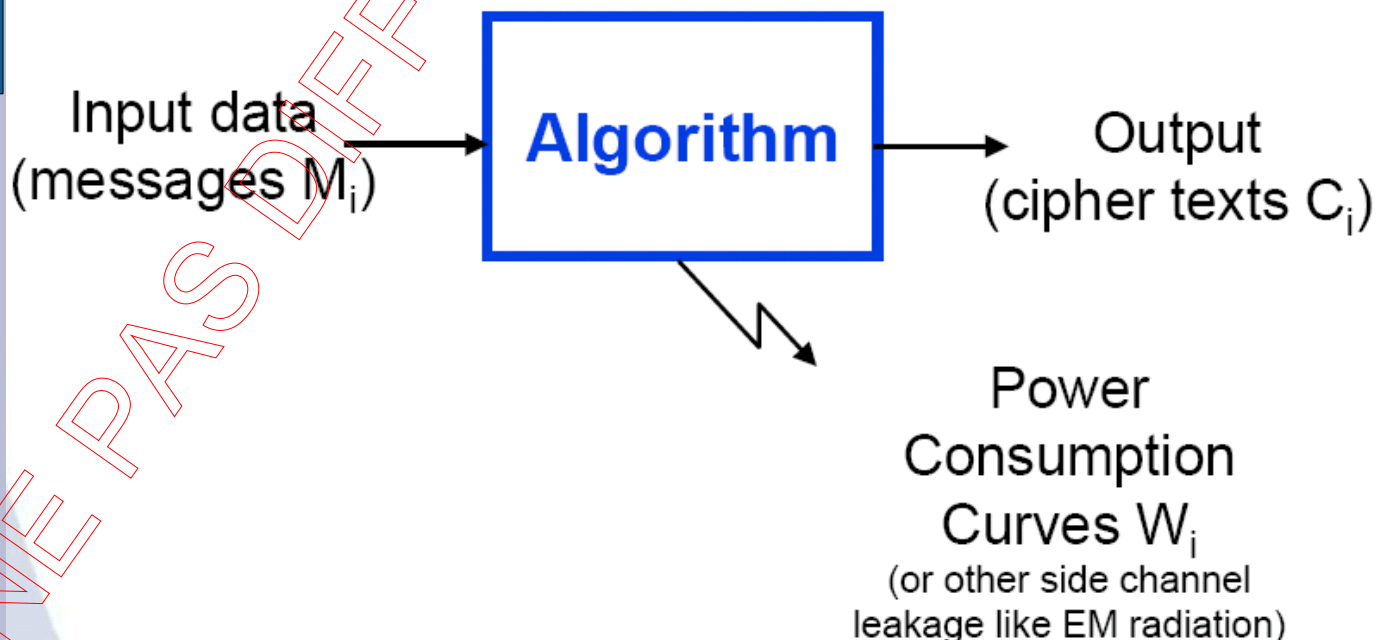
- Comparing:
  - decryption with key = 0000 1111 ...
  - decryption with key = 1111 1111 ...



token designed and manufactured in 1998...

## DPA Hypothesis

Play the algorithm N times  
( $100 < N < 100000$ )



# Acquisition procedure

- After data collection, what is available ?

- N plain and/or cipher random texts

00

**B688EE57BB63E03E**

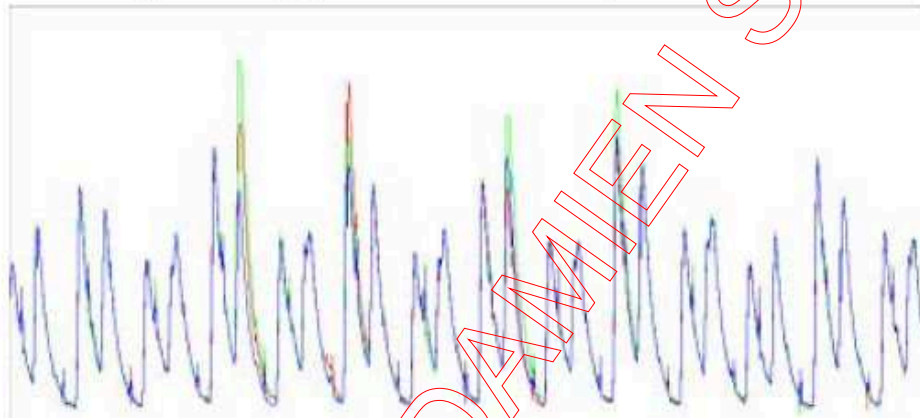
01

**185D04D77509F36F**

02

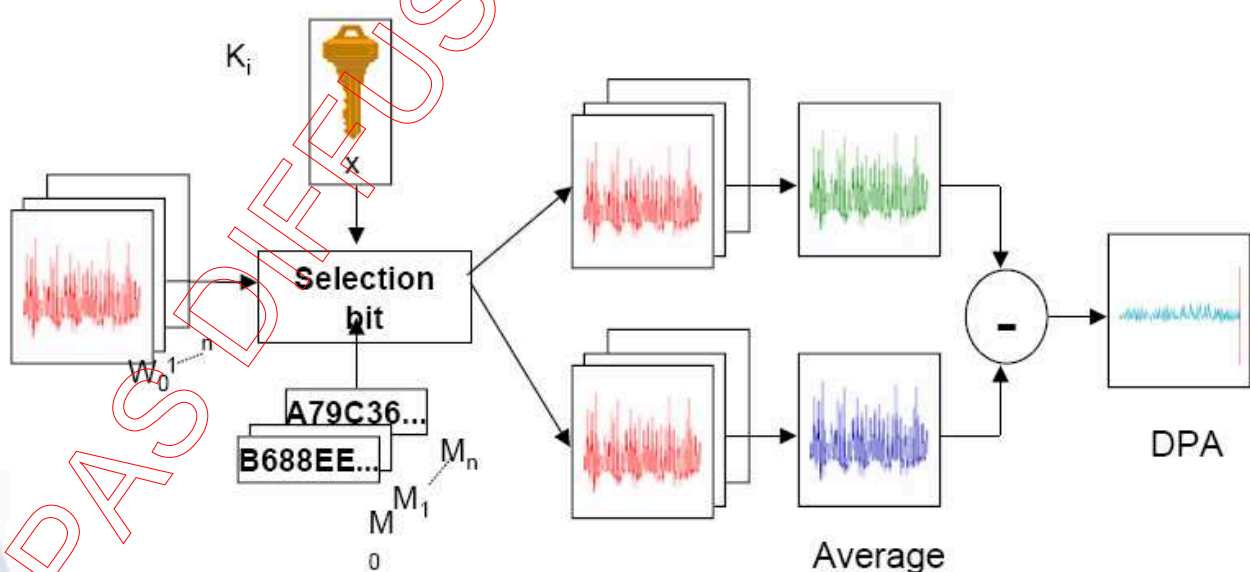
**C031A0392DC881E6 ...**

- N corresponding power consumption waveforms



143

## Hypothèse et test



144

## La HODPA (High Order DPA)

La HODPA ou DPA d'ordre  $n$  est aussi basée sur une étude statistique de la consommation de courant de la carte.

Différence : elle utilise des corrélations entre la consommation de courant et  $n$  variables intermédiaires ne dépendant que d'un fragment de la clé et du message d'entrée.

Elle est beaucoup plus difficile à réaliser, mais beaucoup plus puissante.

145

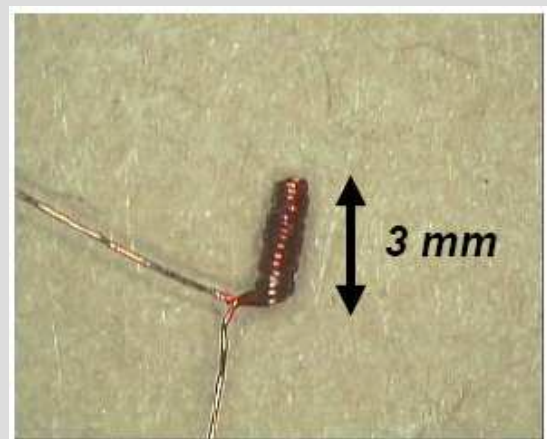
## Les émissions EM

Principe : Les courants qui circulent dans la puce induisent des champs électromagnétiques qui sont susceptibles de donner le même type d'information que le courant.

Différence : L'information est plus locale. On peut déplacer la micro-sonde électromagnétique au dessus de la zone qui nous donnera le plus d'informations (exemple : co-processeur cryptographique).

Avantage : Insensible aux contre-mesures physiques tels que l'ajout de bruit en sortie ou le lissage de la consommation globale de courant.

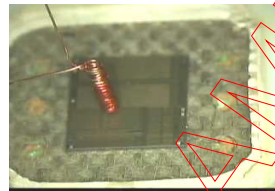
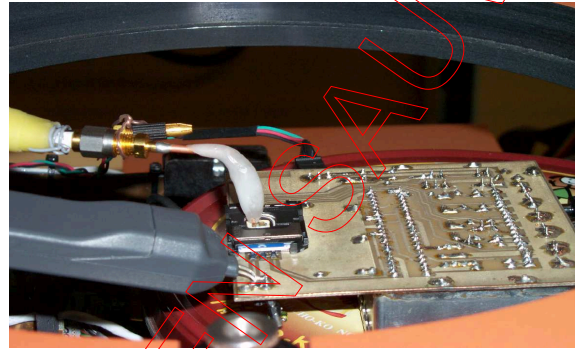
Inconvénient : La reproductibilité des mesures est difficile.



146

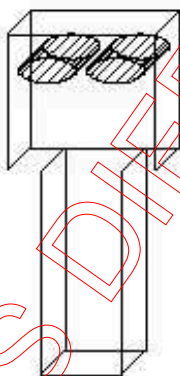
# COUNTER-COUNTER MEASURE

- Against *adding noise to the power consumption signal*.
- Capture electromagnetic radiation at various chip locations!
- Equipment:



## Le dispositif de cartographie EM

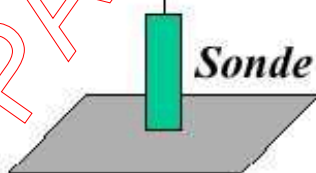
**Binoculaire**



**Oscilloscope**

**Traitement des  
signaux avec  
MATLAB**

**Sonde**

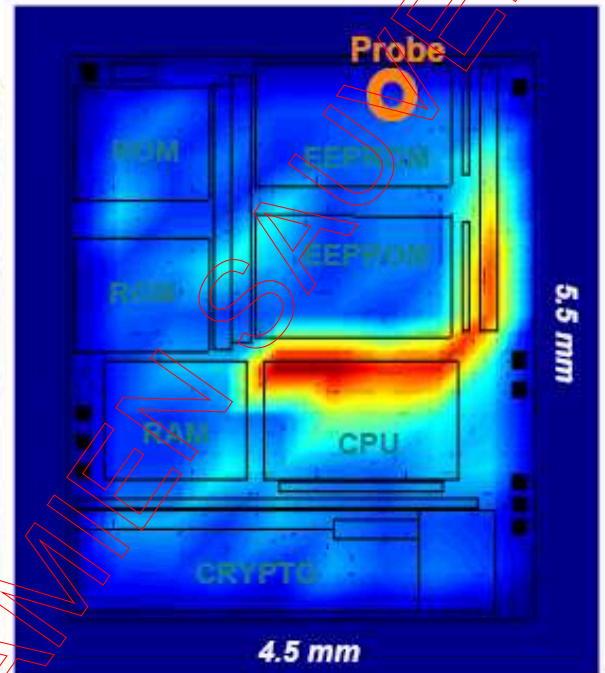
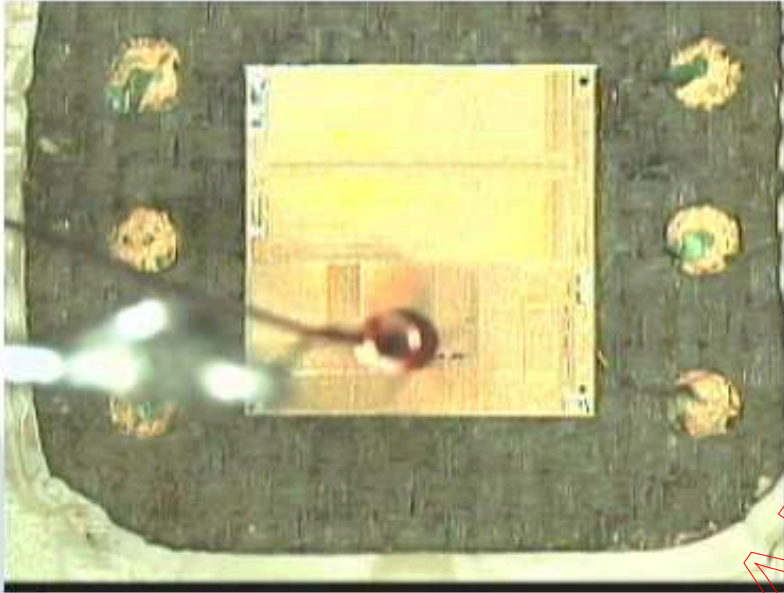


**Produit**

**Préamplificateur R&S  
CPA9231A (30dB)**

## Le dispositif de cartographie EM

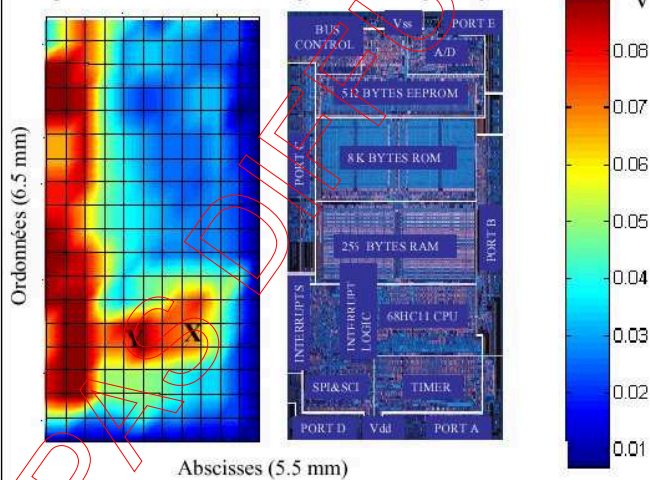
- Horizontal cartography (XY plane)
  - to pinpoint instruction related areas
  - better if automated



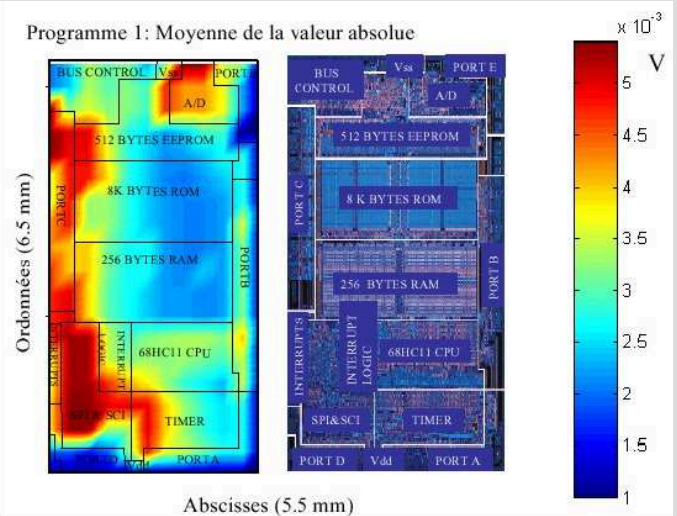
149

## Cartographie pour l'algo 1

Programme 1: Maximum en amplitude de chaque acquisition

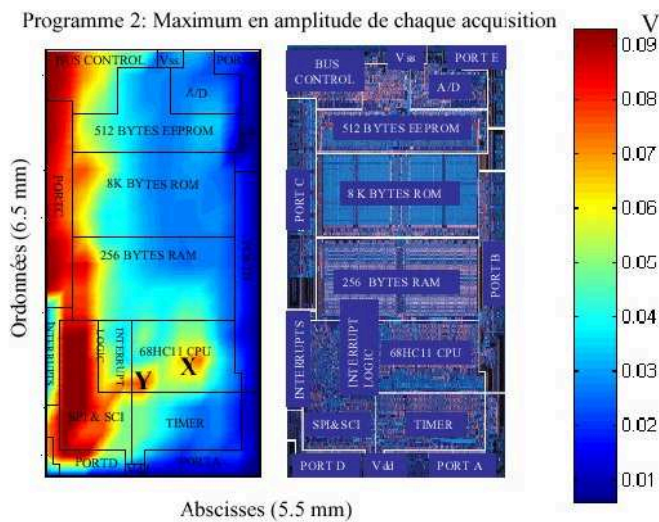


Programme 1: Moyenne de la valeur absolue

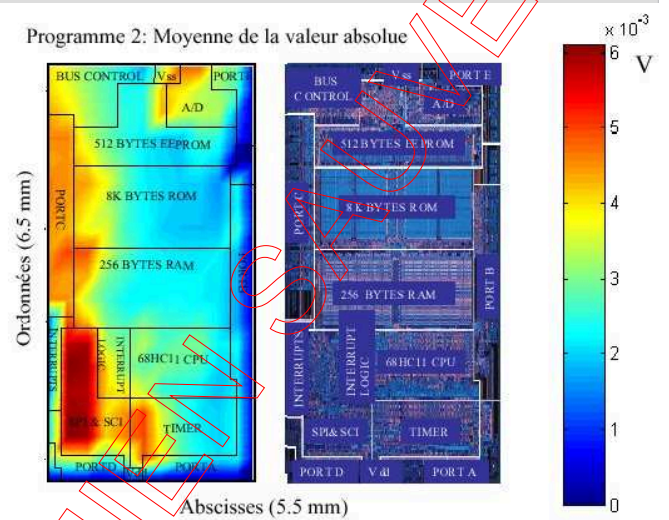


## Cartographie pour l'algo 2

Programme 2: Maximum en amplitude de chaque acquisition



Programme 2: Moyenne de la valeur absolue

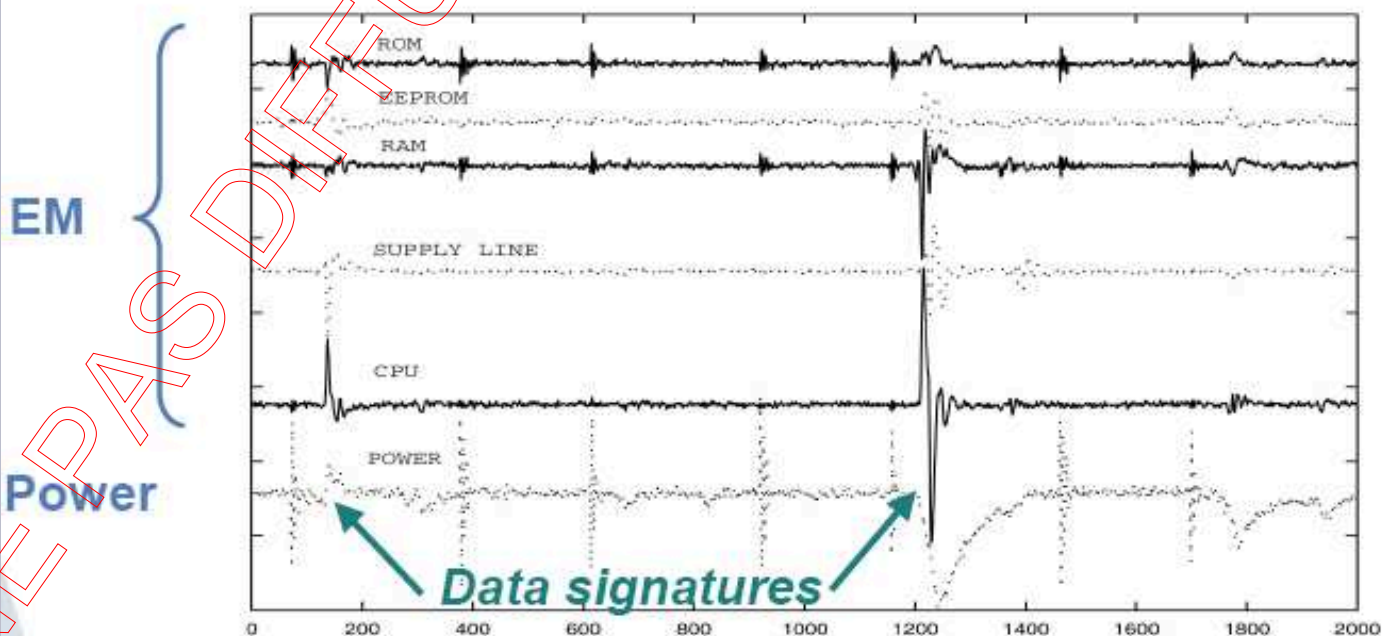


151

## Différence EM/Power

### • EM signals versus XY probe position

Differential traces between (00h  $\oplus$  00h) and (FFh  $\oplus$  00h) picked up at different locations



152

## Attaques EM

la SEMA (Simple EM Analysis)

la DEMA (Differential EM Analysis)

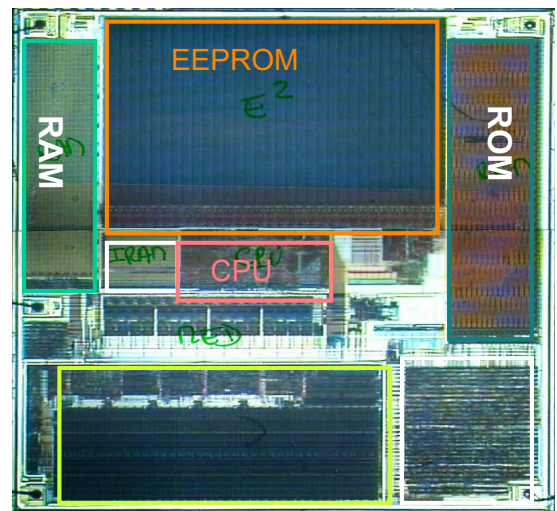
=> nécessite moins d'acquisitions

153

*LESSON LEARNED: SHIELD IT!*

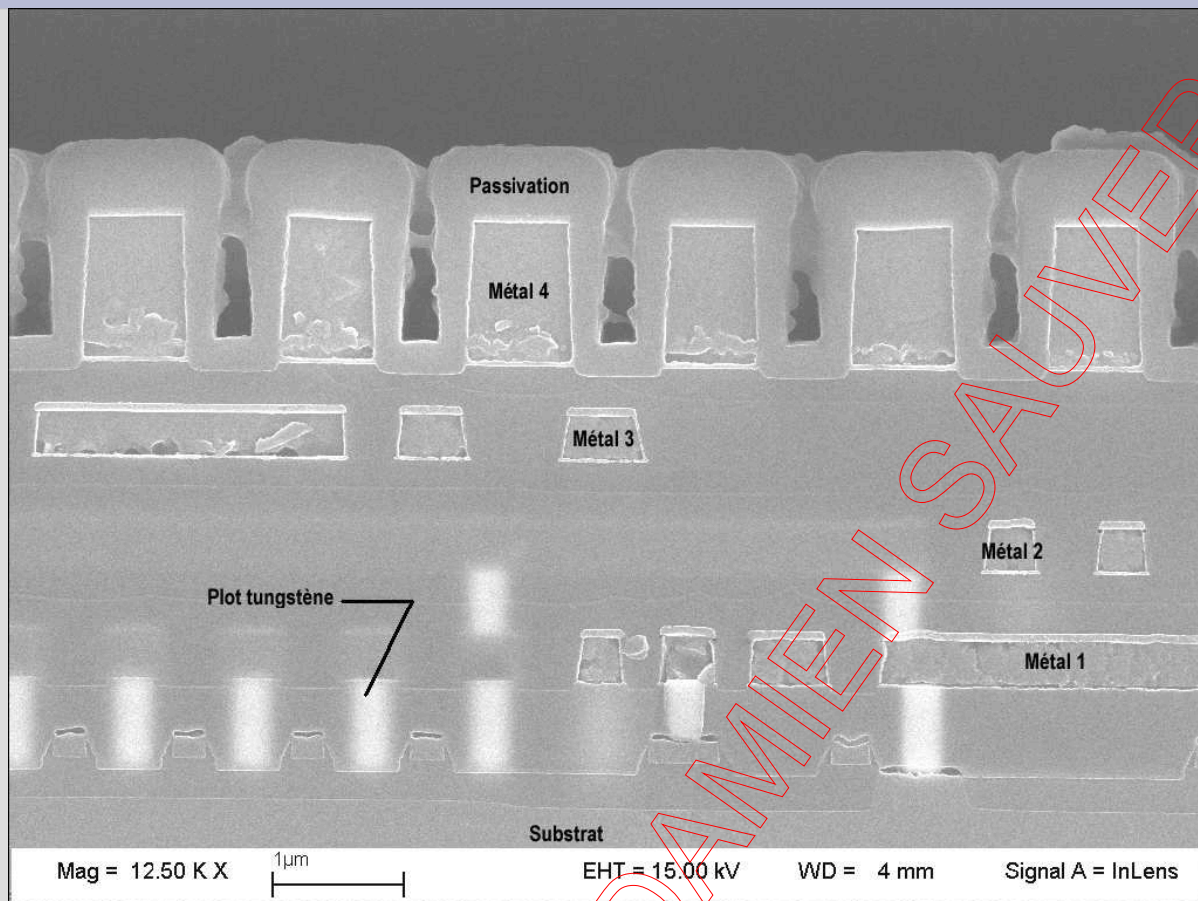


- Shield
- Scrambled glue logic
- No Buses visible



- Blocks easily identified
- No shield
- No glue logic
- Buses clearly visible

## La coupe d'une puce

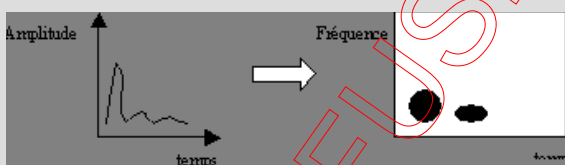


155

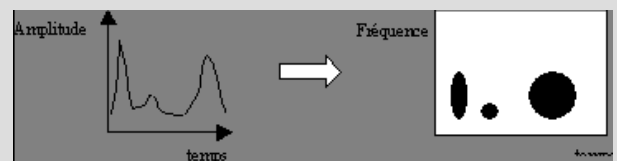
## La rétro-conception logicielle

méthode du « dictionnaire » :

Une instruction :



Une autre instruction :



- La séquence des deux :



Utilisation possible de la consommation en courant ou des émissions EM.

Statut : recherches en cours.

156

## Invasives

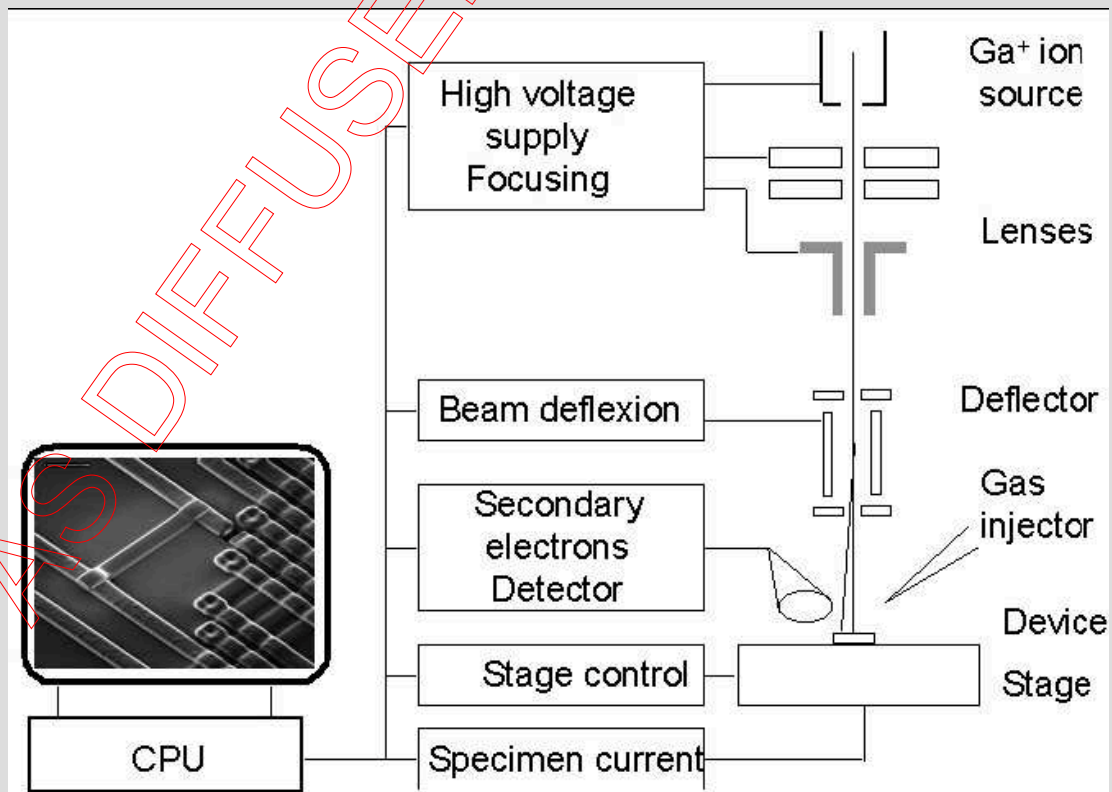
micro-probing

modification de circuit (FIB)

réetro-conception du circuit

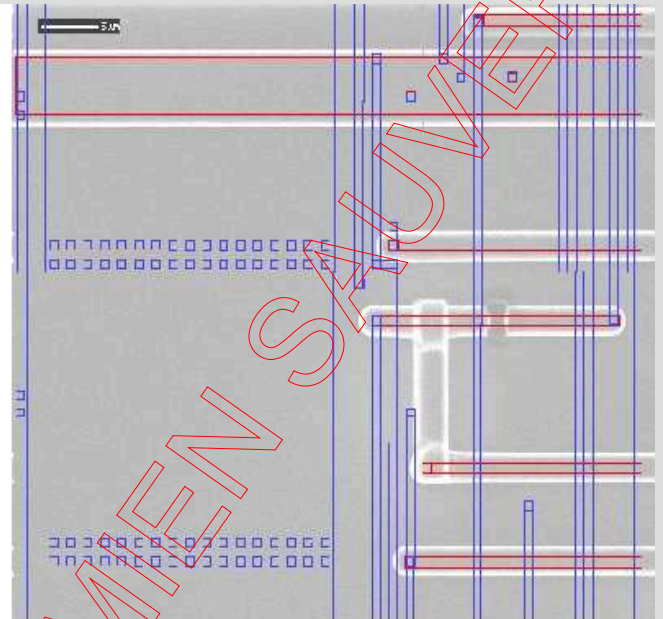
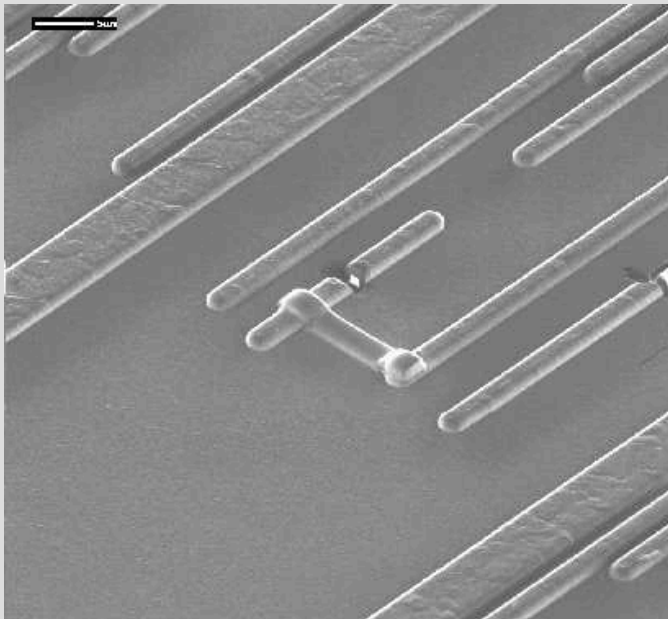
157

## Le FIB (Focused Ion Beam)



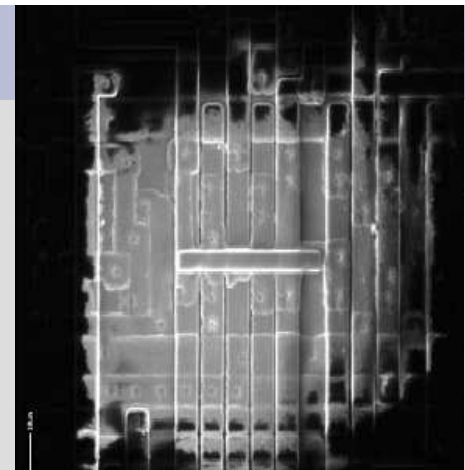
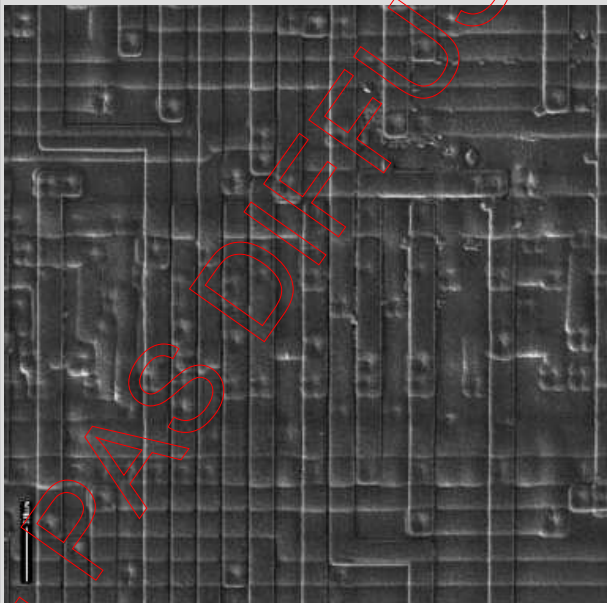
158

## Modifications de circuits (1/2)



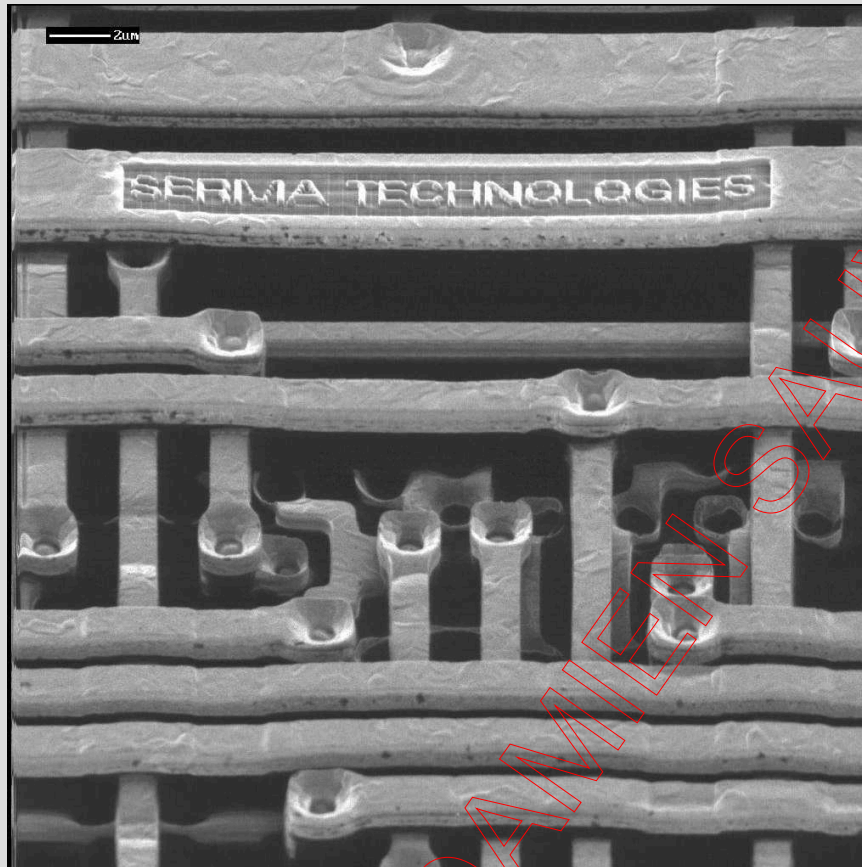
159

## Chip Re-Wiring / Addition of a Track



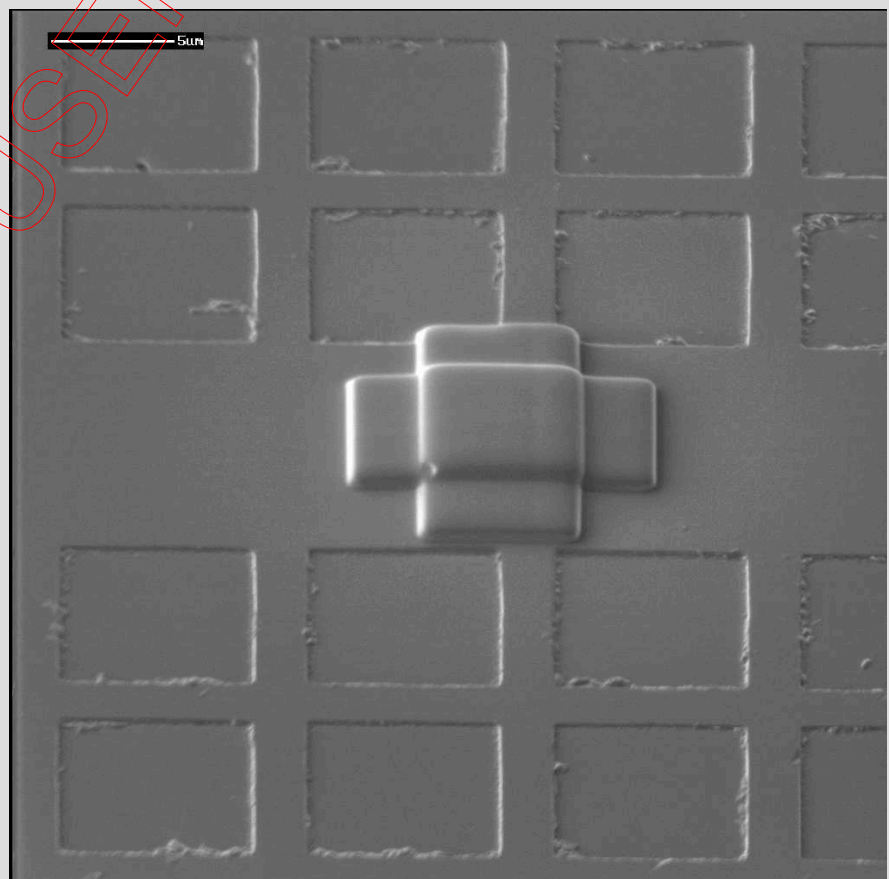
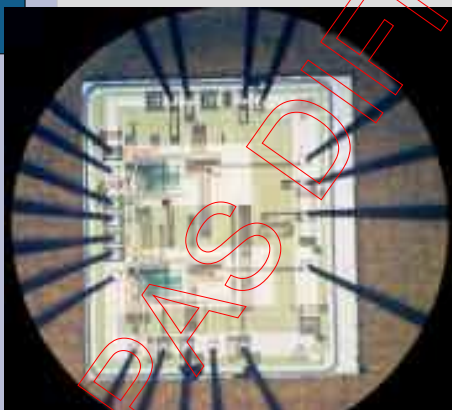
160

## Modifications de circuits (2/2)



161

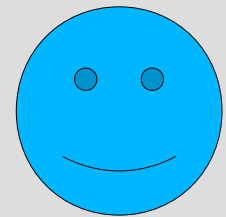
## Micro-probing



162

# Très cher !

- If you have more money or if you are a student.



163

## Côtation d'une attaque

### Niveau d'expertise requise

Expert, ..., homme de la rue

### Connaissance du produit

Information publique, diffusion restreinte, sensible, critique

### Accès au produit

Nombre d'échantillon nécessaire : <10, <100, <1000, non praticable

### Temps d'identification

<1 heure, 1 jour, 1 semaine, 1 mois, ...

### Temps d'exploitation

<1 heure, 1 jour, 1 semaine, 1 mois, ...

### Equipement

Aucun, standard, spécialisé, ...

...

=> La sécurité et le business s'opposent. Il faut donc trouver un juste compromis !

164

# La norme FIPS 140

## FIPS 140-2, June 2001, Security requirements for Cryptographic Modules :

<http://www.csrc.nist.gov/publications/fips/>

## Recommandations pour :

- Physique,
- OS,
- Key Management
- EM
- Self Tests
- Design Assurance

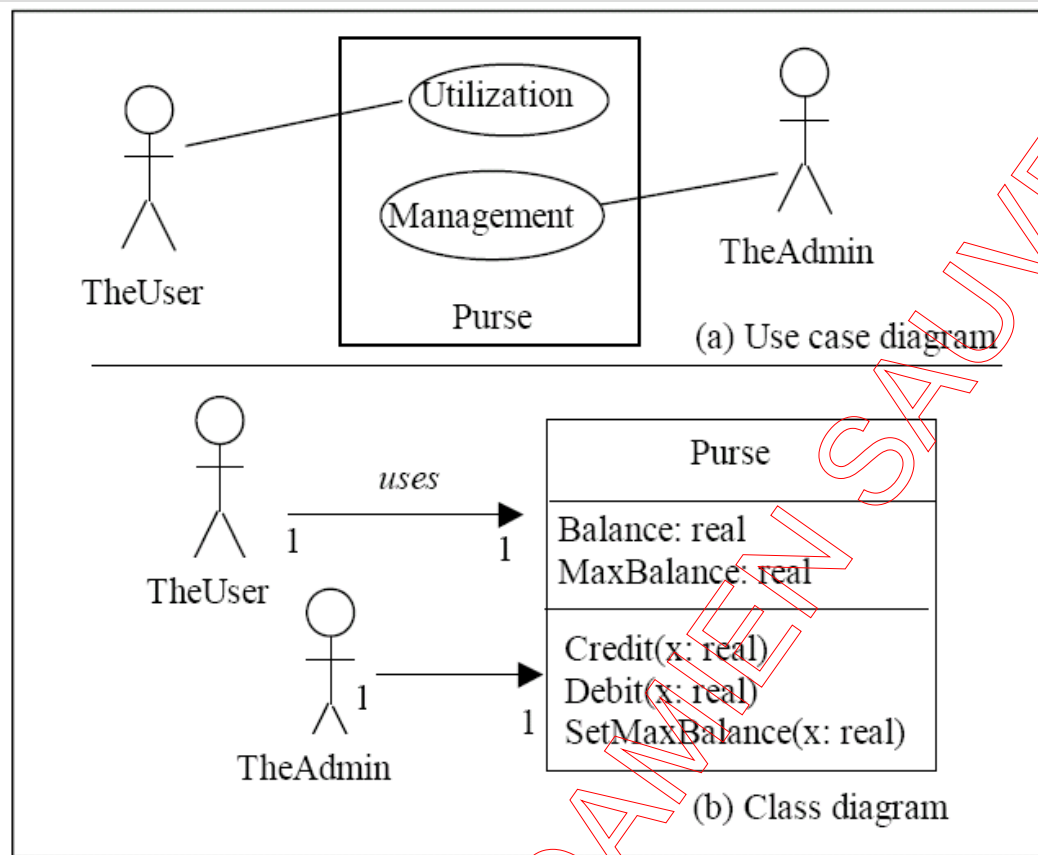
165

## Sécurité physique dans FIPS

|                     | General Requirements<br>for all Embodiments                                                                                                    | Single-Chip<br>Cryptographic Modules                                                                                 | Multiple-Chip Embedded<br>Cryptographic Modules                                                                                                                       | Multiple-Chip Standalone<br>Cryptographic Modules                                                                                                                             |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security<br>Level 1 | Production-grade components<br>(with standard passivation).                                                                                    | No additional requirements.                                                                                          | If applicable, production-grade<br>enclosure or removable cover.                                                                                                      | Production-grade enclosure.                                                                                                                                                   |
| Security<br>Level 2 | Evidence of tampering (e.g.,<br>cover, enclosure, or seal).                                                                                    | Opaque tamper-evident coating<br>on chip or enclosure.                                                               | Opaque tamper-evident<br>encapsulating material or<br>enclosure with tamper-evident<br>seals or pick-resistant locks for<br>doors or removable covers.                | Opaque enclosure with tamper-<br>evident seals or pick-resistant<br>locks for doors or removable<br>covers.                                                                   |
| Security<br>Level 3 | Automatic zeroization when<br>accessing the maintenance<br>access interface. Tamper<br>response and zeroization<br>circuitry. Protected vents. | Hard opaque tamper-evident<br>coating on chip or strong<br>removal-resistant and<br>penetration resistant enclosure. | Hard opaque potting material<br>encapsulation of multiple chip<br>circuitry embodiment or<br>applicable Multiple-Chip<br>Standalone Security Level 3<br>requirements. | Hard opaque potting material<br>encapsulation of multiple chip<br>circuitry embodiment or strong<br>enclosure with<br>removal/penetration attempts<br>causing serious damage. |
| Security<br>Level 4 | EFP or EFT for temperature and<br>voltage.                                                                                                     | Hard opaque removal-resistant<br>coating on chip.                                                                    | Tamper detection envelope with<br>tamper response and zeroization<br>circuitry.                                                                                       | Tamper detection/ response<br>envelope with tamper response<br>and zeroization circuitry.                                                                                     |

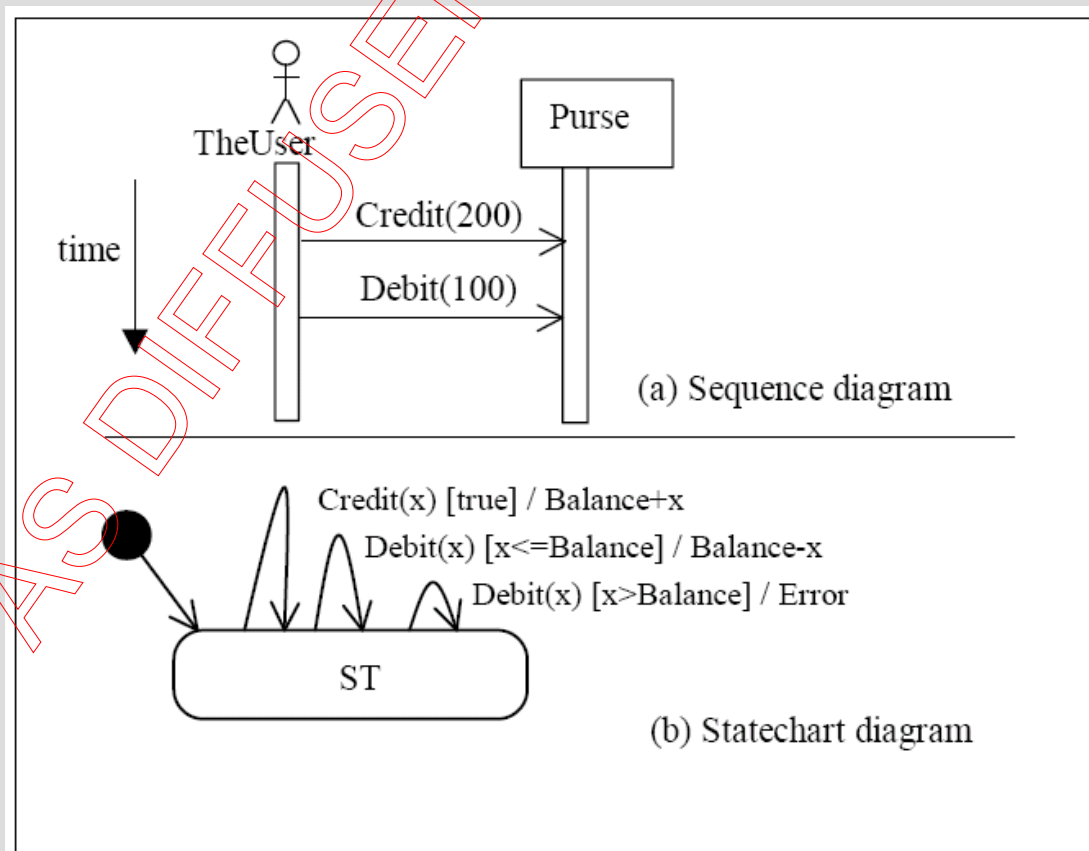
Table 2: Summary of physical security requirements

## Simple UML use case and class diagrams



167

## Simple UML sequence diagram and statechart for the Purse object



168

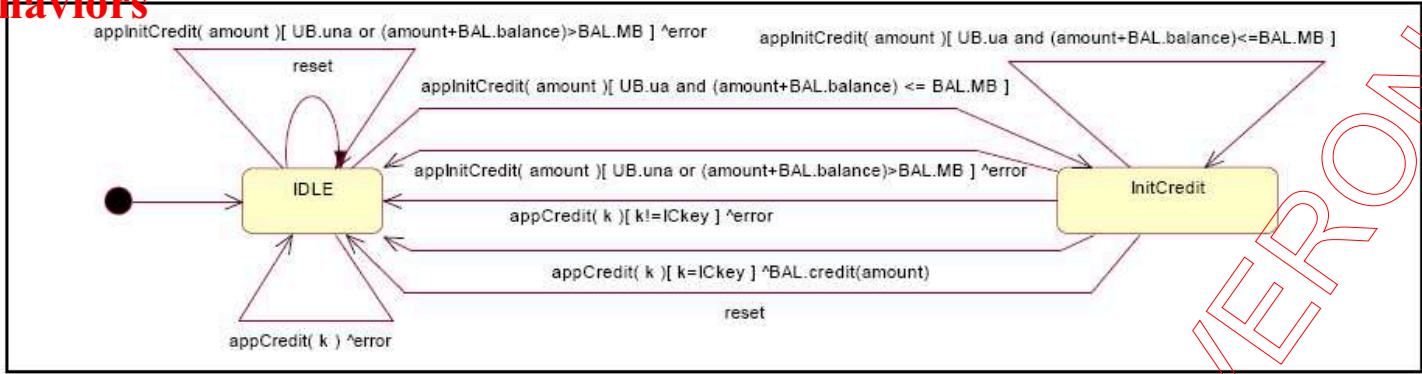


Figure 4. Limited Purse behavior

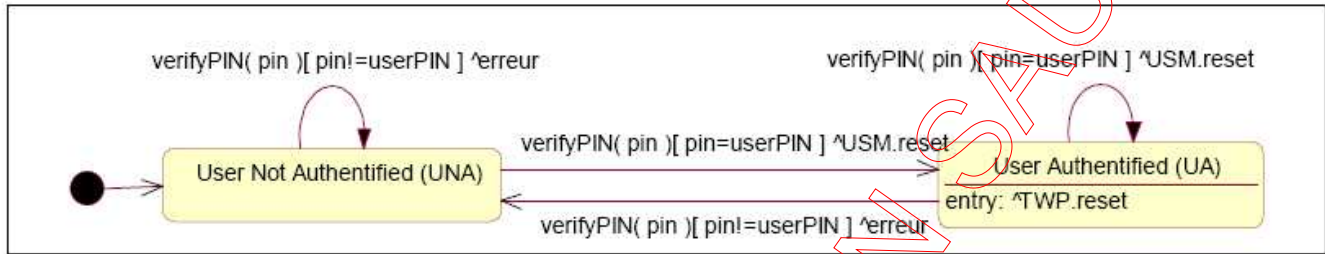


Figure 5. Purse authentication behavior

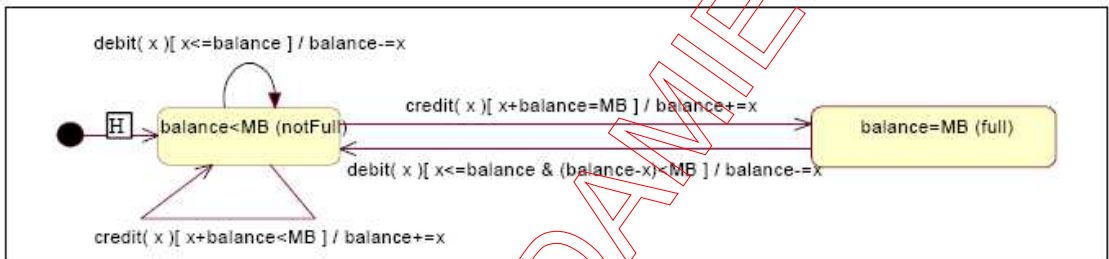


Figure 6. Balance behavior

Les méthodes formelles et le test

Conception formelle de certains partie de l'OS (voire de l'OS complet)

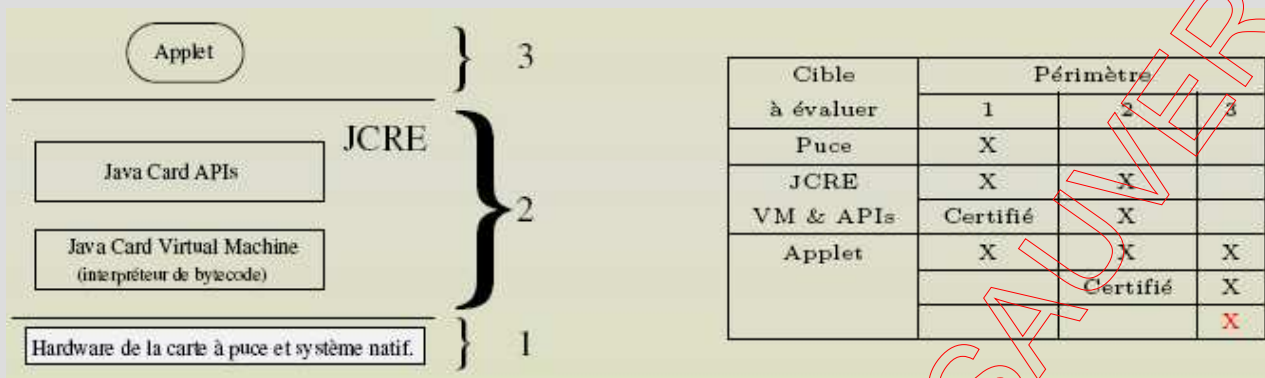
Preuve formelle sur des aspects sécuritaire

Génération de jeux de tests associés aux spécifications

...

## Le périmètre d'évaluation

Défini dans la cible de sécurité dans la description de la cible d'évaluation.



### Nouveaux problèmes apportés par les applets Java Card :

- pas de définition précise du périmètre d'évaluation ;
- pas de méthodologie d'évaluation d'une applet ;
- la multi-application.

The end (temporaire !)