
# Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information

## Partie 1 : Introduction et modèle général

Août 1999

Version 2.1

CCIMB-99-031

# Avant-propos

L'ISO (International Organisation for Standardisation, l'organisation internationale pour la normalisation) et l'IEC (International Electrotechnical Commission, la commission internationale électrotechnique) forment le système dédié à la normalisation mondiale. Les organisations nationales qui sont membres de l'ISO ou de l'IEC participent au développement des normes internationales par le biais de comités techniques établis par les organisations respectives pour traiter de domaines particuliers d'activités techniques. Les comités techniques de l'ISO et de l'IEC collaborent dans les domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, prennent également part au travail.

Dans le domaine des technologies de l'information, l'ISO et l'IEC ont établi un comité technique commun, l'ISO/IEC JTC 1. Les normes internationales provisoires (Draft International Standards) adoptées par le comité technique commun sont mises en circulation dans les organisations nationales pour être soumises à un vote. La publication comme norme internationale (International Standard) nécessite l'approbation d'au moins 75% des organisations nationales ayant voté.

La norme internationale ISO/IEC 15408 a été préparée par le comité technique commun ISO/IEC JTC 1, Technologies de l'Information, en collaboration avec le comité d'édition des critères communs (Common Criteria Implementation Board), une entité qui regroupe des membres des organisations commanditaires du projet Critères Communs. Le texte identique à la norme ISO/IEC 15408 est publié par les organisations commanditaires du projet Critères Communs sous le titre *Common Criteria for Information Technology Security Evaluation, version 2.0 (Critères Communs pour l'évaluation de la sécurité des technologies de l'information, version 2.0).* Des informations supplémentaires concernant le projet Critères Communs ainsi que les coordonnées des organisations commanditaires, sont fournies dans l'annexe A de la partie 1.

La norme ISO/IEC 15408, sous le titre général *Critères Communs pour l'évaluation de la sécurité des technologies de l'information,* comprend les parties suivantes :

Partie 1 : Introduction et modèle général

Partie 2 : Exigences fonctionnelles de sécurité

Partie 3 : Exigences d'assurance de sécurité

***La présente NOTICE À CARACTÈRE LÉGAL a été introduite dans toutes les parties de la norme ISO/IEC 15408 sur demande :***
*Les sept organisations gouvernementales (collectivement dénommées les "organisations commanditaires du projet Critères Communs") citées ci-dessous et identifiées plus complètement dans l'Annexe A de la Partie 1, en tant que détentrices communes du copyright du document Critères Communs pour l'évaluation de la sécurité des technologies de l'information (Common Criteria for Information Technology Security Evaluation), version 2.0, comprenant les Parties 1 à 3 (appelé "CC 2.0"), accordent par la présente notice à l'ISO/IEC la licence non exclusive d'utilisation du document CC 2.0 pour le développement de la norme internationale ISO/IEC 15408. Cependant, les organisations commanditaires du projet Critères Communs conservent le droit d'utiliser, copier, distribuer ou modifier le document CC 2.0 quand elles le jugent bon.*

| | |
|---|---|
| *- Allemagne :* | *Bundesamt für Sicherheit in der Informationstechnik* |
| *- Canada :* | *Communications Security Establishment* |
| *- Etats-Unis :* | *National Institute of Standards and Technology* |
| *- Etats-Unis :* | *National Security Agency* |
| *- France :* | *Service Central de la Sécurité des Systèmes d'Information* |
| *- Pays-Bas :* | *Netherlands National Communications Security Agency* |
| *- Royaume Uni :* | *Communications-Electronics Security Group* |

## Table des matières

## Liste des figures

## Liste des tableaux

# 1 Champ d'application

1 La présente norme, les Critères Communs (Common Criteria, CC), a pour vocation d'être utilisés comme base pour l'évaluation des propriétés de sécurité des produits et systèmes des Technologies de l'Information (TI). En établissant une telle base de critères communs, les résultats d'une évaluation de la sécurité des TI seront significatifs pour une plus large audience.

2 Les CC permettront de comparer les résultats d'évaluations de sécurité menées indépendamment les unes des autres. Cela est rendu possible grâce à un ensemble commun d'exigences pour les fonctions de sécurité des produits et systèmes TI et pour les mesures d'assurance qui leur sont appliquées pendant une évaluation de sécurité. Le processus d'évaluation établit un niveau de confiance dans le fait que les fonctions de sécurité de tels produits et systèmes et les mesures d'assurance qui leur sont appliquées satisfont à ces exigences. Les résultats de l'évaluation peuvent aider les acheteurs à déterminer si le produit ou le système TI est suffisamment sûr pour l'application qu'ils envisagent et si les risques liés à la sécurité qui sont implicites dans son utilisation sont tolérables.

3 Les CC sont utiles en tant que guide pour le développement des produits ou systèmes incluant des fonctions de sécurité des TI et pour l'approvisionnement de produits ou systèmes commerciaux dotés de telles fonctions. Pendant l'évaluation, un tel produit ou système TI est qualifié de cible d'évaluation ou TOE (Target Of Evaluation). De telles TOE peuvent être par exemple des systèmes d'exploitation, des réseaux informatiques, des systèmes distribués et des applications.

4 Leq CC traitent de la protection des informations contre leur divulgation, modification ou perte d'usage non autorisés. Les types de protection vis-à-vis de ces trois sortes de défaillances de sécurité sont dénommées dans la pratique respectivement confidentialité, intégrité et disponibilité. Les CC peuvent s'appliquer en outre à d'autres aspects de la sécurité des TI. Elle est focalisée sur les menaces (qui pèsent sur ces informations) générées par des activités humaines, qu'elles soient mal intentionnées ou non, mais peut aussi bien s'appliquer à des menaces non liées à l'homme. De plus, les CC peuvent être utilisés dans d'autres domaines des TI mais elle ne prétend pas apporter de compétences particulières en dehors du domaine strictement limité à la sécurité des TI.

5 Les CC s'appliquent aux mesures de sécurité des TI implémentées dans du matériel, des microprogrammes ou du logiciel. Lorsque des aspects particuliers de l'évaluation sont destinés à ne s'appliquer qu'à certaines méthodes d'implémentation, cela est indiqué dans les critères concernés.

6 On considère que certains sujets sont en dehors du champ d'application des CC parce qu'ils impliquent l'utilisation de techniques spécialisées ou parce qu'ils sont situés à la périphérie de la sécurité des TI. Quelques uns d'entre eux sont identifiés ci-dessous.

a) Les CC ne contiennent pas de critères d'évaluation de la sécurité relatifs à des mesures de sécurité administratives non liées directement aux mesures de la sécurité des TI. Il est cependant admis qu'une part significative de la sécurité d'une TOE peut souvent être obtenue au moyen de mesures administratives telles que des contrôles organisationnels, relatifs au personnel, physiques et procéduraux. Les mesures de sécurité administratives mises en œuvre dans l'environnement opérationnel de la TOE sont considérées comme des hypothèses d'utilisation sûre quand elles ont un impact sur la capacité des mesures de sécurité des TI à contrer les menaces identifiées.

b) L'évaluation d'aspects physiques techniques de la sécurité des TI tels que le contrôle des rayonnements électromagnétiques n'est pas spécifiquement couverte, bien que nombre des concepts traités soient applicables à ce domaine. En particulier, les CC abordent certains aspects de la protection physique de la TOE.

c) Les CC ne traitent ni de la méthodologie d'évaluation ni du cadre administratif et légal dans lequel les critères peuvent être utilisés par les autorités d'évaluation. Il est cependant prévu que les CC soit utilisés dans un but d'évaluation dans le contexte d'un tel cadre et d'une telle méthodologie.

d) Les procédures d'utilisation des résultats d'évaluation pour l'homologation de produits ou de systèmes sont en dehors du champ d'application des CC. On appelle homologation de produits ou de systèmes le processus administratif par lequel une autorité se voit accorder le droit d'exploiter un produit ou système TI dans son environnement opérationnel complet. L'évaluation se focalise sur les parties relatives à la sécurité des TI du produit ou du système et des parties de l'environnement opérationnel qui peuvent affecter directement l'utilisation sûre des éléments TI. Les résultats du processus d'évaluation constituent en conséquence un paramètre intéressant pour le processus d'homologation. Cependant, comme il existe d'autres techniques plus appropriées pour l'estimation des propriétés de sécurité du produit ou du système non liées aux TI et de leur relation avec les parties relatives à la sécurité des TI, les homologateurs devraient traiter ces aspects séparément.

e) Les CC ne contiennent pas de critères pour estimer les qualités inhérentes aux algorithmes cryptographiques n'est pas couvert par les CC. S'il est nécessaire de faire une estimation indépendante des propriétés mathématiques des fonctions cryptographiques embarquées dans une TOE, les dispositions correspondantes devront être prévues dans le schéma d'évaluation dans le cadre duquel sont appliqués les CC.

# 2 Définitions

## 2.1 Abréviations communes

7 Les abréviations[1] suivantes se retrouvent dans au moins deux parties des CC :

**CC** (Common Criteria) - Critères Communs

**EAL** (Evaluation Assurance Level) - Niveau d'assurance de l'évaluation

**PP** (Protection Profile) - Profil de protection

**SF** (Security Function) - Fonction de sécurité

**SFP** (Security Function Policy) - Politique d'une fonction de sécurité

**SOF** (Strength of Function) - Résistance d'une fonction

**ST** (Security Target) - Cible de sécurité

**TI** (IT : Information Technology) - Technologie de l'Information

**TOE** (Target of Evaluation) - Cible d'évaluation

**TSC** (TSF Scope of Control) - Champ de contrôle de la TSF

**TSF** (TOE Security Functions) - Ensemble des fonctions de sécurité de la TOE

**TSFI** (TSF Interface) - Interface de la TSF

**TSP** (TOE Security Policy) - Politique de sécurité de la TOE

## 2.2 Portée du glossaire

8 La présente section contient seulement les termes qui sont utilisés dans un sens particulier partout dans les CC. La majorité des termes contenus dans les CC sont employés soit dans un sens conforme aux définitions du dictionnaire, soit dans leur acceptation généralement admise qu'il est possible de trouver dans les glossaires de l'ISO concernant la sécurité ou dans d'autres glossaires de sécurité bien connus. Certaines combinaisons de termes courants utilisés dans les CC, ne méritant pas une définition dans le glossaire, sont expliqués dans leur contexte pour les besoins de la clarté. Des explications sur l'utilisation de termes et de concepts utilisés dans un sens précis dans la partie 2 et la partie 3 des CC peuvent être trouvées dans leur section respective intitulée 'paradigme'.

1. À chaque abréviation est associé entre parenthèses le terme anglais correspondant

## 2.3 Glossaire

9 **Affectation** (Assignment) — La spécification d'un paramètre identifié dans un composant.

10 **Attribut de sécurité** (Security attribute) — Information associée à des sujets, des utilisateurs ou des objets, qui est utilisée pour l'application de la TSP.

11 **Assurance** (Assurance) — Fondements de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.

12 **Augmentation** (Augmentation) — L'addition d'un ou de plusieurs composants d'assurance de la Partie 3 à un EAL ou à un paquet d'assurance.

13 **Autorité d'évaluation** (Evaluation authority) — Une organisation qui met en œuvre les CC pour les besoins d'une communauté spécifique dans le cadre d'un schéma d'évaluation et qui, par ce moyen, définit les normes et contrôle la qualité des évaluations menées par des organisations au sein de cette communauté.

14 **Biens** (Assets) — Informations ou ressources à protéger par les contre-mesures d'une TOE.

15 **Canal de communication interne** (Internal communication channel) — Un canal de communication qui relie des parties séparées de la TOE.

16 **Canal sûr** (Trusted channel) — Un moyen par lequel une TSF et un produit TI de confiance distant peuvent communiquer avec la confiance nécessaire pour contribuer à la TSP.

17 **Champ de contrôle de la TSF** (TSF Scope of Control ou TSC) — L'ensemble des interactions qui peuvent survenir avec ou à l'intérieur d'une TOE et qui sont soumises aux règles édictées par la TSP.

18 **Chemin sûr** (Trusted path) — Un moyen par lequel un utilisateur et une TSF peuvent communiquer avec la confiance nécessaire pour contribuer à la TSP.

19 **Cible d'évaluation** (Target of Evaluation ou TOE) — Un produit ou un système TI et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.

20 **Cible de sécurité** (Security Target ou ST) — Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une TOE identifiée.

21 **Classe** (Class) — Un groupement de familles qui partagent un thème commun.

22 **Composant** (Component) — Le plus petit ensemble sélectionnable d'éléments qui peut être inclus dans un PP, une ST ou un paquet.

23 **Connectivité** (Connectivity) — La propriété d'une TOE qui permet des interactions avec des entités TI externes à la TOE, comprenant les échanges de

données par liaison filaire ou non, sur une distance, dans un environnement ou dans une configuration quelconques.

24 **Dépendance** (Dependency) — Une relation entre exigences, telle que l'exigence mentionnée par la dépendance (dont on dépend) doit normalement être satisfaite pour que les autres exigences (qui dépendent de) soient en mesure de satisfaire à leurs objectifs.

25 **Données d'authentification** (Authentication data) — Informations utilisées pour vérifier l'identité annoncée d'un utilisateur.

26 **Données de la TSF** (TSF data) — Données créées par et pour la TOE, qui pourraient affecter le fonctionnement de la TOE.

27 **Données utilisateur** (User data) — Données créées par et pour l'utilisateur, qui n'affectent pas le fonctionnement de la TSF.

28 **Élément** (Element) — Une exigence de sécurité indivisible.

29 **Entité TI externe** (External IT entity) — Tout produit ou système TI, considéré ou non comme sûr, situé à l'extérieur d'une TOE et qui a des interactions avec elle.

30 **Évaluation** (Evaluation) — Estimation d'un PP, d'une ST ou d'une TOE par rapport à des critères définis.

31 **Extension** (Extension)— L'addition à une ST ou à un PP d'exigences fonctionnelles ne figurant pas dans la Partie 2 ou d'exigences d'assurance ne figurant pas dans la Partie 3 des CC.

32 **Famille** (Family) — Un groupement de composants qui ont en commun des objectifs de sécurité mais qui peuvent différer en termes d'importance ou de rigueur.

33 **Fonction de sécurité** (Security Function ou SF) — Une partie ou des parties de la TOE sur lesquelles on s'appuie pour appliquer un sous-ensemble étroitement imbriqué de règles tirées de la TSP.

34 **Fonctions de sécurité d'une TOE** (TOE Security Functions ou TSF) — Un ensemble qui est constitué par tous les éléments matériels, logiciels et microprogrammés de la TOE sur lequel on doit s'appuyer pour l'application correcte de la TSP.

35 **Formel** (Formal) — Qui est exprimé dans un langage syntaxique restreint doté d'une sémantique définie basée sur des concepts mathématiques bien établis.

36 **Identité** (Identity) — Une représentation (par exemple une chaîne de caractères) qui identifie de façon unique un utilisateur autorisé, qui peut être soit le véritable nom ou un nom abrégé de cet utilisateur soit un pseudonyme.

37 **Informel** (Informal) — Qui est exprimé à l'aide d'un langage naturel.

38 **Interface des fonctions de sécurité d'une TOE** (TOE Security Functions Interface ou TSFI) — Un ensemble d'interfaces, qu'elles soient interactives (interface homme-machine) ou programmatiques (programmes d'interface entre applications), par lesquelles on accède aux ressources de la TOE, au travers de la TSF, ou par lesquelles on obtient des informations de la TSF.

39 **Itération** (Iteration) — L'utilisation multiple d'un composant avec des opérations différentes.

40 **Mécanisme de validation de référence** (Reference validation mechanism) — Une implémentation du concept de moniteur de référence qui possède les propriétés suivantes : elle est résistante à l'intrusion, systématiquement appelée et suffisamment simple pour faire l'objet d'une analyse et de tests exhaustifs.

41 **Modèle de politique de sécurité d'une TOE** (TOE security policy model) — Une présentation structurée de la politique de sécurité que doit appliquer la TOE.

42 **Moniteur de référence** (Reference monitor) — Le concept d'une machine abstraite qui applique les politiques de contrôle d'accès d'une TOE.

43 **Niveau d'assurance de l'évaluation** (Evaluation Assurance Level ou EAL) — Un paquet composé de composants d'assurance tirés de la Partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.

44 **Objet** (Object) — Une entité interne au TSC qui contient ou qui reçoit des informations et sur laquelle les sujets effectuent des opérations.

45 **Objectif de sécurité** (Security objective) — Une expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.

46 **Paquet** (Package) — Un ensemble réutilisable soit de composants fonctionnels soit de composants d'assurance (e.g. un EAL), constitué dans le but de satisfaire à un ensemble d'objectifs de sécurité bien identifiés.

47 **Politique d'une fonction de sécurité** (Security Function Policy ou SFP) — La politique de sécurité appliquée par une SF.

48 **Politiques de sécurité organisationnelles** (Organisational security policies) — Un ou plusieurs règles, procédures, codes de conduite ou lignes directrices de sécurité qu'une organisation impose pour son fonctionnement.

49 **Politique de sécurité d'une TOE** (TOE Security Policy ou TSP) — Un ensemble de règles qui précisent comment gérer, protéger et distribuer les biens à l'intérieur d'une TOE.

50 **Potentiel d'attaque** (Attack potential) — Le potentiel qui est perçu comme permettant à une attaque de réussir, dans le cas où une attaque est menée, exprimé en termes d'expertise, de ressources et de motivation d'un attaquant.

51 **Produit** (Product) — Un ensemble de logiciels, microprogrammes ou matériels TI qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.

52 **Profil de Protection** (Protection Profile ou PP) — Un ensemble d'exigences de sécurité valables pour une catégorie de TOE, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

53 **Raffinement** (Refinement) — L'addition de détails à un composant.

54 **Résistance d'une fonction** (Strength of Function ou SOF) — La caractéristique d'une fonction de sécurité de la TOE exprimant les efforts minimum supposés nécessaires pour mettre en défaut le comportement de sécurité attendu par attaque directe des mécanismes de sécurité sous-jacents.

55 **SOF-élémentaire** (SOF-basic) — Un niveau de la résistance d'une fonction de la TOE tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation fortuite de la sécurité de la TOE par des attaquants possédant un potentiel d'attaque faible.

56 **SOF-moyen** (SOF-medium) — Un niveau de la résistance d'une fonction de la TOE tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation facile à mettre en œuvre ou une violation intentionnelle de la sécurité de la TOE par des attaquants possédant un potentiel d'attaque modéré.

57 **SOF-élevé** (SOF-high) — Un niveau de la résistance d'une fonction de la TOE tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation délibérément planifiée ou organisée de la sécurité de la TOE par des attaquants possédant un potentiel d'attaque élevé.

58 **Ressource d'une TOE** (TOE resource) — Tout élément utilisable ou consommable de la TOE.

59 **Rôle** (Role) — Un ensemble prédéfini de règles établissant les interactions autorisées entre un utilisateur et la TOE.

60 **Schéma d'évaluation** (Evaluation scheme) — Le cadre administratif et réglementaire dans lequel sont appliqués les critères par une autorité d'évaluation au sein d'une communauté spécifique.

61 **Secret** (Secret) — Informations qui ne doivent être connues que par des utilisateurs autorisés ou par la TSF afin d'appliquer une SFP spécifique.

62 **Sélection** (Selection) — La spécification d'une ou de plusieurs entités à partir d'une liste au sein d'un composant.

63 **Semi-formel** (Semiformal) — Qui est exprimé à l'aide d'un langage syntaxique restreint muni d'une sémantique définie.

64 **Sujet** (Subject) — Une entité interne au TSC qui provoque le déroulement d'opérations.

65 **Système** (System) — Une installation TI spécifique, avec un objectif et un environnement opérationnel particuliers.

66 **Transfert interne à la TOE** (Internal TOE transfer) — Données de communication entre parties séparées de la TOE.

67 **Transferts Inter-TSF** (Inter-TSF transfers) — Données de communication entre la TOE et les fonctions de sécurité d'autres produits TI de confiance.

68 **Transferts non contrôlés par les TSF** (Transfers outside TSF control) — Données de communication vers des entités qui ne sont pas sous le contrôle de la TSF.

69 **Utilisateur** (User) — Toute entité (utilisateur humain ou entité TI externe) hors de la TOE qui interagit avec elle.

70 **Utilisateur humain** (Human user) — Toute personne qui interagit avec la TOE.

71 **Utilisateur autorisé** (Authorised user) — Un utilisateur qui a le droit d'effectuer une opération, en accord avec la TSP.

# 3 Vue d'ensemble

72 Le présent chapitre introduit les principaux concepts des CC. Il identifie l'audience visée, le contexte de l'évaluation, et l'approche retenue pour présenter le sujet.

## 3.1 Introduction

73 Les informations contenues dans les produits ou systèmes TI constituent une ressource critique qui permet aux organisations de réussir leur mission. De plus, les particuliers s'attendent raisonnablement à ce que les informations personnelles contenues dans les produits ou systèmes TI demeurent confidentielles, soient disponibles quand ils en ont besoin et ne puissent pas faire l'objet de modifications non autorisées. Les produits ou systèmes TI devraient remplir leurs fonctions tout en exerçant un contrôle adéquat des informations afin d'assurer qu'elles sont protégées contre des dangers tels que la dissémination, l'altération ou la perte non désirée ou non autorisée. L'expression "sécurité des TI" est utilisée pour la prévention et la réduction de ces dangers et de dangers analogues.

74 De nombreux utilisateurs des TI ne possèdent pas la connaissance, l'expertise ou les ressources nécessaires pour juger si la confiance qu'ils accordent dans la sécurité de leurs produits ou systèmes TI est appropriée, et il est probable qu'ils ne souhaitent pas se fier uniquement aux affirmations des développeurs. En conséquence, les utilisateurs pourraient renforcer leur confiance dans les mesures de sécurité d'un produit ou système TI en faisant procéder à une analyse de sa sécurité (i.e., une évaluation de sécurité).

75 Les CC peuvent être utilisés pour sélectionner les mesures de sécurité des TI appropriées et contiennent des critères pour l'évaluation des exigences de sécurité.

## 3.2 Audience visée par les CC

76 Trois catégories de personnes sont intéressées de façon générale par l'évaluation des propriétés de sécurité des produits et systèmes TI. Il s'agit des utilisateurs de TOE, des développeurs de TOE et des évaluateurs de TOE. Les critères exposés dans le présent document ont été structurés de façon à satisfaire les besoins de ces trois catégories, qui sont considérées comme étant les utilisateurs principaux des CC. Les avantages que peuvent retirer ces trois catégories de l'utilisation des critères sont détaillés dans les paragraphes qui suivent.

### 3.2.1 Utilisateurs

77 Les CC jouent un rôle important en facilitant les techniques de sélection des exigences de sécurité des TI par les utilisateurs pour exprimer leurs besoins organisationnels. Les CC ont été rédigés de façon à garantir que l'évaluation répond aux besoins des utilisateurs, car il s'agit du but fondamental et de la justification du processus d'évaluation.

78 Les utilisateurs se servent des résultats des évaluations pour les aider à décider si un produit ou un système évalué répond à leurs besoins de sécurité. Ces besoins de sécurité résultent typiquement d'une analyse de risques et de la définition d'une stratégie politique. Les utilisateurs peuvent également utiliser les résultats d'évaluation pour comparer différents produits ou systèmes. La présentation hiérarchique des exigences d'assurance facilite ce besoin.

79 Les CC offrent aux utilisateurs, particulièrement à ceux constitués en groupes et en communautés d'intérêts, une structure appelée Profil de Protection (PP), indépendante de l'implémentation, dans laquelle ils peuvent exprimer leurs exigences spécifiques en termes de mesures de sécurité d'une TOE.

### 3.2.2 Développeurs

80 Les développeurs peuvent s'appuyer sur les CC pour préparer et aider à l'évaluation de leurs produits ou systèmes et pour identifier les exigences de sécurité que leur propre produit ou système doit satisfaire. Il est également tout à fait possible qu'une méthodologie d'évaluation associée, éventuellement accompagnée d'un accord de reconnaissance mutuelle des résultats d'évaluation, puisse permettre ultérieurement à quelqu'un, autre que le développeur de la TOE, et grâce à l'aide des CC, de préparer et d'aider à l'évaluation de la TOE d'un développeur.

81 Par la suite, ils peuvent utiliser les structures des CC pour déclarer que leur TOE est conforme à ses propres exigences grâce à des fonctions de sécurité et des composants d'assurance spécifiés, qui devront être évalués. Les exigences de chaque TOE se trouvent dans une structure qui dépend de l'implémentation, appelée Cible de Sécurité (ST : Security Target). Les exigences d'une grande partie de la clientèle du développeur peuvent être exprimées au moyen d'un ou de plusieurs PP.

82 Les CC décrivent les fonctions de sécurité qu'un développeur peut inclure dans la TOE. Les CC peuvent être utilisés pour déterminer les responsabilités et les actions contribuant à constituer les éléments de preuve nécessaires à l'évaluation de la TOE. Les CC définissent également le contenu et la présentation de ces éléments de preuves.

### 3.2.3 Évaluateurs

83 Les CC contiennent les critères que les évaluateurs doivent utiliser pour juger de la conformité des TOE à leurs exigences de sécurité. Les CC décrivent l'ensemble des actions d'ordre général que l'évaluateur doit mener, ainsi que les fonctions de sécurité auxquelles s'appliqueront ces actions. Il est à noter que les CC ne spécifient pas les procédures à suivre pour mener ces actions.

### 3.2.4 Autres parties

84 Bien que les CC soient orientés vers la spécification et l'évaluation des propriétés de sécurité des TI des TOE, ils peuvent être utiles en tant qu'éléments de référence à toutes les parties ayant un intérêt ou des responsabilités envers la sécurité des TI.

Citons quelques groupes pouvant tirer avantage des informations contenues dans les CC :

a) les personnes chargées de la surveillance des systèmes et les officiers de sécurité chargés de déterminer les politiques de sécurité organisationnelles et les exigences de sécurité, et de veiller à ce qu'elles soient satisfaites ;

b) les auditeurs internes ou externes, chargés d'estimer l'adéquation de la sécurité d'un système ;

c) les architectes et les concepteurs de la sécurité chargés de la spécification des mesures de sécurité des systèmes et produits TI ;

d) les homologateurs chargés d'autoriser la mise en œuvre d'un système TI dans un environnement spécifique ;

e) les commanditaires chargés de faire procéder à une évaluation et d'aider à son bon déroulement ;

f) les autorités d'évaluation chargées de la maîtrise d'œuvre et de la supervision des programmes d'évaluation de la sécurité des TI.

## 3.3 Contexte de l'évaluation

85 Pour faire en sorte que les résultats des évaluations soient plus facilement comparables, ces dernières doivent être conduites dans le cadre d'un schéma d'évaluation officiel qui permet de définir les normes, contrôler la qualité des évaluations et appliquer les règles auxquelles doivent se conformer les centres d'évaluation et les évaluateurs.

86 Les CC n'expriment pas d'exigences concernant le cadre réglementaire. Cependant, pour parvenir à l'objectif de reconnaissance mutuelle des résultats de telles évaluations, une cohérence entre les cadres réglementaires des différentes autorités d'évaluation sera nécessaire. La figure 3.1 décrit les principaux éléments qui constituent le contexte des évaluations.

87 L'utilisation d'une méthodologie d'évaluation commune contribue à la répétabilité et à l'objectivité des résultats, sans être toutefois suffisante par elle-même. La plupart des critères d'évaluation nécessitent des jugements d'expert et une connaissance générale du contexte, pour lesquels il est plus difficile de parvenir à une cohérence. Afin d'accroître la cohérence des résultats d'évaluation, les résultats finals d'évaluation peuvent être soumis à un processus de certification. Le processus de certification consiste en une vérification indépendante des résultats de l'évaluation conduisant à l'élaboration du certificat ou de l'approbation finale. Le certificat est normalement public. On notera que le processus de certification représente un moyen d'obtenir une cohérence plus grande dans l'application de critères de sécurité des TI.

88 Le schéma d'évaluation, la méthodologie et les processus de certification sont de la responsabilité des autorités d'évaluation qui assurent le bon fonctionnement des schémas d'évaluation, et sont en dehors du champ d'application des CC.

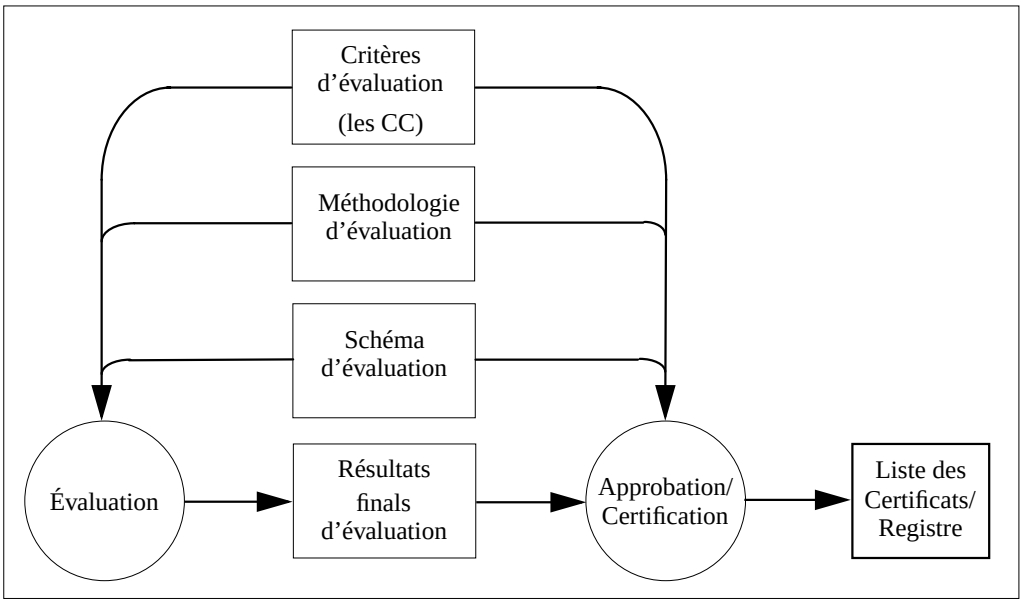


Figure 3.1 - Contexte d'évaluation

## 3.4 Organisation des Critères Communs

89 Les CC sont présentés en un ensemble de parties distinctes mais liées entre elles comme indiqué ci-dessous. Les termes utilisés dans la description de ces parties sont expliqués dans le Chapitre 4.

a) **La partie 1, Introduction et modèle général,** est l'introduction des CC. Elle définit les concepts généraux et les principes de l'évaluation de la sécurité des TI, et présente un modèle général d'évaluation. La partie 1 présente également des structures pour exprimer des objectifs de sécurité des TI, pour sélectionner et définir des exigences de sécurité des TI et pour écrire des spécifications générales pour produits et systèmes. De plus, l'utilité de chaque partie des CC est décrite en fonction de chacune des audiences visées**.**

b) **La partie 2, Exigences fonctionnelles de sécurité,** établit un ensemble de composants fonctionnels pour exprimer de façon standardisée les exigences fonctionnelles des TOE. La partie 2 propose un catalogue de l'ensemble des composants fonctionnels, des familles et des classes.

c) **La partie 3, Exigences d'assurance de sécurité,** établit un ensemble de composants d'assurance pour exprimer de façon standardisée les exigences d'assurance des TOE. La partie 3 propose un catalogue de l'ensemble des

composants d'assurance, des familles et des classes. La partie 3 définit également des critères d'évaluation pour PP et ST et présente les niveaux d'assurance de l'évaluation qui définissent l'échelle prédéfinie des CC pour coter l'assurance pour les TOE, constituée par les niveaux d'assurance de l'évaluation ou EAL (Evaluation Assurance Levels).

90 En complément des trois parties des CC citées ci-dessus, la parution d'autres types de documents comprenant des argumentaires techniques et des guides est attendue.

91 La table suivante présente, pour les trois catégories clé d'audience visées, la façon dont chaque partie des CC pourra les intéresser.

| | **Utilisateurs** | **Développeurs** | **Évaluateurs** |
|---|---|---|---|
| **Partie 1** | Utilisation comme référence et information générale. Guide sur la structure des PP. | Utilisation comme référence et information générale pour le développement des exigences et la formulation des spécifications de sécurité. | Utilisation comme référence et information générale. Guide sur la structure des PP et des ST. |
| **Partie 2** | Utilisation comme guide et comme référence pour formuler les exigences pour les fonctions de sécurité. | Utilisation comme référence pour interpréter les exigences fonctionnelles et formuler les spécifications fonctionnelles pour les TOE. | Utilisation comme critères d'évaluation obligatoires pour déterminer si une TOE réalise effectivement les fonctions de sécurité annoncées. |
| **Partie 3** | Utilisation comme guide pour déterminer les niveaux d'assurance requis. | Utilisation comme référence pour interpréter les exigences d'assurance et déterminer les approches d'assurance des TOE. | Utilisation comme critères d'évaluation obligatoires pour déterminer le niveau d'assurance des TOE et pour évaluer les PP et les ST. |

**Tableau 3.1 - Clés d'accès aux critères communs**

# 4 Modèle général

92 Le présent chapitre présente les concepts généraux utilisés tout au long des CC, ainsi que le contexte dans lequel les concepts doivent être utilisés et l'approche préconisée par les CC pour les appliquer. Les parties 2 et 3 s'étendent sur l'utilisation de ces concepts et supposent que l'approche décrite est suivie. Le présent chapitre suppose chez le lecteur des connaissances dans le domaine de la sécurité des TI et n'est pas censé servir de support de cours dans ce domaine.

93 Les CC traitent de sécurité en utilisant un ensemble de concepts et une terminologie relatifs à la sécurité. Une compréhension de ces concepts et de la terminologie est une condition préalable à l'utilisation efficace des CC. Cependant, les concepts eux-mêmes sont tout à fait généraux et ne sont pas destinés à restreindre la classe des problèmes de sécurité des TI à laquelle s'appliquent les CC.

## 4.1 Le contexte de la sécurité

### 4.1.1 Contexte général de la sécurité

94 La sécurité a trait à la protection de biens contre des menaces, ces dernières étant classées selon leur potentiel de nuisance envers les biens protégés. Toutes les catégories de menaces devraient être prises en compte, mais dans le domaine de la sécurité une plus grande attention est accordée aux menaces liées à des activités humaines malveillantes ou non. La figure 4.1 illustre les concepts de haut niveau avec leurs relations.

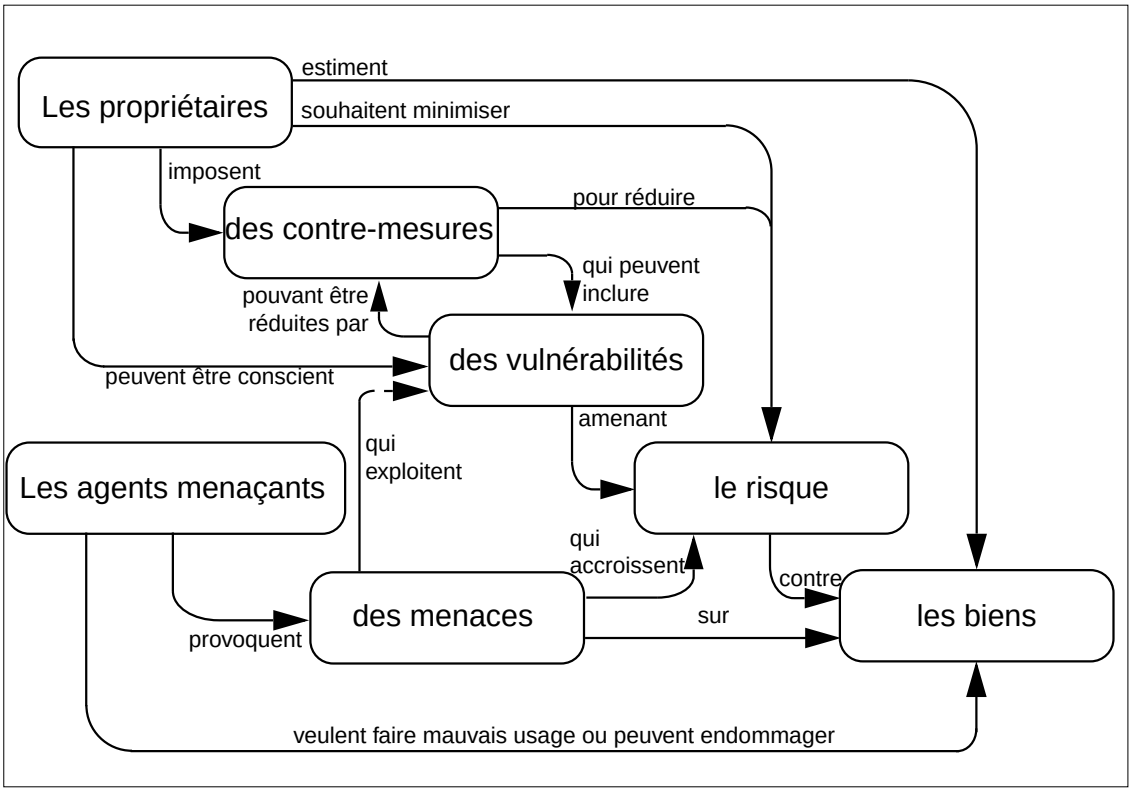


Figure 4.1 - Concepts de sécurité et relations

95 La sauvegarde des biens dignes d'intérêt est de la responsabilité des propriétaires pour qui ces biens ont de la valeur. Des agents menaçants, réels ou présumés, peuvent aussi attacher de la valeur à ces biens et chercher à en faire un usage contraire aux intérêts du propriétaire. Les propriétaires vont percevoir de telles menaces comme un potentiel d'altération des biens dont la valeur serait diminuée à leurs yeux. La liste des altérations spécifiques à la sécurité comprend habituellement, sans y être limitée, la divulgation nuisible du bien à des destinataires non autorisés (perte de confidentialité), un dommage provoqué au bien par une modification non autorisée (perte d'intégrité) ou un déni d'accès au bien (perte de disponibilité).

96 Les propriétaires des biens vont analyser les menaces possibles pour déterminer celles qui s'appliquent à leur environnement. Les résultats de cette analyse sont les risques. Cette analyse peut être utile au choix des contre-mesures pour contrer les risques et les ramener à un niveau acceptable.

97 Les contre-mesures sont imposées pour réduire les vulnérabilités et pour satisfaire aux politiques de sécurité des propriétaires des biens (soit de façon directe, soit de façon indirecte en donnant des instructions aux autres parties). Des vulnérabilités résiduelles peuvent persister après la mise en œuvre de contre-mesures. De telles vulnérabilités peuvent être exploitées par les agents menaçants, constituant ainsi un

niveau de risque résiduel à l'encontre des biens. Les propriétaires vont chercher à minimiser ce risque en prenant en compte d'autres contraintes.

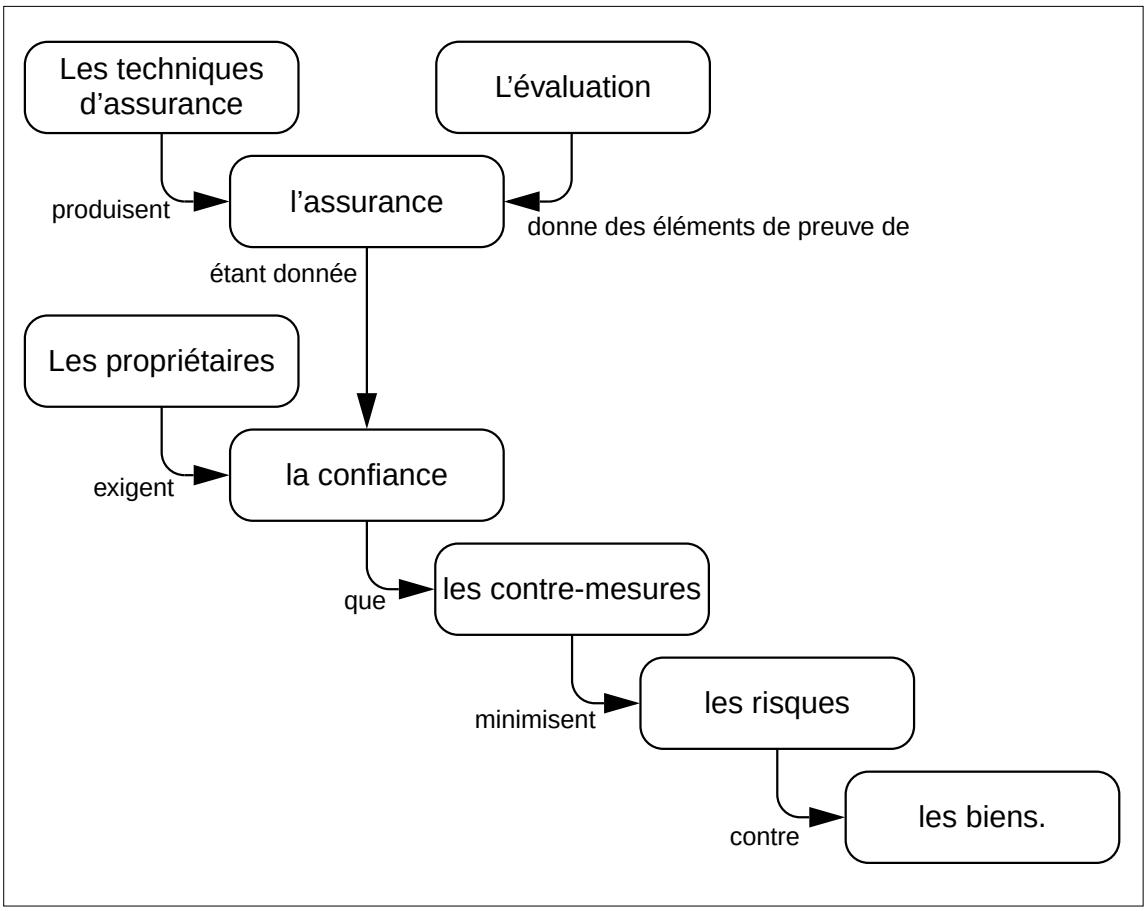


Figure 4.2 - Concepts de l'évaluation et relations

98 Les propriétaires auront besoin d'avoir confiance dans le fait que les contre-mesures sont adéquates pour contrer les menaces qui pèsent sur les biens avant de permettre que leurs biens soient exposés aux menaces spécifiées. Les propriétaires peuvent ne pas posséder par eux-mêmes la capacité de juger tous les aspects des contre-mesures et par conséquent peuvent chercher à les faire évaluer. Le résultat de l'évaluation est une déclaration concernant l'étendue de l'assurance que l'on peut avoir sur la confiance à accorder aux contre-mesures pour réduire les risques contre des biens protégés. La déclaration attribue une cotation de l'assurance des contre-mesures, l'assurance étant la propriété des contre-mesures qui fonde la confiance dans leur bon fonctionnement. Cette déclaration peut être utilisée par le propriétaire des biens pour décider s'il accepte ou non le risque d'exposer les biens aux menaces. La figure 4.2 illustre ces relations.

99 Les propriétaires des biens sont normalement tenus pour responsables de ceux-ci et devraient par conséquent être capables de justifier la décision consistant à accepter

le risque d'exposer les biens aux menaces. Ceci nécessite que les déclarations résultant de l'évaluation puissent être justifiées. Ainsi l'évaluation devrait conduire à des résultats objectifs et répétables pouvant être utilisés comme preuve.

### 4.1.2 Contexte de la sécurité des technologies de l'information

100 Beaucoup de biens se présentent sous la forme d'informations qui sont stockées, traitées et transmises par des produits ou systèmes TI pour satisfaire aux exigences définies par les propriétaires de ces informations. Ces derniers peuvent demander que la diffusion et la modification de toutes les représentations de ces informations (des données) soient strictement contrôlées. Ils peuvent exiger que les produits ou systèmes TI mettent en œuvre des contrôles de sécurité TI spécifiques faisant partie de l'ensemble des contre-mesures de sécurité installées pour contrecarrer les menaces envers les données.

101 Les systèmes TI sont acquis et construits pour satisfaire à des exigences spécifiques et se doivent, pour des raisons économiques, d'utiliser au maximum les produits TI de base existants tels que des systèmes d'exploitation, des applications d'usage général et des plates-formes matérielles. Les contre-mesures de sécurité des TI mises en œuvre par un système peuvent utiliser des fonctions des produits TI sous-jacents et dépendre du fonctionnement correct de fonctions de sécurité du produit TI. Les produits TI peuvent, par conséquent, faire l'objet d'évaluation en tant que partie de l'évaluation de sécurité du système TI.

102 Quand on incorpore ou qu'on envisage d'incorporer un produit TI dans plusieurs systèmes TI, l'évaluation indépendante des aspects de sécurité d'un tel produit et l'élaboration d'un catalogue de produits évalués présentent des avantages en terme de coût. Les résultats d'une telle évaluation devraient être présentés de façon à aider à l'incorporation du produit dans plusieurs systèmes TI sans avoir besoin de répéter inutilement le travail exigé pour examiner la sécurité offerte par le produit.

103 Un homologateur d'un système TI possède, par délégation du propriétaire des informations, l'autorité de déterminer si la combinaison des contre-mesures de sécurité TI et non TI fournit une protection adéquate des données et ainsi de décider s'il autorise la mise en exploitation du système. L'homologateur peut demander l'évaluation des contre-mesures TI pour déterminer si elles fournissent une protection adéquate et si les contre-mesures spécifiées sont correctement mises en œuvre par le système TI. Cette évaluation peut prendre différentes formes et différents degrés dans la rigueur, en fonction des règles imposées pour ou par l'homologateur.

## 4.2 L'approche des Critères Communs

104 La confiance dans la sécurité des TI peut être obtenue par des actions qui peuvent être effectuées pendant les processus de développement, d'évaluation et d'exploitation.

### 4.2.1 Développement

105 Les CC n'imposent aucune méthodologie de développement spécifique ni de modèle de cycle de vie. La figure 4.3 présente les hypothèses sous-jacentes concernant les relations entre les exigences de sécurité et la TOE. La figure donne une base de discussion et ne doit pas être interprétée comme marquant une préférence pour une méthodologie (e.g. l'approche descendante) par rapport à une autre (e.g l'approche par prototypage).

106 Il est essentiel que les exigences de sécurité imposées lors du développement des TI contribuent efficacement aux objectifs de sécurité des utilisateurs. À moins que des exigences adaptées n'aient été établies au début du processus de développement, le produit final qui en résulte, même s'il a été bien conçu, peut ne pas satisfaire les objectifs de ses utilisateurs présumés.

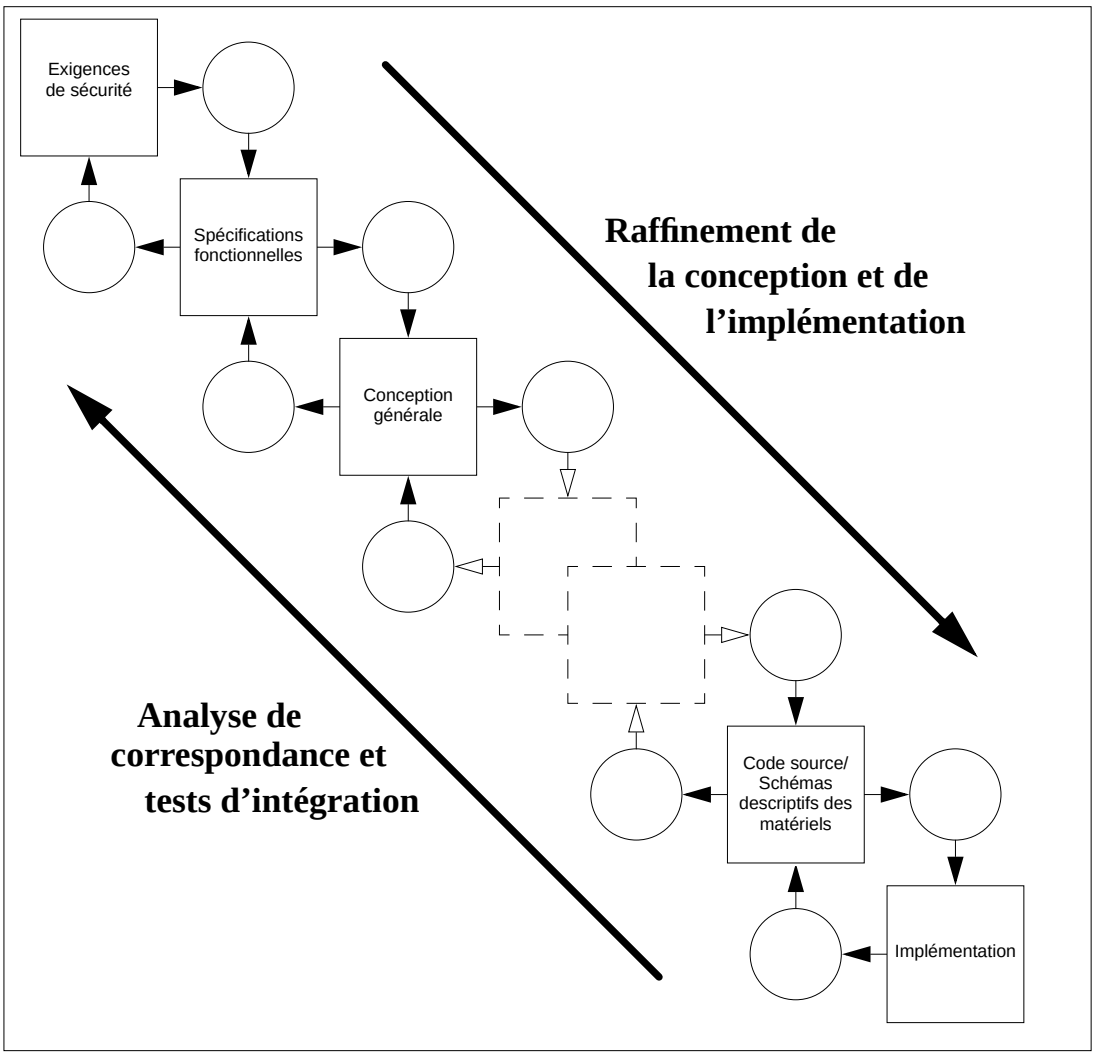


Figure 4.3 - Modèle de développement d'une TOE

107 Le processus est basé sur le raffinement des exigences de sécurité en des spécifications globales de la TOE exprimées dans la cible de sécurité. Chaque niveau suivant de raffinement représente un approfondissement de la conception avec l'addition de détails supplémentaires. Le niveau de représentation le moins abstrait est l'implémentation de la TOE elle-même.

108 Les CC n'imposent pas un ensemble particulier de représentations de la conception. Les CC exigent qu'il y aient suffisamment de représentations de la conception, présentées à un niveau de granularité suffisant pour démontrer lorsque cela est demandé :

a) que chaque niveau de raffinement constitue une instantiation complète des niveaux supérieurs (i.e. toutes les fonctions de sécurité, les propriétés et le comportement de la TOE définis au niveau d'abstraction supérieur doivent être présents de façon démontrable dans le niveau inférieur) ;

b) que chaque niveau de raffinement constitue une instantiation exacte des niveaux supérieurs (i.e. il ne devrait y avoir aucune fonction, propriété ou comportement de sécurité de la TOE définis au niveau d'abstraction inférieur qui ne soit exigé par le niveau supérieur).

109 Les critères d'assurance des CC identifient les niveaux suivants d'abstraction de la conception : spécification fonctionnelle, conception générale, conception détaillée et implémentation. Selon le niveau d'assurance spécifié, il peut être exigé des développeurs qu'ils montrent comment la méthodologie de développement satisfait aux exigences d'assurance des CC.

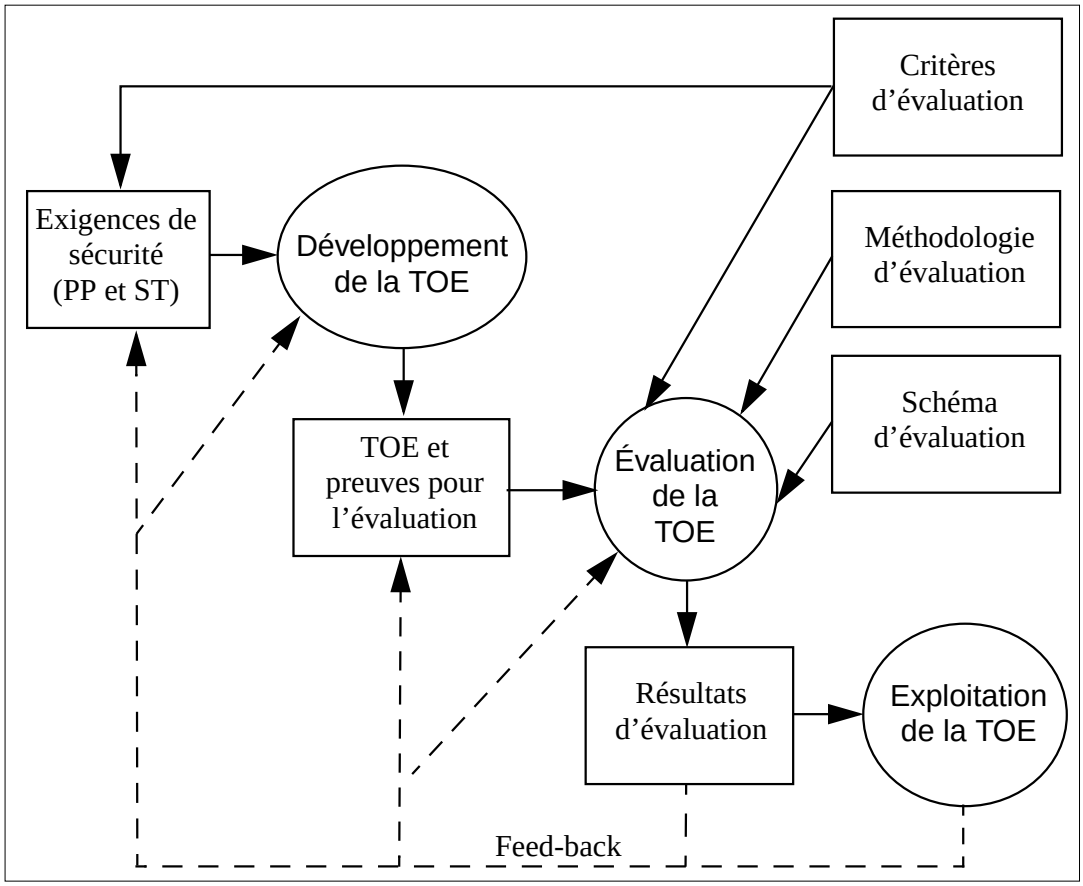


Figure 4.4 - Processus d'évaluation de la TOE

### 4.2.2 Évaluation de la TOE

110 Le processus d'évaluation de la TOE tel qu'il est décrit dans la figure 4.4 peut être mené en parallèle avec le développement, ou consécutivement. Les principales données pour l'évaluation de la TOE sont :

a) l'ensemble des éléments de preuve concernant la TOE, incluant la cible de sécurité (ST) évaluée comme base d'évaluation de la TOE ;

b) la TOE pour laquelle l'évaluation est demandée ;

c) les critères, méthodologie et schéma d'évaluation.

111 En supplément, des éléments à caractère informatif (tels que les notes d'application des CC) et l'expertise en sécurité des TI de l'évaluateur et de la communauté des évaluateurs sont susceptibles d'être utilisés comme données pouvant servir à l'évaluation.

112 Le résultat attendu du processus d'évaluation est une confirmation que la TOE satisfait à ses exigences de sécurité telles qu'elles sont définies dans la ST ainsi qu'un ou plusieurs rapports expliquant les conclusions de l'évaluateur concernant la TOE, conformément aux critères d'évaluation. Ces rapports seront utiles aux utilisateurs effectifs ou potentiels du produit ou du système représenté par la TOE, ainsi qu'au développeur.

113 Le degré de confiance obtenu au moyen d'une évaluation dépend des exigences d'assurance satisfaites (e.g. le niveau d'assurance de l'évaluation).

114 L'évaluation peut permettre d'améliorer les produits de sécurité des TI de deux façons. L'évaluation a pour but d'identifier les erreurs ou les vulnérabilités de la TOE auxquelles le développeur peut remédier, réduisant ainsi la probabilité de défaillances de sécurité lors d'une exploitation ultérieure. De plus, en se préparant au processus rigoureux de l'évaluation, le développeur peut porter plus de soin à la conception et au développement de la TOE. Par conséquent, le processus d'évaluation peut exercer un puissant effet positif, bien qu'indirect, sur les exigences initiales, le processus de développement, le produit final et l'environnement d'exploitation.

### 4.2.3 Exploitation

115 Les utilisateurs peuvent choisir d'utiliser dans leurs environnements propres des TOE évaluées. Une fois que la TOE est en exploitation, il est possible que des erreurs ou des vulnérabilités inconnues précédemment apparaissent ou bien que les hypothèses sur l'environnement aient besoin d'être révisées. Résultant de l'exploitation, un retour d'expérience pourrait être donné qui entraînerait de la part du développeur une correction de la TOE ou bien une redéfinition de ses exigences de sécurité ou des hypothèses sur l'environnement. De telles modifications peuvent entraîner une ré-évaluation de la TOE ou un renforcement de la sécurité de son environnement opérationnel. Dans quelques cas, l'évaluation des modifications nécessaires peut suffire pour donner à nouveau confiance dans la TOE. Bien que les CC contiennent des critères qui couvrent la maintenance de l'assurance, les procédures détaillées pour la ré-évaluation, incluant la réutilisation des résultats d'évaluation, sont en dehors du champ d'application des CC.

## 4.3 Concepts de sécurité

116 Les critères d'évaluation sont très utiles dans le contexte des processus de conception et des cadres réglementaires qui permettent un développement et une évaluation sécurisés de la TOE. La présente section n'est fournie qu'à titre d'illustration et de conseil et n'a pas pour but d'imposer des contraintes aux processus d'analyse, aux approches sur le développement ou aux schémas d'évaluation dans le cadre desquels les CC peuvent être utilisés.

117 Les CC sont applicables dès qu'on utilise les TI et qu'il existe des préoccupations sur la capacité de l'élément TI à protéger les biens. Pour montrer que les biens sont protégés, les préoccupations concernant la sécurité doivent être traitées à tous les niveaux, depuis le niveau le plus abstrait jusqu'à l'implémentation finale des TI

dans leur environnement opérationnel. Ces niveaux de représentation, tels qu'ils sont décrits dans les sous-sections suivantes, permettent aux problèmes et aux questions de sécurité d'être caractérisés et débattus, mais ils ne constituent pas par eux-mêmes une démonstration que l'implémentation finale des TI présente réellement le comportement de sécurité exigé et qu'on peut, par conséquent, leur faire confiance.

118 Les CC exigent que certains niveaux de représentation contiennent un argumentaire concernant la représentation de la TOE à ce niveau. Ainsi, un tel niveau doit contenir des arguments bien pensés et convaincants montrant qu'il est en adéquation avec le niveau supérieur et qu'il est lui-même complet, correct et forme un tout cohérent. Les énoncés de l'argumentaire relatifs à la conformité avec la représentation de niveau immédiatement supérieur contribuent à démontrer la conformité de la TOE. Un argumentaire qui démontre directement l'adéquation avec les objectifs de sécurité permet de soutenir que la TOE contre efficacement les menaces et qu'elle met en œuvre la politique de sécurité organisationnelle.

119 Les CC décomposent en couches les différents niveaux de représentation comme cela est décrit dans la figure 4.5, qui illustre les moyens par lesquels on peut parvenir à déduire les exigences et les spécifications de sécurité en développant un PP ou une ST. Toutes les exigences de sécurité de la TOE proviennent en fin de compte des considérations concernant le but et le contexte de la TOE. Ce graphique n'est pas destiné à imposer des contraintes sur les moyens de développement des PP et ST, mais il illustre la façon dont les résultats de certaines approches analytiques se rapportent au contenu des PP et ST.

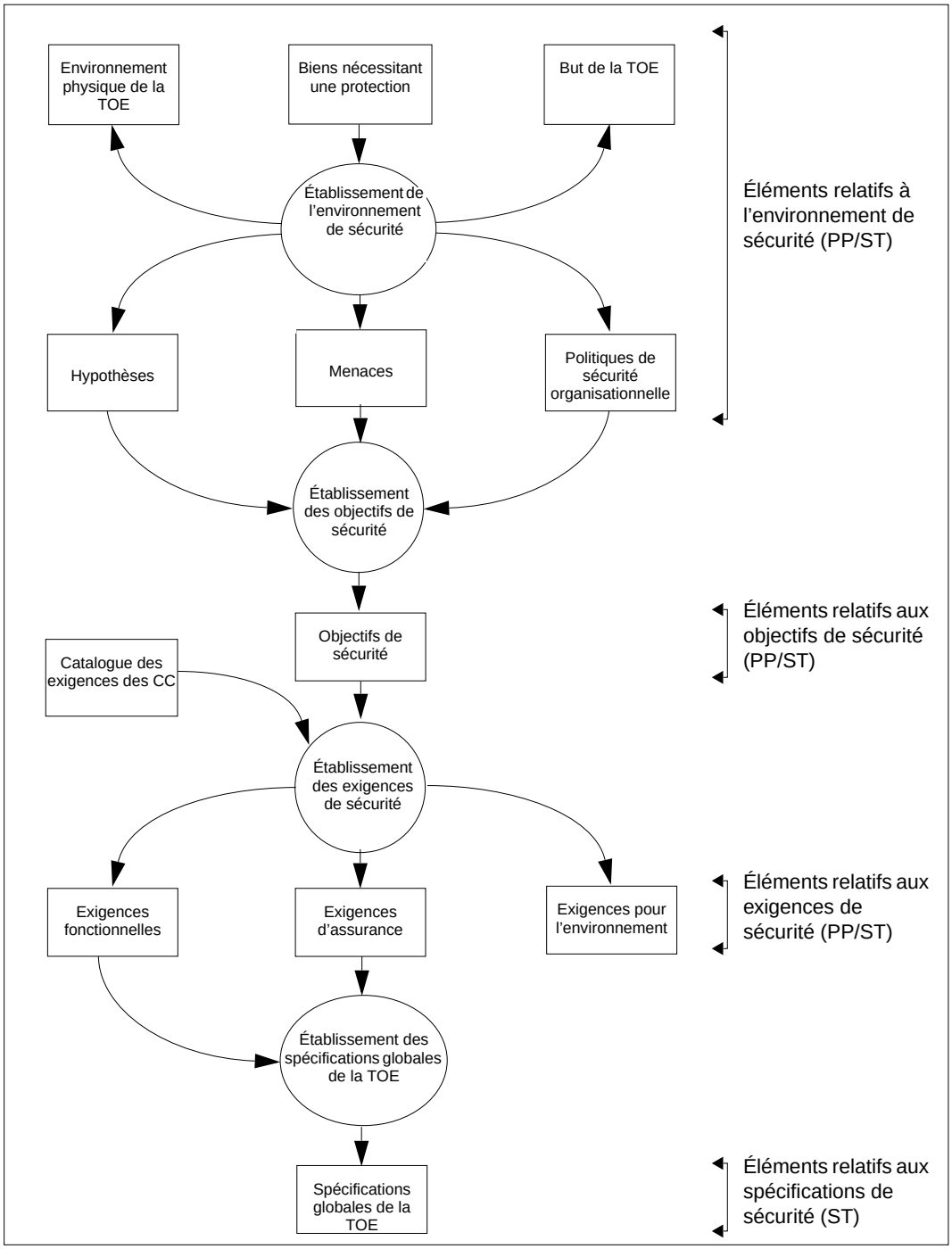


Figure 4.5 - Déduction des exigences et des spécifications

### 4.3.1 Environnement de sécurité

120 L'environnement de sécurité inclut toutes les lois, les politiques de sécurité organisationnelles, les coutumes, l'expertise et la connaissance considérées comme pertinentes. Il définit ainsi le contexte dans lequel il est prévu d'utiliser la TOE. L'environnement de sécurité inclut également les menaces contre la sécurité qui sont présentes dans l'environnement ou censées l'être.

121 Pour établir l'environnement de sécurité, le rédacteur du PP ou de la ST doit prendre en compte :

a) l'environnement physique de la TOE qui identifie tous les aspects de l'environnement d'exploitation de la TOE concernant la sécurité de la TOE, y compris les modalités pratiques connues relatives à la sécurité physique et au personnel ;

b) les biens nécessitant une protection par l'élément de la TOE auquel s'appliqueront les exigences ou les politiques de sécurité ; cela peut inclure des biens auxquels on se réfère directement tels que des fichiers et bases de données, ainsi que des biens indirectement assujettis à des exigences de sécurité, tels que la liste des droits des utilisateurs et l'implémentation des TI elle-même ;

c) le but de la TOE, indiquant son utilisation prévue et le type de produit qu'elle concerne.

122 L'investigation des politiques de sécurité, des menaces et des risques devrait permettre de formuler les déclarations suivantes relatives à la sécurité de la TOE :

a) Une formulation des hypothèses devant être satisfaites par l'environnement de la TOE afin de pouvoir considérer la TOE comme sûre. Cette déclaration peut être considérée comme un axiome pour l'évaluation de la TOE.

b) Une formulation des menaces contre la sécurité des biens identifiant toutes celles perçues lors de l'analyse de sécurité comme s'appliquant à la TOE. Les CC caractérisent une menace en termes d'un élément menaçant, d'une méthode d'attaque présumée, de toutes les vulnérabilités qui sont à la base de l'attaque et de l'identification du bien attaqué. Une évaluation des risques contre la sécurité attribuerait à chaque menace une estimation de la probabilité qu'une telle menace donne lieu à une véritable attaque, la probabilité qu'une telle attaque réussisse et les conséquences de tous les dommages qui peuvent en résulter.

c) Une formulation des politiques de sécurité applicables identifiant les politiques et règles pertinentes. Pour un système TI, de telles politiques peuvent être référencées explicitement, tandis que pour un produit ou une classe de produits TI d'usage général, il peut être nécessaire de faire des hypothèses de travail concernant la politique de sécurité organisationnelle.

### 4.3.2 Objectifs de sécurité

123 Les résultats de l'analyse de l'environnement de sécurité pourraient alors être utilisés pour présenter les objectifs de sécurité qui contrent les menaces identifiées et prennent en compte les politiques de sécurité organisationnelles et les hypothèses identifiées. Les objectifs de sécurité devraient être cohérents avec le but opérationnel ou l'usage déclaré de la TOE, et toute connaissance sur son environnement physique.

124 La détermination des objectifs de sécurité a pour but de traiter toutes les préoccupations relatives à la sécurité et de déclarer les aspects de sécurité qui sont soit pris en compte directement par la TOE, soit par son environnement. Cette distinction est basée sur un processus incluant un jugement sur le développement, la politique de sécurité, les facteurs économiques et les décisions d'accepter les risques.

125 Les objectifs de sécurité pour l'environnement seraient pris en compte dans le domaine des TI et par des mesures non techniques ou procédurales.

126 Seuls les objectifs de sécurité concernant la TOE et son environnement TI sont pris en compte par les exigences de sécurité des TI.

### 4.3.3 Exigences de sécurité des TI

127 Les exigences de sécurité des TI résultent du raffinement des objectifs de sécurité en un ensemble d'exigences de sécurité pour la TOE et d'exigences de sécurité pour l'environnement qui, si elles sont satisfaites, garantiront que la TOE peut satisfaire à ses objectifs de sécurité.

128 Les CC présentent les exigences de sécurité en deux catégories différentes : exigences fonctionnelles et exigences d'assurance.

129 Les exigences fonctionnelles portent sur les fonctions de la TOE qui contribuent tout particulièrement à la sécurité des TI et qui déterminent le comportement voulu en terme de sécurité. La partie 2 définit les exigences fonctionnelles des CC. Citons comme exemples d'exigences fonctionnelles, les exigences concernant l'identification, l'authentification, l'audit de sécurité et la non répudiation de l'origine.

130 Lorsque la TOE contient des fonctions de sécurité qui sont réalisées au moyen d'un mécanisme utilisant les probabilités ou les permutations (e.g. un mot de passe ou une fonction de hachage), les exigences d'assurance peuvent spécifier qu'un niveau minimum de résistance cohérent avec les objectifs de sécurité doit être visé. Dans ce cas, le niveau spécifié sera choisi parmi les niveaux suivants : SOF-élémentaire, SOF-moyen, SOF-élevé. Chacune de ces fonctions devra satisfaire ce niveau minimum ou du moins une métrique spécifique bien définie.

131 Le degré d'assurance peut varier pour un ensemble donné d'exigences fonctionnelles ; il s'exprime donc typiquement en termes de niveaux croissants de rigueur construits avec des composants d'assurance. La partie 3 définit les

exigences d'assurance des CC ainsi qu'une échelle de niveaux d'assurance de l'évaluation (EAL) construite en utilisant ces composants. Les exigences d'assurance portent sur les actions du développeur, les éléments de preuve produits et les actions de l'évaluateur. Citons comme exemples d'exigences d'assurance, les contraintes sur la rigueur du processus de développement et les exigences pour rechercher et analyser l'impact des vulnérabilités de sécurité potentielles.

132 L'assurance que les objectifs de sécurité sont atteints au moyen des fonctions de sécurité sélectionnées provient des deux facteurs suivants :

a) la confiance dans la conformité de l'implémentation des fonctions de sécurité, i.e. l'estimation qu'elles sont correctement implémentées ;

b) la confiance dans l'efficacité des fonctions de sécurité, i.e. l'estimation qu'elles satisfont effectivement aux objectifs de sécurité exprimés.

133 Les exigences de sécurité comprennent en général à la fois des exigences pour la présence de comportements souhaités et pour l'absence de comportements non souhaités. Il est normalement possible de démontrer, par l'utilisation ou le test, qu'un comportement souhaité est bien présent. Il n'est pas toujours possible d'effectuer une démonstration concluante sur l'absence d'un comportement non souhaité. Le test, l'examen de la conception et l'examen de l'implémentation contribuent de façon significative à la réduction du risque qu'un tel comportement soit présent. Les éléments de l'argumentaire fournissent un complément d'information pour montrer qu'un tel comportement non souhaité est absent.

### 4.3.4 Spécifications globales de la TOE

134 Les spécifications globales de la TOE qui sont données dans la ST définissent l'instantiation des exigences de sécurité pour la TOE. Elles procurent une définition de haut niveau des fonctions de sécurité censées satisfaire aux exigences fonctionnelles, ainsi que les mesures d'assurance prises pour satisfaire aux exigences d'assurance.

### 4.3.5 Implémentation de la TOE

135 L'implémentation de la TOE est le résultat de la réalisation de la TOE sur la base de ses exigences fonctionnelles et des spécifications globales de la TOE contenues dans la ST. L'implémentation de la TOE est accomplie par un processus qui combine l'application de la sécurité avec la connaissance et le savoir-faire en conception des TI. La TOE satisfera aux objectifs de sécurité si elle met en œuvre correctement et efficacement toutes les exigences contenues dans la ST.

## 4.4 Éléments descriptifs des CC

136 Les CC présentent le cadre dans lequel peut se dérouler une évaluation. En fournissant les exigences concernant les éléments de preuve et l'analyse, des résultats d'évaluation plus objectifs et donc plus utiles peuvent être obtenus. Les CC intègrent un ensemble commun de structures et un langage dans lequel on peut

exprimer et communiquer les aspects pertinents de la sécurité des TI, et permettent aux responsables de la sécurité des TI de tirer avantage de l'expérience et de l'expertise acquises par d'autres.

### 4.4.1 Expression des exigences de sécurité

137 Les CC définissent un catalogue de structures qui se combinent en ensembles significatifs d'exigences de sécurité d'une validité déterminée, qui peuvent être utilisés pour établir les exigences de sécurité d'éventuels produits et systèmes. Les relations existant entre les différentes structures pour l'expression des exigences sont décrites ci-après et illustrées dans la figure 4.6.

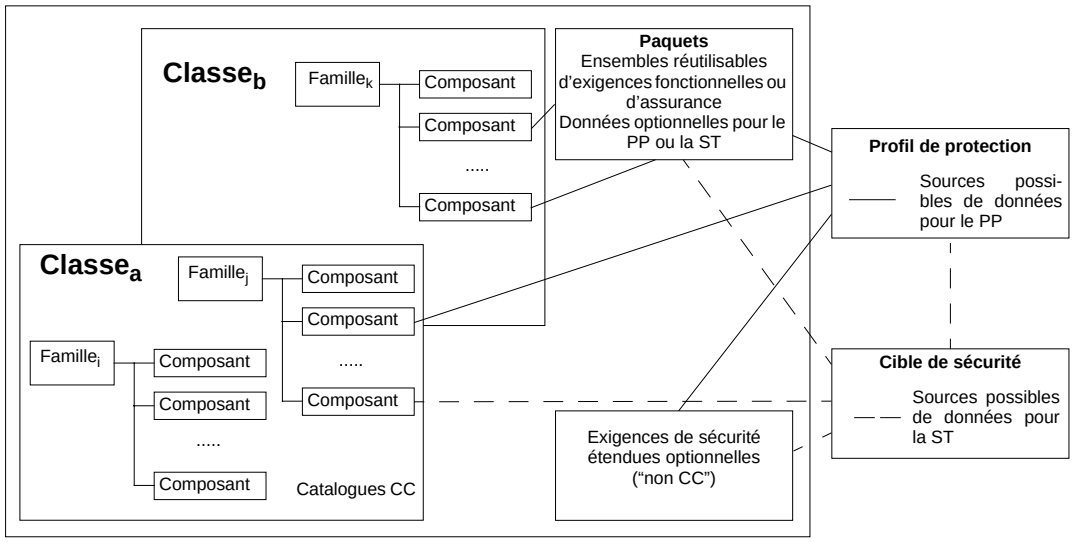


Figure 4.6 - Organisation et construction des exigences

138 L'organisation des exigences de sécurité des CC dans la hiérarchie classe-famille-composant est présentée dans le but d'aider les utilisateurs à repérer des exigences de sécurité spécifiques.

139 Les CC présentent des exigences pour les aspects fonctionnels et d'assurance dans le même style général et utilisent la même organisation et la même terminologie pour chacun d'entre eux.

#### 4.4.1.1 Classe

140 Le terme "classe" est utilisé pour désigner le groupement le plus général d'exigences de sécurité. Tous les membres d'une classe partagent un thème commun, mais diffèrent dans la couverture des objectifs de sécurité.

141 Les membres d'une classe sont appelés familles.

#### 4.4.1.2 Famille

142 Une famille est un groupement d'ensembles d'exigences de sécurité qui ont en commun les mêmes objectifs de sécurité mais qui peuvent différer dans l'accentuation ou dans la rigueur.

143 Les membres d'une même famille sont appelés composants.

#### 4.4.1.3 Composant

144 Un composant décrit un ensemble spécifique d'exigences de sécurité et constitue le plus petit ensemble d'exigences de sécurité que l'on peut sélectionner pour l'inclure dans les structures définies dans les CC. L'ensemble des composants à l'intérieur d'une famille peut être ordonné pour représenter des exigences de sécurité de force ou de capacité croissantes partageant un but commun. Les composants peuvent aussi être partiellement ordonnés pour représenter des ensembles liés mais non hiérarchiques. Dans certains cas, il n'y a qu'un composant dans une famille et l'ordonnancement est sans objet.

145 Les composants sont construits à partir d'éléments individuels. L'élément constitue le plus bas niveau d'expression d'exigences de sécurité et l'exigence de sécurité indivisible qui peut être vérifiée par l'évaluation.

##### Dépendances entre composants

146 Il peut exister des dépendances entre composants. Des dépendances apparaissent quand un composant n'est pas auto-suffisant et dépend de la présence d'un autre composant. Il peut exister des dépendances entre composants fonctionnels, entre composants d'assurance, et entre composants fonctionnels et composants d'assurance.

147 Les descriptions de dépendance des composants font partie de la définition des composants CC. Pour assurer la complétude des exigences de la TOE, les dépendances devraient être satisfaites lors de l'incorporation de composants dans les PP et les ST, quand cela est approprié.

##### Opérations autorisées sur les composants

148 Les composants CC peuvent être utilisés exactement comme cela est défini dans les CC, ou bien ils peuvent être adaptés par l'utilisation d'opérations autorisées pour les besoins d'une politique de sécurité spécifique ou pour contrer une menace spécifique. Chaque composant CC identifie et définit toute opération autorisée d'affectation et de sélection, les circonstances dans lesquelles ces opérations peuvent être appliquées aux composants et les résultats de l'application de l'opération. Les opérations d'itération et de raffinement peuvent être effectuées pour tout composant. Les quatre opérations possibles sont décrites ci-dessous :

a) **l'itération** qui autorise l'utilisation d'un composant plus d'une fois avec des opérations variées ;

b) **l'affectation** qui permet de spécifier un paramètre qui doit être renseigné quand le composant est utilisé ;

c) **la sélection** qui permet de spécifier des objets qui doivent être sélectionnés à partir d'une liste donnée dans le composant ;

d) **le raffinement** qui permet l'addition de détails supplémentaires quand le composant est utilisé.

149 Certaines opérations exigées peuvent être effectuées (en totalité ou en partie) dans le PP ou peuvent attendre d'être effectuées dans la ST. De toutes façons, toutes les opérations devront avoir été effectuées dans la ST.

### 4.4.2 Utilisation des exigences de sécurité

150 Les CC définissent trois types de structures d'exigences : paquet, PP et ST. Les CC définissent également un ensemble de critères pour la sécurité des TI qui peuvent couvrir les besoins de nombreuses communautés et servir ainsi d'expertise majeure pour alimenter la production de ces structures. Les CC ont été développés avec l'idée centrale d'utiliser chaque fois que possible les composants d'exigences de sécurité qui y sont définis, et qui représentent un domaine bien connu et bien compris. La figure 4.7 indique les relations existant entre ces différentes structures.

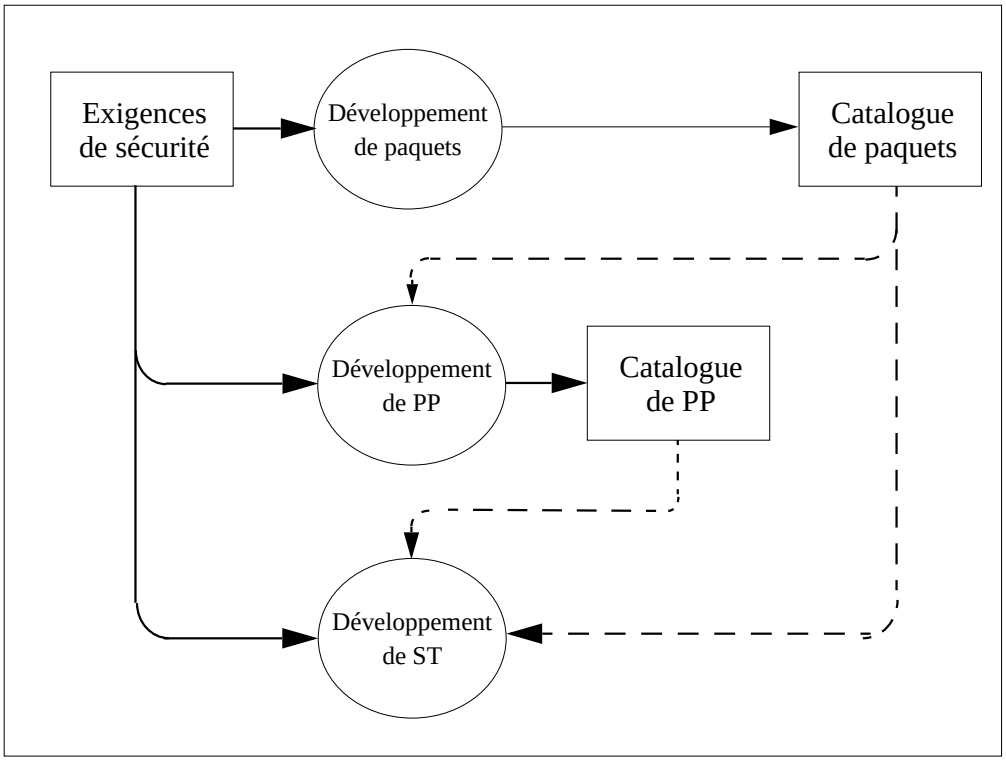


Figure 4.7 - Utilisation des exigences de sécurité

#### 4.4.2.1 Paquet

151 Une combinaison intermédiaire de composants est appelée un paquet. Le paquet permet d'exprimer un ensemble d'exigences fonctionnelles ou d'assurance qui répondent à un sous-ensemble identifiable d'objectifs de sécurité. Un paquet est prévu pour être réutilisable et pour définir des exigences qui sont connues pour être utiles et efficaces pour répondre aux objectifs identifiés. Un paquet peut être utilisé dans la construction de paquets plus importants, de PP et de ST.

152 Les niveaux d'assurance de l'évaluation (EAL) sont des paquets d'assurance prédéfinis contenus dans la partie 3. Un EAL est un ensemble de base d'exigences d'assurance pour l'évaluation. Chaque EAL définit un ensemble cohérent d'exigences d'assurance. Les EAL forment un ensemble ordonné qui constitue l'échelle d'assurance prédéfinie des CC.

#### 4.4.2.2 Profil de protection

153 Le PP contient un ensemble d'exigences de sécurité qui sont soit issues des CC, soit formulées explicitement et qui devrait inclure un EAL (éventuellement augmenté par des composants d'assurance supplémentaires). Le PP permet, de façon indépendante de l'implémentation, l'expression d'exigences de sécurité pour un ensemble de TOE qui se conformeront complètement à un ensemble d'objectifs de sécurité. Un PP est prévu pour être réutilisable et pour définir des exigences pour la TOE qui sont connues pour être utiles et efficaces pour répondre aux objectifs identifiés, à la fois pour les fonctions et pour l'assurance. Un PP contient également l'argumentaire pour les objectifs de sécurité et les exigences de sécurité.

154 Un PP pourrait être développé par des communautés d'utilisateurs, des développeurs de produits TI, ou d'autres parties intéressées par la définition d'un tel ensemble commun d'exigences. Un PP donne aux utilisateurs un moyen de se référer à un ensemble spécifique de besoins de sécurité et facilite une évaluation future par rapport à ces besoins.

#### 4.4.2.3 Cible de sécurité

155 Une ST contient un ensemble d'exigences de sécurité qui peut être constitué par référence à un PP, ou directement par référence à des composants fonctionnels ou d'assurance des CC, ou encore formulés explicitement. Une ST permet l'expression d'exigences de sécurité pour une TOE spécifique dont l'évaluation montre qu'elles sont utiles et efficaces pour satisfaire aux objectifs identifiés.

156 Une ST contient les spécifications globales de la TOE ainsi que les exigences et les objectifs de sécurité et leurs argumentaires respectifs. Une ST constitue la base de l'accord entre toutes les parties sur la sécurité offerte par la TOE.

### 4.4.3 Les sources d'exigences de sécurité

157 Les exigences de sécurité de la TOE peuvent être élaborées à partir des données suivantes :

a) Les PP existants

Les exigences de sécurité de la TOE dans une ST peuvent être exprimées de manière adéquate par des exigences pré-existantes contenues dans un PP existant, ou bien être prévues pour s'y conformer.

Les PP existants peuvent être utilisés comme base pour élaborer un nouveau PP.

b) Les paquets existants

Une partie des exigences de sécurité de la TOE dans un PP ou une ST peut avoir déjà été exprimée dans un paquet qui peut être utilisé.

Un ensemble de paquets prédéfinis constitue les EAL définis dans la partie 3. Les exigences d'assurance de la TOE dans un PP ou une ST devraient inclure un EAL contenu dans la partie 3.

c) Les composants d'exigences fonctionnelles ou d'assurance existants

Les exigences fonctionnelles ou d'assurance de la TOE dans un PP ou une ST peuvent être exprimées directement, en utilisant les composants des parties 2 ou 3.

d) Les exigences étendues

Des exigences fonctionnelles supplémentaires non contenues dans la partie 2 ou des exigences d'assurance supplémentaires non contenues dans la partie 3 peuvent être utilisées dans un PP ou une ST.

158 Des éléments concernant les exigences figurant dans les parties 2 et 3 devraient être utilisés chaque fois que possible. L'utilisation d'un PP existant aide à garantir que la TOE répond à un ensemble bien connu de besoins dont l'utilité est connue et qu'elle peut ainsi être reconnue plus largement.

## 4.5 Les types d'évaluation

### 4.5.1 L'évaluation d'un PP

159 L'évaluation d'un PP est menée par rapport aux critères d'évaluation pour les PP contenus dans la partie 3. Le but d'une telle évaluation est de démontrer que le PP est complet, cohérent, et techniquement correct et qu'il peut être utilisé comme formulation des exigences pour une TOE évaluable.

### 4.5.2 L’évaluation d’une ST

160 L’évaluation de la ST d’une TOE est menée par rapport aux critères d’évaluation pour les ST contenus dans la partie 3. Le but d’une telle évaluation est double : premièrement, de démontrer que la ST est complète, cohérente, et techniquement valide et donc qu’elle convient pour être utilisée comme base de l’évaluation de TOE correspondante, deuxièmement, dans le cas où une ST est présentée comme se conformant à un PP, de démontrer que la ST satisfait correctement aux exigences du PP.

### 4.5.3 L’évaluation d’une TOE

161 L’évaluation d’une TOE est menée par rapport aux critères d’évaluation contenus dans la partie 3 sur la base d’une ST évaluée. Le but d’une telle évaluation est de démontrer que la TOE satisfait aux exigences de sécurité contenues dans la ST.

## 4.6 Maintenance de l’assurance

162 La maintenance de l’assurance de la TOE est menée par rapport aux critères d’évaluation contenus dans la partie 3 sur la base d’une TOE préalablement évaluée. Le but est de déduire la confiance dans le fait que l’assurance déjà établie pour la TOE est maintenue et que la TOE continuera à satisfaire à ses exigences de sécurité alors que des changements sont faits dans la TOE ou dans son environnement.

# 5 Exigences des Critères Communs et résultats d'évaluation

## 5.1 Introduction

163 Le présent chapitre présente les résultats attendus d'une évaluation de PP et de TOE. Les évaluations de PP ou de TOE alimentent respectivement les catalogues des PP ou des TOE évalués. L'évaluation d'une ST conduit à des résultats intermédiaires qui sont utilisés dans le cadre de l'évaluation d'une TOE.

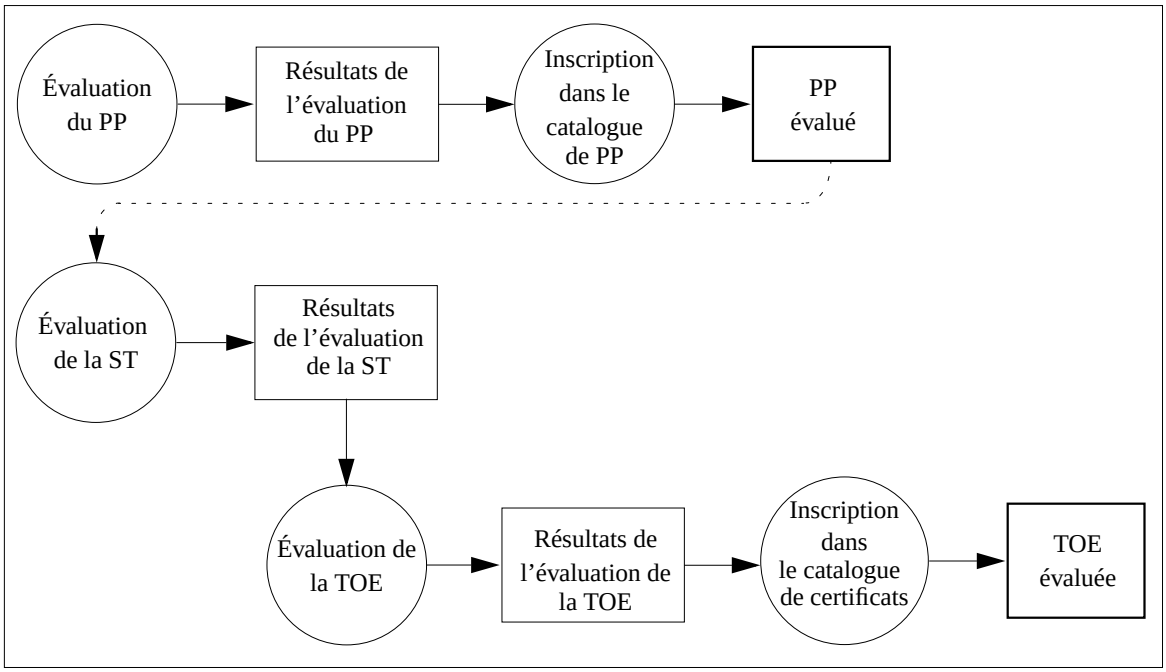


**Figure 5.1 - Résultats d'évaluation**

164 L'évaluation doit conduire à des résultats objectifs et répétables qui peuvent être cités en tant que preuve, même s'il n'existe pas d'échelle totalement objective pour représenter les résultats d'une évaluation de sécurité des TI. L'existence d'un ensemble de critères d'évaluation constitue une condition préalable nécessaire pour parvenir à un résultat significatif et fournit une base technique pour la reconnaissance mutuelle des résultats d'évaluation entre autorités d'évaluation. Mais l'application des critères contient des éléments à la fois objectifs et subjectifs ; c'est la raison pour laquelle une cotation précise et universelle de la sécurité des TI n'est pas faisable.

165 Une cotation élaborée par rapport aux CC représente les conclusions d'un examen spécifique des propriétés de sécurité d'une TOE. Une telle cotation ne garantit pas que la TOE convient pour tout environnement opérationnel. La décision d'accepter l'utilisation d'une TOE pour un environnement opérationnel spécifique est basée

sur l'examen de nombreuses questions liées à la sécurité, y compris les résultats d'évaluation.

## 5.2 Exigences contenues dans les PP et les ST

166 Les CC définissent un ensemble de critères de sécurité des TI qui peuvent couvrir les besoins de nombreuses communautés. Les CC ont été développés avec l'idée centrale que l'utilisation des composants fonctionnels de sécurité contenus dans la partie 2, des EAL et des composants d'assurance contenus dans la partie 3, constitue la ligne de conduite à adopter de préférence pour l'expression des exigences de la TOE dans les PP et les ST, car ces composants représentent un domaine bien connu et bien compris.

167 Les CC laissent la possibilité de recourir à des exigences fonctionnelles et d'assurance non contenues dans les listes fournies, pour représenter l'ensemble complet d'exigences de sécurité des TI. Les consignes suivantes doivent s'appliquer à l'incorporation de ces exigences fonctionnelles ou d'assurance étendues :

a) Toute exigence fonctionnelle ou d'assurance étendue contenue dans un PP ou une ST doit être exprimée clairement et sans ambiguïté pour que l'évaluation et la démonstration de conformité soient faisables. Le niveau de détail et le mode d'expression des composants fonctionnels ou d'assurance existants dans les CC doivent être utilisés comme modèles.

b) Les résultats d'évaluation obtenus en utilisant des exigences fonctionnelles ou d'assurance étendues doivent le mentionner par un avertissement.

c) L'incorporation d'exigences fonctionnelles ou d'assurance étendues dans un PP ou une ST doit se faire conformément aux classes APE ou ASE de la partie 3, quand cela est approprié.

### 5.2.1 Résultats d'évaluation d'un PP

168 Les CC contiennent les critères d'évaluation permettant à un évaluateur de déclarer si un PP est complet, cohérent, techniquement correct et donc si il convient pour formuler des exigences pour une TOE évaluable.

169 L'évaluation du PP doit aboutir à un résultat indiquant la réussite ou l'échec. Un PP dont l'évaluation a réussi remplit les conditions pour figurer dans un registre.

## 5.3 Exigences contenues dans une TOE

170 Les CC contiennent les critères d'évaluation permettant à un évaluateur de déterminer si la TOE satisfait aux exigences de sécurité exprimées dans la ST. En utilisant les CC pour évaluer la TOE, l'évaluateur sera en mesure de déclarer :

a) si les fonctions de sécurité spécifiées dans la TOE satisfont aux exigences fonctionnelles et sont par là même efficaces en répondant aux objectifs de sécurité de la TOE ;

b) si les fonctions de sécurité spécifiées dans la TOE sont correctement implémentées.

171 Les exigences de sécurité exprimées dans les CC définissent le domaine d'applicabilité connu des critères d'évaluation de la sécurité des TI. Une TOE dont les exigences de sécurité sont exprimées uniquement en termes d'exigences fonctionnelles et d'assurance tirées des CC sera évaluable par rapport aux CC. L'utilisation de paquets d'assurance qui ne contiennent pas un EAL doit être justifiée.

172 Cependant, une TOE peut nécessiter de satisfaire à des exigences de sécurité qui ne sont pas directement exprimées dans les CC. Les CC reconnaissent la nécessité d'évaluer une telle TOE mais, comme les exigences supplémentaires sont en dehors du domaine d'applicabilité connu des CC, les résultats d'une telle évaluation doivent le mentionner par un avertissement. Un tel avertissement peut compromettre la reconnaissance universelle des résultats d'évaluation par les autorités d'évaluation concernées.

173 Les résultats de l'évaluation d'une TOE doivent contenir une déclaration de conformité vis-à-vis des CC. L'utilisation de la terminologie des CC pour décrire la sécurité d'une TOE permet de comparer les caractéristiques de sécurité des TOE en général.

### 5.3.1 Résultats d'évaluation d'une TOE

174 Le résultat de l'évaluation d'une TOE doit être une déclaration qui décrit jusqu'à quel point on peut avoir confiance dans la conformité de la TOE vis-à-vis des exigences.

175 L'évaluation de la TOE doit aboutir à un résultat indiquant réussite ou échec. Une TOE dont l'évaluation a réussi remplit les conditions pour figurer dans un registre.

## 5.4 Qualification des résultats d'évaluation

176 Le verdict de réussite d'une évaluation doit être une déclaration qui décrit jusqu'à quel point on peut avoir confiance dans la conformité du PP ou de la TOE vis-à-vis des exigences. L'expression des résultats doit faire mention de leur conformité à la partie 2 (exigences fonctionnelles), à la partie 3 (exigences d'assurance), ou directement à un PP.

a) **Conforme à la partie 2** - Un PP ou une TOE est conforme à la partie 2 si les exigences fonctionnelles sont basées uniquement sur les composants fonctionnels de la partie 2.

b) **Partie 2 étendue** - Un PP ou une TOE est qualifié de "partie 2 étendue" si les exigences fonctionnelles contiennent des composants fonctionnels ne figurant pas dans la partie 2.

c) **Conforme à la partie 3** - Un PP ou une TOE est conforme à la partie 3 si les exigences d'assurance sont présentées sous forme d'un **EAL** ou d'un **paquet d'assurance** qui est basé uniquement sur des composants d'assurance de la partie 3.

d) **Partie 3 augmentée** - Un PP ou une TOE est qualifié de "partie 3 augmentée" si les exigences d'assurance sont présentées sous forme d'un **EAL** ou d'un **paquet d'assurance**, complété par d'autres composants d'assurance de la partie 3.

e) **Partie 3 étendue** - Un PP ou une TOE est qualifié de "partie 3 étendue" si les exigences d'assurance sont présentées sous forme d'un **EAL** associé à des exigences d'assurance supplémentaires ne figurant pas dans la partie 3, ou d'un **paquet d'assurance** qui contient des exigences d'assurance ne figurant pas dans la partie 3 (ou qui est bâti entièrement à partir d'elles).

f) **Conforme à un PP** - Une TOE est conforme à un PP seulement si elle est conforme à toutes les parties de ce PP.

## 5.5 Utilisation des résultats d'évaluation d'une TOE

177 Les produits et les systèmes TI diffèrent en ce qui concerne les résultats d'évaluation. La figure 5.2 représente les options de traitement des résultats d'évaluation. Les produits peuvent être évalués et catalogués avec des niveaux d'intégration de plus en plus élevés jusqu'à l'élaboration de systèmes opérationnels qui peuvent alors être soumis à évaluation dans le cadre de la procédure d'homologation de système.

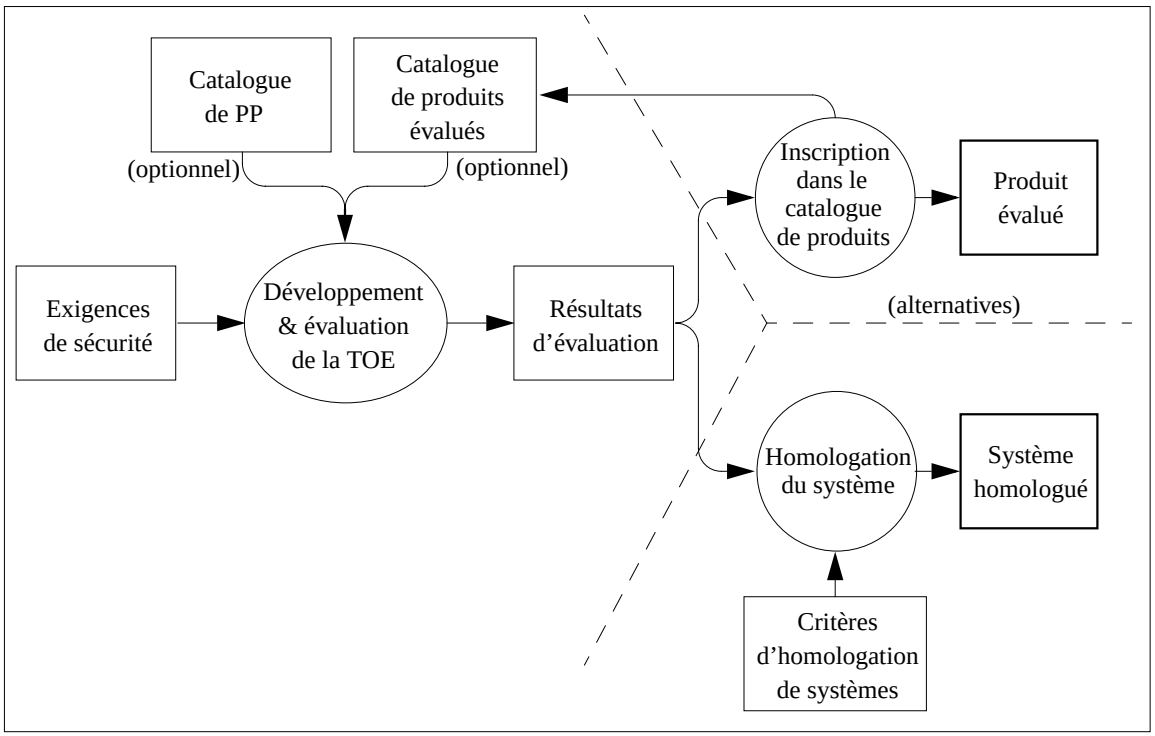


**Figure 5.2 - Utilisation des résultats d'évaluation d'une TOE**

178 La TOE est développée en réponse à des exigences qui peuvent prendre en compte les propriétés de sécurité de n'importe lequel des produits évalués qui sont incorporés et des PP qui sont référencés. L'évaluation de la TOE, faite par la suite, conduit à un ensemble de résultats d'évaluation qui explicite les conclusions de l'évaluation.

179 À la suite de l'évaluation d'un produit TI prévu pour une large gamme d'utilisations, un résumé des conclusions de l'évaluation pourrait être inclus dans un catalogue des produits évalués, devenant ainsi accessible à un marché plus large qui vise l'utilisation de produits TI sûrs.

180 Dans le cas où la TOE est ou doit être incorporée dans un système TI installé qui a été soumis à évaluation, les résultats d'évaluation seront mis à disposition de l'homologateur du système. Les résultats de l'évaluation CC peuvent ainsi être pris en compte par l'homologateur lorsqu'il applique les critères d'homologation spécifiques à l'organisation commanditaire de l'évaluation CC. Les résultats d'évaluation CC constituent l'une des données d'un processus d'homologation qui conduit à une décision d'acceptation du risque lié à la mise en exploitation du système.

# Annexe A
# (Informative)

# Le projet Critères Communs

## A.1 Historique du projet Critères Communs

181 Les CC représentent l'aboutissement d'une série d'efforts pour développer des critères pour l'évaluation de la sécurité des TI qui soient largement utiles pour la communauté internationale. Au début des années 80, les TCSEC (Trusted Computer System Evaluation Criteria) ont été développés aux États-Unis. Dans la décennie suivante, divers pays ont entrepris de développer des critères d'évaluation basés sur les concepts des TCSEC mais plus flexibles et plus adaptables au caractère évolutif des TI en général.

182 En Europe, les ITSEC (Critères d'Évaluation des Systèmes Informatiques), version 1.2, ont été publiés en 1991 par la Commission Européenne à la suite d'un développement assuré conjointement par l'Allemagne, la France, les Pays-Bas et le Royaume Uni. Au Canada, les CTCPEC (Canadian Trusted Computer Product Evaluation Criteria), version 3.0, ont été publiés début 1993, réalisant une combinaison de l'approche des ITSEC et des TCSEC. Aux États-Unis, les critères provisoires FC (Federal Criteria for Information Technology Security) version 1.0 ont été publiés début 1993, comme une deuxième approche pour combiner les concepts des critères d'évaluation nord-américains et européens.

183 Le travail de développement de critères d'évaluation internationaux normalisés en vue d'un usage général a commencé en 1990 à l'ISO (International Organisation for Standardisation). Les nouveaux critères devaient répondre aux besoins d'une reconnaissance mutuelle de résultats standardisés d'évaluation de sécurité dans un marché global des TI. Cette tâche a été confiée au groupe d'experts 3 (Working Group 3 ou WG3) du sous-comité 27 (subcommittee 27 ou SC27) du Comité technique n° 1 (Joint Technical Committee 1 ou JTC1). Au début, les progrès ont été lents au sein du WG3 à cause de l'ampleur considérable du travail et de la nécessité de procéder à des négociations multilatérales intensives.

## A.2 Développement des Critères Communs

184 En juin 1993, les organisations commanditaires des CTCPEC, FC, TCSEC et des ITSEC (qui sont identifiées dans la section suivante) réunirent leurs efforts et lancèrent le projet commun d'aligner leurs différents critères pour créer un ensemble unique de critères de sécurité des TI qui pourrait être largement utilisé. Cette activité a été baptisée le projet CC. L'intention était de résoudre les différences conceptuelles et techniques figurant dans les critères sources et de présenter les résultats à l'ISO comme contribution à son travail de développement d'une norme internationale. Les représentants des organisations commanditaires

ont constitué le comité d'édition des CC (CCEB : CC Editorial Board) pour développer les CC. Une liaison a alors été établie entre le CCEB et le WG3, et le CCEB a apporté comme contributions au WG3 plusieurs versions intermédiaires des CC via cette liaison. De l'interaction entre le WG3 et le CCEB a résulté l'adoption de ces versions en tant que versions de travail successives des différentes parties des critères ISO dès 1994.

185 La version 1.0 a été achevée en janvier 1996 par le CCEB et approuvée en avril 1996 par l'ISO pour distribution en tant que CD (Committee Draft). Dans le cadre du projet CC, un certain nombre d'évaluations d'essai ont alors été conduites en utilisant la version 1.0 des CC et une large revue publique du document a été réalisée. Dans le cadre du projet CC ont été entrepris par la suite une révision détaillée des CC, basée sur les commentaires reçus lors d'évaluations d'essai, de revues publiques et d'échanges avec l'ISO. Le travail de révision a été mené par le groupe qui a succédé au CCEB, appelé désormais comité d'implémentation des CC (CCIB : CC Implementation Board).

186 Le CCIB a achevé la version 2.0 "Beta" des CC en octobre 1997 et l'a présentée au WG 3, qui l'a approuvée en tant que Second Committee Draft. Des versions ultérieures provisoires ont été fournies de façon informelle aux experts du WG3 pour feed-back, dès leur élaboration par le CCIB. Ce dernier a reçu une série de commentaires, auxquels il a répondu, provenant directement à la fois des experts du WG3 et des organisations nationales de l'ISO via la procédure de vote du CD. Le résultat final de ce processus est le document CC Version 2.0.

187 Pour des raisons historiques et de continuité, l'ISO/IEC JTC 1/SC 27/WG 3 a accepté de pérenniser l'usage du terme "Critères Communs" (CC) dans le document, tout en reconnaissant que son nom officiel dans le contexte de l'ISO est "Critères d'évaluation pour la sécurité des Technologies de l'Information".

## A.3 Les organisations commanditaires

188 Les sept organisations gouvernementales européennes et nord-américaines citées ci-dessous constituent les organisations commanditaires du projet CC. Ces organisations ont accompli pratiquement tous les efforts pour développer les CC depuis le début jusqu'à son élaboration finale. Ces organisations sont également "autorité d'évaluation" pour leurs gouvernements nationaux respectifs. Elles se sont engagées à remplacer leurs propres critères d'évaluation par les CC version 2.0 maintenant que le développement technique de ces derniers est achevé et que les

dernières étapes pour qu'ils deviennent une norme internationale sont en passe d'être franchies.

**ALLEMAGNE :**
Bundesamt für Sicherheit in der Informationstechnik (BSI)
German Information Security Agency (GISA)
Abteilung V
Postfach 20 03 63
D-53133 Bonn
Germany
Tel: +49.228.9582.300, Fax: +49.228.9582.427
E-mail: cc@bsi.de
WWW: http://www.bsi.bund.de/cc

**CANADA :**
Communications Security Establishment
Criteria Coordinator
I2A Computer and Network Security
P.O. Box 9703, Terminal
Ottawa, Canada K1G 3Z4
Tel: +1.613.991.7882, Fax: +1.613.991.7455
E-mail: criteria@cse-cst.gc.ca
WWW: http://www.cse-cst.gc.ca/cse/english/cc.html
FTP: ftp://ftp.cse-cst.gc.ca/pub/criteria/CC2.0

**ÉTATS-UNIS - NIST :**
National Institute of Standards and Technology
Computer Security Division
820 Diamond, MS: NN426
Gaithersburg, Maryland 20899
U.S.A.
Tel: +1.301.975.2934, Fax: +1.301.948.0279
E-mail: criteria@nist.gov
WWW: http://csrc.nist.gov/cc

**ÉTATS-UNIS - NSA :**
National Security Agency
Attn: V2, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 20755-6740
U.S.A.
Tel: +1.410.859.4458, Fax: +1.410.684.7512
E-mail: common_criteria@radium.ncsc.mil
WWW: http://www.radium.ncsc.mil/tpep/

**FRANCE :**
Service Central de la Sécurité des Systèmes d'Information (SCSSI)
Centre de Certification de la Sécurité des Technologies de l'Information
18, rue du docteur Zamenhof
F-92131 Issy les Moulineaux
France
Tel: +33.1.41463784, Fax: +33.1.41463701
E-mail: ssi20@calva.net

**PAYS-BAS :**
Netherlands National Communications Security Agency
P.O. Box 20061
NL 2500 EB The Hague
The Netherlands
Tel: +31.70.3485637, Fax: +31.70.3486503
E-mail: criteria@nlncsa.minbuza.nl
WWW: http://www.tno.nl/instit/fel/refs/cc.html

**ROYAUME UNI :**
Communications-Electronics Security Group
Compusec Evaluation Methodology
P.O. Box 144
Cheltenham GL52 5UE
United Kingdom
Tel: +44.1242.221.491 ext. 5257, Fax: +44.1242.252.291
E-mail: criteria@cesg.gov.uk
WWW: http://www.cesg.gov.uk/cchtml
FTP: ftp://ftp.cesg.gov.uk/pub

# Annexe B
# (Normative)

# Spécification des profils de protection

## B.1 Vue d'ensemble

189 Un PP définit un ensemble d'exigences de sécurité des TI pour une catégorie de TOE, indépendant de leur implémentation. De telles TOE sont conçues pour satisfaire les besoins communs des utilisateurs pour la sécurité des TI. Les utilisateurs peuvent donc construire ou citer un PP pour exprimer leurs besoins de sécurité des TI sans faire référence à une TOE spécifique.

190 Cette annexe contient les exigences pour le PP sous une forme descriptive. La classe d'assurance APE, figurant dans le chapitre 4 de la partie 3, contient ces exigences sous la forme de composants d'assurance à utiliser pour l'évaluation du PP.

## B.2 Contenu du profil de protection

### B.2.1 Contenu et présentation

191 Un PP doit être conforme aux exigences concernant le contenu, décrites dans la présente annexe. Un PP devrait être présenté comme un document orienté utilisateur minimisant les références à d'autres documents qui pourraient ne pas être facilement disponibles à l'utilisateur du PP. L'argumentaire peut être fourni séparément si cela est approprié.

192 Le contenu du PP est représenté dans la figure B.1, qui devrait être utilisée pour construire les grandes lignes structurelles du PP.

### B.2.2 Introduction du PP

193 L'introduction du PP doit contenir les informations suivantes concernant la gestion du document et la vue d'ensemble nécessaires pour la tenue d'un registre de PP :

a) L'**identification du PP** doit donner l'identification et les informations descriptives nécessaires pour identifier, cataloguer, enregistrer et élaborer les références croisées d'un PP.

b) La **vue d'ensemble** doit résumer le PP sous forme narrative. La vue d'ensemble doit être suffisamment détaillée pour qu'un utilisateur potentiel du PP puisse déterminer si le PP présente un intérêt. La vue d'ensemble devrait aussi être utilisable pour figurer en tant que résumé auto-suffisant dans les catalogues et les registres.

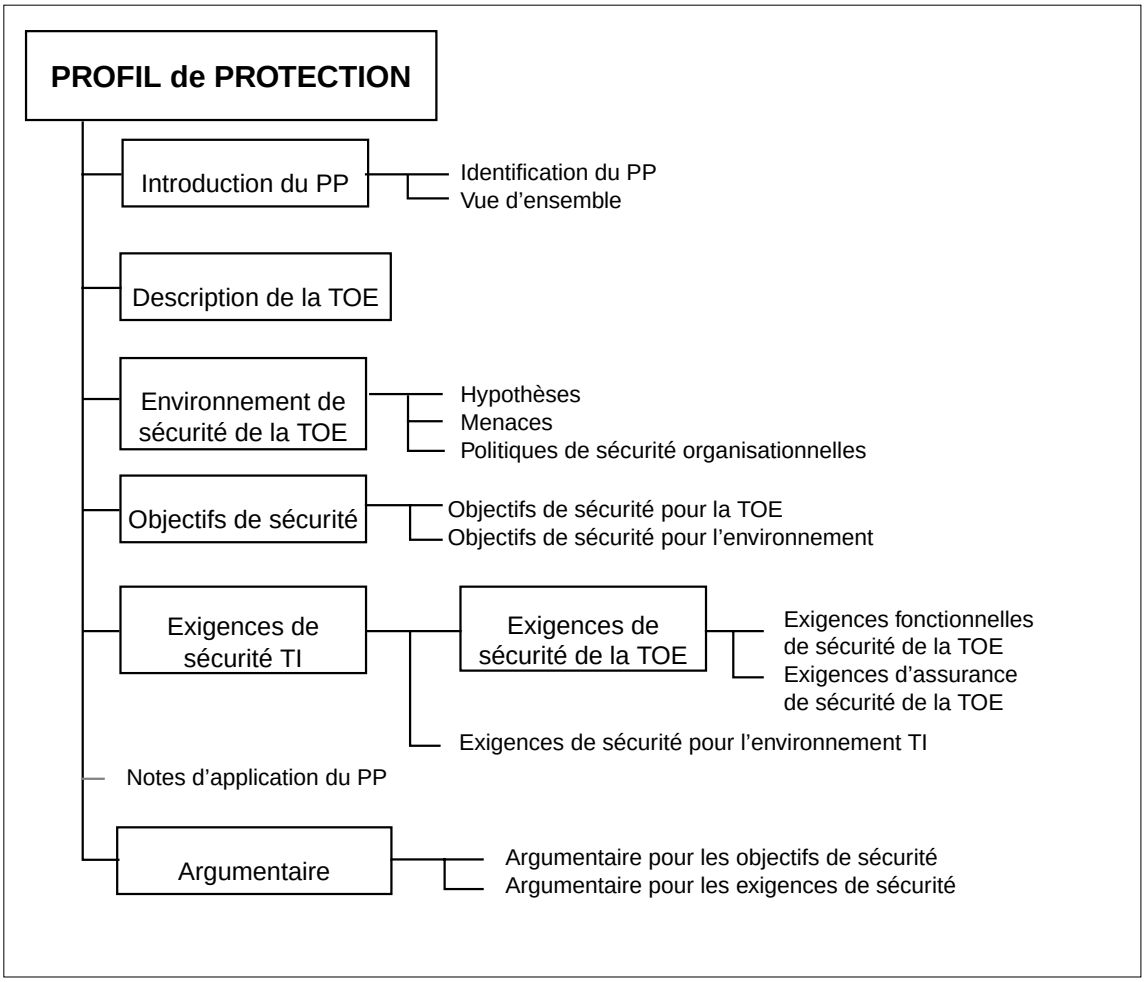


Figure B.1 - Contenu d'un profil de protection

### B.2.3 Description de la TOE

194 Cette partie du PP doit décrire la TOE pour aider à la compréhension de ses exigences de sécurité, et doit indiquer le type de produit et les caractéristiques TI générales de la TOE.

195 La description de la TOE fournit un contexte pour l'évaluation. Les informations présentées dans la description de la TOE seront utilisées au cours de l'évaluation pour identifier les incohérences. Comme un PP ne se réfère pas normalement à une implémentation spécifique, les caractéristiques de la TOE qui sont décrites peuvent n'être que des hypothèses. Lorsque la TOE est un produit ou un système dont la principale fonction est la sécurité, cette partie du PP peut être utilisée pour décrire le contexte général d'application dans lequel s'insérera la TOE.

### B.2.4 Environnement de sécurité de la TOE

196 L'énoncé de l'**environnement de sécurité de la TOE** doit décrire les aspects de sécurité de l'environnement dans lequel il est prévu d'utiliser la TOE ainsi que son mode d'emploi attendu. Cette spécification doit inclure les éléments suivants :

a) Une description des **hypothèses** doit indiquer précisément les aspects de sécurité de l'environnement dans lequel la TOE sera utilisée ou dans lequel il est prévu qu'elle le sera. Ceci doit inclure les informations suivantes :

informations relatives à l'usage attendu de la TOE, comprenant des aspects tels que l'application prévue, la valeur potentielle du bien et les limitations possibles d'emploi ;

informations relatives à l'environnement d'utilisation de la TOE, comprenant les aspects physiques, touchant au personnel et concernant la connectivité.

b) Une description des **menaces** doit inclure toutes les menaces contre les biens exigeant une protection spécifique dans la TOE ou dans son environnement. Il est à noter qu'il n'est pas nécessaire de citer toutes les menaces qui pourraient être rencontrées dans l'environnement, mais seulement celles qui sont pertinentes pour un fonctionnement sûr de la TOE.

Une menace doit être décrite en citant l'élément menaçant identifié, l'attaque et le bien qui en est la cible. Les éléments menaçants devraient être caractérisés par des aspects tels que l'expertise, les ressources disponibles et la motivation. Les attaques devraient être caractérisées par des aspects tels que les méthodes d'attaque, toutes vulnérabilités exploitées et l'opportunité.

Dans le cas où les objectifs de sécurité sont déduits uniquement des politiques de sécurité et des hypothèses organisationnelles, la description des menaces peut être omise.

c) Une description des **politiques de sécurité organisationnelles** doit identifier, et si nécessaire expliquer, toutes les spécifications ou les règles relatives à la politique de sécurité organisationnelle auxquelles la TOE doit se conformer. Des explications et des interprétations peuvent s'avérer nécessaires pour présenter toute spécification individuelle de la politique d'une façon permettant d'établir des objectifs de sécurité clairs.

Dans le cas où les objectifs de sécurité sont déduits uniquement des menaces et des hypothèses, la description des politiques de sécurité organisationnelles peut être omise.

197 Lorsque la TOE est physiquement répartie, il peut être nécessaire d'examiner en détail les aspects de sécurité environnementaux (hypothèses, menaces, politiques

de sécurité organisationnelles) séparément pour chaque domaine distinct de l'environnement de la TOE.

### B.2.5 Objectifs de sécurité

198 L'énoncé des **objectifs de sécurité** doit définir les objectifs de sécurité pour la TOE et son environnement. Les objectifs de sécurité doivent traiter de tous les aspects de sécurité de l'environnement identifiés. Les objectifs de sécurité doivent refléter l'intention déclarée et doivent être à même de contrer toutes les menaces identifiées et de couvrir toutes les politiques de sécurité organisationnelles et les hypothèses identifiées. Les catégories suivantes d'objectifs doivent être identifiées. Note : dans le cas où une menace ou une politique de sécurité organisationnelle doit être couverte en partie par la TOE et en partie par son environnement, l'objectif concerné doit être répété dans chaque catégorie.

a) Les **objectifs de sécurité pour la TOE** doivent être formulés clairement et reliés aux aspects des menaces identifiées devant être contrées par la TOE ou aux politiques de sécurité organisationnelles devant être satisfaites par la TOE.

b) Les **objectifs de sécurité pour l'environnement** doivent être formulés clairement et reliés aux aspects des menaces identifiées qui ne sont pas complètement contrées par la TOE ou par les politiques de sécurité organisationnelles ou les hypothèses qui ne sont pas complètement satisfaites par la TOE.

Il est à noter que les objectifs de sécurité pour l'environnement peuvent n'être qu'une reformulation, en totalité ou non, de la partie relative aux hypothèses de l'environnement de sécurité de la TOE.

### B.2.6 Exigences de sécurité des TI

199 Cette partie du PP définit les exigences de sécurité des TI détaillées qui doivent être satisfaites par la TOE ou par son environnement. Les exigences de sécurité des TI doivent être formulées comme suit :

a) L'énoncé des **exigences de sécurité de la TOE** doit définir les exigences fonctionnelles et d'assurance de sécurité auxquelles la TOE et les éléments de preuve fournis dans le cadre de son évaluation doivent satisfaire pour atteindre les objectifs de sécurité pour la TOE. Les exigences de sécurité de la TOE doivent être formulées comme suit :

1) L'énoncé des **exigences fonctionnelles de sécurité de la TOE** devrait définir les exigences fonctionnelles pour la TOE à partir de composants fonctionnels tirés de la partie 2 lorsque cela est possible.

Lorsqu'il est nécessaire de couvrir des aspects différents de la même exigence (par exemple l'identification de plus d'un type d'utilisateur), l'utilisation répétée (i.e. l'application de l'opération d'itération) du même composant de la partie 2 est possible pour

couvrir chacun des aspects.

Lorsque AVA_SOF.1 est inclus dans les exigences d'assurance de sécurité de la TOE (e.g. au niveau EAL2 et plus), l'énoncé des exigences fonctionnelles de sécurité de la TOE doit inclure un niveau de résistance minimum pour les fonctions de sécurité de la TOE réalisées au moyen d'un mécanisme faisant appel au calcul des probabilités ou des permutations (e.g., un mot de passe ou une fonction de hachage). Toutes les fonctions de ce type doivent atteindre ce niveau minimum. Le niveau doit être l'un des suivants : SOF-élémentaire, SOF-moyen, SOF-élevé. Le choix du niveau doit être cohérent avec les objectifs de sécurité identifiés pour la TOE. De façon optionnelle, des métriques spécifiques de résistance des fonctions peuvent être définies pour des exigences fonctionnelles sélectionnées, afin d'atteindre certains objectifs de sécurité pour la TOE.

On estimera, au titre de l'évaluation de la résistance des fonctions de sécurité de la TOE (AVA_SOF.1), si les niveaux de résistance annoncés pour chaque fonction de sécurité de la TOE et le niveau de résistance global sont atteints par la TOE.

2) L'énoncé des **exigences d'assurance de sécurité de la TOE** devrait être l'un des EAL, éventuellement augmenté par des composants d'assurance de la partie 3. Le PP peut également étendre l'EAL en spécifiant explicitement des exigences d'assurance additionnelles ne figurant pas dans la partie 3.

b) L'énoncé optionnel des **exigences de sécurité pour l'environnement TI** doit identifier les exigences de sécurité des TI devant être satisfaites par l'environnement TI de la TOE. Dans le cas où il n'est pas spécifié de dépendances de la TOE envers l'environnement TI, cette partie du PP peut être omise.

Il est à noter que les **exigences de sécurité pour l'environnement non TI**, bien qu'étant souvent utiles dans la pratique, ne sont pas tenues de faire formellement partie du PP car elles ne sont pas directement reliées à l'implémentation de la TOE.

c) Les **conditions communes** suivantes doivent s'appliquer d'égale façon à l'expression des exigences fonctionnelles et d'assurance de sécurité de la TOE et pour son environnement TI :

1) Toutes les exigences de sécurité des TI devraient être formulées par référence à des composants d'exigences de sécurité tirés de la partie 2 ou de la partie 3 quand cela est possible. Dans le cas où aucun des composants d'exigences de la partie 2 ou de la partie 3 n'est facilement applicable à tout ou partie des exigences de sécurité, le PP peut formuler ces exigences de façon explicite sans référence aux CC.

2) Tout énoncé explicite des exigences fonctionnelles ou d'assurance de sécurité de la TOE doit être exprimé clairement et sans ambiguïté de telle façon que l'évaluation et la démonstration de conformité soient faisables. Le niveau de détail et le mode d'expression des composants fonctionnels ou d'assurance existants dans les CC doivent être utilisés comme modèles.

3) Lorsque des composants d'exigences qui spécifient les opérations exigées (spécification ou sélection) sont choisis, le PP doit utiliser ces opérations pour enrichir les exigences jusqu'au niveau de détail nécessaire pour démontrer que les objectifs de sécurité sont atteints. Toute opération exigée qui n'aura pas été appliquée dans le PP doit être mentionnée.

4) En utilisant des opérations sur les composants d'exigences, les énoncés d'exigences de sécurité de la TOE peuvent, de façon optionnelle, prescrire ou prohiber l'utilisation de mécanismes de sécurité particuliers quand cela est nécessaire.

5) Toutes les dépendances entre exigences de sécurité des TI devraient être satisfaites. Les dépendances peuvent être satisfaites en incluant l'exigence pertinente dans les exigences de sécurité de la TOE, ou en tant qu'exigence pour l'environnement.

### B.2.7 Notes d'application

200 Cett partie optionnelle du PP peut contenir des informations supplémentaires qui sont considérées comme pertinentes ou utiles pour construire, évaluer ou utiliser la TOE.

### B.2.8 Argumentaire

201 Cette partie du PP présente les éléments de preuve utilisés lors de l'évaluation du PP. Ces éléments de preuve appuient les annonces suivant lesquelles le PP constitue un ensemble d'exigences complet et cohérent, et qu'une TOE s'y conformant offrirait un ensemble efficace de contre-mesures de sécurité des TI au sein de l'environnement de sécurité. L'argumentaire doit inclure les éléments suivants :

a) L'**argumentaire relatif aux objectifs de sécurité** doit démontrer que les objectifs de sécurité déclarés sont reliés à tous les aspects identifiés dans l'environnement de sécurité de la TOE et sont à même de les couvrir.

b) L'**argumentaire relatif aux exigences de sécurité** doit démontrer que l'ensemble des exigences de sécurité (TOE et environnement) convient pour satisfaire aux objectifs de sécurité et qu'ils sont reliés à ces derniers. Il doit pouvoir être démontré :

1) que la combinaison des composants individuels d'exigences fonctionnelles et d'assurance de la TOE et pour son environnement TI satisfait aux objectifs de sécurité déclarés ;

2) que l'ensemble des exigences de sécurité constitue un tout ayant une cohérence interne et dont les éléments se soutiennent mutuellement ;

3) que le choix des exigences de sécurité est justifié. Chacune des circonstances suivantes doit être justifiée de manière spécifique :

— choix d'exigences ne figurant pas dans les parties 2 ou 3 ;
— choix d'exigences d'assurance n'incluant pas d'EAL ;
— non satisfaction des dépendances ;

4) que le niveau de résistance des fonctions choisi pour le PP, de même que toute résistance de fonction explicite annoncée, est cohérent avec les objectifs de sécurité pour la TOE.

202 Ces éléments pouvant être volumineux, ils peuvent être distribués séparément car ils ne sont pas forcément appropriés ou utiles pour tous les utilisateurs du PP.

# Annexe C
# (Normative)

# Spécification des cibles de sécurité

## C.1 Vue d'ensemble

203 Une ST contient les exigences de sécurité des TI d'une TOE identifiée et spécifie les mesures de sécurité fonctionnelles et d'assurance offertes par cette TOE pour satisfaire aux exigences annoncées.

204 La ST pour une TOE est une base d'accord entre les développeurs, les évaluateurs et, le cas échéant, les utilisateurs sur les propriétés de sécurité de la TOE et sur la portée de l'évaluation. Le public visé par la ST ne se limite pas aux responsables de la réalisation de la TOE et de son évaluation, mais peut inclure également les responsables de la gestion, du marketing, des achats, de l'installation, de la configuration, de l'exploitation et de l'utilisation de la TOE.

205 La ST peut inclure les exigences d'un ou plusieurs PP ou s'y déclarer conforme. Les conséquences d'une telle annonce de conformité à un PP ne sont pas prises en compte lors de la définition initiale du contenu exigé de la ST figurant dans la section C.2. La section C.2.8 traite de ces conséquences sur le contenu exigé de la ST.

206 Cette annexe contient les exigences pour la ST sous une forme descriptive. La classe d'assurance ASE, figurant dans le chapitre 3 de la partie 3, contient ces exigences sous la forme de composants d'assurance à utiliser pour l'évaluation de la ST.

## C.2 Contenu de la cible de sécurité

### C.2.1 Contenu et présentation

207 Une ST doit être conforme aux exigences concernant le contenu, décrites dans la présente annexe. Une ST devrait être présentée comme un document orienté utilisateur minimisant les références à d'autres documents qui pourraient ne pas être facilement disponibles à l'utilisateur de la ST. L'argumentaire peut être fourni séparément si cela est approprié.

208 Le contenu de la ST est représenté dans la figure C.1, qui devrait être utilisée pour construire les grandes lignes structurelles de la ST.

### C.2.2 Introduction de la ST

209 L'introduction de la ST doit contenir les informations suivantes concernant la gestion du document et la vue d'ensemble :

a) L'**identification de la ST** doit donner l'identification et les informations descriptives nécessaires au contrôle et à l'identification de la ST et de la TOE à laquelle elle se réfère.

b) La **vue d'ensemble de la ST** doit résumer la ST sous forme narrative. La vue d'ensemble doit être suffisamment détaillée pour qu'un utilisateur potentiel de la TOE puisse déterminer si la TOE présente un intérêt. La vue d'ensemble devrait aussi être utilisable pour figurer en tant que résumé auto-suffisant dans les listes de produits évalués.

c) Une **annonce de conformité aux CC** doit mentionner toute annonce de conformité aux CC évaluable pour la TOE, comme indiqué dans la section 5.4 de la présente partie 1.

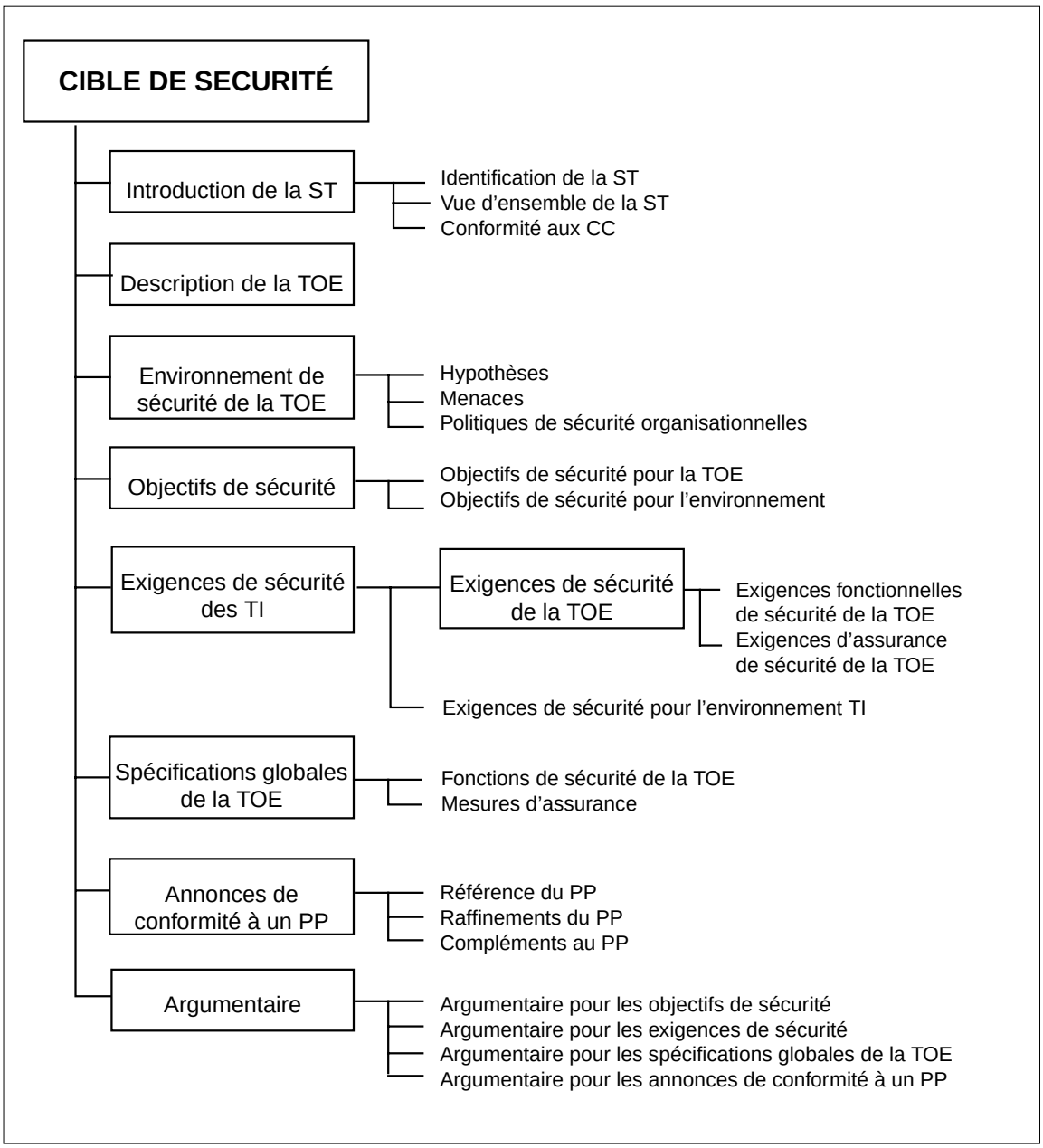


Figure C.1 - Contenu d'une cible de sécurité

### C.2.3 Description de la TOE

210 Cette partie de la ST doit décrire la TOE pour aider à la compréhension de ses exigences de sécurité, et doit indiquer le type de produit ou système. Le champ d'application et les limites de la TOE doivent être décrits en termes généraux aussi bien d'un point de vue physique (composants ou modules matériels ou logiciels) que d'un point de vue logique (caractéristiques TI et de sécurité offertes par la TOE).

211 La description de la TOE fournit un contexte pour l'évaluation. Les informations présentées dans la description de la TOE seront utilisées au cours de l'évaluation pour identifier les incohérences. Lorsque la TOE est un produit ou un système dont la principale fonction est la sécurité, cette partie de la ST peut être utilisée pour décrire le contexte général d'application dans lequel s'insérera une telle TOE.

### C.2.4 Environnement de sécurité de la TOE

212 L'énoncé de l'**environnement de sécurité de la TOE** doit décrire les aspects de sécurité de l'environnement dans lequel il est prévu d'utiliser la TOE ainsi que son mode d'emploi attendu. Cette spécification doit inclure les éléments suivants :

a) Une description des **hypothèses** doit indiquer précisément les aspects de sécurité de l'environnement dans lequel la TOE sera utilisée ou dans lequel il est prévu qu'elle le sera. Ceci doit inclure les informations suivantes :

informations relatives à l'usage attendu de la TOE, comprenant des aspects tels que l'application prévue, la valeur potentielle du bien et les limitations possibles d'emploi ; et informations relatives à l'environnement d'utilisation de la TOE, comprenant les aspects physiques, touchant au personnel et concernant la connectivité.

b) Une description des **menaces** doit inclure toutes les menaces contre les biens exigeant une protection spécifique dans la TOE ou dans son environnement. Il est à noter qu'il n'est pas nécessaire de citer toutes les menaces qui pourraient être rencontrées dans l'environnement, mais seulement celles qui sont pertinentes pour un fonctionnement sûr de la TOE.

Une menace doit être décrite en citant l'élément menaçant identifié, l'attaque et le bien qui en est la cible. Les éléments menaçants devraient être caractérisés par des aspects tels que l'expertise, les ressources disponibles et la motivation. Les attaques devraient être caractérisées par des aspects tels que les méthodes d'attaque, toutes vulnérabilités exploitées et l'opportunité.

Dans le cas où les objectifs de sécurité sont déduits uniquement des politiques de sécurité et des hypothèses organisationnelles, la description des menaces peut être omise.

c) Une description des **politiques de sécurité organisationnelles** doit identifier, et si nécessaire expliquer, toutes les spécifications ou les règles relatives à la politique de sécurité organisationnelle auxquelles la TOE doit se conformer. Des explications et des interprétations peuvent s'avérer nécessaires pour présenter toute spécification individuelle de la politique d'une façon permettant d'établir des objectifs de sécurité clairs.

Dans le cas où les objectifs de sécurité sont déduits uniquement des menaces et des hypothèses, la description des politiques de sécurité organisationnelles peut être omise.

213 Lorsque la TOE est physiquement répartie, il peut être nécessaire d'examiner en détail les aspects de sécurité environnementaux (hypothèses, menaces, politiques de sécurité organisationnelles) séparément pour chaque domaine distinct de l'environnement de la TOE.

### C.2.5 Objectifs de sécurité

214 L'énoncé des **objectifs de sécurité** doit définir les objectifs de sécurité pour la TOE et son environnement. Les objectifs de sécurité doivent traiter de tous les aspects de sécurité de l'environnement identifiés. Les objectifs de sécurité doivent refléter l'intention déclarée et doivent être à même de contrer toutes les menaces identifiées et de couvrir toutes les politiques de sécurité organisationnelles et les hypothèses identifiées. Les catégories suivantes d'objectifs doivent être identifiées. Note : dans le cas où une menace ou une politique de sécurité organisationnelle doit être couverte en partie par la TOE et en partie par son environnement, l'objectif concerné doit être répété dans chaque catégorie.

a) Les **objectifs de sécurité pour la TOE** doivent être formulés clairement et reliés aux aspects des menaces identifiées devant être contrées par la TOE ou aux politiques de sécurité organisationnelles devant être satisfaites par la TOE.

b) Les **objectifs de sécurité pour l'environnement** doivent être formulés clairement et reliés aux aspects des menaces identifiées qui ne sont pas complètement contrées par la TOE ou par les politiques de sécurité organisationnelles ou les hypothèses qui ne sont pas complètement satisfaites par la TOE.

Il est à noter que les objectifs de sécurité pour l'environnement peuvent n'être qu'une reformulation, en totalité ou non, de la partie relative aux hypothèses de l'environnement de sécurité de la TOE.

### C.2.6 Exigences de sécurité des TI

215 Cette partie de la ST définit les exigences de sécurité des TI détaillées qui doivent être satisfaites par la TOE ou par son environnement. Les exigences de sécurité des TI doivent être formulées comme suit :

a) L'énoncé des **exigences de sécurité de la TOE** doit définir les exigences fonctionnelles et d'assurance de sécurité auxquelles la TOE et les éléments de preuve fournis dans le cadre de son évaluation doivent satisfaire pour atteindre les objectifs de sécurité pour la TOE. Les exigences de sécurité de la TOE doivent être formulées comme suit :

1) L'énoncé des **exigences fonctionnelles de sécurité de la TOE** devrait définir les exigences fonctionnelles pour la TOE à partir de composants fonctionnels tirés de la partie 2 lorsque cela est possible.

Lorsqu'il est nécessaire de couvrir des aspects différents de la même exigence (par exemple l'identification de plus d'un type

d'utilisateur), l'utilisation répétée (i.e. l'application de l'opération d'itération) du même composant de la partie 2 est possible pour couvrir chacun des aspects.

Lorsque AVA_SOF.1 est inclus dans les exigences d'assurance de sécurité de la TOE (e.g. au niveau EAL2 et plus), l'énoncé des exigences fonctionnelles de sécurité de la TOE doit inclure un niveau de résistance minimum pour les fonctions de sécurité de la TOE réalisées au moyen d'un mécanisme faisant appel au calcul des probabilités ou des permutations (e.g., un mot de passe ou une fonction de hachage). Toutes les fonctions de ce type doivent atteindre ce niveau minimum. Le niveau doit être l'un des suivants : SOF-élémentaire, SOF-moyen, SOF-élevé. Le choix du niveau doit être cohérent avec les objectifs de sécurité identifiés pour la TOE. De façon optionnelle, des métriques spécifiques de résistance des fonctions peuvent être définies pour des exigences fonctionnelles sélectionnées, afin d'atteindre certains objectifs de sécurité pour la TOE.

On estimera, au titre de l'évaluation de la résistance des fonctions de sécurité de la TOE (AVA_SOF.1), si les niveaux de résistance annoncés pour chaque fonction de sécurité de la TOE et le niveau de résistance global sont atteints par la TOE.

2) L'énoncé des **exigences d'assurance de sécurité de la TOE** devrait être l'un des EAL, éventuellement augmenté par des composants d'assurance de la partie 3. La ST peut également étendre l'EAL en spécifiant explicitement des exigences d'assurance additionnelles ne figurant pas dans la partie 3.

b) L'énoncé optionnel des **exigences de sécurité pour l'environnement TI** doit identifier les exigences de sécurité des TI devant être satisfaites par l'environnement TI de la TOE. Dans le cas où il n'est pas spécifié de dépendances de la TOE envers l'environnement TI, cette partie de la ST peut être omise.

Il est à noter que les **exigences de sécurité pour l'environnement non TI**, bien qu'étant souvent utiles dans la pratique, ne sont pas tenues de faire formellement partie de la ST car elles ne sont pas directement reliées à l'implémentation de la TOE.

c) Les **conditions communes** suivantes doivent s'appliquer d'égale façon à l'expression des exigences fonctionnelles et d'assurance de sécurité de la TOE et pour son environnement TI :

1) Toutes les exigences de sécurité des TI devraient être formulées par référence à des composants d'exigences de sécurité tirés de la partie 2 ou de la partie 3 quand cela est possible. Dans le cas où aucun des composants d'exigences de la partie 2 ou de la partie 3 n'est facilement applicable à tout ou partie des exigences de sécurité, la

ST peut formuler ces exigences de façon explicite sans référence aux CC.

2) Tout énoncé explicite des exigences fonctionnelles ou d'assurance de sécurité de la TOE doit être exprimé clairement et sans ambiguïté de telle façon que l'évaluation et la démonstration de conformité soient faisables. Le niveau de détail et le mode d'expression des composants fonctionnels ou d'assurance existants dans les CC doivent être utilisés comme modèles.

3) Toutes les opérations exigées doivent être utilisées pour enrichir les exigences jusqu'au niveau de détail nécessaire pour démontrer que les objectifs de sécurité sont atteints. Toutes les opérations spécifiées sur les composants d'exigences doivent être appliquées.

4) Toutes les dépendances entre exigences de sécurité des TI devraient être satisfaites. Les dépendances peuvent être satisfaites en incluant l'exigence pertinente dans les exigences de sécurité de la TOE, ou en tant qu'exigence pour l'environnement.

### C.2.7 Spécifications globales de la TOE

216 Les spécifications globales de la TOE doivent définir l'instantiation des exigences de sécurité pour la TOE. Ces spécifications doivent fournir une description des fonctions de sécurité et des mesures d'assurance de la TOE qui satisfait aux exigences de sécurité de la TOE. Il est à noter que les informations fonctionnelles fournies par les spécifications globales de la TOE pourraient dans certains cas être identiques aux informations qui doivent être fournies pour la TOE pour les exigences de ADV_FSP.

217 Les spécifications globales de la TOE contiennent les éléments suivants :

a) L'énoncé **des fonctions de sécurité de la TOE** doit couvrir les fonctions de sécurité des TI et doit spécifier comment ces fonctions satisfont aux exigences fonctionnelles de sécurité de la TOE. Cet énoncé doit inclure une table de correspondance bidirectionnelle entre les fonctions et les exigences qui montre clairement quelles fonctions satisfont quelles exigences et que toutes les exigences sont satisfaites. Chaque fonction de sécurité doit au minimum contribuer à satisfaire au moins une exigence fonctionnelle de sécurité de la TOE.

1) Les fonctions de sécurité des TI doivent être définies dans un style informel avec un niveau de détail nécessaire pour comprendre leur finalité.

2) Toutes les références à des mécanismes de sécurité inclus dans la ST doivent être reliées aux fonctions de sécurité concernées de telle sorte qu'on puisse déterminer quels sont les mécanismes de sécurité utilisés pour l'implémentation de chaque fonction.

3) Lorsque AVA_SOF.1 est inclus dans les exigences d'assurance de la TOE, toutes les fonctions de sécurité des TI réalisées au moyen d'un mécanisme faisant appel au calcul des probabilités ou des permutations (e.g. un mot de passe ou une fonction de hachage) doivent être identifiées. La probabilité de mettre en défaut les mécanismes de telles fonctions par une attaque délibérée ou accidentelle touche directement à la sécurité de la TOE. Une analyse de la résistance des fonctions de sécurité de la TOE doit être fournie pour chacune de ces fonctions. La résistance de chaque fonction identifiée doit être déterminée et annoncée comme étant SOF-élémentaire, SOF-moyen ou SOF-élevé ou selon la métrique spécifique définie en option. Les éléments de preuve fournis au sujet de la résistance des fonctions doivent être suffisants pour permettre aux évaluateurs d'estimer de façon indépendante et de confirmer que les niveaux de résistance annoncés sont adéquats et corrects.

b) L'énoncé **des mesures d'assurance** spécifie des mesures d'assurance de la TOE qui sont annoncées comme satisfaisant les exigences d'assurance présentées. Les mesures d'assurance doivent être reliées aux exigences d'assurance de telle sorte qu'on puisse déterminer quelles sont les mesures qui contribuent à quelles exigences.

Le cas échéant, la définition des mesures d'assurance peut être faite par référence aux plans de qualité, aux plans de cycle de vie ou aux plans de gestion adéquats.

### C.2.8 Annonces de conformité à un PP

218 La ST peut de façon optionnelle annoncer que la TOE est conforme aux exigences d'un PP (ou éventuellement de plusieurs). Pour chaque annonce de conformité à un PP, la ST doit inclure une déclaration **de conformité au PP** qui contient l'explication, la justification et tout autre élément nécessaire pour établir le bien fondé de l'annonce.

219 Le contenu et la présentation des déclarations de la ST relatives aux objectifs et aux exigences pour la TOE pourraient être affectés par les annonces de conformité à un PP faites pour la TOE. L'impact sur la ST peut être résumé en considérant les cas suivants pour chaque PP auquel il est fait référence :

a) Si aucune annonce de conformité à un PP n'est faite, la représentation complète des objectifs et des exigences pour la TOE devrait être faite comme cela est décrit dans la présente annexe. Aucune annonce de conformité à un PP n'est incluse.

b) Dans le cas où la ST annonce uniquement une conformité avec les exigences d'un PP ne nécessitant pas de précision supplémentaire, la référence au PP est suffisante pour définir et pour justifier les objectifs et les exigences de la TOE. Il n'est pas nécessaire de répéter le contenu du PP.

c) Dans le cas où la ST annonce une conformité avec les exigences d'un PP, et que ce PP nécessite par la suite d'être précisé, la ST doit montrer que les exigences du PP sur les précisions sont satisfaites. Une telle situation pourrait survenir typiquement lorsque le PP contient des opérations non effectuées en totalité. Dans une telle situation, la ST peut faire référence aux exigences spécifiques mais doit compléter les opérations non effectuées. Dans certaines circonstances, lorsque les exigences pour effectuer les opérations sont conséquentes, il peut être préférable de répéter le contenu du PP dans la ST pour aider à la clarté.

d) Dans le cas où la ST annonce une conformité avec les exigences d'un PP, mais étend ce PP en ajoutant des objectifs et des exigences supplémentaires, la ST doit définir les ajouts, alors qu'une référence au PP peut être suffisante pour définir les objectifs et les exigences du PP. Dans certaines circonstances, lorsque les ajouts sont conséquents, il peut être préférable de répéter le contenu du PP dans la ST pour aider à la clarté.

e) Le cas où la ST annonce une conformité partielle à un PP n'est pas admissible pour une évaluation CC.

220 Les CC n'imposent pas de choix entre une recopie et une référence aux objectifs et aux exigences du PP. L'exigence fondamentale est que le contenu de la ST soit complet, clair et non ambigu de telle sorte que l'évaluation de la ST soit possible, que la ST soit une base acceptable pour l'évaluation de la TOE, et que la traçabilité avec tout PP référencé apparaisse clairement.

221 Dans le cas où une annonce de conformité à un PP est faite, la déclaration correspondante doit contenir les éléments suivants pour chaque PP concerné.

a) L'énoncé de la **référence du PP** doit identifier le PP vis-à-vis duquel la conformité est annoncée ainsi que tout complément qui peut être nécessaire relativement à cette annonce. Une annonce valide implique que la TOE satisfait à toutes les exigences du PP.

b) L'énoncé des **adaptations du PP** doit identifier les énoncés des exigences de sécurité des TI qui satisfont les opérations autorisées du PP ou précisent d'une autre manière les exigences du PP.

c) L'énoncé des **ajouts au PP** doit identifier les objectifs et les exigences pour la TOE qui viennent compléter les objectifs et les exigences du PP.

### C.2.9 Argumentaire

222 Cette partie de la ST présente les éléments de preuve utilisés lors de l'évaluation de la ST. Ces éléments de preuve appuient les annonces suivant lesquelles la ST constitue un ensemble d'exigences complet et cohérent, et qu'une TOE s'y conformant offrirait un ensemble efficace de contre-mesures de sécurité des TI au sein de l'environnement de sécurité, et que les spécifications globales de la TOE prennent en compte les exigences. L'argumentaire doit également démontrer que

toute annonce de conformité à un PP est valide. L'argumentaire doit inclure les éléments suivants :

a) L'**argumentaire relatif aux objectifs de sécurité** doit démontrer que les objectifs de sécurité déclarés sont reliés à tous les aspects identifiés dans l'environnement de sécurité de la TOE et sont à même de les couvrir.

b) L'**argumentaire relatif aux exigences de sécurité** doit démontrer que l'ensemble des exigences de sécurité (TOE et environnement) convient pour satisfaire aux objectifs de sécurité et qu'ils sont reliés à ces derniers. Il doit pouvoir être démontré :

1) que la combinaison des composants individuels d'exigences fonctionnelles et d'assurance de la TOE et pour son environnement TI satisfait aux objectifs de sécurité déclarés ;

2) que l'ensemble des exigences de sécurité constitue un tout ayant une cohérence interne et dont les éléments se soutiennent mutuellement ;

3) que le choix des exigences de sécurité est justifié. Chacune des circonstances suivantes doit être justifiée de manière spécifique :

— choix d'exigences ne figurant pas dans les parties 2 ou 3 ;
— choix d'exigences d'assurance n'incluant pas d'EAL ;
— non satisfaction des dépendances ;

4) que le niveau de résistance des fonctions choisi pour la ST, de même que toute résistance de fonction explicite annoncée, est cohérent avec les objectifs de sécurité pour la TOE.

c) L'**argumentaire relatif aux spécifications globales de la TOE** doit montrer que les fonctions de sécurité et les mesures d'assurance de la TOE conviennent pour satisfaire aux exigences de sécurité de la TOE. Il doit être démontré :

1) que les fonctions de sécurité des TI de la TOE qui sont spécifiées coopèrent de manière à satisfaire aux exigences fonctionnelles de sécurité de la TOE ;

2) que les annonces relatives à la résistance des fonctions de la TOE sont valides ou que les affirmations que de telles annonces ne sont pas nécessaires sont valides ;

3) que l'annonce suivant laquelle les mesures d'assurance présentées sont conformes aux exigences d'assurances est justifiée.

L'argumentaire doit être présenté à un niveau de détail correspondant à celui utilisé pour la définition des fonctions de sécurité.

d) L'**argumentaire relatif aux annonces de conformité à un PP** doit expliquer toute différence entre les objectifs et les exigences de sécurité de la ST et ceux de tout PP dont on se réclame. Cette partie de la ST peut être omise dans le cas où aucune annonce de conformité à un PP n'est faite ou dans le cas où les exigences et les objectifs de sécurité de la ST sont identiques à ceux de tout PP dont on se réclame.

223 Ces éléments pouvant être volumineux, ils peuvent être distribués séparément car ils ne sont pas forcément appropriés ou utiles pour tous les utilisateurs de la ST.

# Annexe D
# (Informative)

# Bibliographie

[B&L] Bell, D. E. and LaPadula, L. J., Secure Computer Systems: Unified Exposition and MULTICS Interpretation, Revision 1, US Air Force ESD-TR-75-306, MITRE Corporation MTR-2997, Bedford MA, March 1976.

[Biba] Biba, K. J., Integrity Considerations for Secure Computer Systems, ESD-TR-372, ESD/AFSC, Hanscom AFB, Bedford MA., April 1977.

[CTCPEC] Canadian Trusted Computer Product Evaluation Criteria, Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993.

[FC] Federal Criteria for Information Technology Security, Draft Version 1.0, (Volumes I and II), jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993.

[Gogu1] Goguen, J. A. and Meseguer, J., “Security Policies and Security Models,” 1982 Symposium on Security and Privacy, pp.11-20, IEEE, April 1982.

[Gogu2] Goguen, J. A. and Meseguer, J., “Unwinding and Inference Control,” 1984 Symposium on Security and Privacy, pp.75-85, IEEE, May 1984.

[ITSEC] Information Technology Security Evaluation Criteria, Version 1.2, Office for Official Publications of the European Communities, June 1991.

[ISO/IEC 7498-2:1989] Information processing systems - Open Systems Interconnection - Basic Reference Model, Part 2: Security Architecture.

[TCSEC] Trusted Computer Systems Evaluation Criteria, US DoD 5200.28-STD, December 1985.