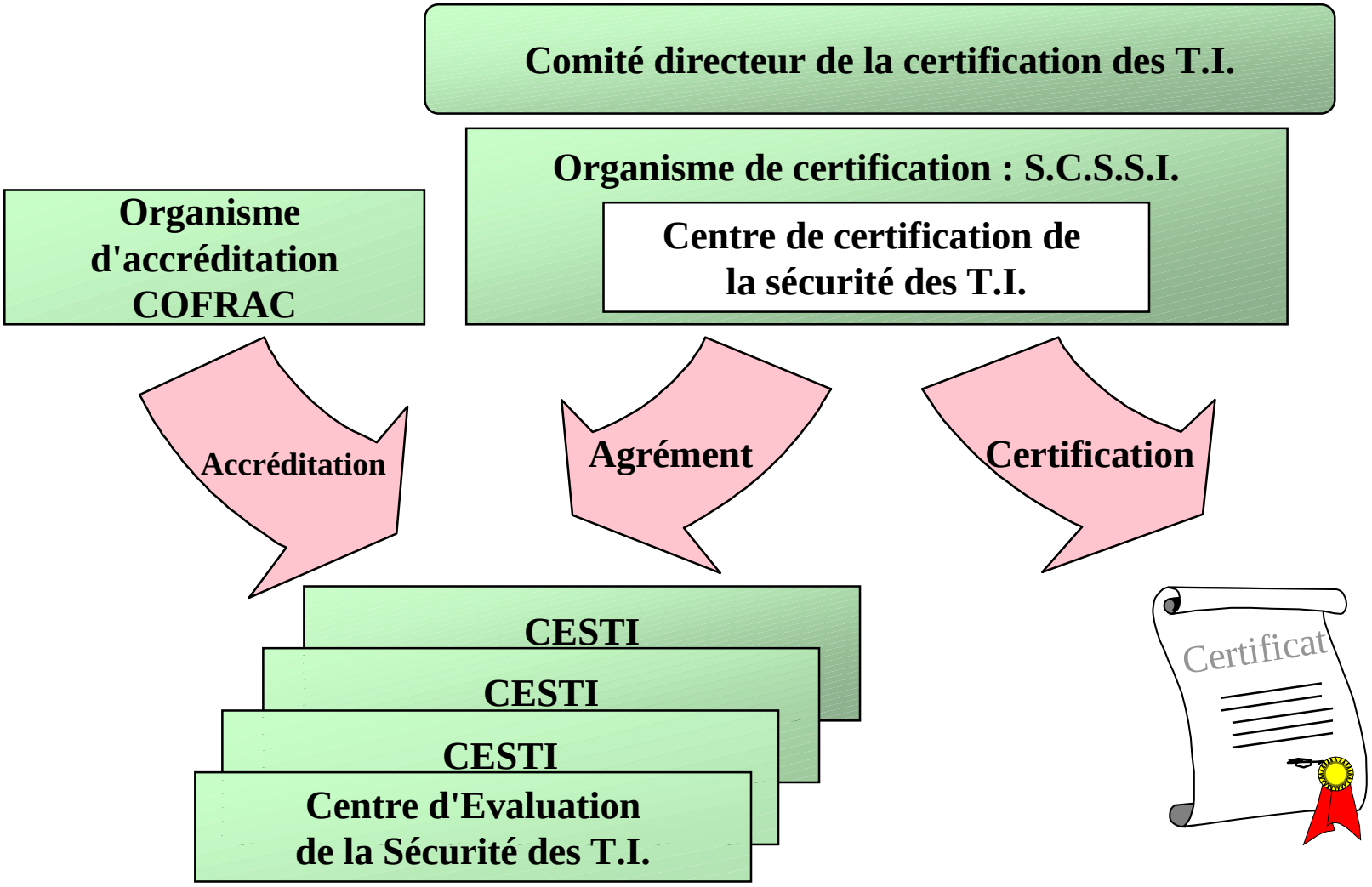
Évaluation et Certification

Carlos MARTIN
Responsable
du
Centre de Certification de la Sécurité des Technologies de l'Information

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

Premier ministre - Secrétariat général de la Défense nationale
Direction centrale de la sécurité des systèmes d'information

Organisme de certification



Un environnement international...

Organismes de certification:

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

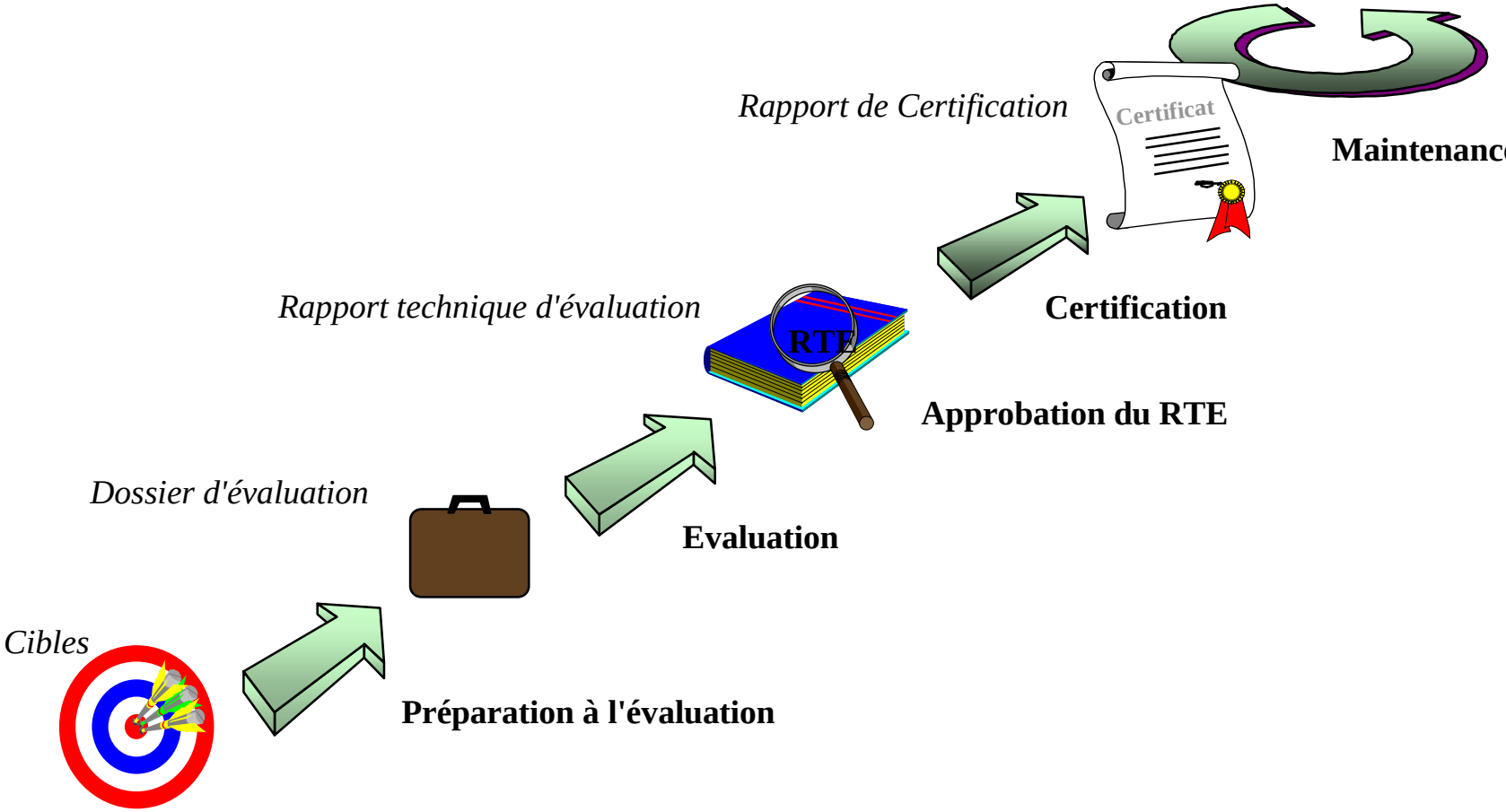
Centres d'évaluation

CESTI

Opérationnel	En formation
Algoriel AQL CEACI (CNES-SOREP) CEA/LETI SERMA Technologies	ES^2

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

Processus d'évaluation : les grandes étapes



Les références (1/2)

ITSEC

Critères ITSEC v1.2, Juin 1991
Méthodologie ITSEM v1.0, Septembre 1993
Bibliothèque d'interprétation commune JIL v2.0, Novembre 1998

Qualité

Normes NF EN 45001 et NF EN 45011

Les références (2/2)

ECF

- ECF 00 Glossaire
- ECF 01 Présentation du schéma
- ECF 02 Agrément des centres d'évaluation
- ECF 03 Procédures d'évaluation et de certification
- ECF 04 Formats des rapports et certificats
- ECF 06 Catalogues
- ECF 11 Procédure d'enregistrement des profils de protection

Guides GARDE

Guide d'Aide à la Rédaction de la Documentation pour l'Evaluation (pour les niveaux E1 à E3 des critères ITSEC)

Références (3/3)

Critères Communs

- Partie 1 Introduction et modèle général

- Partie 2 Exigences de sécurité fonctionnelles

- Partie 3 Exigences de sécurité d'assurance

Méthodologie d'évaluation

- Méthodologie d'évaluation des PP et des ST

- Méthodologie d'évaluation pour les niveaux EAL1 à EAL4

Les critères ITSEC

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

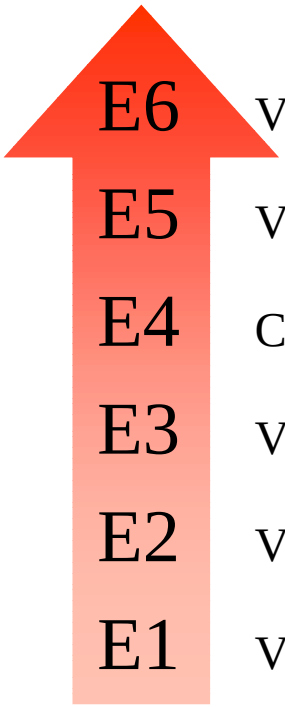
Premier ministre - Secrétariat général de la Défense nationale
Direction centrale de la sécurité des systèmes d'information

Information Technology Security Evaluation Criteria

- Des critères harmonisés :
  - approche commune :
    quel que soit le secteur : commercial, gouvernemental ou militaire
    quel que soit le pays
  - base commune pour la certification
    résultat de l'expérience existante

- Objet d'une recommandation du Conseil Européen

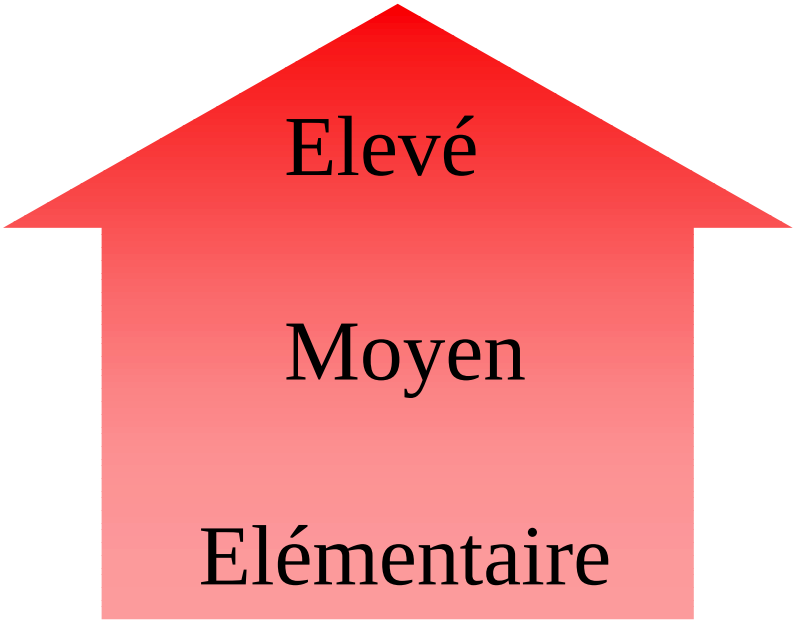
Niveaux de conformité



E6	Vérification formelle de la conception générale et tests
E5	Vérification semi-formelle de la conception et tests
E4	Conception semi-formelle et tests
E3	Vérification de la réalisation et test des mécanismes
E2	Vérification de la conception détaillée et gestion de la configuration
E1	Vérification de la conception générale et tests

Niveau d’efficacité

Représente le niveau d’expertise, d’opportunité et de ressources nécessaires à un attaquant pour mettre en défaut les caractéristiques de sécurité



Etat de l’art

Modéré

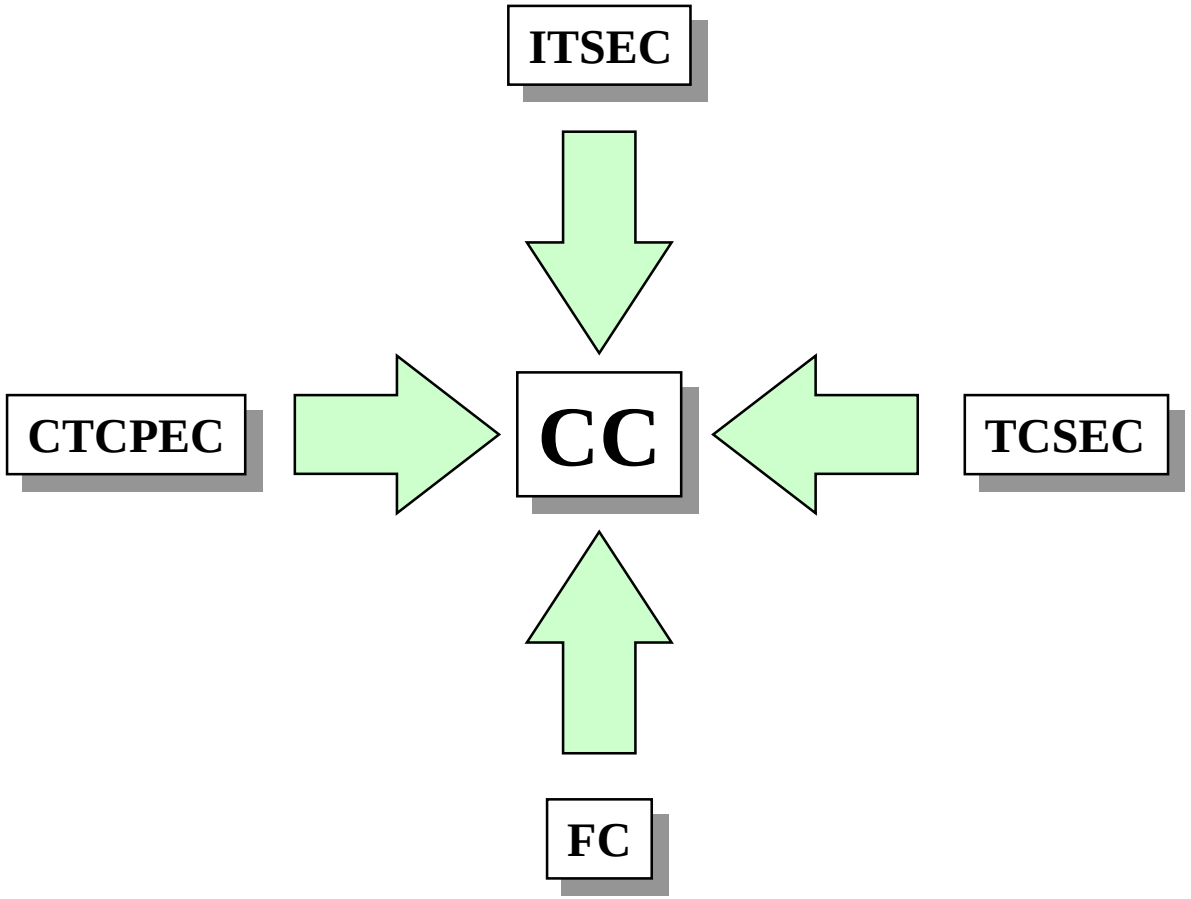
Limité

Les Critères Communs

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

Premier ministre - Secrétariat général de la Défense nationale
Direction centrale de la sécurité des systèmes d'information

Harmonisation des critères existants



Une norme internationale

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

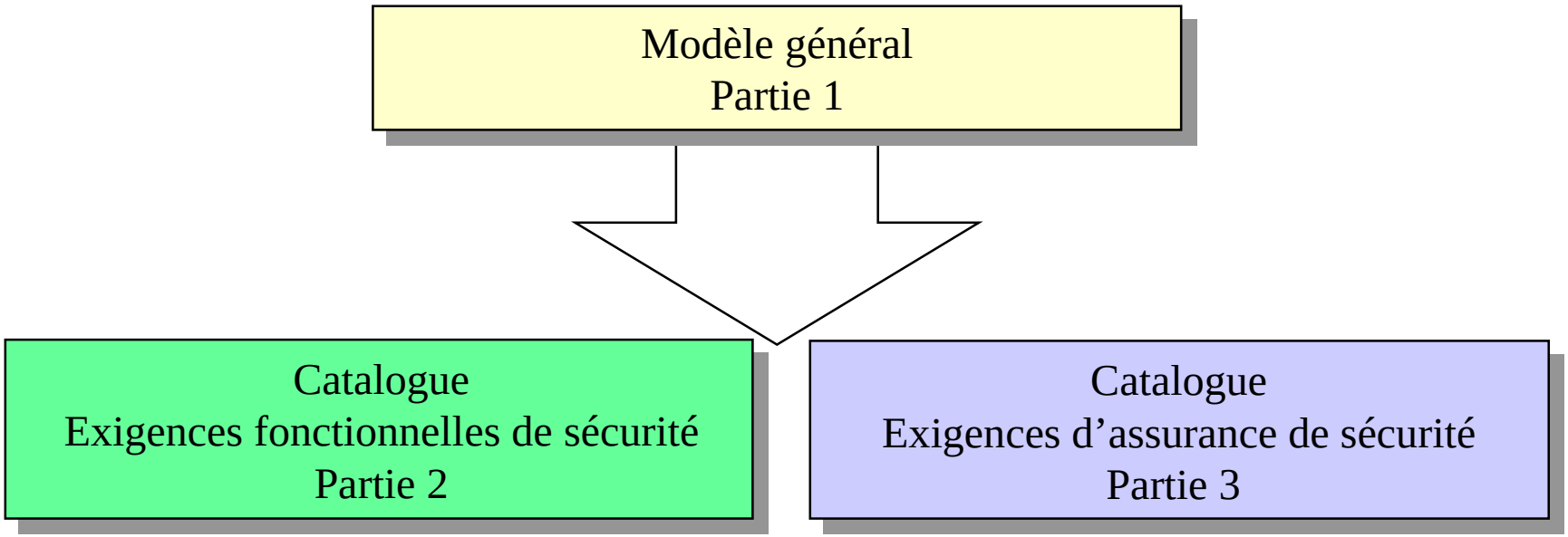
Juin 1999 Normalisation des Critères Communs

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

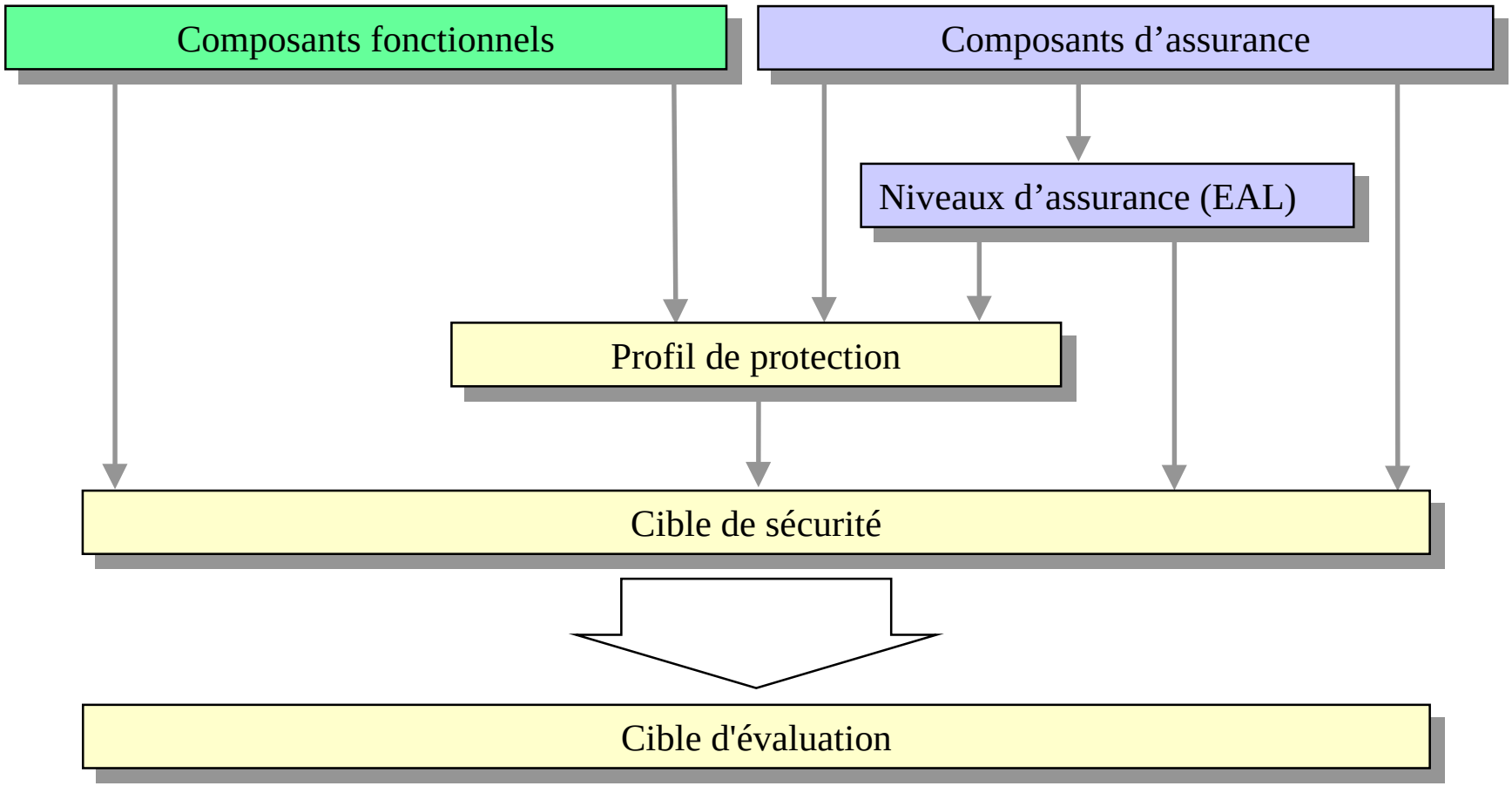
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

Premier ministre - Secrétariat général de la Défense nationale
Direction centrale de la sécurité des systèmes d'information

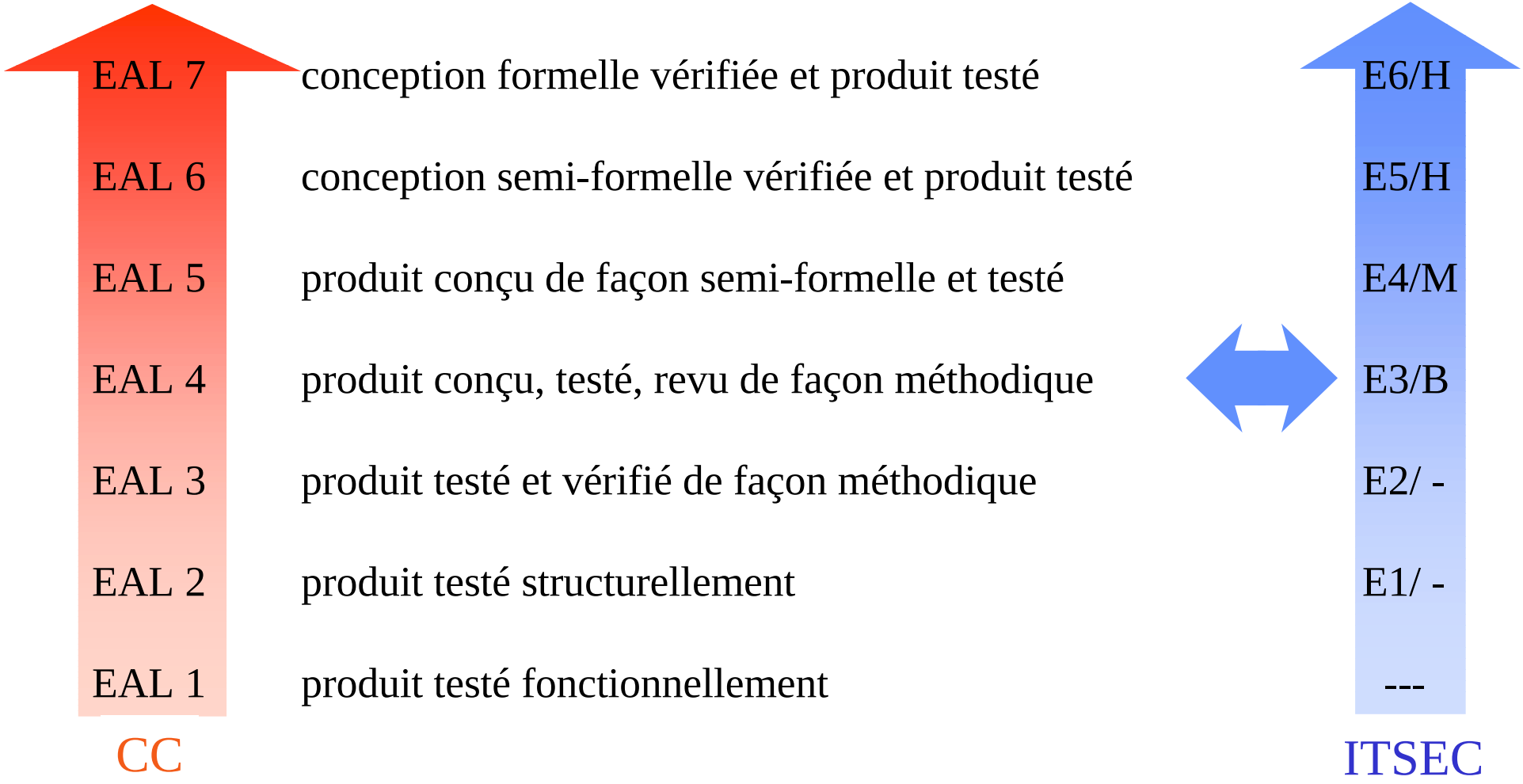
Expression des exigences



Utilisation des catalogues



Echelle d’assurance : 7 niveaux



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, PIX, Gauntlet, Lucent, …*

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

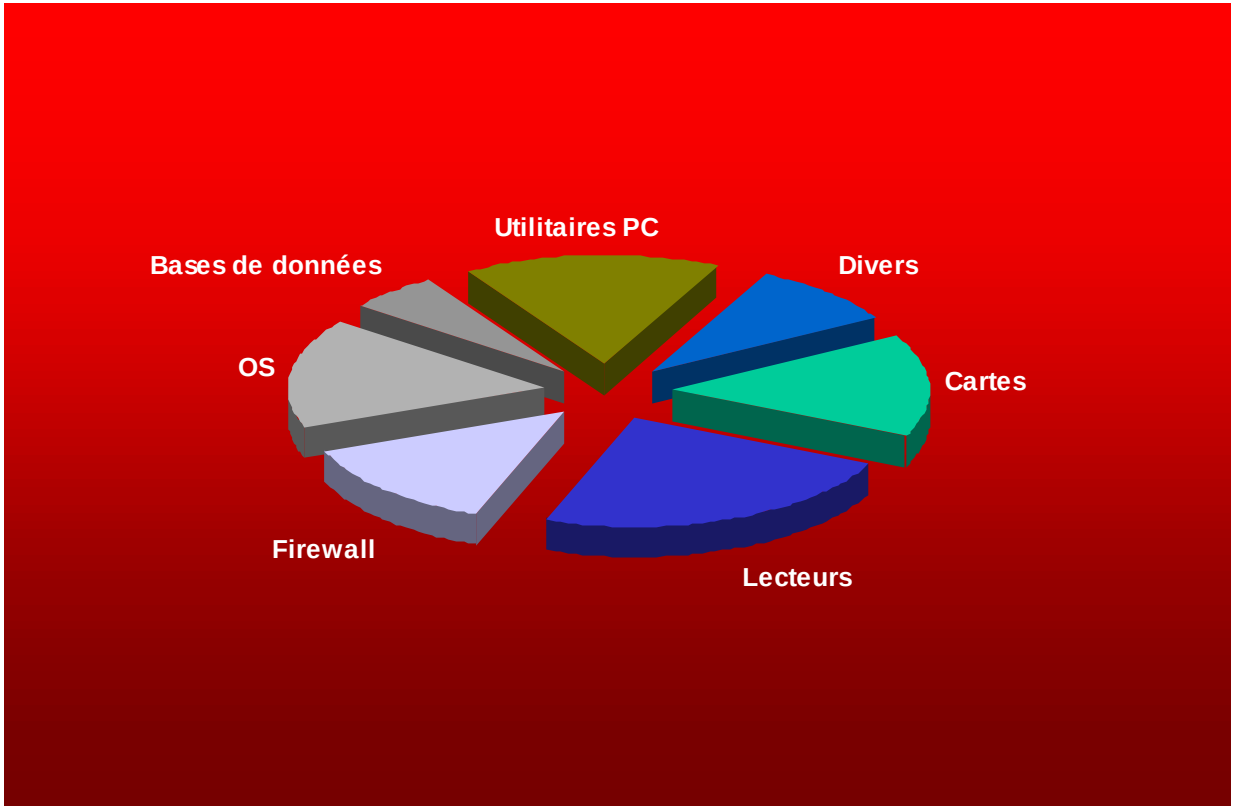
Utilitaires PC (19) : *Contrôle d’accès, utilitaires disques, …*

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

➥ www.scssi.gouv.fr

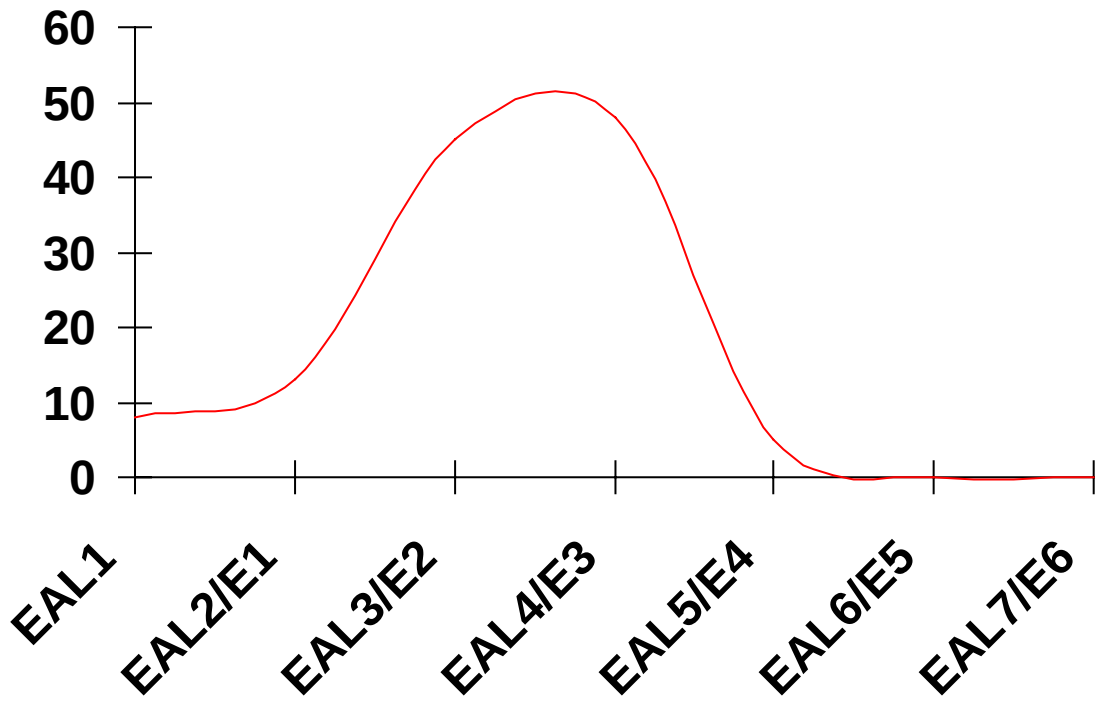
Source : Certificats reconnus par le schéma français au 1er Jan. 2000

Certificats : Domaines couverts



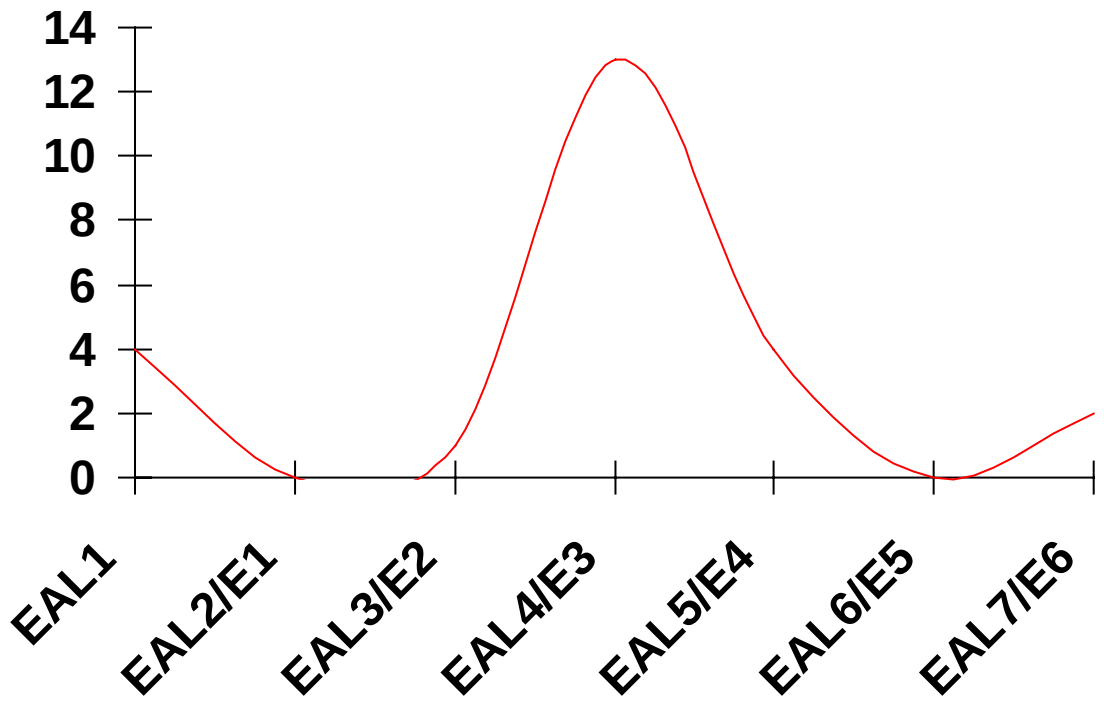
Source : Certificats reconnus par le schéma français au 1er Jan. 2000

Certificats : Répartition par niveau d'assurance



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

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*

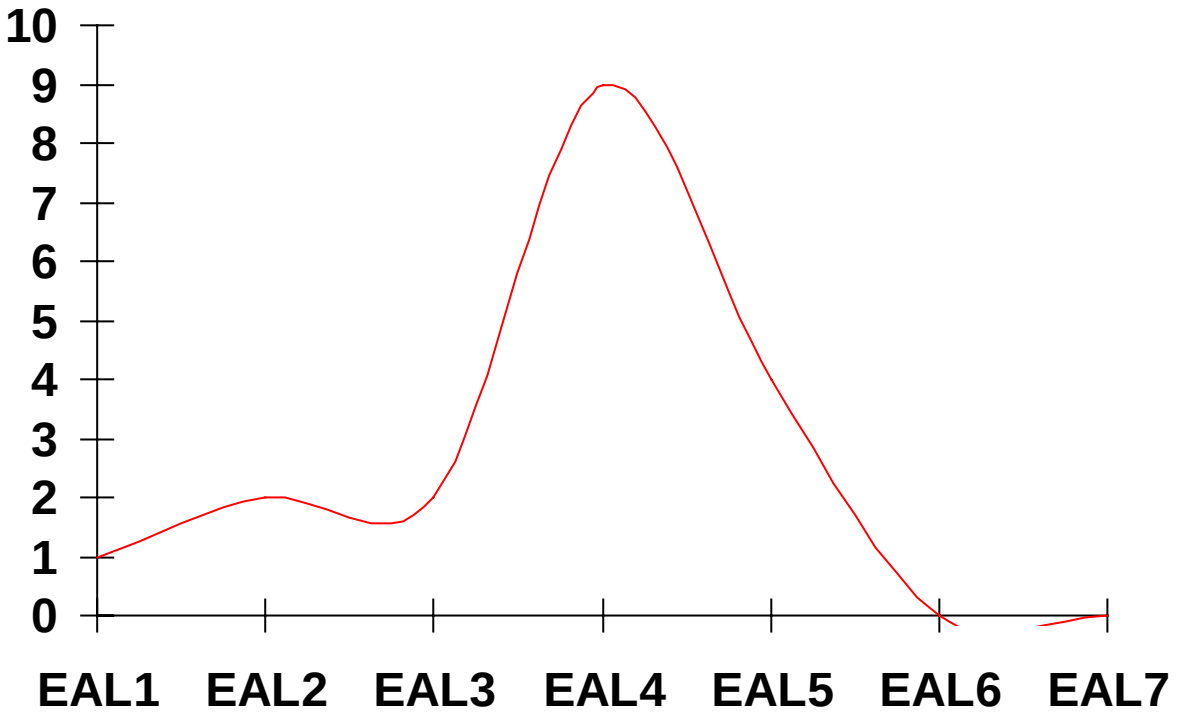
Bases de données : *Oracle*

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

➥ www.scssi.gouv.fr

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

PP : Répartition par niveau d'assurance



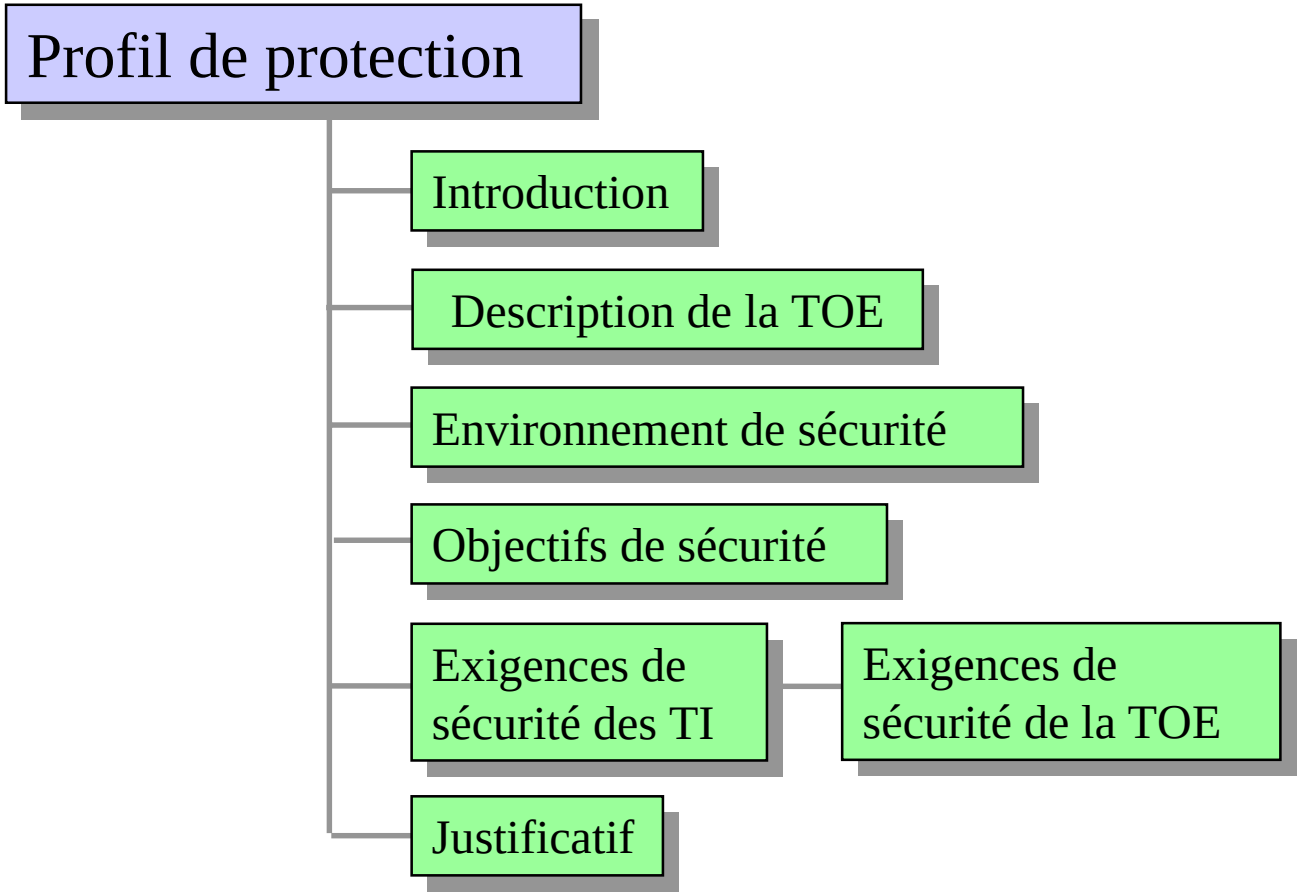
Source : Certificats reconnus par le schéma français au 1er Jan. 2000

Profil de Protection

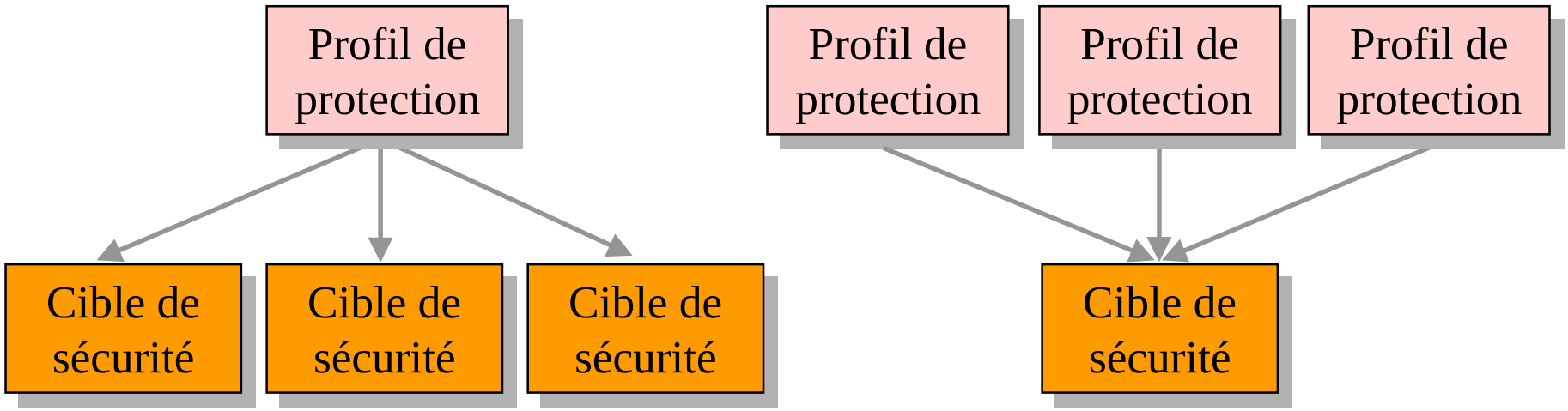
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

Premier ministre - Secrétariat général de la Défense nationale
Direction centrale de la sécurité des systèmes d'information

Profil de protection : structure



Utilisation des profils de protection



Enregistrement des profils de protection

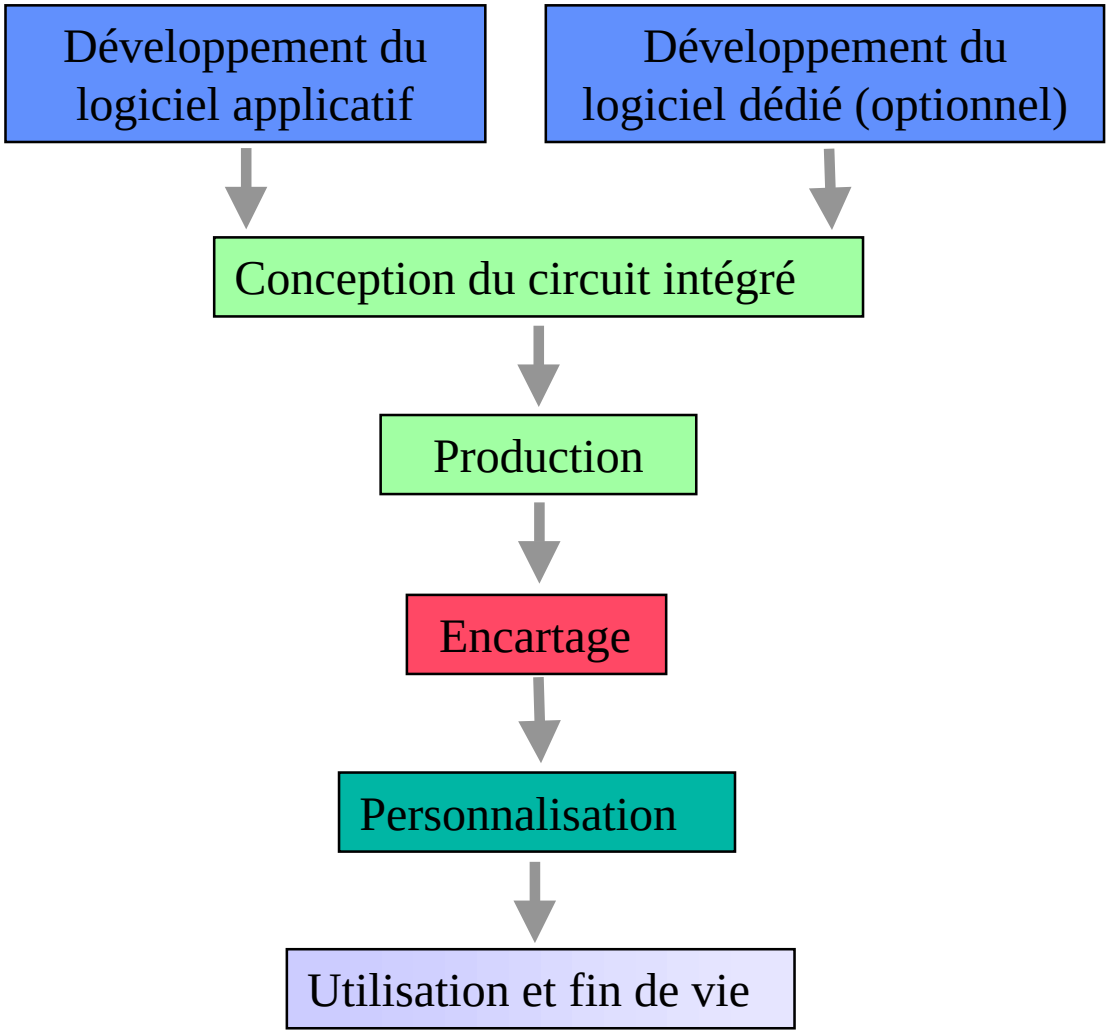
Registres des profils de protection

Catalogue
des profils de protection non certifiés

Catalogue
des profils de protection certifiés

Les procédures d'enregistrement sont définies
dans le guide technique ECF 11

PP Cartes à puce



PP Masque PP/9810 et PP/9911
PP Billettique PP/9903
PP PME PP/9908 et PP/9909

SCUSG-SCPP
PPnc/0001 Plate-forme multi-application

PP Circuit intégré PP/9806

PP Encartage PPnc/9910

PP Personnalisation PPnc/9912

PP Masque

PP/9810: Smartcard embedded software

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

Schulmberger

PP/9911: Smartcard integrated circuit with embedded software

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

EuroSmart

EUROSMART
European Smart Card Industry Association

PP Billetique

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

EAL4+ (ADV_IMP.2, AVA_VLA.4)

SNCF, RATP

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

EUROSMART
European Smart Card Industry Association

BANQUE DE FRANCE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

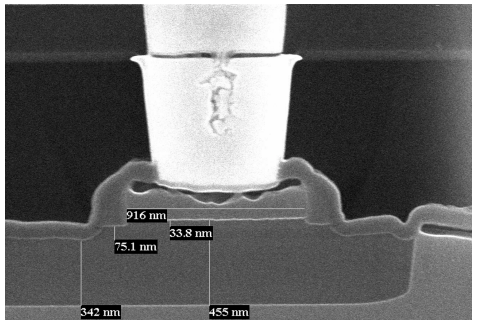
Premier ministre - Secrétariat général de la Défense nationale
Direction centrale de la sécurité des systèmes d'information

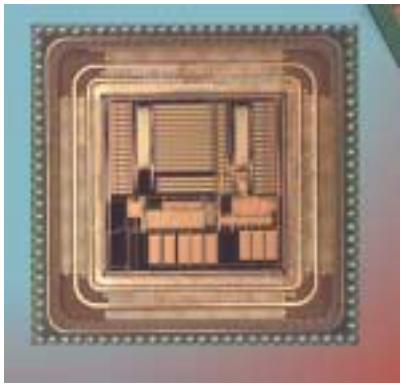
PP Composant pour carte a puce

PP/9806: Smartcard integrated circuit

EAL4+ (ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)
EuroSmart,
Motorola, Philips, Siemens, STMicroelectronics,
Texas-Instruments

EUROSMART
European Smart Card Industry Association





PP Encartage et personnalisation

PPnc/9910: SmartCard embelling Sites

Paquet d'assurance spécifique

AFPC (Association des Fabricants et des Personnalisateurs de Carte)

PPnc/9912: SmartCard personalization Sites

Paquet d'assurance spécifique

GIP CPS

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

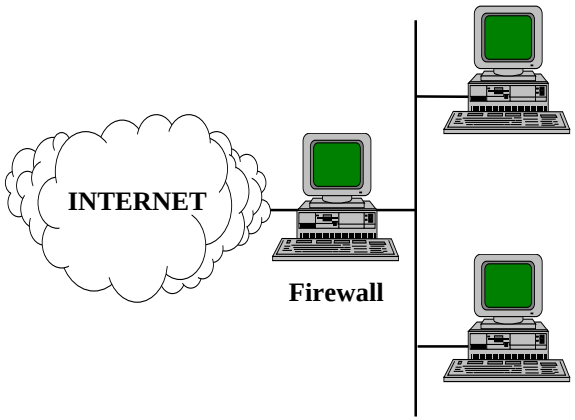
PP/9803: Transactions portant sur des données confidentielles

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

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

MINISTERE 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

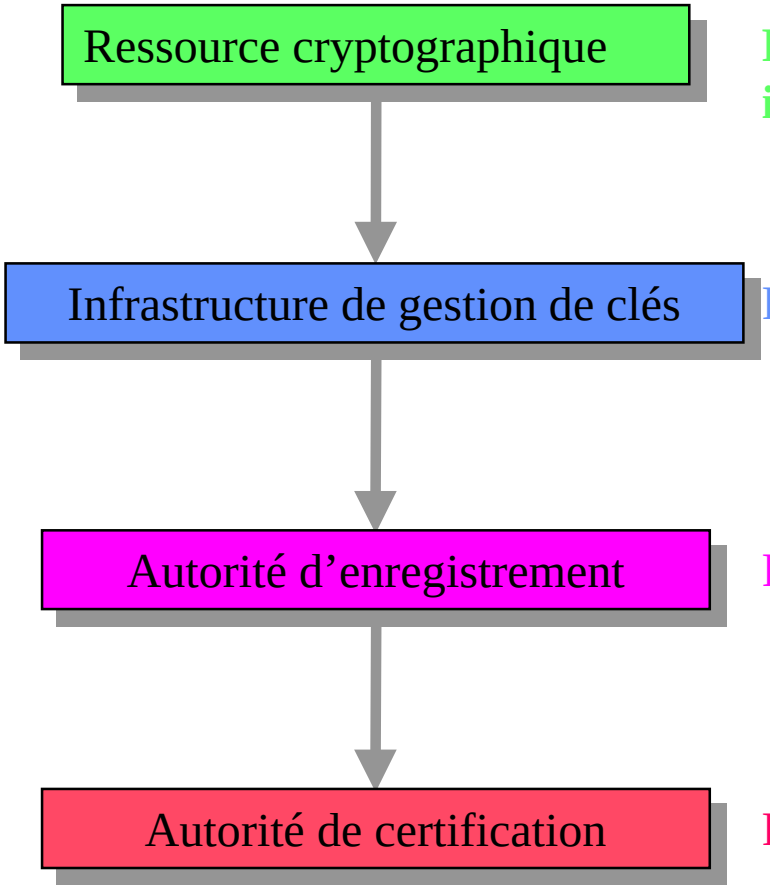
PP/9906: Passerelle filtrante de sécurité configurable

EAL5

DGA

DGA
Délégation Générale pour l'Armement

PP Infrastructure de Gestion de Clés



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

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

SCSSI

PPnc/0004: Infrastructure de gestion de clés

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

SCSSI

PPnc/0005: Autorité d'enregistrement

EAL 3+ (AVA_VLA.3, ADV_ IMP.1, ADV_LLD.1, ADV_SPM.1, ALC_TAT.1)

SCSSI

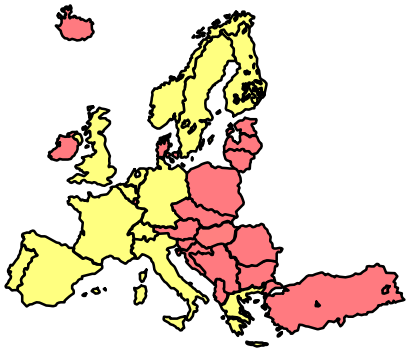
PPnc/0006: Autorité de certification

EAL 3+ (AVA_VLA.3, ADV_ IMP.1, ADV_LLD.1, ADV_SPM.1, ALC_TAT.1)

SCSSI

Reconnaissance international

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

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

Coordonnées

@www.scssi.gouv.fr

Direction Central de la Sécurité des Systèmes d'information

Centre de certification de la sécurité des technologies de l'information

18, rue du Docteur Zamenhof
F - 92131 ISSY LES MOULINEAUX CEDEX

tel : +33.1.41.46.37.53
fax : +33.1.41.46.37.01
email : martincarlos@compuserve.com