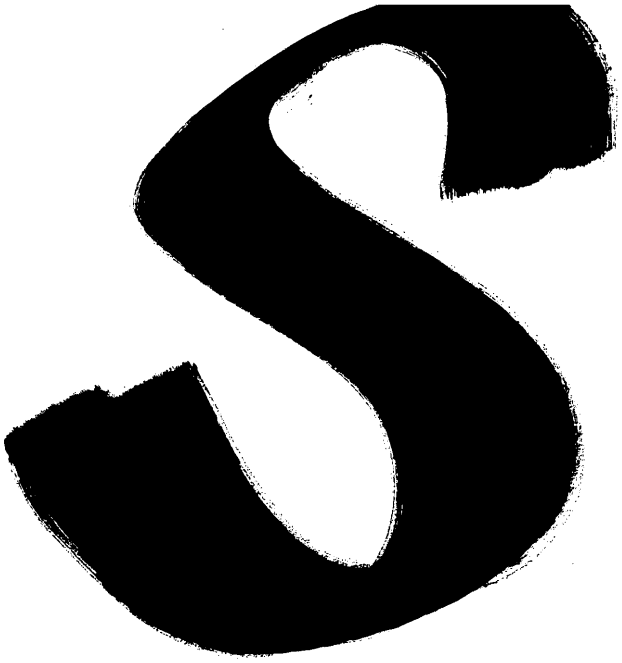


Critères d'évaluation de la sécurité des systèmes informatiques (ITSEC)

Critères harmonisés provisoires

Juin 1991

I T S E C

A la suite d'une consultation internationale approfondie, la version 1.2 de ITSEC est publiée, pour un emploi opérationnel dans le cadre d'organisations d'évaluation et de certification, pour une période prévisionnelle de deux ans à compter de la date de parution. La pratique acquise sera utilisée pour revoir et développer davantage ITSEC à la fin de cette période. De plus, les considérations provenant d'une harmonisation internationale plus poussée seront prise en compte.

Une fiche bibliographique figure à la fin de l'ouvrage.

Luxembourg: Office des publications officielles des Communautés européennes, 1992

ISBN 92-826-3005-6

Numéro de catalogue : CD-71-91-502-FR-C

Printed in France

TABLE DES MATIERES

0 INTRODUCTION

0.1 En quarante ans seulement, les technologies de l'information (TI) en sont venues à jouer un rôle important et souvent vital dans presque tous les secteurs des sociétés organisées. En conséquence, la sécurité est devenue un aspect essentiel des technologies de l'information.

0.2 Dans ce contexte, la sécurité des TI est caractérisée par :

- la **confidentialité** - prévention d'une divulgation non autorisée de l'information ;

- l'**intégrité** - prévention d'une modification non autorisée de l'information ;

- la **disponibilité** - prévention d'un déni non autorisé d'accès à l'information ou à des ressources.

0.3 Un **système** TI ou un **produit** TI (issu des Technologies de l'Information) aura ses exigences propres pour maintenir la confidentialité, l'intégrité et la disponibilité. Pour satisfaire à ces exigences, il implémentera un certain nombre de mesures techniques de sécurité, appelées dans ce document fonctions **dédiées à la sécurité**, qui recouvrent par exemple des domaines tels que le contrôle d'accès, l'audit et la reprise sur incident. Une confiance appropriée dans ces fonctions sera nécessaire : dans le présent document, on emploie le terme d'**assurance**, qu'il s'agisse de la confiance dans la **conformité** des fonctions dédiées à la sécurité (tant du point de vue de leur développement que de celui de leur exploitation) ou de la confiance dans l'**efficacité** de ces fonctions.

0.4 Les utilisateurs de systèmes doivent pouvoir se fier à la sécurité des systèmes qu'ils utilisent. Il leur faut aussi un étalon pour pouvoir comparer les aptitudes, en matière de sécurité, des produits TI qu'ils envisagent d'acheter. Bien qu'ils aient la possibilité soit de se fier à la parole des fabricants ou des fournisseurs des systèmes et des produits en question, soit de les tester eux-mêmes, il est probable que beaucoup préféreront se reposer sur les résultats d'une évaluation impartiale effectuée par un organisme indépendant. Une telle **évaluation** d'un système ou d'un produit exige des critères d'évaluation de la sécurité objectifs et bien définis ainsi que l'existence d'un **organisme de certification** qui puisse confirmer que l'évaluation a été correctement conduite. Les **cibles de sécurité** de système sont spécifiques aux besoins particuliers des utilisateurs du système en question, alors que les cibles de sécurité de produit sont plus générales, afin que les produits qui satisfont à ces cibles puissent être incorporés dans de nombreux systèmes ayant des exigences de sécurité similaires mais non nécessairement identiques.

0.5 Pour un système, une évaluation de ses capacités en matière de sécurité peut être considérée comme faisant partie d'une procédure plus formelle de réception d'un système TI devant être utilisé dans un environnement particulier. Le terme d'**homologation** est souvent utilisé pour décrire cette procédure. Elle exige de prendre en compte de nombreux facteurs avant de considérer que le système convient pour l'usage prévu : elle exige l'assurance dans la sécurité fournie par le système, la confirmation des responsabilités d'administration de la sécurité, la conformité avec les exigences qui s'appliquent au plan technique, légal ou réglementaire, et la confiance dans l'adéquation des autres mesures non techniques de sécurité fournies par l'environnement du système. Les critères contenus dans le présent document concernent en premier lieu les mesures techniques de sécurité, mais prennent en compte certains aspects non techniques, tels que les procédures d'exploitation sûre pour la sécurité liée au personnel, la sécurité physique et la sécurité organisationnelle (mais seulement quand elles empiètent sur les mesures techniques de sécurité).

0.6 Beaucoup de travaux ont déjà été réalisés pour développer des critères d'évaluation de la sécurité des TI, malgré quelques légères divergences sur les objectifs selon les exigences spécifiques des pays ou des organismes concernés. Le plus important, et à bien des égards un précurseur pour les autres travaux, a été le document Trusted Computer System Evaluation Criteria [TCSEC], communément appelé TCSEC ou "Livre orange" (Orange Book) qui a été publié et utilisé par le département de la défense des Etats-Unis pour l'évaluation de produits. D'autres pays, principalement européens, ont aussi une expérience importante en matière d'évaluation de la sécurité des TI et ont mis au point leurs propres critères de sécurité des TI. Au Royaume Uni, c'est le cas du mémorandum CESG numéro 3 [CESG3] développé à usage gouvernemental, et des propositions du ministère du Commerce et de l'Industrie réunies dans le "Livre vert" [DTIEC] pour les produits commerciaux de sécurité des TI. En Allemagne, le service allemand de Sécurité de l'Information a publié une première version de ses propres critères en 1989 [ZSIEC], et à la même époque des critères ont été développés en France sous le nom du "Livre bleu-blanc-rouge" [SCSSI].

0.7 Constatant que le travail se poursuivait dans ce domaine et qu'il restait encore beaucoup à faire, la France, le Royaume Uni, les Pays-Bas et l'Allemagne ont reconnu qu'il fallait aborder ce travail en concertation, et qu'il fallait établir des critères de sécurité des TI communs et harmonisés. Trois raisons justifiaient cette harmonisation :

a) une vaste expérience avait été accumulée dans les divers pays et il y avait beaucoup à gagner à construire en commun à partir de cette expérience ;

b) les industriels ne voulaient pas de critères de sécurité différents selon les pays ;

c) les concepts de base et les approches étaient les mêmes dans les différents pays, et même dans les diverses applications commerciales, gouvernementales et militaires.

0.8 En conséquence, il a été décidé de s'appuyer sur les diverses initiatives nationales en prenant le meilleur de tout ce qui avait déjà été réalisé et en réunissant le tout dans une construction cohérente et structurée. Assurer au maximum l'applicabilité et la compatibilité avec les travaux existants, en particulier avec le document TCSEC américain, a été une préoccupation permanente tout au long de ce processus. Bien que l'on ait estimé, au début, que le travail se limiterait à une harmonisation des critères existants, il a quelquefois été nécessaire d'y apporter des compléments.

0.9 Une des raisons pour produire ces critères harmonisés au plan international est de fournir une base compatible pour la **certification** par les organismes de certification nationaux des quatre pays qui y coopèrent, avec pour objectif final de permettre la reconnaissance mutuelle des résultats des évaluations.

0.10 Le présent document expose les critères harmonisés. Le chapitre 1 contient une brève présentation de leur champ d'application. Le chapitre 2 traite de la fonctionnalité de sécurité, c'est-à-dire de la définition et de la description des besoins en matière de sécurité. Le chapitre 3 définit les critères d'évaluation de l'assurance de l'efficacité d'une **cible d'évaluation** comme solution à ces besoins. Le chapitre 4 complète cette évaluation par l'examen de la conformité de la solution. Le chapitre 5 décrit les résultats attendus d'une évaluation, et le chapitre 6 contient un glossaire des termes qui prennent dans le présent document un sens plus précis ou différent de celui du langage courant (ceux-ci sont imprimés en caractère gras lorsqu'ils sont utilisés pour la première fois, alors que les caractères italiques sont utilisés pour faire ressortir certains termes). Le but du glossaire est d'aider le lecteur à comprendre non seulement la définition des termes, mais aussi les idées et les concepts qui sont propres aux critères harmonisés.

0.11 Les critères d'évaluation des chapitres 3 et 4 sont présentés d'une manière standardisée ; ils spécifient ce qui doit être fourni par le **commanditaire** de l'évaluation (la personne ou l'organisation qui demande l'évaluation) et ce qui doit être fait par l'**évaluateur** (la personne ou l'organisation indépendante qui effectue l'évaluation). Cette distinction a pour objectif d'aider à assurer la cohérence et l'uniformité des résultats d'évaluation. Pour chaque domaine d'évaluation, la documentation à fournir par le commanditaire de l'évaluation est identifiée. Viennent ensuite les critères à prendre en compte pour chaque aspect ou phase

d'évaluation relatif à ce domaine. Ces critères sont décomposés en **exigences concernant le contenu et la présentation** de la documentation qui doit être fournie par le commanditaire, en **exigences concernant les éléments de preuve** que cette documentation doit présenter, et en **tâches de l'évaluateur** que celui-ci doit effectuer aussi bien pour vérifier la documentation fournie que pour effectuer, chaque fois que nécessaire, des tests additionnels ou d'autres activités. Dans le cas des critères concernant la manière dont le système ou le produit doit être utilisé en environnement opérationnel, le commanditaire ne sera pas, en général, capable de fournir des preuves tirées de l'emploi réel. Par conséquent l'évaluateur doit supposer pour les besoins de l'évaluation que les procédures spécifiées par le commanditaire seront suivies dans la pratique.

0.12 Dans le cadre des présents critères certains verbes sont utilisés d'une manière particulière. *Devoir* est utilisé pour exprimer les critères auxquels il est impératif de satisfaire ; *pouvoir* est utilisé pour exprimer des critères qui ne sont pas obligatoires ; et le *futur* est utilisé pour exprimer des actions qui auront lieu ultérieurement. De même, les verbes *présenter*, *décrire* et *expliquer* sont utilisés dans les présents critères pour exiger des niveaux de rigueur croissants dans la fourniture des éléments de preuve. *Présenter* signifie que les éléments pertinents doivent être fournis ; *décrire* signifie que ces éléments doivent être fournis et leurs caractéristiques pertinentes énumérées ; *expliquer* signifie que ces éléments doivent être fournis, leurs caractéristiques pertinentes énumérées et des justifications données.

0.13 En dehors du chapitre 4, les paragraphes sont numérotés séquentiellement à l'intérieur de chaque chapitre. Au chapitre 4, les critères sont présentés séparément pour chaque niveau d'évaluation. Les paragraphes d'introduction de ce chapitre sont numérotés comme dans les autres chapitres, mais ensuite les paragraphes contenant les critères sont numérotés séquentiellement pour chaque niveau, le même numéro de paragraphe s'appliquant au même sujet à chaque niveau. Néanmoins chaque paragraphe de ce document est identifié de manière unique par la combinaison du chapitre ou du numéro du niveau et du numéro du paragraphe.

0.14 Le présent travail a exploité des documents qui ont déjà été abondamment discutés et utilisés dans la pratique ; de plus, on peut considérer que les idées et les concepts ont été pesés avec soin et que la structure choisie pour l'ouvrage convient pour lui assurer le maximum de cohérence et de facilité d'emploi. La version actuelle de l'ITSEC tire profit de révisions significatives faites après une large consultation internationale. La procédure de revue a été faite avec le concours de la Commission des Communautés Européennes qui a organisé une conférence internationale au cours de laquelle la version 1.0 a été discutée, puis un atelier au cours duquel une version intermédiaire, la version 1.1, a été affinée. Ces réunions ont été complétées

par des commentaires écrits des personnes ayant participé à cette consultation que les auteurs ont cherché à prendre en compte pour préparer la version 1.2.

0.15 On peut donc s'attendre à ce que ces critères soient largement acceptés et utilisés dans une large gamme d'utilisations et de secteurs de marché ; toutefois, il est admis que des améliorations peuvent être apportées à ces critères, et le seront. En conséquence, les suggestions et les commentaires sont encouragés et peuvent être envoyés à l'une des adresses ci-après, en portant la mention "Commentaires sur l'ITSEC"

Commission des Communautés Européennes
Directorat XIII/F
SOG-IS Secrétariat
Rue de la Loi 200
B-1049 BRUXELLES
Belgique

Ou, pour la France :

Service Central de la Sécurité des Systèmes d'Information
Division Informatique et Systèmes
18, rue du Docteur Zamenhof
F-92131 Issy-les-Moulineaux

Pour l'Allemagne :

Bundesamt für Sicherheit in der Informationstechnik
Am Nippenkreuz 19
D-5300 BONN 2

Pour les Pays-Bas :

Netherlands National Comsec Agency
Bezuidenhoutseweg 67
P.O. Box 20061
NL-2500 EB THE HAGUE

Pour le Royaume Uni :

Head of the Certification Body
UK IT Security Evaluation and Certification Scheme
Room 2/0805
Fiddlers Green Lane

CHELTENHAM
Glos GB-GL 52 5 AJ

0.16 Des exemplaires de la version 1.2 de l'ITSEC peuvent être obtenus auprès de la Commission des Communautés Européennes à l'adresse indiquée ci-dessus.

1 CHAMP D'APPLICATION

Mesures techniques de sécurité

1.1 La sécurité d'un système TI peut souvent être assurée en grande partie par des mesures non techniques, telles que des contrôles de l'organisation, des contrôles du personnel, des contrôles physiques et des contrôles administratifs. Toutefois, on constate une tendance et un besoin croissants à recourir à des mesures techniques de sécurité des TI. Bien que les critères de sécurité qui suivent portent surtout sur les mesures techniques de sécurité, ils concernent cependant aussi quelques aspects non techniques, principalement les procédures d'exploitation sûre qui leur sont associées pour la sécurité liée au personnel, la sécurité physique et la sécurité organisationnelle (mais seulement quand elles empiètent sur les mesures techniques de sécurité).

1.2 Les présents critères ont été conçus pour être dans leur plus grande partie également applicables aux mesures techniques de sécurité implémentées au moyen de matériel, de logiciel ou de microprogrammes. Lorsque des aspects particuliers de l'évaluation ne sont destinés à s'appliquer qu'à certains modes de réalisation, cela est indiqué dans le texte des critères correspondants.

1.3 Les présents critères ne sont pas destinés à couvrir les aspects physiques de la sécurité matérielle tels que la fourniture d'enceintes résistant à l'intrusion ou le contrôle des signaux parasites compromettants.

Systèmes et Produits

1.4 Dans le cadre du présent document, la différence entre systèmes et produits peut s'expliquer comme suit. Un *système TI* est une installation spécifique de TI ayant un objectif particulier et un environnement opérationnel connu. Un *produit TI* est un matériel informatique, un progiciel ou un ensemble des deux qui peut être acheté sur étagère et intégré dans divers systèmes. Un système TI est généralement construit à partir d'un certain nombre de **composants** matériels et logiciels. Certains composants (par exemple un logiciel d'application) seront réalisés spécialement ; d'autres composants (par exemple le matériel) seront généralement des produits standards. Pour certaines applications, il pourrait être possible d'acquérir un seul produit pour servir de système complet, mais habituellement il sera nécessaire de réaliser un minimum d'adaptation et d'intégration pour satisfaire aux exigences spécifiques du système.

1.5 Du point de vue de la sécurité, la principale différence entre systèmes et produits tient à ce qui est certain quant à leur environnement opérationnel. Un système est conçu pour satisfaire les besoins d'un groupe particulier d'**utilisateurs finals**. Son environnement est réel, il peut être défini et observé dans ses moindres détails ; en particulier les caractéristiques et les besoins de ses utilisateurs finals seront connus, et les menaces contre sa sécurité sont des menaces réelles, qui peuvent être déterminées. Un produit doit être apte à être incorporé dans un grand nombre de systèmes ; le concepteur du produit ne peut faire que des hypothèses générales sur l'environnement opérationnel d'un système dont ce produit pourrait devenir un composant. Il revient à celui qui achète le produit et construit le système de s'assurer que ces hypothèses sont cohérentes avec l'environnement véritable du système.

1.6 Il est important, pour des raisons de cohérence, d'utiliser les mêmes critères de sécurité pour les produits et les systèmes : il sera ainsi plus facile et moins coûteux d'évaluer les systèmes qui contiennent des produits déjà évalués avec succès. C'est pourquoi les présents critères traitent de l'évaluation de la sécurité à la fois pour les produits et les systèmes TI. Dans le reste de ce document, l'expression cible d'évaluation ou TOE (Target Of Evaluation) est utilisée pour désigner un produit ou un système à évaluer.

1.7 Une TOE peut être construite à partir de plusieurs composants. Certains composants ne contribueront pas à satisfaire aux **objectifs de sécurité** de la TOE. D'autres contribueront à satisfaire aux objectifs de sécurité ; ces derniers composants sont appelés dédiés à la sécurité. Enfin il peut y avoir des composants qui ne sont pas dédiés à la sécurité mais qui doivent cependant fonctionner correctement pour que la TOE puisse faire respecter la sécurité ; ils sont appelés **touchant à la sécurité**. La combinaison de composants dédiés à la sécurité et de composants touchant à la sécurité à l'intérieur d'une TOE est souvent appelée base informatique de confiance ou TCB (Trusted Computing Base) (voir les figures 1 et 2).

1.8 La plus grande partie du travail d'évaluation sera concentrée sur les composants d'une TOE dont il est établi qu'ils sont dédiés à la sécurité ou touchant à la sécurité, mais tous les autres devront être examinés au cours de l'évaluation et il devra être démontré qu'ils ne sont ni dédiés à la sécurité ni touchant à la sécurité.

Fonctionnalité et Assurance, Classes et Niveaux

1.9 Pour qu'une TOE atteigne ses objectifs de sécurité, elle doit comporter des fonctions dédiées à la sécurité appropriées couvrant par exemple des domaines tels que le contrôle d'accès, l'audit et la reprise sur incident.

1.10 Ces fonctions doivent être définies d'une façon claire et compréhensible tant pour le commanditaire de l'évaluation que pour l'évaluateur indépendant. Elles peuvent être soit spécifiées individuellement, soit définies par référence à une **classe de fonctionnalité** prédéfinie. Dix exemples de classes de fonctionnalité sont inclus dans les présents critères. Ces exemples de classes sont basés sur les classes définies dans les critères nationaux allemands [ZSIEC], parmi lesquelles cinq classes sont en étroite correspondance avec les exigences fonctionnelles du document américain Trusted Computer System Evaluation Criteria [TCSEC].

1.11 Dans tous les cas, le commanditaire d'une évaluation doit définir la cible de sécurité pour l'évaluation. Cette cible doit définir les fonctions dédiées à la sécurité qui doivent être fournies par la TOE et contiendra également d'autres informations pertinentes, telles que les objectifs de sécurité de la TOE et les **menaces** envisagées à l'encontre de ces objectifs. Les détails des **mécanismes de sécurité** particuliers qui seront utilisés pour implémenter les fonctions dédiées à la sécurité peuvent également être donnés.

1.12 Les fonctions dédiées à la sécurité choisies pour atteindre les objectifs de sécurité d'une TOE ne constituent qu'un des aspects de la cible de sécurité d'un produit ou d'un système. L'assurance que les objectifs de sécurité sont atteints par les fonctions et les mécanismes dédiés à la sécurité choisis est tout aussi importante.

1.13 L'assurance doit être abordée de différents points de vue et, pour les présents critères harmonisés, il a été décidé de distinguer la confiance dans la conformité de la réalisation des fonctions et mécanismes dédiés à la sécurité, de la confiance dans leur efficacité.

1.14 L'évaluation de l'efficacité consiste à estimer si les fonctions et les mécanismes dédiés à la sécurité fournis dans la TOE satisfont effectivement aux objectifs de sécurité déclarés. L'estimation porte sur la pertinence de la fonctionnalité, la cohésion de la fonctionnalité (si les fonctions choisies opèrent ensemble en synergie), les conséquences de vulnérabilités connues et découvertes (tant au point de vue de la construction de la TOE que de la manière dont elle sera utilisée en exploitation réelle) et la facilité d'emploi.

1.15 En outre, l'évaluation de l'efficacité consiste à estimer la capacité des mécanismes de sécurité de la TOE à résister à une attaque directe (résistance des mécanismes). Trois niveaux de résistance sont définis - élémentaire, moyen et élevé - représentant des degrés de confiance croissants dans la capacité des mécanismes de sécurité de la TOE à résister à une attaque directe.

1.16 L'évaluation de la conformité consiste à estimer si les fonctions et les mécanismes dédiés à la sécurité sont implémentés correctement. Il a été défini sept niveaux

d'évaluation numérotés de E0 à E6, représentant des degrés croissants de confiance dans la conformité. E0 correspond à une confiance insuffisante. E1 correspond au point d'entrée au-dessous duquel il ne peut être accordé aucune confiance utile, et E6 correspond au degré de confiance le plus élevé : les autres niveaux correspondent à des degrés de confiance intermédiaires. La conformité est considérée du point de vue de la construction de la TOE, ce qui recouvre à la fois le processus de développement et l'environnement de développement, et aussi du point de vue de l'exploitation de la TOE.

1.17 Les niveaux d'évaluation sont définis dans le contexte des critères de conformité. Les exigences concernant l'efficacité (incluant la résistance des mécanismes) ne changent pas selon les niveaux mais s'appuient plutôt sur l'estimation de la conformité et sont examinées sur la base des documents fournis par le commanditaire pour cette estimation ; naturellement, dans la pratique, les tâches d'estimation de la conformité et de l'efficacité seront imbriquées.

1.18 Si une TOE ne parvient pas à satisfaire à l'un quelconque des aspects de l'évaluation à un niveau donné, par manque d'information ou pour toute autre raison, l'imperfection doit être corrigée, ou la TOE doit être retirée de l'évaluation pour ce niveau. Sinon il lui sera attribué le niveau E0.

1.19 La réussite de l'évaluation à l'un des six niveaux E1 à E6 couvre un large éventail de confiance possible. L'ensemble de ces six niveaux ne sera pas forcément nécessaire ni approprié pour tous les secteurs du marché qui ont besoin d'une évaluation indépendante des mesures techniques de sécurité. Toutes les combinaisons de fonctionnalité et de confiance ne seront pas nécessairement judicieuses ou utiles. Par exemple, un bas degré de confiance dans la fonctionnalité requise pour satisfaire à une exigence de sécurité multi-niveau militaire ne sera normalement pas approprié. De plus, il est peu probable qu'un haut degré de confiance dans la conformité d'une TOE soit associé à l'exigence d'un bas niveau de résistance des mécanismes.

1.20 Les présents critères harmonisés ne constituent pas un guide de conception pour réaliser des produits ou des systèmes sûrs. Il appartient au commanditaire d'une évaluation de fixer les objectifs de sécurité de sa TOE et de choisir les fonctions de sécurité propres à atteindre ces objectifs. Toutefois, pour chaque niveau d'évaluation, la partie "assurance" des critères peut être vue comme une "liste de contrôles de sécurité" obligatoire auxquels il faut satisfaire.

Profils d'Assurance

1.21 Les critères du présent document exigent du commanditaire de déclarer le niveau d'évaluation dans la cible de sécurité. Toutes les fonctions dédiées à la sécurité énumérées dans la cible de sécurité sont alors estimées pour le même degré de confiance, comme exigé par le niveau d'évaluation déclaré.

1.22 Pour certaines TOE, il peut être exigé d'atteindre un degré de confiance supérieur pour certaines fonctions de sécurité et inférieur pour d'autres ; par exemple, certaines fonctions de sécurité peuvent être plus importantes que d'autres. Dans ces circonstances, le commanditaire peut envisager de produire plus d'une cible de sécurité pour la TOE. Les détails sur la façon dont ceci est effectué, et dans quelles conditions, sont hors du champ d'application des présents critères.

Le processus d'évaluation

1.23 L'objectif du processus d'évaluation est de permettre à l'évaluateur de préparer un rapport impartial indiquant si oui ou non une TOE satisfait à sa cible de sécurité avec le degré de confiance précisé par le niveau d'évaluation déclaré.

1.24 Le processus d'évaluation est représenté dans son contexte en figure 3. Il exige que le commanditaire de l'évaluation y soit fortement impliqué. Plus le niveau d'évaluation est élevé, plus l'implication du commanditaire devra être importante. Les utilisateurs aussi bien que les fournisseurs peuvent agir en tant que commanditaires d'une évaluation. Il est vraisemblable que l'évaluation d'un système sera commanditée par les utilisateurs finals ou leurs représentants techniques, et que l'évaluation d'un produit sera commanditée par le fabricant ou le fournisseur, mais cela n'est pas obligatoire. Tous les intéressés qui peuvent fournir l'information technique nécessaire peuvent être commanditaires d'une évaluation.

1.25 En premier lieu, le commanditaire doit déterminer les exigences opérationnelles et les menaces auxquelles la TOE doit faire face. Dans le cas d'un système, il est nécessaire d'examiner son environnement opérationnel réel afin de déterminer les menaces qui doivent effectivement être prises en compte. Pour un produit, il faut décider quelles menaces contre la sécurité celui-ci devrait prendre en compte. On s'attend à ce que des groupements d'industriels et des organismes internationaux de normalisation définissent dans l'avenir des classes standards de fonctionnalité pour servir de cibles de sécurité de produits. Les développeurs de produits, qui n'ont pas d'idée précise sur des créneaux particuliers du marché ni sur des types d'utilisateurs, peuvent trouver que de telles classes de fonctionnalité pré-définies constituent de bonnes cibles de sécurité pour concevoir des produits qui y correspondent.

1.26 Les objectifs de sécurité de la TOE peuvent alors être déterminés en tenant compte des lois et des autres réglementations. Ils constituent la contribution à la sécurité (en termes de confidentialité, d'intégrité et de disponibilité) que cette TOE est destinée à fournir. Une fois ces objectifs fixés, les fonctions dédiées à la sécurité qui sont nécessaires peuvent être établies, éventuellement par itération, en même temps que le niveau d'évaluation auquel la TOE devra satisfaire pour fournir le degré de confiance nécessaire.

1.27 L'ensemble des résultats de ce travail - définition des fonctions dédiées à la sécurité, menaces identifiées, objectifs de sécurité identifiés, mécanismes spécifiques de sécurité à utiliser - devient la cible de sécurité à prendre en compte pour le développement.

1.28 Pour chaque niveau d'évaluation, les critères énumèrent les éléments que le commanditaire doit fournir à l'évaluateur. Le commanditaire doit s'assurer que ces éléments sont fournis, en veillant à ce que toutes les exigences sur le contenu et la présentation soient satisfaites, et aussi que ces éléments apportent directement ou aident à établir les éléments de preuve demandés.

1.29 Pour que l'évaluation puisse être conduite efficacement, et à un coût minimum, l'évaluateur doit travailler en liaison étroite avec le développeur et le commanditaire de la TOE, l'idéal étant qu'il le fasse dès le début de ce développement, de façon à établir une bonne compréhension de la cible de sécurité et à pouvoir repérer ce que les décisions impliquent pour l'évaluation au fur et à mesure qu'elles sont prises. Toutefois, l'évaluateur doit rester indépendant et ne doit pas faire de suggestion quant à la conception et la réalisation de la TOE. Son rôle est analogue à celui d'un auditeur financier extérieur, qui doit de la même façon construire une bonne relation de travail avec un service financier, et qui, dans bien des cas, utilisera, après examen, les rapports et les résultats des contrôles internes. Et pourtant il doit lui aussi rester indépendant et poser des questions.

1.30 Les exigences concernant les tests et les analyses de sécurité dans les critères méritent une mention particulière ; dans tous les cas, la responsabilité des tests et des analyses échoit au commanditaire. Pour tous les niveaux d'évaluation sauf E1, l'évaluateur vérifiera principalement les résultats des tests et des analyses fournis par le commanditaire. L'évaluateur n'effectuera lui-même des tests et des analyses que pour vérifier les résultats fournis, pour compléter les éléments de preuve fournis et pour se livrer à des investigations sur les vulnérabilités. Au niveau E1, la fourniture des résultats des tests est facultative. Si ces résultats ne sont pas fournis, l'évaluateur doit en plus effectuer des tests fonctionnels par rapport à la cible de sécurité.

Le processus de certification

1.31 Pour que les présents critères aient une valeur pratique, ils devront s'appuyer sur des organisations pratiques permettant d'assurer la mise en place et le contrôle d'une évaluation indépendante, pilotés par des organismes de certification convenablement qualifiés et reconnus au plan national. Ces organismes délivreront des certificats confirmant la cotation de la sécurité des TOE, telle que déterminée par des évaluations indépendantes convenablement conduites. Comme il est exigé par les présents critères, ils devront approuver les procédures propres à garantir l'authenticité de la TOE livrée. Ils seront également responsables du choix et du contrôle des évaluateurs agréés. Le détail des procédures à suivre par de tels organismes est hors du champ d'application des présents critères.

1.32 Les présents critères ont été conçus pour minimiser la subjectivité inhérente aux résultats d'une évaluation. Les organismes nationaux de certification auront la responsabilité de maintenir l'uniformité des résultats d'évaluation certifiés. La manière d'y parvenir est hors du champ d'application des présents critères.

1.33 Pour que les résultats d'une évaluation par rapport aux présents critères puissent être certifiés par un organisme national de certification, l'évaluateur devra produire un rapport contenant les résultats de l'évaluation sous une forme qui convienne à son examen par l'organisme de certification. Le format et le contenu précis de tels rapports sont hors du champ d'application des présents critères.

1.34 La plupart des cibles de sécurité et des TOE vont évoluer avec le temps. Le maintien d'une cotation certifiée à la suite de changements apportés à la TOE (qu'ils concernent ou non la sécurité) ou à la suite de changements apportés à la cible de sécurité (tels que l'apparition de nouvelles menaces ou de nouveaux objectifs de sécurité) sera réglementé par l'organisme national de certification approprié. Une réévaluation sera nécessaire dans certains cas et pas dans d'autres. Les détails de telles réglementations et procédures sont également hors du champ d'application des présents critères.

Correspondance avec le document TCSEC

1.35 Le document Trusted Computer System Evaluation Criteria [TCSEC], communément appelé TCSEC ou "Livre orange", constitue une base largement reconnue et acceptée pour l'évaluation de la sécurité des systèmes d'exploitation. Publié initialement en 1983, il est utilisé par le département de la défense des Etats-Unis dans l'organisation américaine d'évaluation des produits mise en oeuvre par le NCSC (National Computer Security Center). Les critères du TCSEC sont destinés à satisfaire à la politique de sécurité du département de la défense des Etats-Unis.

Cette politique s'intéresse principalement au maintien de la confidentialité des informations classifiées au niveau national.

1.36 Le TCSEC définit sept ensembles de critères d'évaluation appelés classes (D, C1, C2, B1, B2, B3 et A1) regroupés en quatre divisions (D, C, B et A). Chaque classe de critères couvre quatre aspects de l'évaluation : la politique de sécurité, l'imputabilité, l'assurance et la documentation. Les critères relatifs à ces quatre domaines deviennent de plus en plus détaillés d'une classe à l'autre et forment une hiérarchie dans laquelle D est le niveau le plus bas et A1 le plus haut. Chaque classe couvre à la fois les exigences de fonctionnalité et les exigences de confiance.

1.37 Les critères exposés dans l'ITSEC permettent de sélectionner des fonctions de sécurité arbitraires et définissent sept niveaux d'évaluation représentant une confiance croissante dans la capacité d'une TOE à atteindre sa cible de sécurité. Ainsi ces critères peuvent-ils être appliqués sur une gamme de systèmes et de produits possibles plus large que celle couverte par le TCSEC. D'une manière générale, pour une fonctionnalité identique et à un degré de confiance équivalent, une TOE a plus de liberté sur le plan de l'architecture pour satisfaire aux critères de l'ITSEC qu'à ceux du TCSEC, mais supporte plus de contraintes sur les modes de développement autorisés.

1.38 Plusieurs exemples de classes de fonctionnalité ont été définis pour correspondre étroitement aux exigences de fonctionnalité des classes C1 à A1 du TCSEC. Ce sont les classes F-C1 à F-B3, parmi les exemples de classes de fonctionnalité donnés en annexe A. Il n'est toutefois pas possible de relier directement les niveaux d'évaluation aux exigences de confidentialité des classes du TCSEC, car les niveaux de l'ITSEC sont issus de l'harmonisation des divers ensembles européens de critères de sécurité des TI, qui contiennent un certain nombre d'exigences qui n'apparaissent pas explicitement dans le TCSEC.

1.39 La correspondance recherchée entre les présents critères et les classes du TCSEC est la suivante :

Classe ITSEC		Classe TCSEC
E0	<--->	D
F-C1, E1	<--->	C1
F-C2, E2	<--->	C2
F-B1, E3	<--->	B1
F-B2, E4	<--->	B2
F-B3, E5	<--->	B3
F-B3, E6	<--->	A1

1.40 Il est à noter qu'il n'y a pas de classe de fonctionnalité F-A1, puisque les exigences de fonctionnalité de la classe A1 du TCSEC sont les mêmes que celles de la classe B3. Un produit conçu pour être évalué avec succès aussi bien par rapport à l'ITSEC qu'au TCSEC, et dont il a été montré qu'il satisfaisait à l'une des classes ou des combinaisons du tableau ci-dessus, devrait réussir l'évaluation par rapport aux autres critères pour la classe ou pour la combinaison correspondante. Toutefois, au niveau C1, le TCSEC exige la production d'éléments de preuve concernant les tests effectués par le développeur. Ainsi une évaluation [F-C1, E1] ne serait équivalente à une évaluation C1 que si le commanditaire avait choisi l'exigence optionnelle du niveau E1 de fourniture de la documentation relative aux tests, comme preuve que des tests adéquats par rapport à la cible de sécurité ont été effectués avant l'évaluation.

1.41 Tout au long du TCSEC la combinaison du sous-ensemble dédié à la sécurité et du sous-ensemble touchant à la sécurité est appelée *base informatique de confiance* ou TCB (Trusted Computing Base). Pour le TCSEC, les TOE des classes les plus hautes de la division B et de la division A tirent une confiance supplémentaire d'exigences croissantes de rigueur dans l'architecture et la conception de la TCB imposées par les critères du TCSEC. Les classes de niveau B2 et au dessus exigent que le contrôle d'accès soit réalisé par un mécanisme de validation de référence, mécanisme qui implémente le concept de moniteur de référence [AND]. Un tel mécanisme de validation de référence doit être résistant à l'intrusion, il doit être systématiquement mis en oeuvre, et il doit être assez petit pour pouvoir être soumis à des analyses et à des tests dont la complétude puisse être assurée.

1.42 Pour être compatibles avec le TCSEC, les exemples de classes de fonctionnalité F-B2 et F-B3 de l'ITSEC imposent que le contrôle d'accès soit implémenté avec un tel mécanisme. De plus, pour les niveaux supérieurs d'évaluation, l'ITSEC impose des contraintes d'architecture et de conception sur la réalisation de toutes les fonctions dédiées à la sécurité. Tout ceci, combiné avec les exigences d'efficacité de l'ITSEC relatives au fait que la fonctionnalité de sécurité est pertinente et que ses éléments se soutiennent mutuellement, signifie qu'une TOE capable de satisfaire aux niveaux supérieurs d'évaluation de l'ITSEC, et fournissant une fonctionnalité égale aux fonctionnalités des classes équivalentes du TCSEC, doit nécessairement satisfaire aux exigences du TCSEC quant à l'existence d'une TCB et utiliser le concept de moniteur de référence.

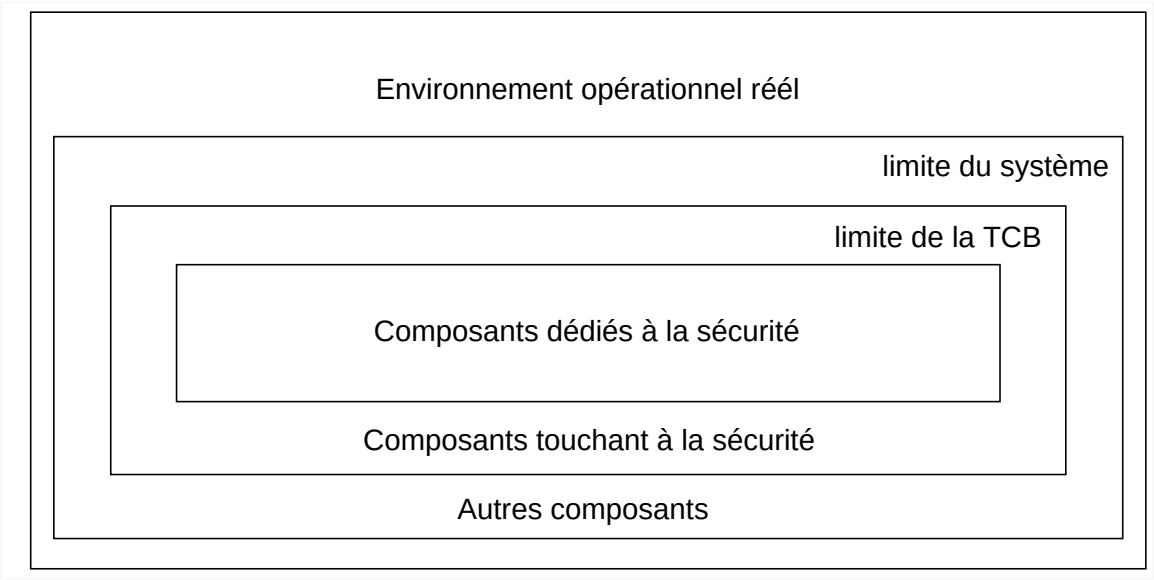


Fig. 1 Système TI

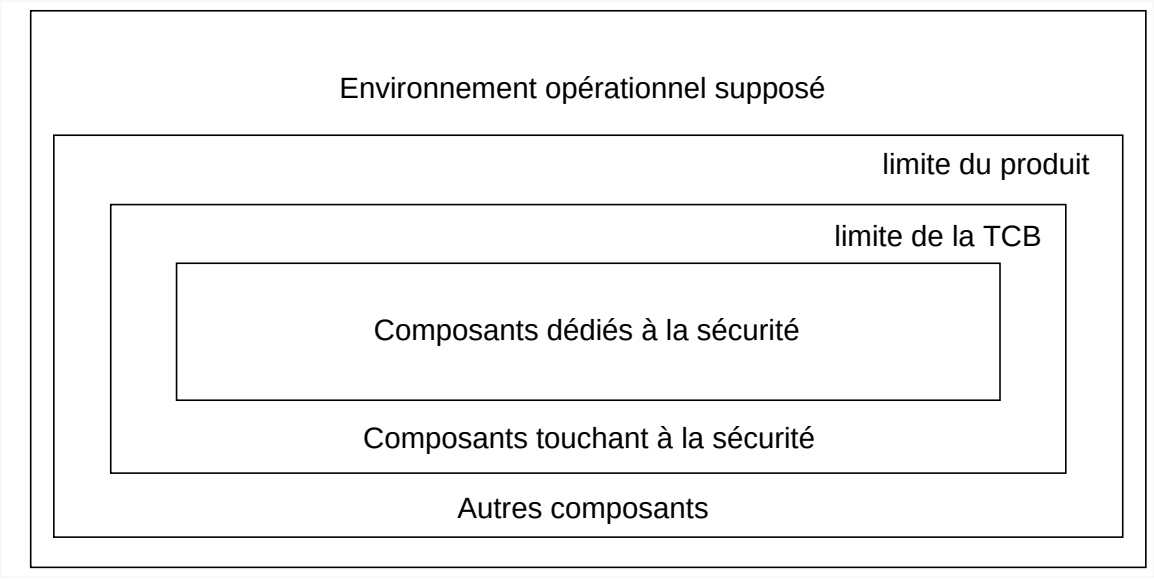


Fig. 2 Produit TI

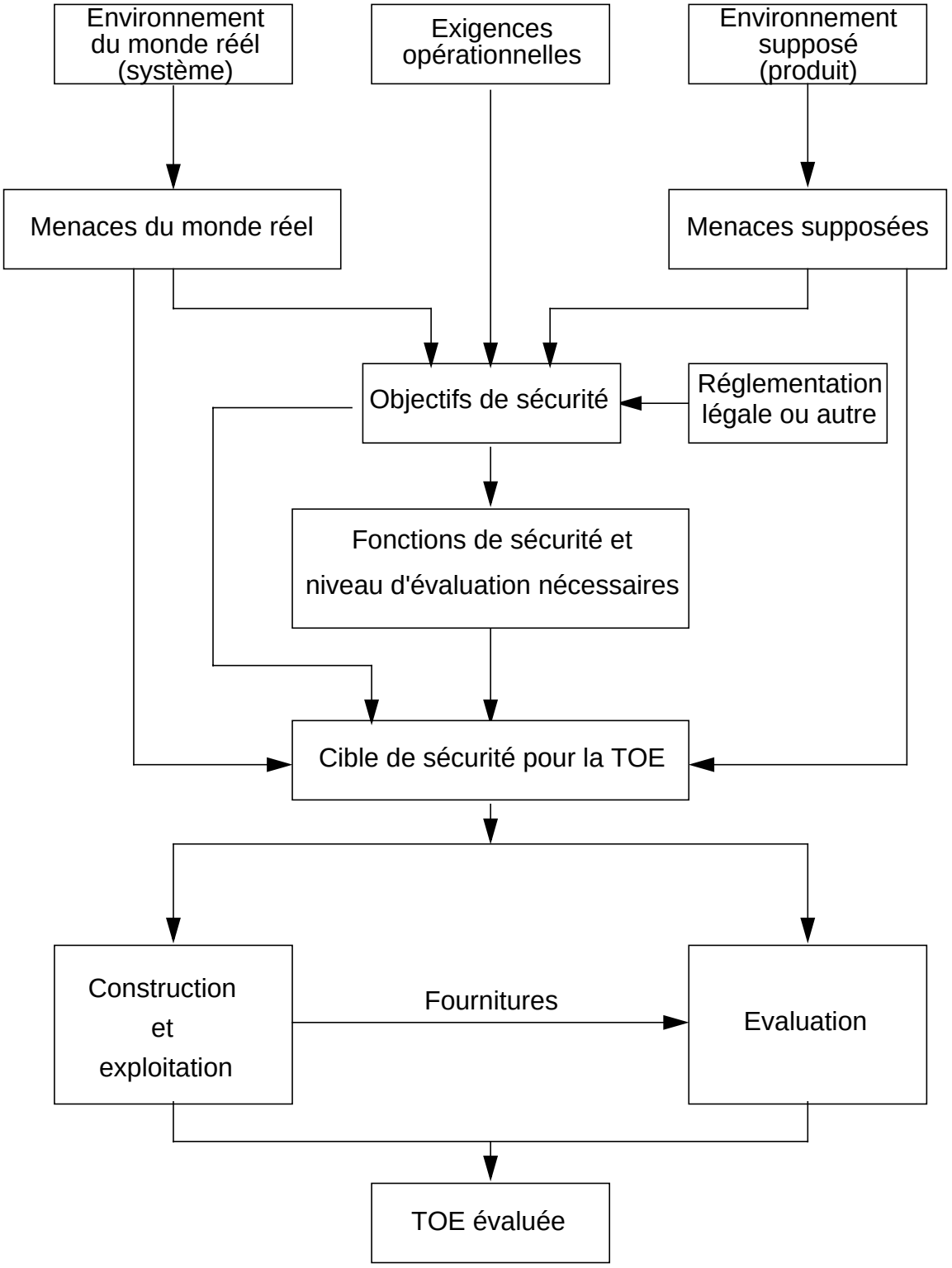


Fig. 3 Processus de développement et d'évaluation

2 FONCTIONNALITE

Introduction

2.1 Une cible d'évaluation (TOE) qui fournit de la sécurité (une combinaison de confidentialité, d'intégrité et de disponibilité) doit présenter des caractéristiques de sécurité appropriées. Il sera normalement nécessaire de déterminer qu'un degré de confiance approprié peut être accordé à ces caractéristiques. Pour cela, les caractéristiques elles-mêmes doivent être spécifiées. Le ou les documents qui spécifient ces caractéristiques, ainsi que le niveau d'évaluation désiré, constituent la cible de sécurité pour cette TOE.

2.2 Dans les présents critères, les caractéristiques de sécurité sont considérées à trois niveaux. Le point de vue le plus abstrait est celui des objectifs de sécurité qui représentent la contribution à la sécurité qu'une TOE se propose d'apporter. Pour atteindre ces objectifs, la TOE doit contenir certaines fonctions dédiées à la sécurité. Ces fonctions dédiées à la sécurité doivent, à leur tour, être implémentées grâce à des mécanismes de sécurité spécifiques. Ces trois niveaux peuvent être schématisés comme suit :

a) Objectifs de sécurité - Pourquoi la fonctionnalité est voulue.

b) Fonctions dédiées à la sécurité - Quelle fonctionnalité est réellement fournie.

c) Mécanismes de sécurité - Comment la fonctionnalité est fournie.

La cible de sécurité

2.3 La cible de sécurité sert à la fois de spécification des fonctions dédiées à la sécurité, par rapport à laquelle la TOE sera évaluée, et de description des liens entre la TOE et l'environnement dans lequel celle-ci sera exploitée. Sont donc intéressés par la cible de sécurité non seulement les responsables de la production de la TOE et de son évaluation, mais également les responsables de sa gestion, de son achat, de son installation, de sa configuration, de son exploitation et de son emploi.

2.4 Le contenu exigé d'une cible de sécurité peut être résumé ainsi :

a) *Soit* une **politique de sécurité du système**
soit un **argumentaire du produit**.

b) Une spécification des fonctions dédiées à la sécurité requises.

c) Une définition des mécanismes de sécurité requis *(optionnelle)*.

d) La cotation annoncée de la résistance minimum des mécanismes.

e) Le niveau d'évaluation visé.

Chacun de ces éléments est décrit plus en détail ci-dessous.

2.5 Les exigences pour la présentation de la cible de sécurité dépendent du niveau d'évaluation visé. Le niveau d'évaluation détermine également les autres documents de la TOE qui doivent être fournis pour l'évaluation, ainsi que les exigences sur leur contenu et leur présentation, et les exigences concernant les éléments de preuve qui doivent être fournis afin de montrer que la TOE satisfait à la cible de sécurité.

2.6 La cible de sécurité peut se présenter sous la forme d'un document unique ou de plusieurs documents. Lorsque plusieurs documents sont utilisés, leurs relations doivent être clairement indiquées.

2.7 Le commanditaire de l'évaluation est responsable de la fourniture et de la fidélité de la cible de sécurité pour l'évaluation.

Politique de sécurité d'un système

2.8 Les éléments constituant une cible de sécurité sont différents selon qu'il s'agit d'un système ou d'un produit. Dans le cas d'un système, l'environnement réel dans lequel la TOE sera utilisée est connu, ses objectifs de sécurité peuvent être déterminés, et les menaces réelles et les contre-mesures existantes peuvent être prises en compte. Ces détails sont donnés dans un document de politique de sécurité du système.

2.9 La politique de sécurité d'un système spécifie l'ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les informations et autres ressources sensibles au sein d'un système spécifique. Elle doit identifier les objectifs de sécurité du système et les menaces auxquelles celui-ci devra faire face. Ces objectifs de sécurité doivent être pris en compte par une combinaison de fonctions dédiées à la sécurité du système (implémentées au sein de la TOE), et également par des moyens physiques, relatifs au personnel ou organisationnels, associés au système. La politique de sécurité d'un système doit couvrir tous les aspects de la sécurité relatifs au système, en incluant ces mesures physiques, organisationnelles et relatives au personnel qui lui sont associées.

2.10 Toutes les organisations auront des normes générales de sécurité qui s'appliqueront à tous les systèmes au sein de l'organisation et qui définiront les relations concernant la sécurité entre l'organisation et le monde extérieur. Ces normes peuvent être considérées comme une **politique de sécurité interne** : l'ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les biens, en particulier les informations sensibles, au sein de l'organisation. Beaucoup d'organisations auront une politique de sécurité interne explicite et écrite, qui spécifiera les règles, les pratiques ainsi que les lois nationales et internationales applicables auxquelles elles doivent se conformer. Dans ce cas, on doit y faire référence dans la politique de sécurité du système. Dans le cas contraire, tous les aspects pertinents doivent être présentés par écrit dans chacune des politiques de sécurité des systèmes de l'organisation.

2.11 Le premier rôle de la politique de sécurité interne est de fournir le contexte nécessaire à l'identification des objectifs de sécurité du système. Le fait d'identifier les biens propres à prendre en considération, les menaces générales et les résultats des analyses de risques aideront à identifier ces objectifs de sécurité du système. Un débat sur les méthodes d'analyse de risques est hors du champ d'application des présents critères.

2.12 Dans le cas d'un système individuel, la politique de sécurité du système doit définir les mesures de sécurité à mettre en oeuvre pour satisfaire aux objectifs de sécurité du système en cohérence avec la politique sécurité interne. Les mesures de sécurité requises par la politique de sécurité du système seront réalisées par une combinaison de fonctions dédiées à la sécurité implémentées par la TOE, et par des moyens physiques, relatifs au personnel et organisationnels. La politique de sécurité du système doit indiquer clairement le partage des responsabilités entre les fonctions dédiées à la sécurité et les autres moyens.

2.13 Les mesures de sécurité des TI d'une politique de sécurité d'un système peuvent être séparées du reste de la politique de sécurité système et définies dans un document séparé : la **politique de sécurité technique**. Il s'agit de l'ensemble des lois, règlements et pratiques qui régissent le traitement des informations sensibles et l'utilisation des ressources par le matériel et le logiciel d'un système TI.

2.14 Dans bien des cas il peut être commode d'inclure les spécifications des fonctions dédiées à la sécurité dans la politique de sécurité du système ou dans la politique de sécurité technique.

2.15 La politique de sécurité du système ou la politique de sécurité technique peuvent servir de base au choix de produits de sécurité des TI qui conviennent pour être incorporés dans le système ; un tel choix de produits est hors du champ d'application des présents critères.

Argumentaire d'un produit

2.16 Dans le cas d'un produit, l'environnement précis dans lequel la TOE va être utilisée n'est pas connu de son développeur, puisque le produit peut être incorporé dans différents systèmes spécifiques et différents environnements système. En remplacement, il doit être fourni un argumentaire qui donne les informations nécessaires à un acheteur éventuel pour décider si ce produit va l'aider à satisfaire aux objectifs de sécurité de son système, et pour définir ce qui reste à faire pour les satisfaire complètement.

2.17 L'argumentaire d'un produit doit identifier la manière dont il est prévu d'utiliser ce produit, l'environnement prévu pour son utilisation et les menaces supposées dans cet environnement. Il doit inclure un résumé des caractéristiques de sécurité du produit, et définir toutes les hypothèses concernant l'environnement et la manière dont le produit sera utilisé. Ceci doit inclure les mesures de sécurité relatives au personnel, physiques, organisationnelles et des TI requises en appui du produit, ainsi que ses dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système qui ne sont pas fournis avec le produit.

Spécification des fonctions dédiées à la sécurité

2.18 La cible de sécurité doit inclure une spécification des fonctions dédiées à la sécurité que la TOE doit fournir. Ces fonctions peuvent être déclarées explicitement, ou par référence à une ou plusieurs classes de fonctionnalité prédéfinies, ou encore par référence à une norme acceptée qui définit une fonctionnalité de sécurité. Des classes prédéfinies sont exposées plus loin dans ce chapitre.

2.19 Un ou plusieurs documents normatifs qui concernent la sécurité peuvent faire partie d'une cible de sécurité, soit qu'elle y fasse référence, soit qu'elle les inclue. Lorsque les normes permettent des options, les options choisies doivent être clairement identifiées. Lorsqu'une norme ne fournit pas toutes les informations requises, les informations complémentaires nécessaires doivent être explicitement fournies dans la cible de sécurité.

2.20 Dans le cas d'un système, les fonctions dédiées à la sécurité doivent être reliées aux objectifs de sécurité, de sorte qu'on puisse voir quelles fonctions satisfont à quels objectifs (une fonction peut satisfaire, ou aider à satisfaire, à plusieurs objectifs). Chacune des fonctions prises en compte dans la spécification des fonctions dédiées à la sécurité doit au minimum aider à satisfaire au moins à un objectif. La spécification des fonctions dédiées à la sécurité doit également montrer pourquoi les fonctions conviennent pour contrer les menaces identifiées ou déclarées contre les objectifs de sécurité.

2.21 Dans le cas d'un produit, les fonctions dédiées à la sécurité doivent être reliées aux modes prévus d'utilisation du produit et les hypothèses faites concernant l'environnement dans lequel le produit sera installé doivent être données dans l'argumentaire du produit. Cette mise en correspondance doit inclure toutes les dépendances envers d'autres fonctions dédiées à la sécurité et d'autres mesures ne relevant pas de la sécurité des TI, supposées fournies par l'environnement.

2.22 Du point de vue de l'évaluation, la spécification des fonctions dédiées à la sécurité est la partie la plus importante de la cible de sécurité. Ces fonctions doivent toujours être spécifiées dans un mode informel, en langage naturel. De plus, pour les niveaux supérieurs d'évaluation, elles doivent également être spécifiées suivant un style de présentation semi-formel ou formel. Des détails concernant de tels styles de présentation sont donnés plus loin dans ce chapitre.

Définition des mécanismes de sécurité requis

2.23 Une cible de sécurité peut, de façon optionnelle, imposer ou revendiquer l'emploi de mécanismes de sécurité particuliers. Tous les mécanismes de sécurité inclus dans la cible de sécurité doivent être reliés aux fonctions dédiées à la sécurité correspondantes, de sorte qu'on puisse voir quels mécanismes réalisent chaque fonction (un mécanisme peut réaliser plusieurs fonctions, et une fonction peut être réalisée par une combinaison de plusieurs mécanismes).

2.24 Lorsque des mécanismes de sécurité sont imposés par la cible de sécurité, c'est au développeur d'implémenter les mécanismes requis. Dans le cas contraire, c'est au développeur de développer et réaliser des mécanismes qui, combinés, réalisent les fonctions dédiées à la sécurité requises.

Cotation annoncée de la résistance minimum des mécanismes

2.25 Chaque cible de sécurité doit spécifier une cotation annoncée de la résistance minimum des mécanismes de sécurité de la TOE vis à vis d'une attaque directe. Ce doit être l'une des cotations *élémentaire, moyenne* ou *élevée* définies au chapitre 3 des présents critères.

Niveau d'évaluation visé

2.26 Chaque cible de sécurité doit spécifier le niveau d'évaluation visé pour l'évaluation de la TOE. Ce doit être l'un des niveaux *E1*, *E2*, *E3*, *E4*, *E5*, *E6* définis au chapitre 4 des présents critères.

Exemples d'utilisation de documents existants de politique de sécurité

2.27 Les présents critères visent à permettre l'utilisation de documents existants de politique de sécurité développés pour d'autres critères ou d'autres normes, pour constituer tout ou partie de la cible de sécurité d'un système. En conséquence, le contenu précis des documents qui constituent la cible de sécurité n'est pas imposé. L'information minimum exigée pour une évaluation par rapport aux présents critères a été présentée plus haut. Dans la mesure où une cible de sécurité peut être constituée de plus d'un document, des modèles existants de documents de politique peuvent être adaptés (bien que des documents complémentaires puissent être exigés pour compléter les informations exigées pour une cible de sécurité).

2.28 Deux exemples sont donnés ci-dessous pour montrer comment des types particuliers de documents de politique de sécurité peuvent satisfaire aux exigences pour une cible de sécurité.

2.29 Au Royaume Uni il est obligatoire de produire une politique de sécurité système ou SSP (System Security Policy) pour tous les systèmes qui traiteront des informations classifiées au niveau national. Si l'autorité qui donne son autorisation décide qu'une évaluation de la sécurité est nécessaire, une politique de sécurité de l'information dans les systèmes électroniques ou SEISP (System Electronic Information Security Policy) doit également être produite. Pour certains niveaux d'évaluation visés, un modèle de politique de sécurité ou SPM (Security Policy Model) doit aussi être produit. La SSP comprend une définition de l'étendue du système, les objectifs de sécurité du système, les mesures de sécurité à faire respecter et l'attribution des responsabilités pour les faire respecter (c'est à dire qu'elle correspond étroitement à la politique de sécurité du système telle que décrite dans les présents critères). Elle contient également un dérivé du niveau d'évaluation requis pour la cible, basé sur les caractéristiques clés du système et de son environnement. Si nécessaire, une SEISP est élaborée à partir de la SSP. Il s'agit d'une présentation plus détaillée des aspects matériels et logiciels de la SSP, mais encore en style informel : elle correspond à la politique de sécurité technique décrite dans les présents critères. Le SPM est une spécification parallèle des fonctions dédiées à la sécurité rédigée en style formel ou semi-formel. Il est élaboré lorsqu'une telle spécification parallèle est exigée pour le niveau d'évaluation visé.

2.30 Un "Claims Document" est une liste d'annonces concernant la fonctionnalité dédiée à la sécurité fournie par un produit, élaborée par le développeur du produit, et rédigée en style semi-formel utilisant le "Claims Language" défini dans l'annexe B du présent document. Il inclut les hypothèses et les contraintes concernant la manière dont le produit doit être utilisé pour que ces annonces soient valides. Il inclut également une identification des objectifs de sécurité, une spécification informelle des annonces, une correspondance entre les fonctions dédiées à la

sécurité annoncées et ces objectifs de sécurité, ainsi que le niveau d'évaluation désiré, afin de compléter une cible de sécurité de produit telle qu'exigée par les présents critères.

Rubriques génériques

2.31 Il sera plus facile de comprendre une cible de sécurité si la spécification de ses fonctions dédiées à la sécurité a été présentée dans un ordre logique. Cela aidera à comparer les cibles de sécurité et simplifiera le travail des évaluateurs. Il existe des regroupements naturels de fonctions dédiées à la sécurité qui donnent un tel ordre, et un ensemble recommandé de huit *rubriques génériques* pour un tel regroupement figure dans les présents critères.

2.32 Les rubriques recommandées sont les suivants :

Identification et authentification
Contrôle d'accès
Imputabilité
Audit
Réutilisation d'objet
Fidélité
Fiabilité de service
Echange de données

2.33 Il est recommandé d'utiliser ces rubriques standards chaque fois que possible. Leur utilisation simplifiera la comparaison avec d'autres cibles de sécurité et permettra de déterminer plus facilement si une cible de sécurité particulière inclut ou exclut des fonctions d'un certain type.

Identification et authentification

2.34 Pour beaucoup de TOE, il y aura des exigences pour la détermination et le contrôle des utilisateurs qui sont autorisés à avoir accès aux ressources contrôlées par la TOE. Cela implique non seulement d'établir l'identité annoncée par un utilisateur, mais aussi de vérifier que cet utilisateur est bien la personne qu'il prétend être. Pour ce faire, l'utilisateur fournira à la TOE une information que la TOE sait être associée à l'utilisateur en question.

2.35 Cette rubrique doit rassembler toutes les fonctions destinées à établir et vérifier une identité annoncée.

2.36 Cette rubrique doit inclure toutes les fonctions qui permettent d'ajouter de nouvelles identités et d'éliminer ou d'invalider d'anciennes identités. De même, elle doit inclure toutes les fonctions destinées à créer, modifier ou permettre à des utilisateurs autorisés de contrôler les informations d'authentification nécessaires pour vérifier l'identité d'utilisateurs particuliers. Elle doit aussi inclure des fonctions pour assurer l'intégrité des informations d'authentification ou prévenir leur usage non autorisé. Elle doit inclure toutes les fonctions destinées à limiter la possibilité d'essais répétés d'établissement d'une fausse identité.

Contrôle d'accès

2.37 Pour beaucoup de TOE, il y aura des exigences pour garantir que les utilisateurs et les processus qui agissent pour le compte de ceux-ci sont empêchés d'accéder aux informations et aux ressources auxquelles ils ne sont pas autorisés à accéder ou auxquelles ils n'ont pas besoin d'accéder. De même, il y aura des exigences concernant la création ou la modification (y compris la suppression) non autorisées d'informations.

2.38 Cette rubrique doit rassembler toutes les fonctions destinées à contrôler les flux d'informations entre les utilisateurs, les processus de traitement et les objets, ainsi que l'utilisation qu'ils font des ressources. Ceci inclut l'administration (c'est à dire l'octroi et le retrait) des droits d'accès et leur vérification.

2.39 Cette rubrique doit inclure les fonctions servant à établir et entretenir toutes les listes ou règles qui régissent les droits d'effectuer différents types d'accès. Elle doit inclure toutes les fonctions relatives aux restrictions temporaires d'accès à des objets simultanément accessibles par plusieurs utilisateurs ou processus, et nécessaires au maintien de la cohérence et de la fidélité de ces objets. Elle doit inclure toutes les fonctions destinées à assurer que, dès leur création, des listes d'accès par défaut ou des règles d'accès par défaut s'appliquent aux objets. Elle doit inclure toutes les fonctions destinées à contrôler la propagation des droits d'accès aux objets. Elle doit inclure également toutes les fonctions destinées à contrôler la déduction d'information par agrégation de données auxquelles on peut légitimement accéder d'une autre manière.

Imputabilité

2.40 Pour beaucoup de TOE, il y aura des exigences pour garantir l'enregistrement des informations pertinentes sur les actions soit d'un utilisateur, soit d'un processus agissant pour le compte de celui-ci, de façon que les conséquences de ces actions puissent être ultérieurement associées à l'utilisateur en question et qu'on puisse le tenir pour responsable.

2.41 Cette rubrique doit rassembler toutes les fonctions destinées à enregistrer l'exercice des droits qui se rapportent à la sécurité.

2.42 Cette rubrique doit inclure des fonctions relatives au recueil, à la protection et à l'analyse de telles informations. Certaines fonctions peuvent satisfaire à la fois aux exigences d'imputabilité et de capacité à être auditées et relever ainsi des deux rubriques. De telles fonctions peuvent être incluses dans l'une de ces deux rubriques, mais doivent être référencées dans l'autre.

Audit

2.43 Pour beaucoup de TOE, il y aura des exigences pour garantir que sont enregistrées suffisamment d'informations sur les événements, aussi bien courants qu'exceptionnels, pour qu'un examen ultérieur puisse déterminer s'il y a effectivement eu violation de la sécurité, et, dans ce cas, quelles informations ou autres ressources ont été compromises.

2.44 Cette rubrique doit rassembler toutes les fonctions destinées à déceler et à examiner les événements susceptibles de constituer une menace pour la sécurité.

2.45 Cette rubrique doit inclure des fonctions relatives au recueil, à la protection et à l'analyse de telles informations. Une telle analyse peut également inclure des analyses de tendance pour tenter de détecter des violations potentielles de la cible de sécurité avant que celles-ci ne se produisent. Certaines fonctions peuvent satisfaire à la fois aux exigences d'imputabilité et de capacité à être audité et relever ainsi des deux rubriques. De telles fonctions peuvent être incluses dans l'une de ces deux rubriques, mais doivent être référencées dans l'autre.

Réutilisation d'objet

2.46 Pour beaucoup de TOE, il y aura des exigences pour garantir que les ressources telles que la mémoire centrale ou des zones de stockage sur disque peuvent être réutilisées tout en préservant la sécurité.

2.47 Cette rubrique doit inclure toutes les fonctions destinées à contrôler la réutilisation des objets supports de données.

2.48 Cette rubrique doit inclure des fonctions destinées à initialiser les objets supports de données non alloués ou à effacer ceux qui sont réalloués. Elle doit inclure toutes les fonctions pour initialiser ou effacer les supports réutilisables tels que les bandes magnétiques, ou pour effacer les périphériques de sortie tels que les écrans de visualisation lorsqu'ils ne sont pas utilisés.

Fidélité

2.49 Pour beaucoup de TOE, il y aura des exigences pour garantir que les relations spécifiques entre les différentes données sont correctement maintenues et que les données sont échangées entre processus sans être altérées.

2.50 Cette rubrique doit rassembler toutes les fonctions destinées à garantir que des données n'ont pas été modifiées d'une manière non autorisée.

2.51 Cette rubrique doit inclure des fonctions pour déterminer, établir et maintenir la fidélité des relations entre les données qui sont liées. Elle doit aussi inclure des fonctions qui garantissent qu'il est possible, lorsque des données sont échangées entre processus, utilisateurs ou objets, de déceler ou d'empêcher toute perte, ajout ou modification, et qu'il est impossible de modifier la source et la destination, annoncées ou réelles, du transfert de données.

Fiabilité de service

2.52 Pour beaucoup de TOE, il y aura des exigences pour garantir que les tâches critiques en temps sont exécutées au moment voulu, ni plus tôt ni plus tard, et que les tâches non critiques en temps ne peuvent pas le devenir. De même, pour beaucoup de TOE il y aura des exigences pour garantir que l'accès aux ressources est possible quand on en a besoin, et que des ressources ne sont pas sollicitées ou conservées inutilement.

2.53 Cette rubrique doit inclure toutes les fonctions destinées à garantir que les ressources sont accessibles et utilisables à la demande d'une entité autorisée (c'est à dire un utilisateur ou un processus agissant en son nom) et à prévenir ou à limiter les interférences avec les opérations critiques en temps.

2.54 Cette rubrique doit inclure des fonctions de détection d'erreur et de reprise sur incident destinées à limiter les conséquences d'erreurs sur l'exploitation de la TOE, et ainsi à réduire au minimum l'interruption ou l'arrêt de service. Elle doit également inclure toutes les fonctions de séquencement qui assurent que la TOE répond aux événements externes et produit des résultats dans les délais limites spécifiés.

Echange de données

2.55 Pour beaucoup de TOE il y aura des exigences pour la sécurité des données pendant leur transmission à travers des canaux de communication. On parle généralement de sécurité des communications, car elles sont distinctes de la sécurité informatique.

2.56 Cette rubrique doit couvrir toutes les fonctions destinées à garantir la sécurité des données au cours de leur transmission sur des canaux de communication. Il est recommandé de découper de telles fonctions suivant les sous-rubriques tirées de l'architecture de sécurité OSI :

Authentification
Contrôle d'accès
Confidentialité des données
Intégrité des données
Non répudiation

2.57 Les fonctions doivent être regroupées sous ces sous-rubriques d'une manière cohérente avec leur utilisation et leur définition dans l'architecture de sécurité OSI [OSI].

2.58 Certaines fonctions peuvent satisfaire aux exigences à la fois de sécurité informatique et de sécurité des communications et ainsi relever d'autres rubriques. Dans ce cas, il doit y avoir une référence aux autres rubriques correspondantes.

Classes prédéfinies

2.59 Beaucoup de systèmes auront des objectifs de sécurité similaires ; il sera souvent possible d'identifier des ensembles communs de fonctions dédiées à la sécurité qui satisfont à ces objectifs. De même, beaucoup de produits de sécurité viseront à satisfaire le même besoin du marché et posséderont donc une fonctionnalité similaire. De telles *classes prédéfinies* de fonctions courantes peuvent être prises pour base de la cible de sécurité d'un système ou d'un produit particulier, ou peuvent servir de lignes directrices pour aider les utilisateurs à choisir la fonctionnalité de sécurité qui convient pour satisfaire à leurs objectifs de sécurité particuliers, et pour aider les constructeurs à choisir les fonctions à inclure dans leurs produits. Pour tirer le maximum de bénéfice de cet aspect commun, il est souhaitable que des normes existent pour des classes de fonctionnalité prédéfinies. Les présents critères ont donc été conçus pour autoriser dans les cibles de sécurité la référence à des classes prédéfinies de fonctions dédiées à la sécurité. Toute cible de sécurité peut faire référence à une ou plusieurs classes prédéfinies pour définir tout ou partie de ses fonctions dédiées à la sécurité.

2.60 Les organismes de normalisation ou ceux qui représentent des secteurs de marché particuliers ont déjà élaboré de telles définitions normalisées. On s'attend à ce que la mise à disposition des présents critères encourage le développement de classes prédéfinies, sous une forme compatible avec les présents critères. Toutefois, puisque la sécurité des TI va continuer à évoluer rapidement, il sera nécessaire de

définir dans l'avenir de nouvelles classes prédéfinies dès que de nouveaux groupes de fonctions deviendront suffisamment courants pour que de telles classes deviennent intéressantes.

2.61 En même temps que la spécification de ses fonctions de sécurité, chaque classe prédéfinie doit indiquer les objectifs de la classe, en fonction de son utilisation prévue, et les raisons du choix des fonctions particulières qu'elle comporte. Les classes prédéfinies peuvent comprendre également d'autres informations qu'il est nécessaire d'inclure dans une cible de sécurité, telles que le détail de tous les mécanismes obligatoires pour une classe. Dans le cas où les détails du contenu de telles classes sont publiés, il n'est pas nécessaire de les répéter dans chaque cible de sécurité qui y fait référence.

2.62 L'utilisation de classes prédéfinies n'est pas obligatoire. Il y aura des cas où le commanditaire de l'évaluation souhaitera ne pas les employer, d'autres où il ne le pourra pas, par exemple lorsqu'aucune classe prédéfinie ne décrit les caractéristiques de sécurité qu'il souhaite. Au lieu d'utiliser des classes prédéfinies, il est toujours possible de spécifier individuellement chaque fonction dédiée à la sécurité. Une déclaration de fonctions de sécurité individuelles peut être couplée avec une ou plusieurs classes prédéfinies qui décrivent partiellement, mais non complètement, la cible de sécurité. Toutefois, une classe prédéfinie ne doit être spécifiée comme faisant partie de la cible de sécurité que si tous les aspects de cette classe entrent dans la cible de sécurité.

2.63 Dix exemples de classes prédéfinies sont données en annexe A. Elles sont toutes dérivées des classes de fonctionnalité données dans [ZSIEC]. Elles sont toutes présentées en style informel, et en version provisoire dans la version actuelle de l'ITSEC :

a) Les exemples de classes de fonctionnalité F-C1,F-C2, F-B1, F-B2 et F-B3 sont les classes de confidentialité ordonnées hiérarchiquement qui correspondent étroitement aux exigences de fonctionnalité des classes C1 à A1 du TCSEC [TCSEC].

b) L'exemple de classe de fonctionnalité F-IN concerne les TOE pour lesquelles il y a des exigences élevées d'intégrité pour les données et les programmes. De telles exigences peuvent être nécessaires par exemple pour des TOE bases de données.

c) L'exemple de classe de fonctionnalité F-AV impose des exigences élevées pour la disponibilité d'une TOE complète ou de fonctions spéciales d'une TOE. De telles exigences sont importantes par exemple pour des TOE qui contrôlent des processus industriels.

d) L'exemple de classe de fonctionnalité F-DI impose des exigences élevées en ce qui concerne la préservation de l'intégrité des données au cours de leur transmission.

e) L'exemple de classe de fonctionnalité F-DC est destinée aux TOE très exigeantes en matière de confidentialité des données au cours de leur transmission. Un dispositif cryptographique est par exemple un candidat pour cette classe.

f) L'exemple de classe de fonctionnalité F-DX est destinée aux réseaux très exigeants en matière de confidentialité et d'intégrité des informations à transmettre. Par exemple, cela peut être le cas lorsque des informations sensibles doivent être transmises à travers des réseaux non protégés (par exemple des réseaux publics).

2.64 Il n'existe pas de restriction concernant la fonctionnalité spécifique qui peut être annoncée ou exigée pour une cible de sécurité. Les fonctions dédiées à la sécurité de toute cible de sécurité peuvent donc être entièrement décrites au moyen des formats de spécification disponibles. L'existence de classes prédéfinies ne restreindra donc nullement les fabricants de produits qui cherchent à faire progresser l'état de l'art, mais elle diminuera le travail qu'implique la spécification de produits ou de systèmes analogues aux stéréotypes décrits, et fournira une base de comparaison de la fonctionnalité offerte. Les cibles de sécurité de produit peuvent, même lorsqu'elles revendiquent la conformité à une classe prédéfinie, spécifier des contraintes additionnelles et des détails quant à l'environnement requis pour aider les utilisateurs potentiels à déterminer si le produit pourrait convenir à leur environnement réel.

Style de spécification

2.65 Les présents critères n'imposent pas l'emploi de méthodes ou de styles particuliers, qu'ils soient privés ou normalisés, pour la spécification des fonctions de sécurité. Ils n'excluent aucune méthode ni aucun style, dans la mesure où les exigences concernant la présentation et les éléments de preuve pour le niveau d'évaluation visé sont satisfaits. Dans le but d'établir des catégories entre les approches possibles de la spécification, trois types de styles ont été identifiés dans le cadre des présents critères : informel, semi-formel et formel. Chacun de ces types est décrit de façon plus approfondie ci-dessous.

2.66 Ceux qui auront besoin d'utiliser une cible de sécurité ne seront pas tous familiarisés avec des spécifications rédigées en style semi-formel ou formel. Aussi toutes les cibles de sécurité doivent contenir une spécification des fonctions dédiées

à la sécurité rédigée en style informel. Bien que les spécifications informelles ne demandent pas une formation spéciale pour être comprises, elles sont sujettes à ambiguïté et à imprécision. Les spécifications en style semi-formel ou formel réduisent cette possibilité d'ambiguïté et d'imprécision. Aussi, pour les niveaux supérieurs d'évaluation, la spécification informelle des fonctions dédiées à la sécurité doit être appuyée par une spécification parallèle semi-formelle ou formelle.

2.67 La technique ou le style de spécification utilisé dans une cible de sécurité pour définir les objectifs de sécurité, et pour définir tout mécanisme de sécurité imposé ou annoncé, est hors du champ d'application des présents critères.

2.68 S'il est exigé qu'une cible de sécurité contienne une spécification des fonctions dédiées à la sécurité dans un style particulier, cette spécification peut être totalement ou partiellement remplacée par une référence à une ou plusieurs classes prédéfinies rédigées dans ce style.

2.69 Chaque fois qu'une spécification est exigée, quelqu'en soit le style, elle peut se présenter sous forme d'un ou de plusieurs documents. Lorsqu'on utilise plusieurs documents, leurs relations doivent être clairement indiquées.

Spécification informelle

2.70 Une spécification informelle est rédigée en langage naturel, plutôt qu'avec une notation exigeant des restrictions ou des conventions particulières. Le terme langage naturel désigne le moyen de communication que constitue toute langue parlée courante (par exemple l'allemand, l'anglais, le français ou le néerlandais). Des spécifications rédigées en langage naturel ne sont soumises à aucune restriction particulière mais doivent se conformer aux conventions usuelles de cette langue (par exemple la grammaire et la syntaxe).

2.71 Une spécification en langage naturel doit être rédigée avec le souci de minimiser l'ambiguïté, en s'assurant (c'est un minimum) que tous les termes sont utilisés de façon cohérente, et que tout terme ayant une signification particulière (une signification non définie dans un dictionnaire largement utilisé) est défini dans un ou plusieurs glossaires, inclus ou auquel il est fait référence. Il est peu probable que toute ambiguïté puisse être complètement éliminée. L'évaluation cherchera à identifier et à lever toutes les ambiguïtés restantes.

Spécification semi-formelle

2.72 Une spécification en style semi-formel exige l'emploi d'une ou plusieurs notations restreintes, conformément à un ensemble de conventions incluses dans la

spécification ou auxquelles il est fait référence. Les conventions sont spécifiées de façon informelle. Une telle notation doit permettre de spécifier les effets d'une fonction ainsi que les conditions d'exception ou d'erreur associées à cette fonction.

2.73 Un style semi-formel peut être soit présenté sous forme graphique soit basé sur un usage restreint du langage naturel (par exemple, une structure de phrase restreinte et des mots-clé ayant une signification particulière). On peut prendre comme exemples de style semi-formel les diagrammes de flux de données, les diagrammes de transition d'états, les diagrammes entité-association, les diagrammes de structure de données, les diagrammes décrivant la structure de processus ou de programme, et la notation SDL recommandée par le CCITT pour les spécifications.

2.74 Les méthodes de conception structurée et de développement utilisent généralement au moins l'une de ces notations semi-formelles pour l'expression des spécifications, ainsi que des guides méthodologiques (par exemple, des mesures de complexité et des méthodes de gestion de projet) concernant l'utilisation de la notation. A titre d'exemples de méthodes de conception structurée incluant de telles notations on peut citer : la méthode structurée de Yourdon [YSM], la technique d'analyse et de conception structurées [SADT], la méthode d'analyse et de conception structurées de systèmes [SSADM], ainsi que les méthodes Jackson de conception structurée [JSD] et de programmation structurée [JSP].

2.75 Un exemple particulier de notation semi-formelle qui a été utilisé avec succès pour définir des cibles de sécurité est le Claims Language. Le Claims Language est un sous-ensemble de l'anglais : son vocabulaire et la forme syntaxique de ses phrases sont tous deux soumis à des restrictions. Il a été conçu (comme son nom l'indique) pour fournir un moyen structuré de faire des annonces concernant les caractéristiques de sécurité de produits TI. Il permet d'utiliser le langage naturel pour exprimer les parties de la définition d'une cible de sécurité qui concernent les fonctions dédiées à la sécurité annoncées. On peut trouver une définition complète, cohérente avec les présents critères, du Claims Language en annexe B.

Spécification formelle

2.76 Une spécification en style formel est rédigée avec une notation formelle basée sur des concepts mathématiques bien établis. Les concepts sont utilisés pour définir la syntaxe et la sémantique de la notation, ainsi que les règles de déduction qui soutiennent le raisonnement logique. On doit pouvoir montrer que des spécifications formelles sont construites à partir d'un ensemble d'axiomes déclarés, et ces spécifications doivent pouvoir montrer la validité de propriétés clés, telles que la production d'une sortie valide pour toutes les entrées possibles. Lorsqu'il existe une hiérarchie de niveaux de spécification, il doit être possible de démontrer que chaque niveau maintient les propriétés établies pour le niveau précédent.

2.77 Les règles syntaxiques et sémantiques qui sous-tendent une notation formelle utilisée dans une cible de sécurité doivent définir comment reconnaître sans ambiguïté des constructions et déterminer leur signification. Lorsque des règles de déduction sont utilisées pour soutenir le raisonnement logique, il doit être prouvé qu'il est impossible d'en déduire des contradictions. Toutes les règles qui sous-tendent la notation doivent être définies ou mises en référence. Toutes les constructions utilisées dans une spécification formelle doivent être complètement définies à l'aide de ces règles. La notation formelle doit permettre de spécifier l'effet d'une fonction ainsi que toutes les conditions d'exception ou d'erreur associées à cette fonction.

2.78 Parmi les exemples de notation formelle on peut citer VDM, décrit dans [SSVDM], Z, décrit dans [ZRM], le langage de spécification RAISE, décrit dans [RSL], Ina Jo, décrit dans [IJRM], le langage de spécification Gypsy, décrit dans [GYPSY], et le langage de spécification de protocoles de l'ISO [LOTOS]. L'utilisation de constructions à base de logique des prédicats (ou d'autre logique) et de la théorie des ensembles en tant que notation formelle est acceptable, pourvu que les conventions (règles de démonstration) soient documentées ou mises en référence (comme exposé plus haut).

Cohérence entre des spécifications parallèles en styles différents

2.79 Les spécifications parallèles doivent être présentées de telle manière que les relations entre ces spécifications soient claires, et que lorsque ces spécifications concernent le même point, ce point soit traité de façon cohérente. Des spécifications parallèles peuvent faire l'objet de documents séparés ou être imbriquées dans un document unique.

2.80 Quand il existe une ambiguïté dans une spécification informelle, la spécification formelle ou semi-formelle associée doit lever l'ambiguïté. Néanmoins des spécifications parallèles incohérentes entre elles doivent être considérées comme erronées. On doit corriger ce type d'erreur en faisant référence à des informations complémentaires extérieures à la cible de sécurité et on doit modifier l'une des spécifications ou les deux.

Modèles formels de politique de sécurité

2.81 Au niveau d'évaluation E4 et au dessus, une TOE doit implémenter un modèle sous-jacent de politique de sécurité, c'est à dire qu'il doit y avoir une présentation abstraite des principes de sécurité importants que la TOE doit faire respecter. Cette présentation doit être rédigée dans un style formel, et constitue un **modèle formel de politique de sécurité**. Tout ou partie d'un modèle pertinent déjà publié peut être

mis en référence, sinon un modèle doit être fourni comme partie intégrante de la cible de sécurité. Tous les styles formels de spécification identifiés ci-dessus peuvent être utilisés pour définir un tel modèle.

2.82 Il n'est pas nécessaire que le modèle formel couvre toutes les fonctions dédiées à la sécurité spécifiées dans la cible de sécurité. Toutefois, une interprétation informelle du modèle sous l'angle de la cible de sécurité doit être fournie, et doit montrer que la cible de sécurité implémente la politique de sécurité sous-jacente et ne contient aucune fonction en contradiction avec cette politique sous-jacente.

2.83 Voici des exemples de modèles formels de politique de sécurité qui ont été publiés :

a) Le modèle de Bell-La Padula [BLP] qui modélise les exigences de contrôle d'accès caractéristiques d'une politique nationale de sécurité pour la confidentialité.

b) Le modèle de Clark et Wilson [CWM] qui modélise les exigences d'intégrité des systèmes transactionnels commerciaux.

c) Le modèle de Brewer-Nash [BNM] qui modélise les exigences de contrôle d'accès visant à assurer la confidentialité pour le client, ce qui est typique d'un organisme de services financiers.

d) Le modèle d'Eizenberg [EZBM] qui modélise des droits d'accès qui varient avec le temps.

e) Le modèle de Landwehr [LWM] qui modélise les exigences d'un réseau de traitement de messages en matière d'échange de données.

3 ASSURANCE - EFFICACITE

Introduction

3.1 Le présent chapitre présente les critères d'évaluation qui traitent de l'aspect efficacité de l'assurance pour une cible d'évaluation (TOE). La base de l'évaluation est la cible de sécurité telle qu'elle est définie au chapitre 2, qui est évaluée en même temps pour l'efficacité, selon les critères exposés dans le présent chapitre, et pour la conformité, selon les critères exposés au chapitre 4 qui lui succède.

Description de l'approche

3.2 L'estimation de l'efficacité prend en compte les aspects suivants de la TOE :

a) la pertinence des fonctions de la TOE dédiées à la sécurité pour contrer les menaces contre la sécurité de la TOE identifiées dans la cible de sécurité ;

b) la capacité des fonctions et des mécanismes de la TOE dédiés à la sécurité à se lier et à coopérer pour former un ensemble intégré et efficace ;

c) la capacité des mécanismes de sécurité de la TOE à résister à une attaque directe ;

d) si des vulnérabilités connues dans la *construction* de la TOE pourraient en pratique compromettre la sécurité de la TOE ;

e) que la TOE ne peut pas être configurée ou utilisée d'une manière qui n'est pas sûre, mais qu'un **administrateur** ou un utilisateur final pourrait raisonnablement croire sûre ;

f) si des vulnérabilités connues dans l'*exploitation* de la TOE pourraient en pratique compromettre la sécurité de la TOE.

3.3 L'estimation de chacun des aspects de l'efficacité identifiés ci-dessus est effectuée en utilisant la documentation fournie par le commanditaire ainsi que la documentation et les résultats provenant de l'évaluation de la conformité de la TOE. Cela signifie que, bien que l'évaluation de l'efficacité puisse se dérouler en parallèle avec l'estimation de la conformité, elle ne peut se terminer avant que les résultats finals de l'estimation de la conformité ne soient disponibles.

3.4 Pour être précis, l'estimation de l'efficacité est basée sur une analyse des vulnérabilités de la TOE. Cette analyse a pour objectif de rechercher tous les moyens possibles pour un utilisateur de la TOE de désactiver, de court-circuiter, d'altérer, de contourner, d'attaquer directement, ou de mettre autrement en échec les fonctions et les mécanismes de la TOE dédiés à la sécurité. Au minimum, l'analyse de vulnérabilité du commanditaire doit prendre en compte toutes les informations spécifiées dans la figure 4 pour le niveau d'évaluation en question (c'est à dire qu'il faut effectuer une recherche des vulnérabilités en utilisant une partie de l'ensemble de la documentation fournie par le commanditaire pour le niveau d'évaluation considéré). Quand le niveau d'évaluation augmente, les critères de conformité du chapitre 4 exigent que les informations spécifiées dans la figure 4 soient fournies avec un niveau croissant de rigueur, comme l'indique l'emploi des verbes *présenter*, *décrire* et *expliquer*.

3.5 Tous les mécanismes de sécurité critiques (c'est à dire les mécanismes dont la mise en défaut pourrait créer une faiblesse dans la sécurité), sont estimés quant à leur capacité à résister à une attaque directe. La résistance minimum de chaque **mécanisme critique** doit être cotée comme étant *élémentaire*, *moyenne* ou *élevée*.

3.6 Pour que la résistance minimum d'un mécanisme critique soit cotée élémentaire, il doit être manifeste qu'il fournit une protection contre une subversion accidentelle aléatoire, bien qu'il soit susceptible d'être mis en échec par des agresseurs compétents.

3.7 Pour que la résistance minimum d'un mécanisme critique soit cotée moyenne, il doit être manifeste qu'il fournit une protection contre des agresseurs dont les opportunités ou les ressources sont limitées.

3.8 Pour que la résistance minimum d'un mécanisme critique soit cotée élevée, il doit être manifeste qu'il ne pourra être mis en échec que par des agresseurs disposant d'un haut degré d'expertise, d'opportunité et de ressources, le succès d'une attaque étant jugé de nature exceptionnelle.

3.9 Une TOE n'échouera dans l'évaluation pour ce qui concerne l'efficacité que si une vulnérabilité exploitable, découverte pendant l'évaluation de l'efficacité, n'a pas été éliminée avant la fin de l'évaluation. Cela comprend des méthodes d'attaque directe ayant réussi, décelées pendant l'estimation de la résistance minimum des mécanismes, qui invalideraient la cotation annoncée. Si une telle vulnérabilité existe, la TOE se verra décerner le niveau global d'évaluation E0, indiquant qu'elle ne convient pas à l'emploi proposé.

3.10 L'efficacité de la TOE est toujours estimée dans le contexte de la cible de sécurité donnée. Par exemple, un produit de sécurité vendu pour être incorporé dans des

systèmes peut contenir des **canaux cachés** connus. Pourtant, si la cible de sécurité du système n'a pas d'exigence de contrôle d'accès pour la confidentialité, la présence de canaux cachés dans le produit n'est pas à prendre en compte et n'affectera pas la capacité de la TOE à satisfaire à sa cible de sécurité, et ne provoquera pas l'échec de l'évaluation. Pour des systèmes présentant des exigences de contrôle d'accès pour la confidentialité, la cible de sécurité du système peut spécifier les bandes passantes maximum admissibles des canaux cachés. Si des canaux cachés dépassant ces bandes passantes sont identifiés, ou si aucune bande passante n'est réellement spécifiée, l'évaluateur doit déterminer si les canaux cachés identifiés font échouer l'évaluation de la TOE sur la base d'une fonctionnalité non pertinente.

Systèmes et produits

3.11 Les exigences et options concernant le contenu de la cible de sécurité d'une TOE sont différentes, selon que la TOE est évaluée comme un système ou comme un produit. Ces différences sont exposées au chapitre 4 - Construction - Phase 1 - Spécifications des besoins, et expliquées plus en détail au chapitre 2.

Critères d'efficacité - Construction

Documentation

3.12 Le commanditaire doit fournir la documentation suivante en complément de celle qui est exigée pour l'évaluation de la conformité :

analyse de pertinence,
analyse de cohésion,
analyse de la résistance des mécanismes,
liste des vulnérabilités connues dans la construction.

Aspect 1 - Pertinence de la fonctionnalité

Définition

3.13 Dans le cadre de la documentation exigée pour l'évaluation de la conformité, le commanditaire fournira une cible de sécurité. Au cours de l'estimation de la conformité, cette cible est examinée sous l'angle de la couverture et de la cohérence. En ce qui concerne cet aspect de l'efficacité, la cible de sécurité est utilisée pour déterminer si les fonctions et les mécanismes dédiés à la sécurité

contreront effectivement les menaces pour la sécurité de la TOE identifiées dans la cible de sécurité.

Exigences concernant le contenu et la présentation

3.14 L'analyse de la pertinence doit établir un lien entre les fonctions et mécanismes dédiés à la sécurité et les menaces énumérées dans la cible de sécurité, que leur conception vise à contrer.

Exigences concernant les éléments de preuve

3.15 L'analyse de la pertinence doit montrer comment les menaces sont contrées par les fonctions et les mécanismes dédiés à la sécurité. Elle doit montrer qu'il n'existe aucune menace qui ne soit convenablement contrée par une ou plusieurs des fonctions dédiées à la sécurité qui sont déclarées. L'analyse doit être conduite en utilisant, au minimum, toutes les informations données dans la figure 4 pour le niveau d'évaluation considéré.

Tâches de l'évaluateur

3.16 Vérifier que l'analyse de pertinence fournie satisfait à toutes les exigences concernant le contenu et la présentation ainsi qu'à celles concernant les éléments de preuve. Vérifier que l'analyse a pris en compte toutes les informations données dans la figure 4 pour le niveau considéré.

Aspect 2 - Cohésion de la fonctionnalité

Définition

3.17 Cet aspect de l'efficacité examine la capacité des fonctions et mécanismes dédiés à la sécurité à coopérer pour former un ensemble intégré et efficace.

Exigences concernant le contenu et la présentation

3.18 L'analyse de cohésion doit fournir une analyse de toutes les relations potentielles entre les fonctions et mécanismes dédiés à la sécurité.

Exigences concernant les éléments de preuve

3.19 L'analyse de cohésion doit montrer qu'il est impossible d'amener l'une des fonctions ou l'un des mécanismes dédiés à la sécurité à rentrer en conflit ou à se mettre en contradiction avec d'autres fonctions ou mécanismes dédiés à la sécurité. L'analyse

doit être conduite en utilisant, au minimum, toutes les informations données dans la figure 4 pour le niveau considéré.

Tâches de l'évaluateur

3.20 Vérifier que l'analyse de cohésion fournie satisfait à toutes les exigences concernant le contenu et la présentation ainsi qu'à celles concernant les éléments de preuve. Vérifier que l'analyse a pris en compte toutes les informations données dans la figure 4 pour le niveau considéré.

Aspect 3 - Résistance des mécanismes

Définition

3.21 Même si un mécanisme dédié à la sécurité ne peut pas être court-circuité, désactivé, altéré ou contourné, il peut encore être possible de le mettre en échec par une attaque directe tirant profit d'insuffisances dans ses algorithmes, ses principes ou ses propriétés sous-jacents. Pour cet aspect de l'efficacité la capacité de ces mécanismes à contenir une telle attaque directe est estimée. Cet aspect de l'efficacité se distingue des autres en ce qu'il exige de prendre en considération le niveau des ressources qui seraient nécessaires à un agresseur pour réussir une attaque directe.

Exigences concernant le contenu et la présentation

3.22 L'analyse de la résistance des mécanismes doit énumérer tous les mécanismes dédiés à la sécurité de la TOE qui ont été identifiés comme étant critiques. Elle doit inclure une analyse des algorithmes, des principes ou des propriétés sous-jacents de ces mécanismes, ou y faire référence.

Exigences concernant les éléments de preuve

3.23 L'analyse de la résistance des mécanismes doit montrer que tous les mécanismes critiques satisfont à la cotation annoncée de la résistance minimum des mécanismes, telle qu'elle est définie aux paragraphes 3.6 à 3.8 : dans le cas de mécanismes cryptographiques, ceci doit prendre la forme d'une déclaration de confirmation par l'organisme national approprié. D'autres analyses doivent être conduites en utilisant, au minimum, toutes les informations données dans la figure 4 pour le niveau considéré.

Tâches de l'évaluateur

3.24 Vérifier que tous les mécanismes critiques ont bien été identifiés comme tels. Vérifier que l'analyse fournie pour la résistance des mécanismes satisfait à toutes les exigences concernant le contenu et la présentation ainsi qu'à celles concernant les éléments de preuve. Vérifier que l'analyse a pris en compte toutes les informations données dans la figure 4 pour le niveau considéré. Vérifier que les spécifications ou les définitions de tous les mécanismes critiques correspondent à la cotation annoncée de la résistance minimum. Effectuer des **tests de pénétration** là où c'est nécessaire pour confirmer ou infirmer la résistance minimum des mécanismes annoncée.

Aspect 4 - Estimation de la vulnérabilité de la construction

Définition

3.25 Avant et pendant l'étude des autres aspects de l'évaluation de la TOE, diverses vulnérabilités dans la construction de la TOE (tels que des moyens de désactiver, court-circuiter, altérer ou contourner des fonctions et mécanismes dédiés à la sécurité) auront été identifiées par le commanditaire et par l'évaluateur. Pour cet aspect de l'efficacité, ces vulnérabilités connues sont estimées pour déterminer si elles peuvent dans la pratique compromettre la sécurité de la TOE telle qu'elle est spécifiée dans la cible de sécurité.

Exigences concernant le contenu et la présentation

3.26 La liste des vulnérabilités connues fournie par le commanditaire doit identifier toutes les vulnérabilités dans la construction de la TOE, dont il a connaissance. Elle doit identifier chaque vulnérabilité connue, fournir une analyse de son impact potentiel et identifier les mesures proposées ou fournies pour parer ses conséquences.

Exigences concernant les éléments de preuve

3.27 L'analyse de l'impact potentiel de chacune des vulnérabilités connues doit montrer que la vulnérabilité en question ne peut pas être exploitée dans l'environnement prévu pour la TOE, parce que :

- la vulnérabilité est convenablement couverte par d'autres mécanismes de sécurité non compromis, ou

- il peut être montré que la vulnérabilité ne relève pas de la cible de sécurité, qu'elle n'existera pas dans la pratique, ou qu'elle pourra être convenablement contrée par des mesures de sécurité techniques, relatives au personnel, organisationnelles ou physiques, documentées, et extérieures à la TOE. Ces mesures de sécurité externes doivent avoir été définies dans la documentation appropriée (ou doivent lui avoir été ajoutées).

L'analyse doit être conduite en utilisant, au minimum, toutes les informations données dans la figure 4 pour le niveau considéré.

Tâches de l'évaluateur

3.28 Vérifier que la liste des vulnérabilités dans la construction qui sont connues satisfait à toutes les exigences indiquées ci-dessus concernant le contenu et la présentation ainsi qu'à celles concernant les éléments de preuve. Vérifier que l'analyse de l'impact potentiel de chacune des vulnérabilités a pris en compte toutes les informations données dans la figure 4 pour le niveau considéré. Effectuer une analyse indépendante de vulnérabilité, en prenant en compte à la fois les vulnérabilités de construction énumérées et toute autre découverte pendant l'évaluation. Vérifier que toutes les combinaisons de vulnérabilités connues ont été prises en compte. Vérifier que les analyses d'impact potentiel des vulnérabilités ne contiennent pas d'hypothèses non documentées ou déraisonnables concernant l'environnement prévu. Vérifier que toutes les hypothèses et toutes les exigences concernant des mesures de sécurité externes ont été convenablement documentées. Effectuer des tests de pénétration pour confirmer ou infirmer que les vulnérabilités connues sont réellement exploitables en pratique.

Critères d'efficacité - Exploitation

Documentation

3.29 Le commanditaire doit fournir la documentation suivante en complément de celle qui est exigée pour l'évaluation de la conformité :

analyse de la facilité d'emploi,
liste des vulnérabilités en exploitation connues.

Aspect 1 - Facilité d'emploi

Définition

3.30 Cet aspect de l'efficacité examine si la TOE peut être configurée ou utilisée d'une manière qui n'est pas sûre, mais qu'un administrateur ou un utilisateur final pourrait raisonnablement croire sûre.

Exigences concernant le contenu et la présentation

3.31 L'analyse de la facilité d'emploi doit identifier les modes d'exploitation possibles de la TOE, y compris l'exploitation à la suite d'une panne ou d'une erreur d'exploitation, leurs conséquences et leurs implications sur le maintien de l'exploitation sûre.

Exigences concernant les éléments de preuve

3.32 L'analyse de la facilité d'emploi doit montrer que toute erreur humaine ou autre dans l'exploitation, qui désactive ou rend inopérantes des fonctions ou des mécanismes dédiés à la sécurité, sera facilement détectable. Elle doit montrer que, dans le cas où il est possible de configurer la TOE ou de faire en sorte qu'elle puisse être exploitée de façon non sûre (c'est à dire que les fonctions et les mécanismes dédiés à la sécurité ne satisfont pas à la cible de sécurité), alors qu'un utilisateur final ou un administrateur pourraient raisonnablement la croire sûre, alors cet état de fait sera également détectable. L'analyse doit être conduite en utilisant, au minimum, toutes les informations données dans la figure 4 pour le niveau considéré.

Tâches de l'évaluateur

3.33 Vérifier que l'analyse de la facilité d'emploi fournie satisfait à toutes les exigences concernant le contenu et la présentation ainsi qu'à celles concernant les éléments de preuve. Vérifier que l'analyse a pris en compte toutes les informations données dans la figure 4 pour le niveau considéré. Vérifier que l'analyse ne contient pas d'hypothèses non documentées ou déraisonnables concernant l'environnement prévu. Vérifier que toutes les hypothèses et exigences concernant des mesures de sécurité externes (telles que des contrôles externes organisationnels, physiques ou relatifs au personnel) ont été convenablement documentées. Exécuter à nouveau toutes les procédures de configuration et d'installation pour vérifier que la TOE peut être configurée et utilisée de façon sûre, en n'utilisant comme guide que la documentation de l'utilisateur et la documentation de l'administrateur. Effectuer d'autres tests quand c'est nécessaire pour confirmer ou infirmer l'analyse de la facilité d'emploi.

Aspect 2 - Estimation de la vulnérabilité en exploitation

Définition

3.34 Avant et pendant l'étude des autres aspects de l'évaluation de la TOE, diverses vulnérabilités dans l'exploitation de la TOE auront été identifiées par le commanditaire et par l'évaluateur. Pour cet aspect de l'efficacité ces vulnérabilités connues sont estimées pour déterminer si elles pourraient dans la pratique compromettre la sécurité de la TOE telle qu'elle est spécifiée dans la cible de sécurité.

Exigences concernant le contenu et la présentation

3.35 La liste des vulnérabilités connues fournie par le commanditaire doit identifier toutes les vulnérabilités dont il a connaissance dans l'exploitation de la TOE. Elle doit identifier chaque vulnérabilité connue, fournir une analyse de son impact potentiel, et identifier les mesures proposées ou fournies pour en parer les conséquences.

Exigences concernant les éléments de preuve

3.36 L'analyse de l'impact potentiel de chacune des vulnérabilités connues doit montrer que la vulnérabilité en question ne peut pas être exploitée dans l'environnement prévu pour la TOE, parce que :

- la vulnérabilité est convenablement couverte par d'autres mécanismes externes de sécurité non compromis, ou

- il peut être montré que la vulnérabilité ne relève pas de la cible de sécurité ou ne sera pas exploitable en pratique.

L'analyse doit être conduite en utilisant, au minimum, toutes les informations données dans la figure 4 pour le niveau considéré. Toutes les mesures de sécurité externes requises doivent avoir été définies dans la documentation appropriée (ou doivent lui avoir été ajoutées).

Tâches de l'évaluateur

3.37 Vérifier que la liste des vulnérabilités en exploitation qui sont connues satisfait à toutes les exigences indiquées ci-dessus concernant le contenu et la présentation ainsi qu'à celles concernant les éléments de preuve. Vérifier que l'analyse de l'impact potentiel de chacune des vulnérabilités a pris en compte toutes les informations dans la figure 4 pour le niveau considéré. Effectuer une analyse de

vulnérabilité indépendante, en prenant en compte à la fois les vulnérabilités en exploitation énumérées et toute autre découverte pendant l'évaluation. Vérifier que toutes les combinaisons de vulnérabilités connues ont été prises en compte. Vérifier que l'analyse d'impact potentiel des vulnérabilités ne contient pas d'hypothèses non documentées ou déraisonnables concernant l'environnement prévu. Vérifier que toutes les hypothèses et toutes les exigences concernant des mesures de sécurité externes ont été convenablement documentées. Effectuer des tests de pénétration pour confirmer ou infirmer que les vulnérabilités connues sont réellement exploitables en pratique.

INFORMATIONS OBTENUES D'UNE ESTIMATION DE LA CONFORMITE UTILISEES POUR EFFECTUER UNE ANALYSE DE VULNERABILITE

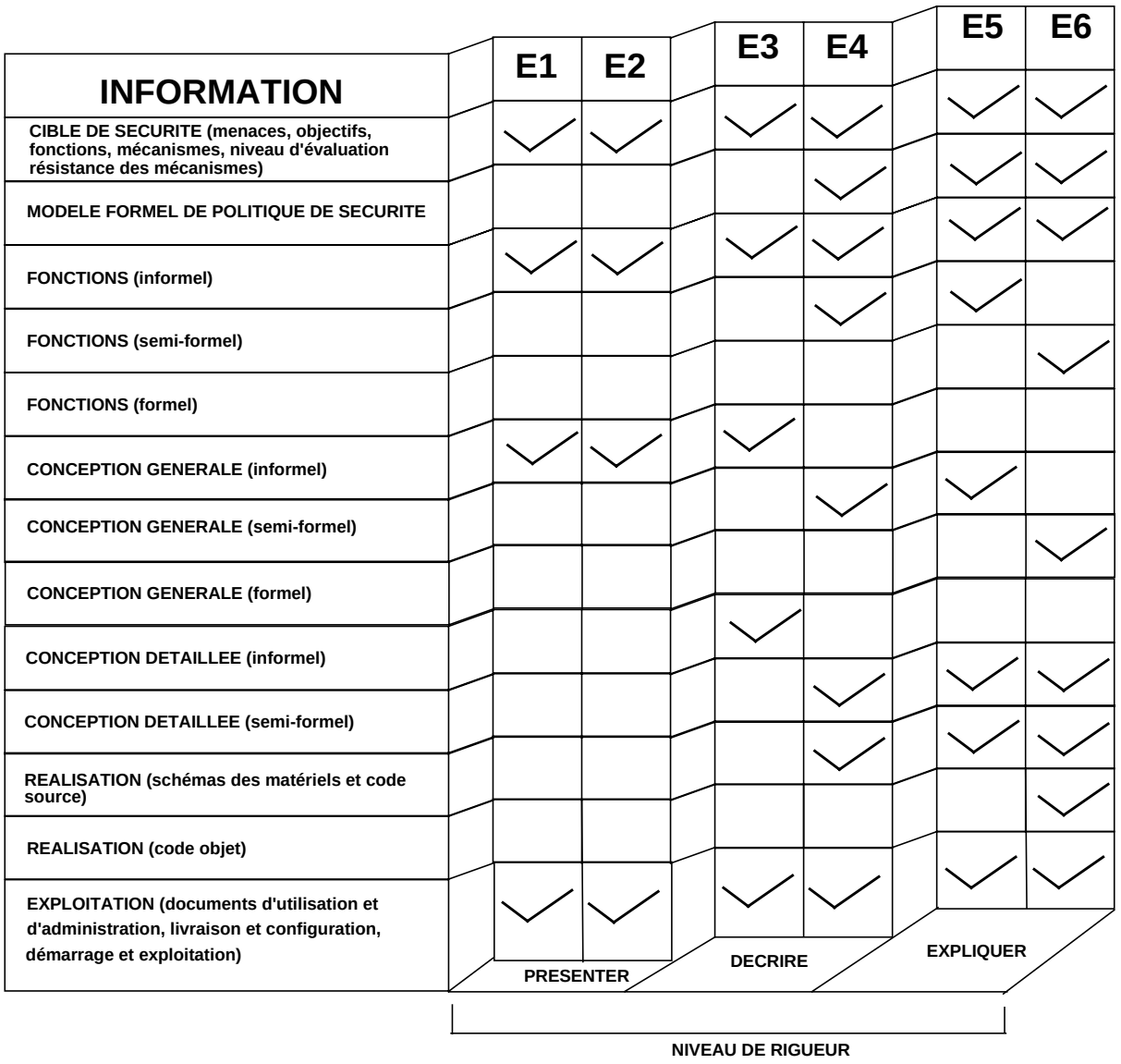


Fig. 4 Informations utilisées dans une analyse de vulnérabilité

4 ASSURANCE - CONFORMITE

Introduction

4.1 Le présent chapitre expose les critères d'évaluation qui traitent de l'aspect conformité de l'assurance pour une cible d'évaluation (TOE). La base d'évaluation est constituée par une cible de sécurité définie conformément au chapitre 2. La cible de sécurité doit contenir les éléments nécessaires spécifiés au chapitre 2 pour un système ou un produit, selon le cas. Elle doit comporter le niveau d'évaluation visé ainsi que la cotation annoncée de la résistance minimum des mécanismes. L'aspect efficacité de l'assurance est couvert par les critères décrits au chapitre 3.

Caractérisation

4.2 Il est défini sept niveaux d'évaluation correspondant à des degrés de confiance dans la conformité d'une TOE. E0 désigne le niveau le plus bas et E6 le plus haut.

4.3 Les sept niveaux d'évaluation peuvent être *caractérisés* comme suit :

Niveau E0

4.4 Ce niveau représente une assurance insuffisante.

Niveau E1

4.5 A ce niveau, il doit exister une cible de sécurité et une description informelle de la conception générale de la TOE. Les tests fonctionnels doivent indiquer que la TOE satisfait à sa cible de sécurité.

Niveau E2

4.6 Outre les exigences du niveau E1, il doit exister une description informelle de la conception détaillée. Les éléments de preuve des tests fonctionnels doivent être évalués. Il doit exister un système de gestion de configuration et un processus approuvé de diffusion.

Niveau E3

4.7 En plus des exigences du niveau E2, le code source et/ou les schémas descriptifs des matériels correspondants aux mécanismes de sécurité doivent être évalués. Les éléments de preuve des tests de ces mécanismes doivent être évalués.

Niveau E4

4.8 En plus des exigences du niveau E3, il doit exister un modèle formel sous-jacent de politique de sécurité supportant la cible d'évaluation. Les fonctions dédiées à la sécurité, la conception générale et la conception détaillée doivent être spécifiées en style semi-formel.

Niveau E5

4.9 En plus des exigences du niveau E4, il doit exister une correspondance étroite entre la conception détaillée et le code source et/ou les schémas descriptifs des matériels.

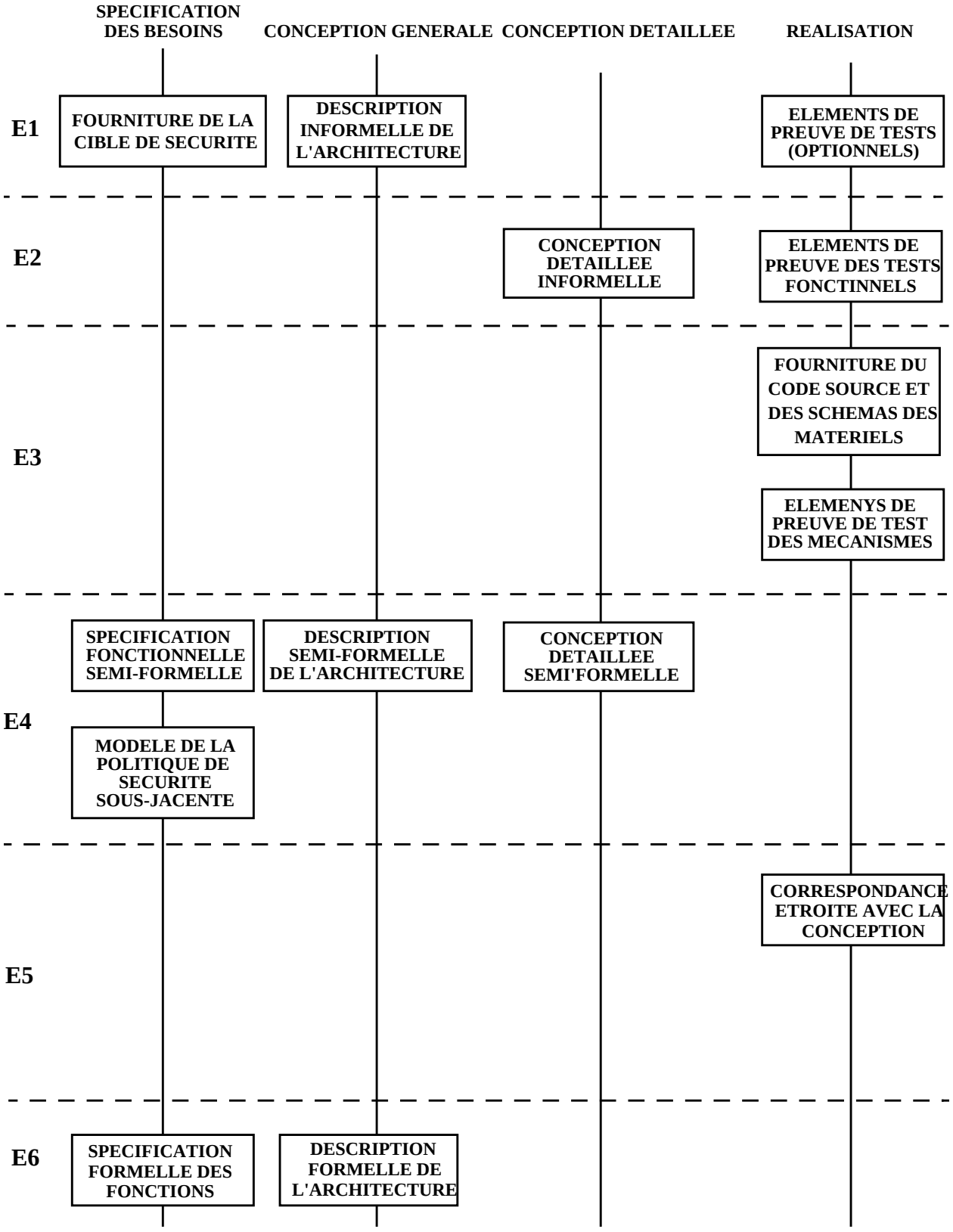
Niveau E6

4.10 En plus des exigences du niveau E5, les fonctions dédiées à la sécurité ainsi que la conception générale doivent être spécifiées en style formel de manière cohérente avec le modèle formel sous-jacent de politique de sécurité.

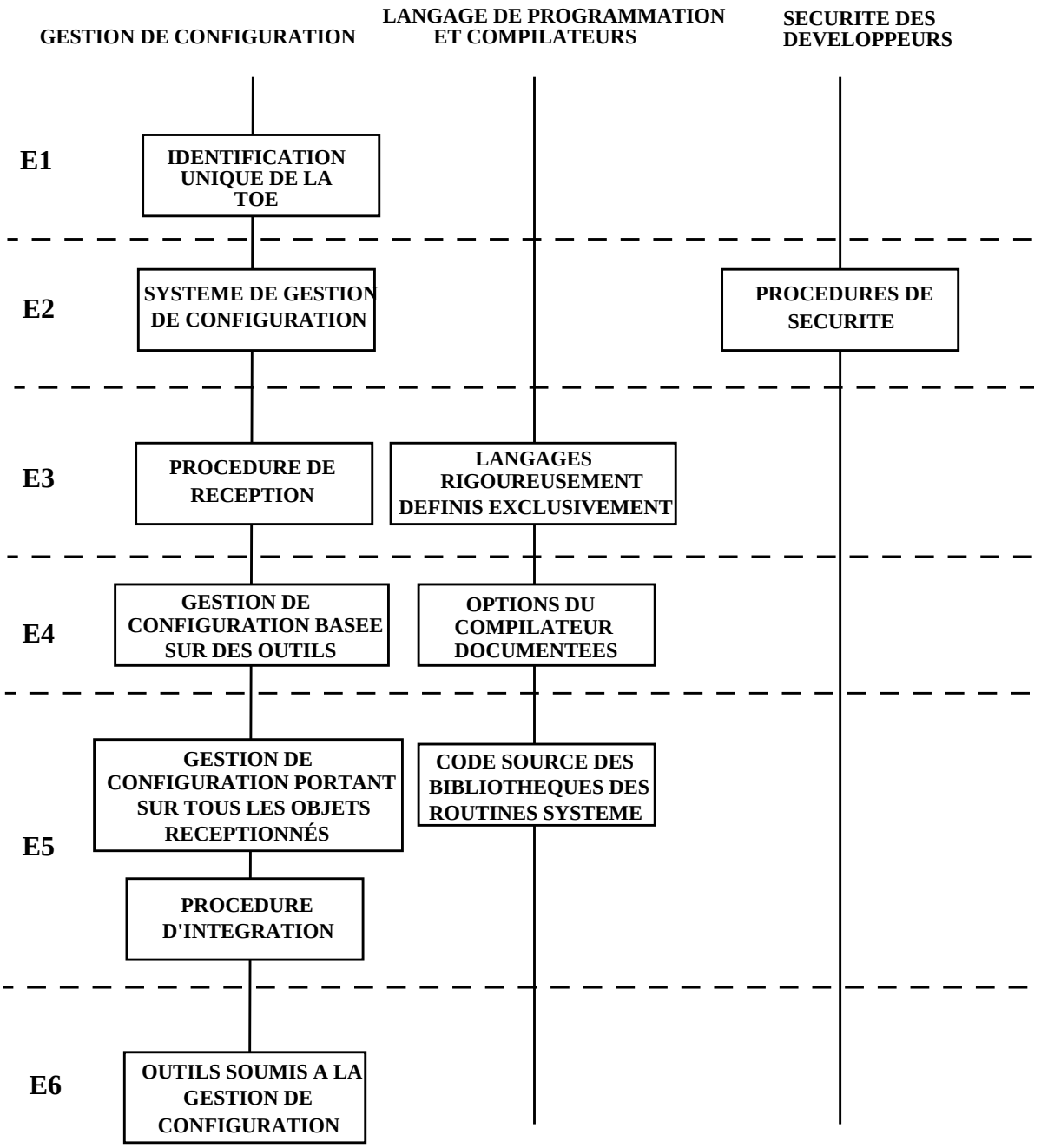
Résumé des exigences

4.11 Les autres parties du chapitre contiennent les critères détaillés auxquels il faut satisfaire à chaque niveau d'évaluation de la conformité, regroupés sous des rubriques détaillées et répétées pour chacun des niveaux E1 à E6. Les principales différences entre les niveaux résultent d'exigences supplémentaires concernant l'examen du processus de développement. Pour aider à comprendre ces différences, les diagrammes ci-après montrent la relation entre les éléments clés qui doivent être fournis par le commanditaire et le niveau d'évaluation auquel ils sont exigés pour la première fois par l'évaluateur.

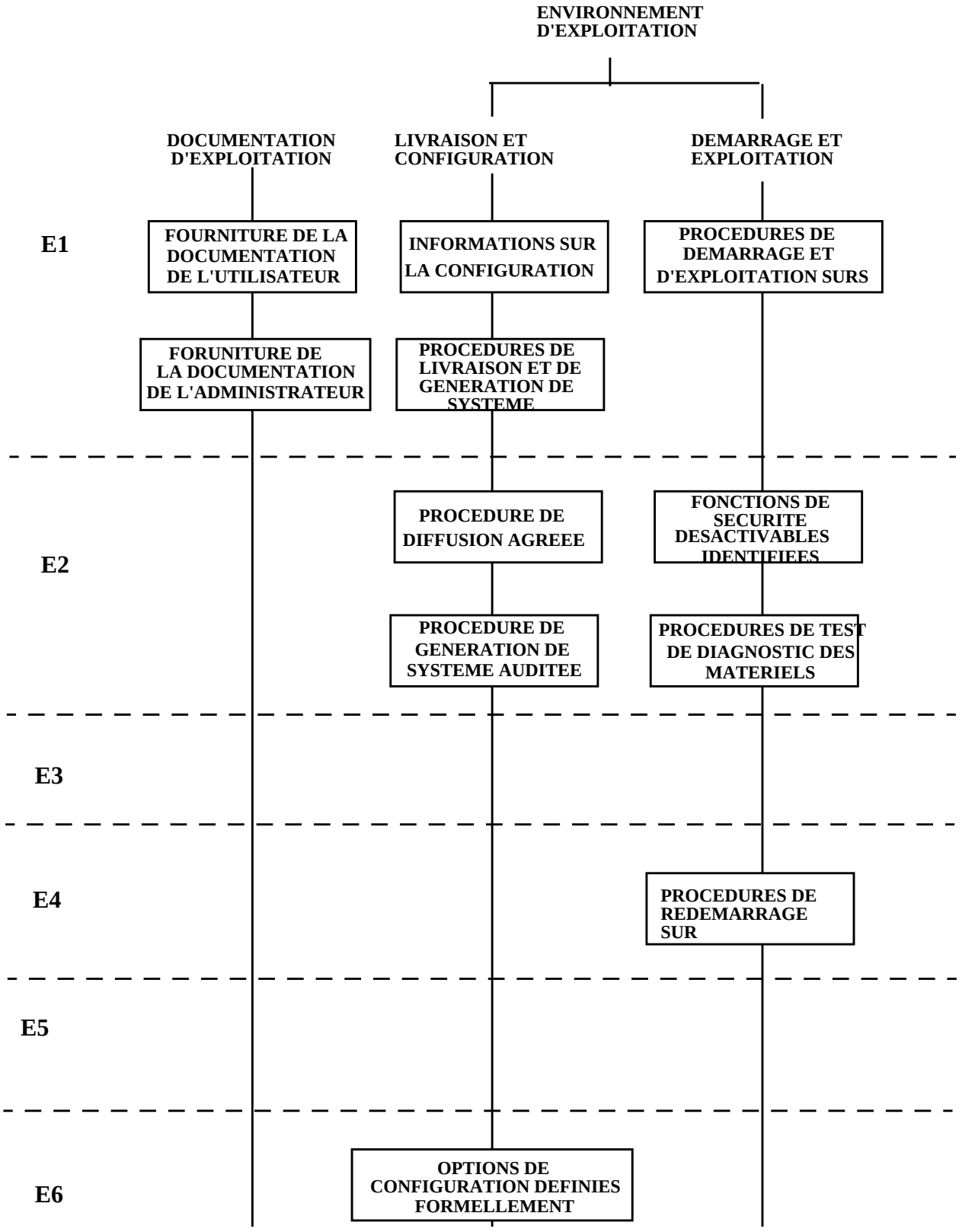
CRITERES DE CONFORMITE PAR NIVEAU - PROCESSUS DE DEVELOPPEMENT



CRITERES DE CONFORMITE PAR NIVEAU - ENVIRONNEMENT DE DEVELOPPEMENT



CRITERES DE CONFORMITE PAR NIVEAU - EXPLOITATION



Approche utilisée pour les descriptions

4.12 Les critères d'évaluation servant à estimer la conformité se répartissent entre ceux qui concernent la manière dont une TOE est développée (construction) et ceux qui portent sur la façon dont elle sera utilisée (exploitation). Pour chaque niveau d'évaluation, ces critères sont ensuite divisés en phases et en aspects.

4.13 Pour chaque aspect ou phase, on trouvera : l'identification de la documentation qui doit être fournie pour examen, puis les exigences sur son contenu et sa présentation ou les procédures et normes qu'elle doit définir, puis les éléments de preuve exigés pour montrer que les critères en question ont été satisfaits, et enfin la présentation des tâches que doit assurer l'évaluateur.

4.14 Par souci de clarté, comme les exigences diffèrent de façon significative d'un niveau d'évaluation à l'autre, les critères pour chaque niveau sont exposés séparément. A chaque niveau, les critères nouveaux ou modifiés sont indiqués en **caractères gras**. De façon générale, il y a besoin de davantage de rigueur et d'approfondissement dans les éléments de preuve fournis à mesure que le niveau d'évaluation s'élève. Cela se reflète dans l'usage progressif, aux différents niveaux, des verbes "*présenter*" "*décrire*" et "*expliquer*" pour traiter du contenu et de la présentation de bon nombre de critères qui par ailleurs ne sont pas autrement modifiés.

4.15 Sauf pour E1, c'est au commanditaire qu'incombe la charge de fournir les éléments de preuve, puis ceux-ci sont vérifiés ou contrôlés par l'évaluateur. Il n'est imposé à l'évaluateur de fournir des éléments de preuve supplémentaires que lorsqu'une action indépendante est exigée pour obtenir le degré de confiance nécessaire. Par exemple, il y a des exigences concernant des éléments de preuve pour des tests dynamiques, à la fois pour le commanditaire et l'évaluateur. L'exigence majeure est pour le commanditaire qui doit fournir des éléments de preuve, en particulier des plans et des résultats de tests, issus du processus de développement normal du système ou du produit en question. L'exigence imposée à l'évaluateur est de montrer qu'il a examiné les résultats fournis par le commanditaire, mais aussi qu'il a effectué ses propres tests pour vérifier la complétude, le niveau de détail et la fidélité des tests fournis par le commanditaire, et aussi pour prendre en compte tout cas d'incohérence ou d'erreur manifeste qu'il pourrait trouver dans les résultats de ces tests.

4.16 Les tests ne représentent qu'un aspect de l'assurance qualité. Tout au long des critères, il est sous-entendu qu'un Programme d'Assurance Qualité a été introduit et s'applique au cycle de vie complet de la TOE. Ce programme d'Assurance Qualité doit couvrir la création, la maintenance et la destruction de tous les documents, programmes et matériels relatifs à la TOE. Les critères établis par ce document,

peuvent guider les experts en assurance qualité pour déterminer si le programme est satisfaisant pour le niveau d'évaluation visé pour la TOE.

Structure des critères de conformité

4.17 Les paragraphes qui suivent décrivent la structure et le contenu des critères qui seront utilisés pour chaque niveau d'évaluation entre E1 et E6. Ils se rapportent à chaque niveau et ne sont pas répétés pour chacun d'entre eux. Dans chaque niveau d'évaluation, les paragraphes sont numérotés de la façon suivante :

<identificateur de niveau>.<numéro de paragraphe à l'intérieur du niveau>

Ainsi, par exemple, le troisième paragraphe du niveau E2 est numéroté E2.3. Des paragraphes vides sont utilisés en cas de besoin, afin que les paragraphes numérotés de façon identique dans chacun des niveaux se rapportent aux mêmes sujets.

Construction - Le processus de développement

4.18 Une des principales sources de confiance dans la conformité des aspects liés à la sécurité d'une TOE est la compréhension de la façon dont elle a été développée. Pour les besoins de ces critères, quatre phases sont identifiées dans le processus de développement. Les facteurs qui contribuent au développement de la confiance sont identifiés dans les critères pour chacune de ces phases dans l'ordre où elles se présentent. Quelle que soit la façon dont la TOE est effectivement produite, les éléments de preuve doivent être présentés de façon à correspondre avec ces phases.

Phase 1 - Spécification des besoins

4.19 Cette première phase du processus de développement comprend la production d'une cible de sécurité pour le système ou le produit. Cette cible est la base de l'évaluation. Elle comprendra le niveau d'évaluation visé et la cotation annoncée de la résistance minimum des mécanismes.

Phase 2 - Conception générale

4.20 Cette phase du processus de développement couvre la définition et la conception d'ensemble de la TOE au plus haut niveau. Elle se présente sous la forme d'une spécification descriptive de haut niveau qui identifie la structure de base de la TOE, ses interfaces externes et sa décomposition en composants principaux, matériels et logiciels. Cette spécification distinguera ce que fera la TOE (la description de haut niveau) et comment elle le fera (la conception de haut niveau). Il est particulièrement important que la conception générale fournisse une séparation

claire et efficace entre les composants dédiés à la sécurité et les autres. Cette séparation peut être réalisée de façon physique, ou en s'appuyant sur des mécanismes de protection fournis par du matériel ou des microprogrammes, ou par tout autre moyen. Une bonne conception permet à l'effort d'évaluation de se concentrer sur les secteurs limités de la TOE qui contribuent à la sécurité, et de suivre facilement la réalisation de la cible de sécurité à mesure que la conception s'affine pour entrer de plus en plus dans les détails.

Phase 3 - Conception détaillée

4.21 Cette phase du processus de développement couvre l'affinement de la conception générale de la TOE vers un niveau de détail qui peut être utilisé comme base pour la programmation et/ou la construction du matériel, c'est à dire toutes les étapes de conception et de spécification en dessous de la spécification initiale de haut niveau. Les composants identifiés au niveau le plus bas de la spécification sont appelés "composants élémentaires" ; c'est à partir des spécifications des composants élémentaires que le logiciel et/ou le matériel seront produits. Les composants dédiés à la sécurité seront identifiés à ce niveau. Egalement à ce niveau, peuvent être identifiés certains composants non dédiés à la sécurité, mais dont la panne ou une mauvaise utilisation pourrait compromettre la sécurité. Ces composants touchent à la sécurité puisque leur fonctionnement correct est nécessaire pour que la TOE puisse faire respecter la sécurité. Des niveaux intermédiaires de spécification peuvent exister, en fonction de la méthodologie de développement utilisée et de la complexité de la cible d'évaluation. Il est important que la transformation des spécifications de la TOE vers plus de détails et moins d'abstraction soit réalisée d'une façon qui préserve correctement les intentions de la description de haut niveau.

Phase 4 - Réalisation

4.22 Cette phase du processus de développement couvre la réalisation de la conception détaillée de la TOE sous forme de matériel et/ou de logiciel. Chacun des composants élémentaires est d'abord programmé ou fabriqué à partir de ses spécifications. Ces composants élémentaires individuels doivent ensuite être vérifiés et testés par rapport à leurs spécifications. Ils sont ensuite intégrés les uns avec les autres de façon ordonnée jusqu'à ce que la TOE complète existe. Celle-ci doit ensuite être vérifiée et testée dans son ensemble par rapport à la cible de sécurité. Il faut reconnaître que le test d'un composant élémentaire ou d'une unité plus importante par rapport à sa spécification peut seulement montrer des erreurs ou des écarts par rapport à la spécification, jamais l'absence d'erreurs. Par conséquent, pour les degrés de confiance supérieurs, il faudra compléter les tests par des analyses.

Construction - L'environnement de développement

4.23 L'environnement de développement comprend les mesures, les procédures et les normes utilisées par le développeur au cours du développement, de la production et de la maintenance de la TOE.

Aspect 1 - Gestion de configuration

4.24 La gestion de configuration couvre les contrôles imposés par le développeur à ses processus de développement, de production et de maintenance ; par exemple, pour garantir que chaque représentation de la conception ou de sa réalisation est produite et modifiée de façon contrôlée et qu'il peut être montré qu'elle correspond correctement aux représentations précédentes sur lesquelles elle est basée. L'estimation de la gestion de configuration comportera la compréhension des procédures de gestion de la qualité du développeur. A la suite de la livraison de la première version d'une TOE, il est presque inévitable que des corrections de défauts ou des modifications destinées à prendre en compte des changements d'objectifs imposeront la réalisation et la diffusion de versions ultérieures de la TOE. Il est donc nécessaire de maintenir la gestion de configuration de la TOE et de la documentation associée après la première version et la première livraison. La gestion de configuration est importante pour le développeur car c'est le moyen de garantir que la TOE n'est pas modifiée d'une façon qui pourrait invalider les résultats de l'évaluation.

Aspect 2 - Langages de programmation et compilateurs

4.25 Cet aspect ne s'applique qu'aux composants logiciels ou micro-programmés. Il comprend des exigences relatives aux langages de programmation, aux outils de compilation et aux bibliothèques de routines système utilisées pour développer la TOE.

Aspect 3 - Sécurité des développeurs

4.26 La sécurité des développeurs recouvre les mesures physiques, organisationnelles, techniques et relatives au personnel, qui sont utilisées dans l'environnement de développement. Elle comprend la sécurité physique des locaux de développement et le contrôle de la façon dont le personnel de développement a été choisi et habilité. Son but est de protéger le développement d'une attaque délibérée et de maintenir la confidentialité des informations de façon appropriée.

Exploitation - La documentation d'exploitation

4.27 La documentation d'exploitation fournit les principaux moyens par lesquels le développeur d'une TOE et ses clients communiquent. Sa facilité à être comprise, sa couverture et sa conformité sont donc des facteurs importants pour une exploitation sûre de la TOE. Cette documentation peut être considérée comme entrant dans l'une des deux catégories d'information suivantes : celle qui concerne l'utilisateur final (documentation utilisateur) et celle qui sert aux administrateurs (documentation d'administration).

Aspect 1 - Documentation utilisateur

4.28 La documentation utilisateur d'une TOE est l'ensemble des informations que fournit le développeur à l'usage de l'utilisateur final. Elle devrait aider celui-ci à comprendre les capacités de la TOE en matière de sécurité et lui permettre de contribuer à maintenir la sécurité en cours d'utilisation.

Aspect 2 - Documentation d'administration

4.29 La documentation d'administration est l'ensemble des informations sur la TOE que le développeur met à la disposition de l'administrateur. Elle peut comprendre des renseignements qui ne concernent pas les utilisateurs finals ou qui ne leur sont pas appropriés. Cette documentation devrait aider l'administrateur à installer et à exploiter la TOE d'une manière qui soit sûre.

Exploitation - L'environnement d'exploitation

4.30 L'environnement d'exploitation comprend les mesures, les procédures et les normes touchant à la livraison, l'installation et l'exploitation sûres d'une TOE. Dans le cas d'un système qui est déjà en service, il est possible d'estimer les procédures d'exploitation réelles. Dans les autres cas, on ne peut évaluer que celles qui sont proposées.

Aspect 1 - Livraison et configuration

4.31 Cette section couvre les procédures servant à assurer la sécurité au cours du transfert de la TOE ou de ses composants à l'utilisateur, aussi bien lors de la livraison initiale qu'à l'occasion d'une modification ultérieure. Elle rassemble toutes les procédures ou opérations particulières nécessaires soit à la configuration de la TOE lors de son installation, soit à la démonstration de l'authenticité de la TOE livrée. Ces procédures et ces mesures sont la base de la garantie que la protection offerte par cette TOE en matière de sécurité n'est pas compromise du fait

du transfert ou d'une interférence avec les caractéristiques de sécurité lors de l'installation et de la configuration sur le site de l'utilisateur.

Aspect 2 - Démarrage et exploitation

4.32 Cette section rassemble les procédures utilisées par l'administrateur pour l'exploitation courante de la TOE de manière sûre. Elle doit comporter non seulement le fonctionnement quotidien (comme le démarrage du système), mais aussi d'autres opérations courantes telles que les sauvegardes et la maintenance indispensables, et des activités exceptionnelles comme le redémarrage et la restauration à la suite d'une panne. Presque toutes les TOE exigent une maintenance, soit pour tenir compte de modifications d'objectifs, soit pour traiter des défauts. Aussi ces procédures doivent-elles permettre d'effectuer les modifications, remplacements ou ajouts autorisés à la TOE.

NIVEAU E1

Construction - Le processus de développement

E1.1 Le commanditaire doit fournir la TOE ainsi que la documentation suivante :

- **la cible de sécurité pour la TOE,**
- **la description informelle de l'architecture de la TOE,**
- **la documentation de test (optionnelle),**
- **la bibliothèque des programmes de test et les outils utilisés pour tester la TOE (optionnelle).**

Phase 1 - Spécification des besoins

Exigences concernant le contenu et la présentation

E1.2 **La cible de sécurité doit présenter les fonctions dédiées à la sécurité qui doivent être fournies par la TOE. Dans le cas d'un système, la cible de sécurité doit comprendre en outre une politique de sécurité système ou SSP (System Security Policy) qui identifie les objectifs de sécurité ainsi que les menaces qui pèsent sur le système. Dans le cas d'un produit, la cible de sécurité doit inclure un argumentaire qui identifie le mode d'utilisation du produit, l'environnement envisagé et les menaces supposées à l'intérieur de cet environnement. Les fonctions dédiées à la sécurité dans le cadre de la cible de sécurité doivent être spécifiées en utilisant un style informel tel que décrit au chapitre 2.**

Exigences concernant les éléments de preuve

E1.3 **Dans le cas d'un système, la cible de sécurité doit présenter comment la fonctionnalité proposée satisfait aux objectifs de sécurité et est adéquate pour contrer les menaces identifiées. Dans le cas d'un produit, la cible de sécurité doit présenter comment la fonctionnalité est appropriée pour ce type d'emploi et adéquate pour contrer les menaces supposées.**

Tâches de l'évaluateur

E1.4 **Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier qu'il n'y a pas d'incohérence dans la cible de sécurité.**

Phase 2 - Conception générale

Exigences concernant le contenu et la présentation

E1.5 **La description de l'architecture doit présenter la structure générale de la TOE. Elle doit présenter les interfaces externes de la TOE. Elle doit présenter tous les matériels et les microprogrammes nécessaires à la TOE avec une présentation de la fonctionnalité des mécanismes de protection réalisés dans ces matériels et ces microprogrammes.**

Exigences concernant les éléments de preuve

E1.6 **La description de l'architecture doit présenter la manière dont seront fournies les fonctions dédiées à la sécurité de la cible de sécurité.**

Tâches de l'évaluateur

E1.7 **Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.**

Phase 3 - Conception détaillée

Exigences concernant le contenu et la présentation

E1.8 **Aucune.**

Exigences concernant les éléments de preuve

E1.9 **Aucune.**

Tâches de l'évaluateur

E1.10 **Aucune.**

Phase 4 - Réalisation

Exigences concernant le contenu et la présentation

E1.11 **La documentation de test peut être fournie, auquel cas elle doit contenir le plan, l'objectif, les procédures et les résultats des tests. Une bibliothèque de programmes de tests peut être fournie, auquel cas elle doit contenir les programmes de test, ainsi que les outils permettant de reproduire les tests couverts par la documentation de test.**

Exigences concernant les éléments de preuve

E1.12 **Il peut être fourni une documentation de test présentant la correspondance entre les tests et les fonctions dédiées à la sécurité définies dans la cible de sécurité.**

Tâches de l'évaluateur

E1.13 **Vérifier que la TOE satisfait à la cible de sécurité en réalisant tous les tests couvrant toutes les fonctions dédiées à la sécurité identifiées dans la cible de sécurité. Réaliser des tests complémentaires pour rechercher des erreurs. L'évaluateur n'a pas besoin de refaire les tests déjà réalisés par ou pour le commanditaire si les éléments de preuve appropriés de ces tests sont fournis, mais il doit vérifier par échantillonnage, les résultats de ces tests.**

Construction - L'environnement de développement

E1.14 Le commanditaire doit fournir la documentation suivante :

- **la liste de configuration identifiant la version de la TOE à évaluer.**

Aspect 1 - Gestion de configuration

Exigences concernant le contenu et la présentation

E1.15 **La liste de configuration doit présenter l'endroit où la TOE est identifiée de façon unique (numéro de version).**

Exigences concernant les éléments de preuve

E1.16 **La liste de configuration doit présenter comment la TOE est identifiée de façon unique.**

Tâches de l'évaluateur

E1.17 **Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.**

Aspect 2 - Langages de programmation et compilateurs

Exigences concernant le contenu et la présentation

E1.18 **Aucune.**

Exigences concernant les éléments de preuve

E1.19 **Aucune.**

Tâches de l'évaluateur

E1.20 **Aucune.**

Aspect 3 - Sécurité des développeurs

Exigences concernant le contenu et la présentation

E1.21 **Aucune.**

Exigences concernant les éléments de preuve

E1.22 **Aucune.**

Tâches de l'évaluateur

E1.23 **Aucune.**

Exploitation - La documentation d'exploitation

E1.24 Le commanditaire doit fournir les documents suivants :

- **la documentation utilisateur**,
- **la documentation d'administration**.

Aspect 1 - Documentation utilisateur

Exigences concernant le contenu et la présentation

E1.25 **La documentation utilisateur doit présenter les fonctions dédiées à la sécurité qui concernent l'utilisateur final. Elle doit aussi donner des lignes directrices suffisantes pour leur exploitation sûre. Ces documents, par exemple les manuels de référence et les guides de l'utilisateur, doivent être structurés, avoir une cohérence interne et être compatibles avec tous les autres documents fournis à ce niveau.**

Exigences concernant les éléments de preuve

E1.26 **La documentation utilisateur doit présenter comment un utilisateur final utilise la TOE de façon sûre.**

Tâches de l'évaluateur

E1.27 **Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.**

Aspect 2 - Documentation d'administration

Exigences concernant le contenu et la présentation

E1.28 **La documentation d'administration doit présenter les fonctions dédiées à la sécurité relevant d'un administrateur. Elle doit distinguer deux types de fonctions : celles qui permettent à un administrateur de contrôler les paramètres de sécurité et celles qui lui permettent seulement d'obtenir des informations. Si un administrateur est nécessaire, elle doit présenter tous les paramètres de sécurité qui sont sous sa responsabilité. Elle doit présenter tous les événements relatifs à la sécurité relevant des fonctions d'administration. Elle doit présenter, d'une façon suffisamment détaillée pour leur utilisation, les procédures relevant de l'administration de la sécurité. Elle doit donner des lignes directrices sur l'utilisation cohérente et efficace des caractéristiques de sécurité de la TOE et sur la façon dont ces caractéristiques interagissent. Elle doit présenter les instructions sur la façon dont le système ou le produit devra être installé et, le cas échéant, sur la façon dont il devra être configuré. La documentation d'administration, par exemple les manuels de référence et les guides de l'administrateur, doit être structurée, avoir une cohérence interne et être compatible avec tous les autres documents fournis à ce niveau.**

Exigences concernant les éléments de preuve

E1.29 **La documentation d'administration doit présenter comment la TOE est administrée de façon sûre.**

Tâches de l'évaluateur

E1.30 **Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.**

Exploitation - L'environnement d'exploitation

E1.31 Le commanditaire doit fournir les documents suivants :

- **la documentation de livraison et de configuration,**
- **la documentation de démarrage et d'exploitation.**

Aspect 1 - Livraison et configuration

Exigences concernant les procédures et les normes

E1.32 **Si différentes configurations sont possibles, l'impact de ces configurations sur la sécurité doit être présenté. Les procédures de livraison et de génération du système doivent être présentées.**

Exigences concernant les éléments de preuve

E1.33 **Les informations fournies doivent présenter comment les procédures maintiennent la sécurité.**

Tâches de l'évaluateur

E1.34 **Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.**

Aspect 2 - Démarrage et exploitation

Exigences concernant les procédures et les normes

E1.35 **Les procédures pour assurer un démarrage et une exploitation sûrs doivent être présentées.**

Exigences concernant les éléments de preuve

E1.36 **Les informations fournies doivent présenter comment les procédures maintiennent la sécurité.**

Tâches de l'évaluateur

E1.37 **Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.**

NIVEAU E2

Construction - Le processus de développement

E2.1 Le commanditaire doit fournir la TOE ainsi que la documentation suivante :

- la cible de sécurité pour la TOE,
- la description informelle de l'architecture de la TOE,
- **la description informelle de la conception détaillée,**
- **la documentation de test,**
- **la bibliothèque des programmes de test et les outils utilisés pour tester la TOE.**

Phase 1 - Spécification des besoins

Exigences concernant le contenu et la présentation

E2.2 La cible de sécurité doit présenter les fonctions dédiées à la sécurité qui doivent être fournies par la TOE. Dans le cas d'un système, la cible de sécurité doit comprendre en outre une politique de sécurité système ou SSP (System Security Policy) qui identifie les objectifs de sécurité ainsi que les menaces qui pèsent sur le système. Dans le cas d'un produit, la cible de sécurité doit inclure un argumentaire qui identifie le mode d'utilisation du produit, l'environnement envisagé et les menaces supposées à l'intérieur de cet environnement. Les fonctions dédiées à la sécurité dans le cadre de la cible de sécurité doivent être spécifiées en utilisant un style informel tel que décrit au chapitre 2.

Exigences concernant les éléments de preuve

E2.3 Dans le cas d'un système, la cible de sécurité doit présenter comment la fonctionnalité proposée satisfait aux objectifs de sécurité et est adéquate pour contrer les menaces identifiées. Dans le cas d'un produit, la cible de sécurité doit présenter comment la fonctionnalité est appropriée pour ce type d'emploi et adéquate pour contrer les menaces supposées.

Tâches de l'évaluateur

E2.4 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier qu'il n'y a pas d'incohérence dans la cible de sécurité.

Phase 2 - Conception générale

Exigences concernant le contenu et la présentation

E2.5 La description de l'architecture doit présenter la structure générale de la TOE. Elle doit présenter les interfaces externes de la TOE. Elle doit présenter tous les matériels et les microprogrammes nécessaires à la TOE avec une présentation de la fonctionnalité des mécanismes de protection réalisés dans ces matériels et ces microprogrammes. **Elle doit présenter la séparation de la TOE entre les fonctions dédiées à la sécurité et les autres composants.**

Exigences concernant les éléments de preuve

E2.6 La description de l'architecture doit présenter la manière dont seront fournies les fonctions dédiées à la sécurité de la cible de sécurité. **Elle doit présenter comment la séparation entre les fonctions dédiées à la sécurité et les autres composants est réalisée.**

Tâches de l'évaluateur

E2.7 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. **Vérifier que la séparation entre les fonctions dédiées à la sécurité et les autres composants est valide.**

Phase 3 - Conception détaillée

Exigences concernant le contenu et la présentation

E2.8 **La conception détaillée doit présenter la réalisation de toutes les fonctions dédiées à la sécurité ou touchant à la sécurité. Elle doit identifier tous les mécanismes de sécurité. Elle doit établir le lien entre les fonctions dédiées à la sécurité et les mécanismes ou les composants. Toutes les interfaces des composants dédiés à la sécurité ou touchant à la sécurité doivent être documentées en présentant leur but et leurs paramètres. Des spécifications ou des définitions des mécanismes doivent être fournies. Ces spécifications doivent convenir à l'analyse des relations entre les**

mécanismes employés. La fourniture de ces spécifications n'est pas nécessaire pour les composants qui ne sont ni dédiés à la sécurité, ni touchant à la sécurité. Lorsque plus d'un niveau de spécification est fourni, il doit exister une relation claire et hiérarchique entre les différents niveaux.

Exigences concernant les éléments de preuve

E2.9 **La conception détaillée doit présenter la manière dont les mécanismes de sécurité fournissent les fonctions dédiées à la sécurité spécifiées dans la cible de sécurité.** Elle doit présenter les raisons pour lesquelles les composants dont la conception n'est pas décrite ne peuvent être considérés ni comme dédiés à la sécurité ni comme touchant à la sécurité.

Tâches de l'évaluateur

E2.10 **Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.**

Phase 4 - Réalisation

Exigences concernant le contenu et la présentation

E2.11 **La documentation de test doit contenir le plan, l'objectif, les procédures et les résultats des tests. La bibliothèque de programmes de test doit contenir les programmes de test et les outils permettant de reproduire tous les tests couverts par la documentation de test.**

Exigences concernant les éléments de preuve

E2.12 **La documentation de test doit présenter la correspondance entre les tests et les fonctions dédiées à la sécurité définies dans la cible de sécurité.**

Tâches de l'évaluateur

E2.13 **Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Utiliser la bibliothèque de programmes de test pour vérifier par échantillonnage les résultats des tests. Vérifier que les tests couvrent toutes les fonctions dédiées à la sécurité identifiées dans la cible de sécurité.** Réaliser des tests complémentaires pour rechercher des erreurs.

Construction - L'environnement de développement

E2.14 Le commanditaire doit fournir la documentation suivante :

- la liste de configuration identifiant la version de la TOE à évaluer,
- **des informations sur le système de gestion de configuration,**
- **des informations sur la sécurité de l'environnement de développement.**

Aspect 1 - Gestion de configuration

Exigences concernant le contenu et la présentation

E2.15 **Le processus de développement doit s'appuyer sur un système de gestion de configuration. La liste de configuration fournie doit énumérer tous les composants élémentaires à partir desquels la TOE est construite. La TOE, ses composants élémentaires ainsi que tous les documents fournis, y compris les manuels, doivent posséder un identifiant unique. L'emploi de cet identifiant unique est obligatoire dans les références. Le système de gestion de configuration doit garantir que la TOE soumise à l'évaluation est conforme à la documentation fournie et que seuls les changements autorisés sont possibles.**

Exigences concernant les éléments de preuve

E2.16 **Les informations sur le système de gestion de configuration doivent présenter comment il est utilisé en pratique et appliqué dans le processus de développement conformément aux procédures de gestion de la qualité du développeur.**

Tâches de l'évaluateur

E2.17 **Vérifier que les procédures documentées sont appliquées.** Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Aspect 2 - Langages de programmation et compilateurs

Exigences concernant le contenu et la présentation

E2.18 Aucune.

Exigences concernant les éléments de preuve

E2.19 Aucune.

Tâches de l'évaluateur

E2.20 Aucune.

Aspect 3 - Sécurité des développeurs

Exigences concernant le contenu et la présentation

E2.21 **Le document portant sur la sécurité de l'environnement de développement doit présenter les protections prévues pour assurer l'intégrité de la TOE et la confidentialité des documents associés. Des mesures de sécurité physiques, organisationnelles, liées au personnel ou autres, utilisées par le développeur, doivent être présentées.**

Exigences concernant les éléments de preuve

E2.22 **Les informations concernant la sécurité de l'environnement de développement doivent présenter la manière dont l'intégrité de la TOE et la confidentialité de la documentation associée sont maintenues.**

Tâches de l'évaluateur

E2.23 **Vérifier que les procédures documentées sont appliquées. Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Rechercher des erreurs dans les procédures.**

Exploitation - La documentation d'exploitation

E2.24 Le commanditaire doit fournir les documents suivants :

- la documentation utilisateur,
- la documentation d'administration.

Aspect 1 - Documentation utilisateur

Exigences concernant le contenu et la présentation

E2.25 La documentation utilisateur doit présenter les fonctions dédiées à la sécurité qui concernent l'utilisateur final. Elle doit aussi donner des lignes directrices suffisantes pour leur exploitation sûre. Ces documents, par exemple les manuels de référence et les guides de l'utilisateur, doivent être structurés, avoir une cohérence interne et être compatibles avec tous les autres documents fournis à ce niveau.

Exigences concernant les éléments de preuve

E2.26 La documentation utilisateur doit présenter comment un utilisateur final utilise la TOE de façon sûre.

Tâches de l'évaluateur

E2.27 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Aspect 2 - Documentation d'administration

Exigences concernant le contenu et la présentation

E2.28 La documentation d'administration doit présenter les fonctions dédiées à la sécurité relevant d'un administrateur. Elle doit distinguer deux types de fonctions : celles qui permettent à un administrateur de contrôler les paramètres de sécurité et celles qui lui permettent seulement d'obtenir des informations. Si un administrateur est nécessaire, elle doit présenter tous les paramètres de sécurité qui sont sous sa responsabilité. Elle doit présenter tous les événements relatifs à la sécurité relevant des fonctions d'administration. Elle doit présenter, d'une façon suffisamment détaillée pour leur utilisation, les procédures relevant de l'administration de la sécurité. Elle doit donner des lignes directrices sur l'utilisation cohérente et efficace des caractéristiques de sécurité de la TOE et sur la façon dont ces caractéristiques interagissent. Elle doit présenter les instructions sur la façon dont le système ou le produit devra être installé et, le cas échéant, sur la façon dont il devra être configuré. La documentation d'administration, par exemple les manuels de référence et les guides de l'administrateur, doit être structurée, avoir une cohérence interne et être compatible avec tous les autres documents fournis à ce niveau.

Exigences concernant les éléments de preuve

E2.29 La documentation d'administration doit présenter comment la TOE est administrée de façon sûre.

Tâches de l'évaluateur

E2.30 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Exploitation - L'environnement d'exploitation

E2.31 Le commanditaire doit fournir les documents suivants :

- la documentation de livraison et de configuration,
- la documentation de démarrage et d'exploitation.

Aspect 1 - Livraison et configuration

Exigences concernant les procédures et les normes

E2.32 Si différentes configurations sont possibles, l'impact de ces configurations sur la sécurité doit être présenté. Les procédures de livraison et de génération du système doivent être présentées. **Une procédure approuvée par l'organisme national de certification pour ce niveau d'évaluation doit être suivie, afin de garantir l'authenticité de la TOE livrée. Pendant la génération de la TOE, toute option ou tout changement de génération doit être audité de telle façon qu'il soit possible a posteriori de reconstituer exactement comment et quand la TOE a été générée.**

Exigences concernant les éléments de preuve

E2.33 Les informations fournies doivent présenter comment les procédures maintiennent la sécurité.

Tâches de l'évaluateur

E2.34 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. **Vérifier que les procédures de livraison sont correctement appliquées. Rechercher des erreurs dans les procédures de génération système.**

Aspect 2 - Démarrage et exploitation

Exigences concernant les procédures et les normes

E2.35 Les procédures pour assurer un démarrage et une exploitation sûrs doivent être présentées. **Si une fonction dédiée à la sécurité peut être désactivée ou modifiée pendant le démarrage, l'exploitation normale ou la maintenance, cela doit être déclaré. Si la TOE comprend des éléments matériels qui incluent des composants matériels dédiés à la sécurité, il doit exister des fonctions de diagnostic mises en oeuvre par l'administrateur, par l'utilisateur final, ou de façon automatique, pouvant être exécutées sur la TOE dans son environnement d'exploitation.**

Exigences concernant les éléments de preuve

E2.36 Les informations fournies doivent présenter comment les procédures maintiennent la sécurité. **Le commanditaire doit fournir des exemples de résultats de toutes les procédures de diagnostic des composants matériels dédiés à la sécurité. Le commanditaire doit fournir des exemples de toute trace d'audit générée au cours du démarrage ou de l'exploitation.**

Tâches de l'évaluateur

E2.37 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. **Vérifier les exemples d'éléments de preuve exigés pour le démarrage et l'exploitation. Rechercher des erreurs dans les procédures.**

NIVEAU E3

Construction - Le processus de développement

E3.1 Le commanditaire doit fournir la TOE ainsi que la documentation suivante :

- la cible de sécurité pour la TOE,
- la description informelle de l'architecture de la TOE,
- la description informelle de la conception détaillée,
- la documentation de test,
- la bibliothèque des programmes de test et les outils utilisés pour tester la TOE,
- **le code source ou les schémas descriptifs des matériels de tous les composants dédiés à la sécurité ou touchant à la sécurité,**
- **la description informelle de la correspondance entre le code source ou les schémas descriptifs des matériels et la conception détaillée.**

Phase 1 - Spécification des besoins

Exigences concernant le contenu et la présentation

E3.2 La cible de sécurité doit **décrire** les fonctions dédiées à la sécurité qui doivent être fournies par la TOE. Dans le cas d'un système, la cible de sécurité doit comprendre en outre une politique de sécurité système ou SSP (System Security Policy) qui identifie les objectifs de sécurité ainsi que les menaces qui pèsent sur le système. Dans le cas d'un produit, la cible de sécurité doit inclure un argumentaire qui identifie le mode d'utilisation du produit, l'environnement envisagé et les menaces supposées à l'intérieur de cet environnement. Les fonctions dédiées à la sécurité dans le cadre de la cible de sécurité doivent être spécifiées en utilisant un style informel tel que décrit au chapitre 2.

Exigences concernant les éléments de preuve

E3.3 Dans le cas d'un système, la cible de sécurité doit **décrire** comment la fonctionnalité proposée satisfait aux objectifs de sécurité et est adéquate pour contrer les menaces

identifiées. Dans le cas d'un produit, la cible de sécurité doit **décrire** comment la fonctionnalité est appropriée pour ce type d'emploi et adéquate pour contrer les menaces supposées.

Tâches de l'évaluateur

E3.4 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier qu'il n'y a pas d'incohérence dans la cible de sécurité.

Phase 2 - Conception générale

Exigences concernant le contenu et la présentation

E3.5 La description de l'architecture doit **décrire** la structure générale de la TOE. Elle doit **décrire** les interfaces externes de la TOE. Elle doit **décrire** les matériels et les microprogrammes nécessaires à la TOE avec une présentation de la fonctionnalité des mécanismes de protection réalisés dans ces matériels et ces microprogrammes. Elle doit **décrire** la séparation de la TOE entre les fonctions dédiées à la sécurité et les autres composants.

Exigences concernant les éléments de preuve

E3.6 La description de l'architecture doit **décrire** la manière dont seront fournies les fonctions dédiées à la sécurité de la cible de sécurité. Elle doit **décrire** comment la séparation entre les fonctions dédiées à la sécurité et les autres composants est réalisée.

Tâches de l'évaluateur

E3.7 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier que la séparation entre les fonctions dédiées à la sécurité et les autres composants est valide.

Phase 3 - Conception détaillée

Exigences concernant le contenu et la présentation

E3.8 **La conception détaillée doit spécifier tous les composants élémentaires.** La conception détaillée doit **décrire** la réalisation de toutes les fonctions dédiées à la sécurité ou touchant à la sécurité. Elle doit identifier tous les mécanismes de

sécurité. Elle doit établir le lien entre les fonctions dédiées à la sécurité et les mécanismes ou les composants. Toutes les interfaces des composants dédiés à la sécurité ou touchant à la sécurité doivent être documentées en présentant leur but et leurs paramètres. Des spécifications ou des définitions des mécanismes doivent être fournies. Ces spécifications doivent convenir à l'analyse des relations entre les mécanismes employés. La fourniture de ces spécifications n'est pas nécessaire pour les composants qui ne sont ni dédiés à la sécurité, ni touchant à la sécurité. Lorsque plus d'un niveau de spécification est fourni, il doit exister une relation claire et hiérarchique entre les différents niveaux.

Exigences concernant les éléments de preuve

E3.9 La conception détaillée doit **décrire** la manière dont les mécanismes de sécurité procurent les fonctions dédiées à la sécurité spécifiées dans la cible de sécurité. Elle doit **décrire** les raisons pour lesquelles les composants dont la conception n'est pas décrite ne peuvent être considérés ni comme dédiés à la sécurité ni comme touchant à la sécurité.

Tâches de l'évaluateur

E3.10 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Phase 4 - Réalisation

Exigences concernant le contenu et la présentation

E3.11 **La description des correspondances doit décrire les relations entre le code source ou les schémas descriptifs des matériels et les composants élémentaires de la conception détaillée.** La documentation de test doit contenir le plan, l'objectif, les procédures et les résultats des tests. La bibliothèque de programmes de test doit contenir les programmes de test et les outils permettant de reproduire tous les tests couverts par la documentation de test.

Exigences concernant les éléments de preuve

E3.12 La documentation de test doit **décrire** la correspondance entre les tests et les fonctions dédiées à la sécurité définies dans la cible de sécurité. **Elle doit décrire la correspondance entre les tests et les fonctions dédiées à la sécurité ou touchant à la sécurité définies dans la cible de sécurité. Elle doit décrire la correspondance entre les tests et les mécanismes de sécurité tels qu'ils sont représentés dans le code source ou les schémas descriptifs des matériels. Il est obligatoire d'apporter la preuve que**

les tests ont été repassés après la découverte et la correction d'erreurs touchant à la sécurité, de façon à démontrer que les erreurs ont été éliminées et qu'aucune nouvelle erreur n'a été introduite.

Tâches de l'évaluateur

E3.13 Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Utiliser la bibliothèque de programmes de test pour vérifier par échantillonnage les résultats des tests. Vérifier que les tests couvrent toutes les fonctions dédiées à la sécurité identifiées dans la cible de sécurité. **Vérifier que les tests couvrent toutes les fonctions dédiées à la sécurité ou touchant à la sécurité identifiées dans la conception détaillée et tous les mécanismes de sécurité identifiables dans le code source ou les schémas descriptifs des matériels. Vérifier que tous les tests ont été repassés après la correction des erreurs.** Réaliser des tests complémentaires pour rechercher des erreurs.

Construction - L'environnement de développement

E3.14 Le commanditaire doit fournir la documentation suivante :

- la liste de configuration identifiant la version de la TOE à évaluer,
- des informations sur le système de gestion de configuration,
- **des informations sur la procédure de réception,**
- des informations sur la sécurité de l'environnement de développement,
- **la description de tous les langages utilisés pour la réalisation.**

Aspect 1 - Gestion de configuration

Exigences concernant le contenu et la présentation

E3.15 Le processus de développement doit s'appuyer sur un système de gestion de configuration **et une procédure de réception**. La liste de configuration fournie doit énumérer tous les composants élémentaires à partir desquels la TOE est construite. La TOE, ses composants élémentaires ainsi que tous les documents fournis, y compris les manuels **et le code source ou les schémas descriptifs des matériels,** doivent posséder un identifiant unique. L'emploi de cet identifiant unique est obligatoire dans les références. Le système de gestion de configuration doit garantir

que la TOE soumise à l'évaluation est conforme à la documentation fournie et que seuls les changements autorisés sont possibles.

Exigences concernant les éléments de preuve

E3.16 Les informations sur le système de gestion de configuration doivent **décrire** comment il est utilisé en pratique et appliqué dans le processus de développement conformément aux procédures de gestion de la qualité du développeur.

Tâches de l'évaluateur

E3.17 Vérifier que les procédures documentées sont appliquées. Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Aspect 2 - Langages de programmation et compilateurs

Exigences concernant le contenu et la présentation

E3.18 **Tous les langages de programmation utilisés pour la réalisation doivent être parfaitement définis, comme par exemple dans une norme ISO. Toutes les options des langages de programmation, dépendant de la réalisation, doivent être documentées.**

Exigences concernant les éléments de preuve

E3.19 **La définition des langages de programmation doit définir sans ambiguïté le sens de toutes les déclarations utilisées dans le code source.**

Tâches de l'évaluateur

E3.20 **Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.**

Aspect 3 - Sécurité des développeurs

Exigences concernant le contenu et la présentation

E3.21 Le document portant sur la sécurité de l'environnement de développement doit **décrire** les protections prévues pour assurer l'intégrité de la TOE et la confidentialité des documents associés. Des mesures de sécurité physiques,

organisationnelles, liées au personnel ou autres, utilisées par le développeur, doivent être **décrites**.

Exigences concernant les éléments de preuve

E3.22 Les informations concernant la sécurité de l'environnement de développement doivent **décrire** la manière dont l'intégrité de la TOE et la confidentialité de la documentation associée sont maintenues.

Tâches de l'évaluateur

E3.23 Vérifier que les procédures documentées sont appliquées. Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Rechercher des erreurs dans les procédures.

Exploitation - La documentation d'exploitation

E3.24 Le commanditaire doit fournir les documents suivants :

- la documentation utilisateur,
- la documentation d'administration.

Aspect 1 - Documentation utilisateur

Exigences concernant le contenu et la présentation

E3.25 La documentation utilisateur doit **décrire** les fonctions dédiées à la sécurité qui concernent l'utilisateur final. Elle doit aussi donner des lignes directrices suffisantes pour leur exploitation sûre. Ces documents, par exemple les manuels de référence et les guides de l'utilisateur, doivent être structurés, avoir une cohérence interne et être compatibles avec tous les autres documents fournis à ce niveau.

Exigences concernant les éléments de preuve

E3.26 La documentation utilisateur doit **décrire** comment un utilisateur final utilise la TOE de façon sûre.

Tâches de l'évaluateur

E3.27 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Aspect 2 - Documentation d'administration

Exigences concernant le contenu et la présentation

E3.28 La documentation d'administration doit **décrire** les fonctions dédiées à la sécurité relevant d'un administrateur. Elle doit distinguer deux types de fonctions : celles qui permettent à un administrateur de contrôler les paramètres de sécurité et celles qui lui permettent seulement d'obtenir des informations. Si un administrateur est nécessaire, elle doit **décrire** tous les paramètres de sécurité qui sont sous sa responsabilité. Elle doit **décrire** tous les événements relatifs à la sécurité relevant des fonctions d'administration. Elle doit **décrire**, d'une façon suffisamment détaillée pour leur utilisation, les procédures relevant de l'administration de la sécurité. Elle doit donner des lignes directrices sur l'utilisation cohérente et efficace des caractéristiques de sécurité de la TOE et sur la façon dont ces caractéristiques interagissent. Elle doit **décrire** les instructions sur la façon dont le système ou le produit devra être installé et, le cas échéant, sur la façon dont il devra être configuré. La documentation d'administration, par exemple les manuels de référence et les guides de l'administrateur, doit être structurée, avoir une cohérence interne et être compatible avec tous les autres documents fournis à ce niveau.

Exigences concernant les éléments de preuve

E3.29 La documentation d'administration doit **décrire** comment la TOE est administrée de façon sûre.

Tâches de l'évaluateur

E3.30 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Exploitation - L'environnement d'exploitation

E3.31 Le commanditaire doit fournir les documents suivants :

- la documentation de livraison et de configuration,

- la documentation de démarrage et d'exploitation.

Aspect 1 - Livraison et configuration

Exigences concernant les procédures et les normes

E3.32 Si différentes configurations sont possibles, l'impact de ces configurations sur la sécurité doit être **décrit**. Les procédures de livraison et de génération du système doivent être **décrites**. Une procédure approuvée par l'organisme national de certification pour ce niveau d'évaluation doit être suivie, afin de garantir l'authenticité de la TOE livrée. Pendant la génération de la TOE, toute option ou tout changement de génération doit être audité de telle façon qu'il soit possible a posteriori de reconstituer exactement comment et quand la TOE a été générée.

Exigences concernant les éléments de preuve

E3.33 Les informations fournies doivent **décrire** comment les procédures maintiennent la sécurité.

Tâches de l'évaluateur

E3.34 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier que les procédures de livraison sont correctement appliquées. Rechercher des erreurs dans les procédures de génération système.

Aspect 2 - Démarrage et exploitation

Exigences concernant les procédures et les normes

E3.35 Les procédures pour assurer un démarrage et une exploitation sûrs doivent être **décrites**. Si une fonction dédiée à la sécurité peut être désactivée ou modifiée pendant le démarrage, l'exploitation normale ou la maintenance, cela doit être **décrit**. Si la TOE comprend des éléments matériels qui incluent des composants matériels dédiés à la sécurité, il doit exister des fonctions de diagnostic mises en oeuvre par l'administrateur, par l'utilisateur final, ou de façon automatique pouvant être exécutées sur la TOE dans son environnement d'exploitation.

Exigences concernant les éléments de preuve

E3.36 Les informations fournies doivent **décrire** comment les procédures maintiennent la sécurité. Le commanditaire doit fournir des exemples de résultats de toutes les procédures de diagnostic des composants matériels dédiés à la sécurité. Le commanditaire doit fournir des exemples de toute trace d'audit générée au cours du démarrage ou de l'exploitation.

Tâches de l'évaluateur

E3.37 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier les exemples d'éléments de preuve exigés pour le démarrage et l'exploitation. Rechercher des erreurs dans les procédures.

NIVEAU E4

Construction - Le processus de développement

E4.1 Le commanditaire doit fournir la TOE ainsi que la documentation suivante :

- la cible de sécurité pour la TOE,
- **la définition ou la référence à un modèle sous-jacent de sécurité, spécifié de façon formelle,**
- **l'interprétation informelle du modèle sous-jacent sous l'angle de la cible de sécurité,**
- la description **semi-formelle** de l'architecture de la TOE,
- la description **semi-formelle** de la conception détaillée,
- la documentation de test,
- la bibliothèque des programmes de test et les outils utilisés pour tester la TOE,
- le code source ou les schémas descriptifs des matériels de tous les composants dédiés à la sécurité ou touchant à la sécurité,
- la description informelle de la correspondance entre le code source ou les schémas descriptifs des matériels et la conception détaillée.

Phase 1 - Spécification des besoins

Exigences concernant le contenu et la présentation

E4.2 La cible de sécurité doit décrire les fonctions dédiées à la sécurité qui doivent être fournies par la TOE. Dans le cas d'un système, la cible de sécurité doit comprendre en outre une politique de sécurité système ou SSP (System Security Policy) qui identifie les objectifs de sécurité ainsi que les menaces qui pèsent sur le système. Dans le cas d'un produit, la cible de sécurité doit inclure un argumentaire qui identifie le mode d'utilisation du produit, l'environnement envisagé et les menaces supposées à l'intérieur de cet environnement. **Il doit être fourni ou fait référence à un modèle formel de politique de sécurité pour définir la politique de sécurité sous-**

jacente qui doit être mise en vigueur par la TOE. Une interprétation informelle de ce modèle sous l'angle de la cible de sécurité doit être fournie. Les fonctions dédiées à la sécurité dans le cadre de la cible de sécurité doivent être spécifiées en utilisant **à la fois** un style informel **et** un style **semi-formel** tels qu'ils sont décrits au chapitre 2.

Exigences concernant les éléments de preuve

E4.3 Dans le cas d'un système, la cible de sécurité doit décrire comment la fonctionnalité proposée satisfait aux objectifs de sécurité et est adéquate pour contrer les menaces identifiées. Dans le cas d'un produit, la cible de sécurité doit décrire comment la fonctionnalité est appropriée pour ce type d'emploi et adéquate pour contrer les menaces supposées. **L'interprétation informelle du modèle formel de politique de sécurité doit décrire la manière dont la cible de sécurité satisfait à la politique de sécurité sous-jacente.**

Tâches de l'évaluateur

E4.4 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier qu'il n'y a pas d'incohérence dans la cible de sécurité. **Vérifier qu'il n'y a pas de caractéristique de sécurité dans la cible de sécurité qui rentre en conflit avec la politique de sécurité sous-jacente.**

Phase 2 - Conception générale

Exigences concernant le contenu et la présentation

E4.5 **Une notation semi-formelle doit être utilisée pour la conception générale afin de produire une description semi-formelle.** La description de l'architecture doit décrire la structure générale de la TOE. Elle doit décrire les interfaces externes de la TOE. Elle doit décrire les matériels et les microprogrammes nécessaires à la TOE avec une présentation de la fonctionnalité des mécanismes de protection réalisés dans ces matériels et ces microprogrammes. Elle doit décrire la séparation de la TOE entre les fonctions dédiées à la sécurité et les autres composants.

Exigences concernant les éléments de preuve

E4.6 La description de l'architecture doit décrire la manière dont seront fournies les fonctions dédiées à la sécurité de la cible de sécurité. Elle doit décrire comment la séparation entre les fonctions dédiées à la sécurité et les autres composants est

réalisée. **Elle doit décrire comment la structure choisie conduit à des composants dédiés à la sécurité qui sont dans une large mesure indépendants.**

Tâches de l'évaluateur

E4.7 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier que la séparation entre les fonctions dédiées à la sécurité et les autres composants est valide.

Phase 3 - Conception détaillée

Exigences concernant le contenu et la présentation

E4.8 **Une notation semi-formelle doit être utilisée pour développer une conception détaillée semi-formelle.** La conception détaillée doit spécifier tous les composants élémentaires. **Elle doit décrire, à chaque niveau hiérarchique de la conception, la réalisation de toutes les fonctions dédiées à la sécurité ou touchant à la sécurité. Elle doit décrire la séparation de la TOE en composants dédiés à la sécurité, en composants touchant à la sécurité et en autres composants. Elle doit être structurée en composants élémentaires, bien définis et dans une large mesure indépendants de façon à faciliter les tests et à minimiser les possibilités de violation de la sécurité.** Elle doit identifier tous les mécanismes de sécurité. Elle doit établir le lien entre les fonctions dédiées à la sécurité et les mécanismes ou les composants. Toutes les interfaces des composants dédiés à la sécurité ou touchant à la sécurité doivent être documentées en présentant leur but et leurs paramètres. Des spécifications ou des définitions des mécanismes doivent être fournies. Ces spécifications doivent convenir à l'analyse des relations entre les mécanismes employés. La fourniture de ces spécifications n'est pas nécessaire pour les composants qui ne sont ni dédiés à la sécurité, ni touchant à la sécurité. Lorsque plus d'un niveau de spécification est fourni, il doit exister une relation claire et hiérarchique entre les différents niveaux.

Exigences concernant les éléments de preuve

E4.9 La conception détaillée doit décrire la manière dont les mécanismes de sécurité procurent les fonctions dédiées à la sécurité spécifiées dans la cible de sécurité. Elle doit décrire les raisons pour lesquelles les composants dont la conception n'est pas décrite ne peuvent être considérés ni comme dédiés à la sécurité ni comme touchant à la sécurité.

Tâches de l'évaluateur

E4.10 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Phase 4 - Réalisation

Exigences concernant le contenu et la présentation

E4.11 La description des correspondances doit décrire les relations entre le code source ou les schémas descriptifs des matériels et les composants élémentaires de la conception détaillée. La documentation de test doit contenir le plan, l'objectif, les procédures et les résultats des tests **ainsi qu'une justification de la suffisance de la couverture des tests**. La bibliothèque de programmes de test doit contenir les programmes de test et les outils permettant de reproduire tous les tests couverts par la documentation de test.

Exigences concernant les éléments de preuve

E4.12 La documentation de test doit décrire la correspondance entre les tests et les fonctions dédiées à la sécurité définies dans la cible de sécurité. Elle doit décrire la correspondance entre les tests et les fonctions dédiées à la sécurité ou touchant à la sécurité définies dans la cible de sécurité. Elle doit décrire la correspondance entre les tests et les mécanismes de sécurité tels qu'ils sont représentés dans le code source ou les schémas descriptifs des matériels. Il est obligatoire d'apporter la preuve que les tests ont été repassés après la découverte et la correction d'erreurs touchant à la sécurité, de façon à démontrer que les erreurs ont été éliminées et qu'aucune nouvelle erreur n'a été introduite.

Tâches de l'évaluateur

E4.13 Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Utiliser la bibliothèque de programmes de test pour vérifier par échantillonnage les résultats des tests. Vérifier que les tests couvrent toutes les fonctions dédiées à la sécurité identifiées dans la cible de sécurité. Vérifier que les tests couvrent toutes les fonctions dédiées à la sécurité ou touchant à la sécurité identifiées dans la conception détaillée et tous les mécanismes de sécurité identifiables dans le code source ou les schémas descriptifs des matériels. Vérifier que tous les tests ont été repassés après la correction des erreurs. Réaliser des tests complémentaires pour rechercher des erreurs.

Construction - L'environnement de développement

E4.14 Le commanditaire doit fournir la documentation suivante :

- la liste de configuration identifiant la version de la TOE à évaluer,
- des informations sur le système de gestion de configuration **et les outils associés**,
- **des informations d'audit sur les modifications de toutes les parties de la TOE soumises à la gestion de configuration,**
- des informations sur la procédure de réception,
- des informations sur la sécurité de l'environnement de développement,
- la description de tous les langages **et compilateurs** utilisés pour la réalisation.

Aspect 1 - Gestion de configuration

Exigences concernant le contenu et la présentation

E4.15 Le processus de développement doit s'appuyer sur un système de gestion de configuration **basé sur des outils** et une procédure de réception. La liste de configuration fournie doit énumérer tous les composants élémentaires à partir desquels la TOE est construite. La TOE, ses composants élémentaires ainsi que tous les documents fournis, y compris les manuels et le code source ou les schémas descriptifs des matériels, doivent posséder un identifiant unique. L'emploi de cet identifiant unique est obligatoire dans les références. Le système de gestion de configuration doit garantir que la TOE soumise à l'évaluation est conforme à la documentation fournie et que seuls les changements autorisés **effectués par des personnes autorisées** sont possibles. **Les outils de gestion de configuration doivent permettre de contrôler et d'auditer les changements apportés entre les différentes versions des objets soumis à la gestion de configuration.**

Exigences concernant les éléments de preuve

E4.16 Les informations sur le système de gestion de configuration doivent décrire comment il est utilisé en pratique et appliqué dans le processus de développement conformément aux procédures de gestion de la qualité du développeur.

Tâches de l'évaluateur

E4.17 Vérifier que les procédures documentées sont appliquées. Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. **Utiliser les outils des développeurs pour régénérer des parties sélectionnées de la TOE et comparer le résultat avec la version de la TOE soumise à l'évaluation.**

Aspect 2 - Langages de programmation et compilateurs

Exigences concernant le contenu et la présentation

E4.18 Tous les langages de programmation utilisés pour la réalisation doivent être parfaitement définis, comme par exemple dans une norme ISO. Toutes les options des langages de programmation, dépendant de la réalisation, doivent être documentées. **Les options de réalisation choisies de tous les compilateurs utilisés doivent être documentées.**

Exigences concernant les éléments de preuve

E4.19 La définition des langages de programmation doit définir sans ambiguïté le sens de toutes les déclarations utilisées dans le code source.

Tâches de l'évaluateur

E4.20 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Aspect 3 - Sécurité des développeurs

Exigences concernant le contenu et la présentation

E4.21 Le document portant sur la sécurité de l'environnement de développement doit décrire les protections prévues pour assurer l'intégrité de la TOE et la confidentialité des documents associés. Des mesures de sécurité physiques, organisationnelles, liées au personnel ou autres, utilisées par le développeur, doivent être décrites.

Exigences concernant les éléments de preuve

E4.22 Les informations concernant la sécurité de l'environnement de développement doivent décrire la manière dont l'intégrité de la TOE et la confidentialité de la documentation associée sont maintenues.

Tâches de l'évaluateur

E4.23 Vérifier que les procédures documentées sont appliquées. Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Rechercher des erreurs dans les procédures.

Exploitation - La documentation d'exploitation

E4.24 Le commanditaire doit fournir les documents suivants :

- la documentation utilisateur,
- la documentation d'administration.

Aspect 1 - Documentation utilisateur

Exigences concernant le contenu et la présentation

E4.25 La documentation utilisateur doit décrire les fonctions dédiées à la sécurité qui concernent l'utilisateur final. Elle doit aussi donner des lignes directrices suffisantes pour leur exploitation sûre. Ces documents, par exemple les manuels de référence et les guides de l'utilisateur, doivent être structurés, avoir une cohérence interne et être compatibles avec tous les autres documents fournis à ce niveau.

Exigences concernant les éléments de preuve

E4.26 La documentation utilisateur doit décrire comment un utilisateur final utilise la TOE de façon sûre.

Tâches de l'évaluateur

E4.27 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Aspect 2 - Documentation d'administration

Exigences concernant le contenu et la présentation

E4.28 La documentation d'administration doit décrire les fonctions dédiées à la sécurité relevant d'un administrateur. Elle doit distinguer deux types de fonctions : celles qui permettent à un administrateur de contrôler les paramètres de sécurité et celles qui lui permettent seulement d'obtenir des informations. Si un administrateur est nécessaire, elle doit décrire tous les paramètres de sécurité qui sont sous sa responsabilité. Elle doit décrire tous les événements relatifs à la sécurité relevant des fonctions d'administration. Elle doit décrire, d'une façon suffisamment détaillée pour leur utilisation, les procédures relevant de l'administration de la sécurité. Elle doit donner des lignes directrices sur l'utilisation cohérente et efficace des caractéristiques de sécurité de la TOE et sur la façon dont ces caractéristiques interagissent. Elle doit décrire les instructions sur la façon dont le système ou le produit devra être installé et, le cas échéant, sur la façon dont il devra être configuré. La documentation d'administration, par exemple les manuels de référence et les guides de l'administrateur, doit être structurée, avoir une cohérence interne et être compatible avec tous les autres documents fournis à ce niveau.

Exigences concernant les éléments de preuve

E4.29 La documentation d'administration doit décrire comment la TOE est administrée de façon sûre.

Tâches de l'évaluateur

E4.30 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Exploitation - L'environnement d'exploitation

E4.31 Le commanditaire doit fournir les documents suivants :

- la documentation de livraison et de configuration,
- la documentation de démarrage et d'exploitation.

Aspect 1 - Livraison et configuration

Exigences concernant les procédures et les normes

E4.32 Si différentes configurations sont possibles, l'impact de ces configurations sur la sécurité doit être décrit. Les procédures de livraison et de génération du système doivent être décrites. Une procédure approuvée par l'organisme national de certification pour ce niveau d'évaluation doit être suivie, afin de garantir l'authenticité de la TOE livrée. Pendant la génération de la TOE, toute option ou tout changement de génération doit être audité de telle façon qu'il soit possible a posteriori de reconstituer exactement comment et quand la TOE a été générée.

Exigences concernant les éléments de preuve

E4.33 Les informations fournies doivent décrire comment les procédures maintiennent la sécurité.

Tâches de l'évaluateur

E4.34 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier que les procédures de livraison sont correctement appliquées. Rechercher des erreurs dans les procédures de génération système.

Aspect 2 - Démarrage et exploitation

Exigences concernant les procédures et les normes

E4.35 Les procédures pour assurer un démarrage et une exploitation sûrs doivent être décrites. Si une fonction dédiée à la sécurité peut être désactivée ou modifiée pendant le démarrage, l'exploitation normale ou la maintenance, cela doit être décrit. **Il doit exister des procédures permettant de restaurer la TOE dans un état sûr après une panne ou une erreur matérielle ou logicielle.** Si la TOE comprend des éléments matériels qui incluent des composants matériels dédiés à la sécurité, il doit exister des fonctions de diagnostic mises en oeuvre par l'administrateur, par l'utilisateur final, ou de façon automatique pouvant être exécutées sur la TOE dans son environnement d'exploitation.

Exigences concernant les éléments de preuve

E4.36 Les informations fournies doivent décrire comment les procédures maintiennent la sécurité. Le commanditaire doit fournir des exemples de résultats de toutes les

procédures de diagnostic des composants matériels dédiés à la sécurité. Le commanditaire doit fournir des exemples de toute trace d'audit générée au cours du démarrage ou de l'exploitation.

Tâches de l'évaluateur

E4.37 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier les exemples d'éléments de preuve exigés pour le démarrage et l'exploitation. Rechercher des erreurs dans les procédures.

NIVEAU E5

Construction - Le processus de développement

E5.1 Le commanditaire doit fournir la TOE ainsi que la documentation suivante :

- la cible de sécurité pour la TOE,
- la définition ou la référence à un modèle sous-jacent de sécurité, spécifié de façon formelle,
- l'interprétation informelle du modèle sous-jacent sous l'angle de la cible de sécurité,
- la description semi-formelle de l'architecture de la TOE,
- la description semi-formelle de la conception détaillée,
- la documentation de test,
- la bibliothèque des programmes de test et les outils utilisés pour tester la TOE,
- le code source ou les schémas descriptifs des matériels de tous les composants dédiés à la sécurité ou touchant à la sécurité,
- la description informelle de la correspondance entre le code source ou les schémas descriptifs des matériels et la conception détaillée.

Phase 1 - Spécification des besoins

Exigences concernant le contenu et la présentation

E5.2 La cible de sécurité doit **expliquer** les fonctions dédiées à la sécurité qui doivent être fournies par la TOE. Dans le cas d'un système, la cible de sécurité doit comprendre en outre une politique de sécurité système ou SSP (System Security Policy) qui identifie les objectifs de sécurité ainsi que les menaces qui pèsent sur le système. Dans le cas d'un produit, la cible de sécurité doit inclure un argumentaire qui identifie le mode d'utilisation du produit, l'environnement envisagé et les menaces supposées à l'intérieur de cet environnement. Il doit être fourni ou fait référence à un modèle formel de politique de sécurité pour définir la

politique de sécurité sous-jacente qui doit être mise en vigueur par la TOE. Une interprétation informelle de ce modèle sous l'angle de la cible de sécurité doit être fournie. Les fonctions dédiées à la sécurité dans le cadre de la cible de sécurité doivent être spécifiées en utilisant à la fois un style informel et un style semi-formel tels qu'ils sont décrits au chapitre 2.

Exigences concernant les éléments de preuve

E5.3 Dans le cas d'un système, la cible de sécurité doit **expliquer** comment la fonctionnalité proposée satisfait aux objectifs de sécurité et est adéquate pour contrer les menaces identifiées. Dans le cas d'un produit, la cible de sécurité doit **expliquer** comment la fonctionnalité est appropriée pour ce type d'emploi et adéquate pour contrer les menaces supposées. L'interprétation informelle du modèle formel de politique de sécurité doit **expliquer** la manière dont la cible de sécurité satisfait à la politique de sécurité sous-jacente.

Tâches de l'évaluateur

E5.4 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier qu'il n'y a pas d'incohérence dans la cible de sécurité. Vérifier qu'il n'a pas de caractéristique de sécurité dans la cible de sécurité qui rentre en conflit avec la politique de sécurité sous-jacente.

Phase 2 - Conception générale

Exigences concernant le contenu et la présentation

E5.5 Une notation semi-formelle doit être utilisée pour la conception générale afin de produire une description semi-formelle. La description de l'architecture doit **expliquer** la structure générale de la TOE. Elle doit **expliquer** les interfaces externes de la TOE. Elle doit **expliquer** les matériels et les microprogrammes nécessaires à la TOE avec une présentation de la fonctionnalité des mécanismes de protection réalisés dans ces matériels et ces microprogrammes. Elle doit **expliquer** la séparation de la TOE entre les fonctions dédiées à la sécurité et les autres composants. **Elle doit expliquer les relations entre les différents composants dédiés à la sécurité.**

Exigences concernant les éléments de preuve

E5.6 La description de l'architecture doit **expliquer** la manière dont seront fournies les fonctions dédiées à la sécurité de la cible de sécurité. Elle doit **expliquer** comment

la séparation entre les fonctions dédiées à la sécurité et les autres composants est réalisée. Elle doit **expliquer** comment la structure choisie conduit à des composants dédiés à la sécurité qui sont dans une large mesure indépendants. **Elle doit expliquer pourquoi les relations entre les composants dédiés à la sécurité sont nécessaires.**

Tâches de l'évaluateur

E5.7 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier que la séparation entre les fonctions dédiées à la sécurité et les autres composants est valide.

Phase 3 - Conception détaillée

Exigences concernant le contenu et la présentation

E5.8 Une notation semi-formelle doit être utilisée pour développer une conception détaillée semi-formelle. La conception détaillée doit spécifier tous les composants élémentaires. Elle doit **expliquer**, à chaque niveau hiérarchique de la conception, la réalisation de toutes les fonctions dédiées à la sécurité ou touchant à la sécurité. Elle doit **expliquer** la séparation de la TOE en composants dédiés à la sécurité, en composants touchant à la sécurité et en autres composants. Elle doit être structurée en composants élémentaires, bien définis et dans une large mesure indépendants de façon à faciliter les tests et à minimiser les possibilités de violation de la sécurité. **Elle doit utiliser de façon importante le découpage en couches, l'abstraction et la dissimulation des données.** Elle doit identifier tous les mécanismes de sécurité. Elle doit établir le lien entre les fonctions dédiées à la sécurité et les mécanismes et **unités fonctionnelles**. **Les fonctionnalités superflues doivent être exclues des composants dédiés à la sécurité et de ceux touchant à la sécurité.** Toutes les interfaces des composants dédiés à la sécurité ou touchant à la sécurité doivent être documentées en présentant leur but, leurs paramètres **et leurs effets. Le rôle de toutes les variables utilisées par plus d'une unité fonctionnelle doit être expliqué.** Des spécifications ou des définitions des mécanismes doivent être fournies. Ces spécifications doivent convenir à l'analyse des relations entre les mécanismes employés. La fourniture de ces spécifications n'est pas nécessaire pour les composants qui ne sont ni dédiés à la sécurité, ni touchant à la sécurité. Lorsque plus d'un niveau de spécification est fourni, il doit exister une relation claire et hiérarchique entre les différents niveaux.

Exigences concernant les éléments de preuve

E5.9 La conception détaillée doit **expliquer** la manière dont les mécanismes de sécurité procurent les fonctions dédiées à la sécurité spécifiées dans la cible de sécurité. **Elle**

doit expliquer pourquoi les fonctionnalités restantes ne peuvent pas être exclues des composants dédiés à la sécurité et de ceux touchant à la sécurité. Elle doit **expliquer** les raisons pour lesquelles les composants dont la conception n'est pas décrite ne peuvent être considérés ni comme dédiés à la sécurité ni comme touchant à la sécurité.

Tâches de l'évaluateur

E5.10 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Phase 4 - Réalisation

Exigences concernant le contenu et la présentation

E5.11 **Le code source et les schémas descriptifs des matériels doivent être complètement structurés en sections séparées, petites et compréhensibles.** La description des correspondances doit **expliquer** les relations entre le code source ou les schémas descriptifs des matériels et les **unités fonctionnelles** de la conception détaillée. La documentation de test doit contenir le plan, l'objectif, les procédures et les résultats des tests ainsi qu'une justification de la suffisance de la couverture des tests. La bibliothèque de programmes de test doit contenir les programmes de test et les outils permettant de reproduire tous les tests couverts par la documentation de test.

Exigences concernant les éléments de preuve

E5.12 La documentation de test doit **expliquer** la correspondance entre les tests et les fonctions dédiées à la sécurité définies dans la cible de sécurité. Elle doit **expliquer** la correspondance entre les tests et les fonctions dédiées à la sécurité ou touchant à la sécurité définies dans la cible de sécurité. Elle doit **expliquer** la correspondance entre les tests et les mécanismes de sécurité tels qu'ils sont représentés dans le code source ou les schémas descriptifs des matériels. Il est obligatoire d'apporter la preuve que les tests ont été repassés après la découverte et la correction d'erreurs touchant à la sécurité, de façon à démontrer que les erreurs ont été éliminées et qu'aucune nouvelle erreur n'a été introduite.

Tâches de l'évaluateur

E5.13 Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Utiliser la bibliothèque de programmes de test pour vérifier par échantillonnage les résultats des tests. Vérifier que les tests couvrent toutes les fonctions dédiées à la sécurité identifiées dans la

cible de sécurité. Vérifier que les tests couvrent toutes les fonctions dédiées à la sécurité ou touchant à la sécurité identifiées dans la conception détaillée et tous les mécanismes de sécurité identifiables dans le code source ou les schémas descriptifs des matériels. Vérifier que tous les tests ont été repassés après la correction des erreurs. Réaliser des tests complémentaires pour rechercher des erreurs.

Construction - L'environnement de développement

E5.14 Le commanditaire doit fournir la documentation suivante :

- la liste de configuration identifiant la version de la TOE à évaluer,
- des informations sur le système de gestion de configuration et les outils associés,
- des informations d'audit sur les modifications de toutes les parties de la TOE soumises à la gestion de configuration,
- des informations sur la procédure de réception,
- **des informations sur la procédure d'intégration,**
- des informations sur la sécurité de l'environnement de développement,
- la description de tous les langages et compilateurs utilisés pour la réalisation,
- **le code source de toutes les bibliothèques de routines système utilisées**.

Aspect 1 - Gestion de configuration

Exigences concernant le contenu et la présentation

E5.15 Le processus de développement doit s'appuyer sur un système de gestion de configuration basé sur des outils et une procédure de réception. **Les outils de gestion de configuration doivent garantir que le responsable de la réception d'un objet dans le système de gestion de configuration, n'était ni un de ses concepteurs ni un de ses développeurs.** La liste de configuration fournie doit énumérer tous les composants élémentaires à partir desquels la TOE est construite. La TOE, ses composants élémentaires ainsi que tous les documents fournis, y compris les manuels et le code source ou les schémas descriptifs des matériels, doivent

posséder un identifiant unique. L'emploi de cet identifiant unique est obligatoire dans les références. Le système de gestion de configuration doit garantir que la TOE soumise à l'évaluation est conforme à la documentation fournie et que seuls les changements autorisés effectués par des personnes autorisées sont possibles. **Tous les objets créés au cours du processus de développement qui subissent la procédure de réception doivent être soumis à la gestion de configuration. Tous les objets dédiés à la sécurité ou touchant à la sécurité doivent être identifiés comme tels.** Les outils de gestion de configuration doivent permettre de contrôler et d'auditer les changements apportés entre les différentes versions des objets soumis à la gestion de configuration. **Toute modification apportée à ces objets doit être auditée avec indication de l'origine, de la date et de l'heure. Les outils de gestion de configuration doivent permettre la création et la manipulation de relations variables entre les objets soumis à la gestion de configuration. En cas de modification de l'un quelconque d'entre eux, les outils doivent permettre d'identifier tous les autres objets soumis à la gestion de configuration et affectés par cette modification, tout en indiquant s'ils sont dédiés à la sécurité ou touchant à la sécurité.**

Exigences concernant les éléments de preuve

E5.16 Les informations sur le système de gestion de configuration **et la procédure d'intégration** doivent **expliquer** comment **ils sont** utilisés et appliqués au processus de développement conformément aux procédures de gestion de la qualité du développeur. **Les informations sur le système de gestion de configuration doivent expliquer comment les outils garantissent que le responsable de la réception d'un objet n'était ni un des ses concepteurs, ni un de ses développeurs. Des traces d'audit produites par le système de gestion de configuration doivent être fournies à titre d'exemple.**

Tâches de l'évaluateur

E5.17 Vérifier que les procédures documentées sont appliquées. Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. **Vérifier les traces d'audit fournies en exemple.** Utiliser les outils des développeurs pour régénérer des parties sélectionnées de la TOE et comparer le résultat avec la version de la TOE soumise à l'évaluation.

Aspect 2 - Langages de programmation et compilateurs

Exigences concernant le contenu et la présentation

E5.18 Tous les langages de programmation utilisés pour la réalisation doivent être parfaitement définis, comme par exemple dans une norme ISO. Toutes les options des langages de programmation, dépendant de la réalisation, doivent être documentées. Les options de réalisation choisies de tous les compilateurs utilisés doivent être documentées. **Le code source de toute bibliothèque de routines système doit être fourni.**

Exigences concernant les éléments de preuve

E5.19 La définition des langages de programmation doit définir sans ambiguïté le sens de toutes les déclarations utilisées dans le code source.

Tâches de l'évaluateur

E5.20 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Aspect 3 - Sécurité des développeurs

Exigences concernant le contenu et la présentation

E5.21 Le document portant sur la sécurité de l'environnement de développement doit **expliquer** les protections prévues pour assurer l'intégrité de la TOE et la confidentialité des documents associés. Des mesures de sécurité physiques, organisationnelles, liées au personnel ou autres, utilisées par le développeur, doivent être **expliquées**.

Exigences concernant les éléments de preuve

E5.22 Les informations concernant la sécurité de l'environnement de développement doivent **expliquer** la manière dont l'intégrité de la TOE et la confidentialité de la documentation associée sont maintenues.

Tâches de l'évaluateur

E5.23 Vérifier que les procédures documentées sont appliquées. Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Rechercher des erreurs dans les procédures.

Exploitation - La documentation d'exploitation

E5.24 Le commanditaire doit fournir les documents suivants :

- la documentation utilisateur,
- la documentation d'administration.

Aspect 1 - Documentation utilisateur

Exigences concernant le contenu et la présentation

E5.25 La documentation utilisateur doit **expliquer** les fonctions dédiées à la sécurité qui concernent l'utilisateur final. Elle doit aussi donner des lignes directrices suffisantes pour leur exploitation sûre. Ces documents, par exemple les manuels de référence et les guides de l'utilisateur, doivent être structurés, avoir une cohérence interne et être compatibles avec tous les autres documents fournis à ce niveau.

Exigences concernant les éléments de preuve

E5.26 La documentation utilisateur doit **expliquer** comment un utilisateur final utilise la TOE de façon sûre.

Tâches de l'évaluateur

E5.27 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Aspect 2 - Documentation d'administration

Exigences concernant le contenu et la présentation

E5.28 La documentation d'administration doit **expliquer** les fonctions dédiées à la sécurité relevant d'un administrateur. Elle doit distinguer deux types de fonctions : celles qui permettent à un administrateur de contrôler les paramètres de sécurité et celles qui lui permettent seulement d'obtenir des informations. Si un administrateur est nécessaire, elle doit **expliquer** tous les paramètres de sécurité qui sont sous sa responsabilité. Elle doit **expliquer** tous les événements relatifs à la sécurité relevant des fonctions d'administration. Elle doit **expliquer**, d'une façon suffisamment détaillée pour leur utilisation, les procédures relevant de l'administration de la sécurité. Elle doit donner des lignes directrices sur l'utilisation cohérente et efficace

des caractéristiques de sécurité de la TOE et sur la façon dont ces caractéristiques interagissent. Elle doit **expliquer** les instructions sur la façon dont le système ou le produit devra être installé et, le cas échéant, sur la façon dont il devra être configuré. La documentation d'administration, par exemple les manuels de référence et les guides de l'administrateur, doit être structurée, avoir une cohérence interne et être compatible avec tous les autres documents fournis à ce niveau.

Exigences concernant les éléments de preuve

E5.29 La documentation d'administration doit **expliquer** comment la TOE est administrée de façon sûre.

Tâches de l'évaluateur

E5.30 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Exploitation - L'environnement d'exploitation

E5.31 Le commanditaire doit fournir les documents suivants :

- la documentation de livraison et de configuration,
- la documentation de démarrage et d'exploitation.

Aspect 1 - Livraison et configuration

Exigences concernant les procédures et les normes

E5.32 Si différentes configurations sont possibles, l'impact de ces configurations sur la sécurité doit être **expliqué**. Les procédures de livraison et de génération du système doivent être **expliquées**. Une procédure approuvée par l'organisme national de certification pour ce niveau d'évaluation doit être suivie, afin de garantir l'authenticité de la TOE livrée. Pendant la génération de la TOE, toute option ou tout changement de génération doit être audité de telle façon qu'il soit possible a posteriori de reconstituer exactement comment et quand la TOE a été générée.

Exigences concernant les éléments de preuve

E5.33 Les informations fournies doivent **expliquer** comment les procédures maintiennent la sécurité.

Tâches de l'évaluateur

E5.34 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier que les procédures de livraison sont correctement appliquées. Rechercher des erreurs dans les procédures de génération système.

Aspect 2 - Démarrage et exploitation

Exigences concernant les procédures et les normes

E5.35 Les procédures pour assurer un démarrage et une exploitation sûrs doivent être **expliquées**. Si une fonction dédiée à la sécurité peut être désactivée ou modifiée pendant le démarrage, l'exploitation normale ou la maintenance, cela doit être **expliqué**. Il doit exister des procédures permettant de restaurer la TOE dans un état sûr après une panne ou une erreur matérielle ou logicielle. Si la TOE comprend des éléments matériels qui incluent des composants matériels dédiés à la sécurité, il doit exister des fonctions de diagnostic mises en oeuvre par l'administrateur, par l'utilisateur final, ou de façon automatique pouvant être exécutées sur la TOE dans son environnement d'exploitation.

Exigences concernant les éléments de preuve

E5.36 Les informations fournies doivent **expliquer** comment les procédures maintiennent la sécurité. Le commanditaire doit fournir des exemples de résultats de toutes les procédures de diagnostic des composants matériels dédiés à la sécurité. Le commanditaire doit fournir des exemples de toute trace d'audit générée au cours du démarrage ou de l'exploitation.

Tâches de l'évaluateur

E5.37 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier les exemples d'éléments de preuve exigés pour le démarrage et l'exploitation. Rechercher des erreurs dans les procédures.

NIVEAU E6

Construction - Le processus de développement

E6.1 Le commanditaire doit fournir la TOE ainsi que la documentation suivante :

- la cible de sécurité pour la TOE,
- la définition ou la référence à un modèle sous-jacent de sécurité, spécifié de façon formelle,
- l'interprétation informelle du modèle sous-jacent sous l'angle de la cible de sécurité,
- la description **formelle** de l'architecture de la TOE,
- la description semi-formelle de la conception détaillée,
- la documentation de test,
- la bibliothèque des programmes de test et les outils utilisés pour tester la TOE**, y compris des outils qui peuvent être utilisés pour détecter les incohérences entre le code source et le code exécutable, dans le cas où il existe des composants sous forme de code source, dédiés à la sécurité ou touchant à la sécurité (par exemple un désassembleur et/ou un débogueur)**,
- le code source ou les schémas descriptifs des matériels de tous les composants dédiés à la sécurité ou touchant à la sécurité,
- la description informelle de la correspondance entre le code source ou les schémas descriptifs des matériels et la conception détaillée**, ainsi que la spécification formelle des fonctions dédiées à la sécurité**.

Phase 1 - Spécification des besoins

Exigences concernant le contenu et la présentation

E6.2 La cible de sécurité doit expliquer les fonctions dédiées à la sécurité qui doivent être fournies par la TOE. Dans le cas d'un système, la cible de sécurité doit comprendre en outre une politique de sécurité système ou SSP (System Security Policy) qui identifie les objectifs de sécurité ainsi que les menaces qui pèsent sur

le système. Dans le cas d'un produit, la cible de sécurité doit inclure un argumentaire qui identifie le mode d'utilisation du produit, l'environnement envisagé et les menaces supposées à l'intérieur de cet environnement. Il doit être fourni un modèle formel de politique de sécurité pour définir la politique de sécurité sous-jacente qui doit être mise en vigueur par la TOE. Une interprétation informelle de ce modèle sous l'angle de la cible de sécurité doit être fournie. Les fonctions dédiées à la sécurité dans le cadre de la cible de sécurité doivent être spécifiées en utilisant à la fois un style informel et un style **formel** tels qu'ils sont décrits au chapitre 2.

Exigences concernant les éléments de preuve

E6.3 Dans le cas d'un système, la cible de sécurité doit expliquer comment la fonctionnalité proposée satisfait aux objectifs de sécurité et est adéquate pour contrer les menaces identifiées. Dans le cas d'un produit, la cible de sécurité doit expliquer comment la fonctionnalité est appropriée pour ce type d'emploi et adéquate pour contrer les menaces supposées. L'interprétation informelle du modèle formel de politique de sécurité doit expliquer la manière dont la cible de sécurité satisfait à la politique de sécurité sous-jacente.

Tâches de l'évaluateur

E6.4 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier qu'il n'y a pas d'incohérence dans la cible de sécurité. Vérifier qu'il n'y a pas de caractéristique de sécurité dans la cible de sécurité qui rentre en conflit avec la politique de sécurité sous-jacente.

Phase 2 - Conception générale

Exigences concernant le contenu et la présentation

E6.5 La conception générale doit être faite en utilisant une notation **formelle** afin de produire une description **formelle**. La description de l'architecture doit expliquer la structure générale de la TOE. Elle doit expliquer les interfaces externes de la TOE. Elle doit expliquer les matériels et les microprogrammes nécessaires à la TOE avec une présentation de la fonctionnalité des mécanismes de protection réalisés dans ces matériels et ces microprogrammes. Elle doit expliquer la séparation de la TOE entre les fonctions dédiées à la sécurité et les autres composants. Elle doit expliquer les relations entre les différents composants dédiés à la sécurité.

Exigences concernant les éléments de preuve

E6.6 La description de l'architecture doit expliquer la manière dont seront fournies les fonctions dédiées à la sécurité de la cible de sécurité. Elle doit expliquer comment la séparation entre les fonctions dédiées à la sécurité et les autres composants est réalisée. Elle doit expliquer comment la structure choisie conduit à des composants dédiés à la sécurité qui sont dans une large mesure indépendants. Elle doit expliquer pourquoi les relations entre les composants dédiés à la sécurité sont nécessaires. **Elle doit expliquer, en utilisant une combinaison de techniques formelles et informelles, la manière dont elle est cohérente avec le modèle formel de la politique de sécurité sous-jacente.**

Tâches de l'évaluateur

E6.7 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier que la séparation entre les fonctions dédiées à la sécurité et les autres composants est valide. **Vérifier la validité des arguments formels.**

Phase 3 - Conception détaillée

Exigences concernant le contenu et la présentation

E6.8 Une notation semi-formelle doit être utilisée pour développer une conception détaillée semi-formelle. La conception détaillée doit spécifier tous les composants élémentaires. Elle doit expliquer, à chaque niveau hiérarchique de la conception, la réalisation de toutes les fonctions dédiées à la sécurité ou touchant à la sécurité. Elle doit expliquer la séparation de la TOE en composants dédiés à la sécurité, en composants touchant à la sécurité et en autres composants. Elle doit être structurée en composants élémentaires, bien définis et dans une large mesure indépendants de façon à faciliter les tests et à minimiser les possibilités de violation de la sécurité. Elle doit utiliser de façon importante le découpage en couches, l'abstraction et la dissimulation des données. Elle doit identifier tous les mécanismes de sécurité. Elle doit établir le lien entre les fonctions dédiées à la sécurité et les mécanismes et unités fonctionnelles. Les fonctionnalités superflues doivent être exclues des composants dédiés à la sécurité et de ceux touchant à la sécurité. Toutes les interfaces des composants dédiés à la sécurité ou touchant à la sécurité doivent être documentées en présentant leur but, leurs paramètres et leurs effets. Le rôle de toutes les variables utilisées par plus d'une unité fonctionnelle doit être expliqué. Des spécifications ou des définitions des mécanismes doivent être fournies. Ces spécifications doivent convenir à l'analyse des relations entre les mécanismes employés. La fourniture de ces spécifications n'est pas nécessaire pour les

composants qui ne sont ni dédiés à la sécurité, ni touchant à la sécurité. Lorsque plus d'un niveau de spécification est fourni, il doit exister une relation claire et hiérarchique entre les différents niveaux.

Exigences concernant les éléments de preuve

E6.9 La conception détaillée doit expliquer la manière dont les mécanismes de sécurité procurent les fonctions dédiées à la sécurité spécifiées dans la cible de sécurité. Elle doit expliquer pourquoi les fonctionnalités restantes ne peuvent pas être exclues des composants dédiés à la sécurité et de ceux touchant à la sécurité. Elle doit expliquer les raisons pour lesquelles les composants dont la conception n'est pas décrite ne peuvent être considérés ni comme dédiés à la sécurité ni comme touchant à la sécurité.

Tâches de l'évaluateur

E6.10 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Phase 4 - Réalisation

Exigences concernant le contenu et la présentation

E6.11 Le code source et les schémas descriptifs des matériels doivent être complètement structurés en sections séparées, petites et compréhensibles. La description des correspondances doit expliquer les relations entre le code source ou les schémas descriptifs des matériels et les unités fonctionnelles de la conception détaillée. **Elle doit expliquer la correspondance entre les mécanismes de sécurité sous la forme de code source ou de schémas matériels et la spécification formelle des fonctions dédiées à la sécurité dans la cible de sécurité.** La documentation de test doit contenir le plan, l'objectif, les procédures et les résultats des tests ainsi qu'une justification de la suffisance de la couverture des tests. La bibliothèque de programmes de test doit contenir les programmes de test et les outils permettant de reproduire tous les tests couverts par la documentation de test.

Exigences concernant les éléments de preuve

E6.12 La documentation de test doit expliquer la correspondance entre les tests et **la spécification formelle des** fonctions dédiées à la sécurité définies dans la cible de sécurité. Elle doit expliquer la correspondance entre les tests et les fonctions dédiées à la sécurité ou touchant à la sécurité définies dans la cible de sécurité. Elle doit expliquer la correspondance entre les tests et les mécanismes de sécurité tels

qu'ils sont représentés dans le code source ou les schémas descriptifs des matériels. Il est obligatoire d'apporter la preuve que les tests ont été repassés après la découverte et la correction d'erreurs touchant à la sécurité, de façon à démontrer que les erreurs ont été éliminées et qu'aucune nouvelle erreur n'a été introduite.

Tâches de l'évaluateur

E6.13 Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Utiliser la bibliothèque de programmes de test pour vérifier par échantillonnage les résultats des tests. Vérifier que les tests couvrent toutes les fonctions dédiées à la sécurité identifiées dans la cible de sécurité. Vérifier que les tests couvrent toutes les fonctions dédiées à la sécurité ou touchant à la sécurité identifiées dans la conception détaillée et tous les mécanismes de sécurité identifiables dans le code source ou les schémas descriptifs des matériels. Vérifier que tous les tests ont été repassés après la correction des erreurs. Réaliser des tests complémentaires pour rechercher des erreurs. **Faire des investigations sur toute présomption d'incohérence entre le code source et le code exécutable apparue durant le déroulement des tests, en utilisant les outils fournis par le commanditaire.**

Construction - L'environnement de développement

E6.14 Le commanditaire doit fournir la documentation suivante :

- la liste de configuration identifiant la version de la TOE à évaluer,
- des informations sur le système de gestion de configuration et les outils associés,
- des informations d'audit sur les modifications de toutes les parties de la TOE soumises à la gestion de configuration,
- des informations sur la procédure de réception,
- des informations sur la procédure d'intégration,
- des informations sur la sécurité de l'environnement de développement,
- la description de tous les langages et compilateurs utilisés pour la réalisation,
- le code source de toutes les bibliothèques de routines système utilisées.

Aspect 1 - Gestion de configuration

Exigences concernant le contenu et la présentation

E6.15 Le processus de développement doit s'appuyer sur un système de gestion de configuration basé sur des outils et une procédure de réception. Les outils de gestion de configuration doivent garantir que le responsable de la réception d'un objet dans le système de gestion de configuration, n'était ni un de ses concepteurs ni un de ses développeurs. La liste de configuration fournie doit énumérer tous les composants élémentaires à partir desquels la TOE est construite. La TOE, ses composants élémentaires ainsi que tous les documents fournis, y compris les manuels et le code source ou les schémas descriptifs des matériels, doivent posséder un identifiant unique. L'emploi de cet identifiant unique est obligatoire dans les références. Le système de gestion de configuration doit garantir que la TOE soumise à l'évaluation est conforme à la documentation fournie et que seuls les changements autorisés effectués par des personnes autorisées sont possibles. **Tous les outils utilisés au cours du processus de développement doivent être soumis à la gestion de configuration.** Tous les objets créés au cours du processus de développement qui subissent la procédure de réception doivent être soumis à la gestion de configuration. Tous les objets dédiés à la sécurité ou touchant à la sécurité doivent être identifiés comme tels. Les outils de gestion de configuration doivent permettre de contrôler et d'auditer les changements apportés entre les différentes versions des objets soumis à la gestion de configuration. Toute modification apportée à ces objets doit être auditée avec indication de l'origine, de la date et de l'heure. Les outils de gestion de configuration doivent permettre la création et la manipulation de relations variables entre les objets soumis à la gestion de configuration. En cas de modification de l'un quelconque d'entre eux, les outils doivent permettre d'identifier tous les autres objets soumis à la gestion de configuration et affectés par cette modification, tout en indiquant s'ils sont dédiés à la sécurité ou touchant à la sécurité.

Exigences concernant les éléments de preuve

E6.16 Les informations sur le système de gestion de configuration et la procédure d'intégration doivent expliquer comment ils sont utilisés et appliqués au processus de développement conformément aux procédures de gestion de la qualité du développeur. Les informations sur le système de gestion de configuration doivent expliquer comment les outils garantissent que le responsable de la réception d'un objet n'était ni un des ses concepteurs, ni un de ses développeurs. Des traces d'audit produites par le système de gestion de configuration doivent être fournies à titre d'exemple.

Tâches de l'évaluateur

E6.17 Vérifier que les procédures documentées sont appliquées. Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier les traces d'audit fournies en exemple. Utiliser les outils des développeurs pour régénérer des parties sélectionnées de la TOE et comparer le résultat avec la version de la TOE soumise à l'évaluation.

Aspect 2 - Langages de programmation et compilateurs

Exigences concernant le contenu et la présentation

E6.18 Tous les langages de programmation utilisés pour la réalisation doivent être parfaitement définis, comme par exemple dans une norme ISO. Toutes les options des langages de programmation, dépendant de la réalisation, doivent être documentées. Les options de réalisation choisies de tous les compilateurs utilisés doivent être documentées. Le code source de toute bibliothèque de routines système doit être fourni.

Exigences concernant les éléments de preuve

E6.19 La définition des langages de programmation doit définir sans ambiguïté le sens de toutes les déclarations utilisées dans le code source.

Tâches de l'évaluateur

E6.20 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Aspect 3 - Sécurité des développeurs

Exigences concernant le contenu et la présentation

E6.21 Le document portant sur la sécurité de l'environnement de développement doit expliquer les protections prévues pour assurer l'intégrité de la TOE et la confidentialité des documents associés. Des mesures de sécurité physiques, organisationnelles, liées au personnel ou autres, utilisées par le développeur, doivent être expliquées.

Exigences concernant les éléments de preuve

E6.22 Les informations concernant la sécurité de l'environnement de développement doivent expliquer la manière dont l'intégrité de la TOE et la confidentialité de la documentation associée sont maintenues.

Tâches de l'évaluateur

E6.23 Vérifier que les procédures documentées sont appliquées. Vérifier que les informations fournies sont conformes aux exigences concernant le contenu, la présentation et les éléments de preuve. Rechercher des erreurs dans les procédures.

Exploitation - La documentation d'exploitation

E6.24 Le commanditaire doit fournir les documents suivants :

- la documentation utilisateur,
- la documentation d'administration.

Aspect 1 - Documentation utilisateur

Exigences concernant le contenu et la présentation

E6.25 La documentation utilisateur doit expliquer les fonctions dédiées à la sécurité qui concernent l'utilisateur final. Elle doit aussi donner des lignes directrices suffisantes pour leur exploitation sûre. Ces documents, par exemple les manuels de référence et les guides de l'utilisateur, doivent être structurés, avoir une cohérence interne et être compatibles avec tous les autres documents fournis à ce niveau.

Exigences concernant les éléments de preuve

E6.26 La documentation utilisateur doit expliquer comment un utilisateur final utilise la TOE de façon sûre.

Tâches de l'évaluateur

E6.27 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Aspect 2 - Documentation d'administration

Exigences concernant le contenu et la présentation

E6.28 La documentation d'administration doit expliquer les fonctions dédiées à la sécurité relevant d'un administrateur. Elle doit distinguer deux types de fonctions : celles qui permettent à un administrateur de contrôler les paramètres de sécurité et celles qui lui permettent seulement d'obtenir des informations. Si un administrateur est nécessaire, elle doit expliquer tous les paramètres de sécurité qui sont sous sa responsabilité. Elle doit expliquer tous les événements relatifs à la sécurité relevant des fonctions d'administration. Elle doit expliquer, d'une façon suffisamment détaillée pour leur utilisation, les procédures relevant de l'administration de la sécurité. Elle doit donner des lignes directrices sur l'utilisation cohérente et efficace des caractéristiques de sécurité de la TOE et sur la façon dont ces caractéristiques interagissent. Elle doit expliquer les instructions sur la façon dont le système ou le produit devra être installé et, le cas échéant, sur la façon dont il devra être configuré. La documentation d'administration, par exemple les manuels de référence et les guides de l'administrateur, doit être structurée, avoir une cohérence interne et être compatible avec tous les autres documents fournis à ce niveau.

Exigences concernant les éléments de preuve

E6.29 La documentation d'administration doit expliquer comment la TOE est administrée de façon sûre.

Tâches de l'évaluateur

E6.30 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve.

Exploitation - L'environnement d'exploitation

E6.31 Le commanditaire doit fournir les documents suivants :

- la documentation de livraison et de configuration,
- la documentation de démarrage et d'exploitation.

Aspect 1 - Livraison et configuration

Exigences concernant les procédures et les normes

E6.32 Si différentes configurations sont possibles, **elles doivent être définies en fonction de la conception générale formelle, et** l'impact de ces configurations sur la sécurité doit être expliqué. Les procédures de livraison et de génération du système doivent être expliquées. Une procédure approuvée par l'organisme national de certification pour ce niveau d'évaluation doit être suivie, afin de garantir l'authenticité de la TOE livrée. Pendant la génération de la TOE, toute option ou tout changement de génération doit être audité de telle façon qu'il soit possible a posteriori de reconstituer exactement comment et quand la TOE a été générée.

Exigences concernant les éléments de preuve

E6.33 Les informations fournies doivent expliquer comment les procédures maintiennent la sécurité.

Tâches de l'évaluateur

E6.34 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier que les procédures de livraison sont correctement appliquées. Rechercher des erreurs dans les procédures de génération système.

Aspect 2 - Démarrage et exploitation

Exigences concernant les procédures et les normes

E6.35 Les procédures pour assurer un démarrage et une exploitation sûrs doivent être expliquées. Si une fonction dédiée à la sécurité peut être désactivée ou modifiée pendant le démarrage, l'exploitation normale ou la maintenance, cela doit être expliqué. Il doit exister des procédures permettant de restaurer la TOE dans un état sûr après une panne ou une erreur matérielle ou logicielle. Si la TOE comprend des éléments matériels qui incluent des composants matériels dédiés à la sécurité, il doit exister des fonctions de diagnostic mises en oeuvre par l'administrateur, par l'utilisateur final, ou de façon automatique pouvant être exécutées sur la TOE dans son environnement d'exploitation.

Exigences concernant les éléments de preuve

E6.36 Les informations fournies doivent expliquer comment les procédures maintiennent la sécurité. Le commanditaire doit fournir des exemples de résultats de toutes les procédures de diagnostic des composants matériels dédiés à la sécurité. Le commanditaire doit fournir des exemples de toute trace d'audit générée au cours du démarrage ou de l'exploitation.

Tâches de l'évaluateur

E6.37 Vérifier que les informations fournies satisfont à toutes les exigences concernant le contenu, la présentation et les éléments de preuve. Vérifier les exemples d'éléments de preuve exigés pour le démarrage et l'exploitation. Rechercher des erreurs dans les procédures.

5 RESULTATS DE L'EVALUATION

Introduction

5.1 L'évaluation d'une TOE suivant les critères de conformité et d'efficacité exposés dans le présent document fournit une mesure de l'assurance que la TOE va satisfaire à ses objectifs de sécurité. Ceci est indiqué par le niveau d'évaluation atteint et une cotation de la résistance minimum des mécanismes de sécurité de la TOE.

Cotation

5.2 La cotation décernée à une TOE résultant de l'évaluation doit comporter les éléments suivants :

- une référence à la cible de sécurité pour cette TOE, utilisée comme base pour l'évaluation ;

- le niveau d'évaluation obtenu par l'estimation de sa correction et la prise en considération de son efficacité ;

- la cotation confirmée de la résistance minimum des mécanismes de sécurité de la TOE.

5.3 La cible de sécurité doit être spécifiée d'une manière qui convienne à une évaluation par un organisme indépendant, et qui soit en accord avec les critères utilisés pour le niveau d'évaluation présenté et pour le type de TOE.

5.4 Le niveau d'évaluation décerné ne doit être que l'un des niveaux E0, E1, E2, E3, E4, E5 ou E6.

5.5 La cotation confirmée de la résistance minimum des mécanismes ne sera décernée que si la TOE a été évaluée avec succès, c'est à dire n'a pas obtenu le niveau E0. La cotation décernée ne doit être qu'élémentaire, moyenne ou élevée.

5.6 Une TOE qui satisfait à tous les critères de correction pour le niveau d'évaluation qu'elle vise et qui répond à tous les aspects considérés à ce niveau en matière d'efficacité, y compris la résistance minimum des mécanismes annoncée, obtiendra la cotation de ce niveau d'évaluation et de cette résistance minimum des mécanismes.

5.7 Une TOE qui se révèle contenir une vulnérabilité exploitable qui n'a pas pu être éliminée pendant le déroulement de l'évaluation doit être retirée de l'évaluation ou se voir décerner le niveau E0.

5.8 Une TOE qui ne parvient pas à produire des éléments de preuve satisfaisants pour satisfaire aux critères du niveau d'évaluation qu'elle vise mais dans laquelle on n'a pas pu trouver de vulnérabilité exploitable pourra se voir décerner un niveau d'évaluation inférieur, dans lequel les éléments de preuve en question ne sont pas exigés pour satisfaire aux critères de ce niveau. S'il n'y a pas suffisamment de temps et de ressources pour examiner la TOE par rapport à ce niveau plus bas, ou s'il existe des questions sans réponse, la TOE doit soit être retirée de l'évaluation, soit se voir décerner le niveau E0.

5.9 Une TOE échouera à l'évaluation sur la base de l'efficacité seulement si une vulnérabilité exploitable est découverte et non éliminée. Dans ce cas elle doit être retirée de l'évaluation ou se voir décerner le niveau E0.

5.10 Une TOE cotée E0 ne sera pas cotée pour la résistance minimum des mécanismes puisqu'il a été démontré qu'il y a une assurance insuffisante dans la TOE.

5.11 Le rapport élaboré par l'évaluateur, contenant et argumentant les résultats de l'évaluation, doit être présenté sous une forme acceptable pour être pris en considération par l'organisme national approprié de certification.

6 GLOSSAIRE ET REFERENCES

Introduction

6.1 Ce chapitre contient les définitions des termes techniques utilisés avec une signification spécifique à ce document. Les termes techniques utilisés dans le présent document qui ne sont pas définis ici sont employés dans tout le document dans un sens conforme à leur acception courante.

Définitions

Note du Traducteur : à chaque terme sont associés, entre parenthèses, le terme anglais et le numéro du paragraphe correspondant dans la version anglaise.

6.2 **Accréditation** (accreditation - 6.3b) : procédure par laquelle on reconnait à la fois la compétence technique et l'impartialité d'un laboratoire de test pour mener ses tâches particulières.

6.3 **Administrateur** (administrator - 6.5) : personne en contact avec la cible d'évaluation qui est responsable de son maintien en condition d'exploitation.

6.4 **Argumentaire de produit** (product rationale - 6.49) : description des capacités d'un produit en matière de sécurité, donnant les informations nécessaires à un acheteur potentiel pour décider si ce produit va l'aider à satisfaire aux objectifs de sécurité de son système.

6.5 **Assurance** (assurance - 6.7) : confiance qui peut être accordée à la sécurité fournie par une cible d'évaluation.

6.6 **Canal caché** (covert channel - 6.21) : utilisation d'un mécanisme non prévu pour la communication, pour transférer des informations d'une manière qui viole la sécurité.

6.7 **Certification** (certification - 6.12) : délivrance d'une déclaration formelle confirmant les résultats d'une évaluation, et le fait que les critères d'évaluation utilisés ont été correctement appliqués.

6.8 **Cible de sécurité** (security target - 6.63) : spécification de la sécurité qui est exigée d'une cible d'évaluation et qui sert de base pour l'évaluation. La cible de sécurité doit spécifier les fonctions dédiées à la sécurité de la cible d'évaluation. Elle

spécifiera aussi les objectifs de sécurité, les menaces qui pèsent sur ces objectifs ainsi que les mécanismes de sécurité particuliers qui seront employés.

6.9 **Cible d'évaluation** (target of evaluation - 6.71) : système ou produit TI qui est soumis à une évaluation de la sécurité.

6.10 **Classe de fonctionnalité** (functionality class - 6.39) : ensemble prédéfini de fonctions complémentaires dédiées à la sécurité qui peuvent être implémentées dans une cible d'évaluation.

6.11 **Client** (customer - 6.23) : personne ou organisme qui achète une cible d'évaluation.

6.12 **Cohésion de la fonctionnalité** (binding of functionality - 6.11) : aspect de l'estimation de l'efficacité d'une cible d'évaluation qui recouvre la capacité de ses fonctions et mécanismes dédiés à la sécurité à coopérer pour former un ensemble intégré et efficace.

6.13 **Commanditaire** (sponsor - 6.64) : personne ou organisme qui demande une évaluation.

6.14 **Composant** (component - 6.14) : partie identifiable et autonome d'une cible d'évaluation.

6.15 **Composant élémentaire** (basic component - 6.10) : composant identifiable au niveau hiérarchique le plus bas de la spécification produite au cours de la conception détaillée.

6.16 **Conception détaillée** (detailed design - 6.25) : phase du processus de développement dans laquelle la définition de haut niveau et la conception générale d'une cible d'évaluation est affinée et poussée à un niveau de détail qui peut servir de base à la réalisation.

6.17 **Conception générale** (architectural design - 6.6) : phase du processus de développement dans laquelle sont spécifiées la définition et la conception de haut niveau d'une cible d'évaluation.

6.18 **Confidentialité** (confidentiality - 6.15) : prévention de la divulgation non autorisée de l'information.

6.19 **Configuration** (configuration - 6.16) : sélection de l'un des ensembles de combinaisons possibles de caractéristiques d'une cible d'évaluation.

6.20 **Conformité** (correctness - 6.20) : propriété d'une représentation d'une cible d'évaluation qui fait qu'elle reflète exactement la cible de sécurité présentée pour ce système ou ce produit.

6.21 **Construction** (construction - 6.18) : processus de création d'une cible d'évaluation.

6.22 **Cotation** (rating - 6.52) : mesure de l'assurance qui peut être accordée à une cible d'évaluation, consistant en une référence à sa cible de sécurité, un niveau d'évaluation établi après estimation de la conformité de sa réalisation et prise en considération de son efficacité dans le contexte de son exploitation réelle ou prévue, et une cotation confirmée de la résistance minimum de ses mécanismes de sécurité.

6.23 **Dédié à la sécurité** (security enforcing - 6.58) : qui contribue directement à satisfaire aux objectifs de sécurité de la cible d'évaluation.

6.24 **Développeur** (developer - 6.26) : personne ou organisme qui fabrique une cible d'évaluation.

6.25 **Disponibilité** (availability - 6.9) : prévention d'un déni non autorisé d'accès à l'information ou à des ressources.

6.26 **Documentation** (documentation - 6.30) : information écrite (ou autrement enregistrée) concernant une cible d'évaluation exigée pour une évaluation. Cette information peut, mais ce n'est pas impératif, être rassemblée en un seul document constitué dans ce but.

6.27 **Documentation d'administration** (administration documentation - 6.4) : information sur une cible d'évaluation fournie par le développeur à l'usage d'un administrateur.

6.28 **Documentation d'exploitation** (operational documentation - 6.45) : information fournie par le développeur d'une cible d'évaluation pour spécifier et expliquer comment les clients devront l'utiliser.

6.29 **Documentation utilisateur** (user documentation - 6.75) : information sur une cible d'évaluation fournie par le développeur à l'usage de ses utilisateurs finals.

6.30 **Efficacité** (effectiveness - 6.32) : propriété d'une cible d'évaluation qui représente la mesure dans laquelle elle assure la sécurité dans le contexte de son exploitation réelle ou prévue.

6.31 **Environnement de développement** (development environment - 6.28) : ensemble des mesures d'organisation, des procédures et des normes utilisées au cours de la construction d'une cible d'évaluation.

6.32 **Environnement d'exploitation** (operational environment - 6.46) : mesures d'organisation, procédures et normes qui doivent être utilisées au cours de l'exploitation d'une cible d'évaluation.

6.33 **Estimation de la vulnérabilité** (vulnerability assessment - 6.77) : aspect de l'estimation de l'efficacité d'une cible d'évaluation qui recouvre la mesure dans laquelle des vulnérabilités connues dans la cible d'évaluation pourraient compromettre en pratique sa sécurité telle qu'elle est spécifiée dans la cible de sécurité.

6.34 **Evaluateur** (evaluator - 6.35) : personne ou organisme indépendant qui effectue une évaluation.

6.35 **Evaluation** (evaluation - 6.34) : estimation d'un système ou d'un produit TI par rapport à des critères d'évaluation définis.

6.36 **Exigences concernant le contenu et la présentation** (requirements for content and presentation - 6.54) : partie des critères d'évaluation pour une phase ou un aspect particulier de l'évaluation qui explicite ce que chaque élément de documentation identifié comme relevant de cette phase ou de cet aspect doit contenir, et comment les informations qu'il contient doivent être présentées.

6.37 **Exigences concernant les éléments de preuve** (requirements for evidence - 6.55) : partie des critères d'évaluation pour une phase ou un aspect particulier de l'évaluation qui définit la nature des éléments de preuve destinés à montrer que les critères relatifs à cette phase ou à cet aspect sont satisfaits.

6.38 **Exigences concernant les procédures et les normes** (requirements for procedures and standards - 6.56) : partie des critères d'évaluation pour une phase ou un aspect particulier de l'évaluation qui identifie la nature et/ou le contenu des procédures ou des approches normalisées qui doivent être adoptées ou utilisées quand la TOE est en exploitation réelle.

6.39 **Exploitation** (operation - 6.44) : processus d'utilisation d'une cible d'évaluation.

6.40 **Facilité d'emploi** (ease of use - 6.31) : aspect de l'estimation de l'efficacité d'une cible d'évaluation consistant à assurer qu'elle ne peut pas être configurée ou utilisée d'une manière non sûre, mais qu'un administrateur ou un utilisateur final pourrait raisonnablement croire sûre.

6.41 **Gestion de configuration** (configuration control - 6.17) : système de contrôle imposé au changement d'objets sous contrôle, produits au cours des processus de développement, de fabrication et de maintenance d'une cible d'évaluation.

6.42 **Homologation** (accreditation - 6.3a) : procédure de réception d'un système TI destiné à être utilisé dans un environnement particulier.

6.43 **Intégrité** (integrity - 6.41) : prévention d'une modification non autorisée de l'information.

6.44 **Langages de programmation et compilateurs** (programming languages and compilers - 6.51) : outils de l'environnement de développement utilisés dans la construction du logiciel et/ou du microprogramme d'une cible d'évaluation.

6.45 **Livraison** (delivery - 6.24) : processus par lequel une copie de la cible d'évaluation est transférée du développeur à un client.

6.46 **Mécanismes de sécurité** (security mechanism - 6.59) : logique ou algorithme qui implémente par matériel ou logiciel une fonction particulière dédiée à la sécurité ou contribuant à la sécurité.

6.47 **Modèle formel de politique de sécurité** (formal model of security policy - 6.37) : modèle sous-jacent de politique de sécurité exprimé en style formel, c'est à dire une présentation abstraite des principes de sécurité importants qu'une TOE devra faire respecter.

6.48 **Mécanisme critique** (critical mechanism - 6.22) : mécanisme interne d'une cible d'évaluation dont la défaillance créerait une faiblesse dans la sécurité.

6.49 **Menace** (threat - 6.73) : action ou événement susceptible de porter préjudice à la sécurité.

6.50 **Objectifs de sécurité** (security objectives - 6.60) : contribution à la sécurité qu'une cible d'évaluation est destinée à apporter.

6.51 **Objet** (object - 6.42) : entité passive qui contient ou reçoit des informations.

6.52 **Objet de stockage** (storage object - 6.65) : objet qui supporte à la fois des accès en lecture et en écriture [TCSEC].

6.53 **Organisme de certification** (certification body - 6.13) : organisme national indépendant et impartial qui effectue des certifications.

6.54 **Outil** (tool - 6.74) : produit utilisé pour la construction et/ou la documentation d'une cible d'évaluation.

6.55 **Pertinence de la fonctionnalité** (suitability of functionality - 6.68) : aspect de l'estimation de l'efficacité d'une cible d'évaluation qui recouvre la pertinence des fonctions et des mécanismes de sécurité de la cible d'évaluation pour réellement contrer les menaces envers la sécurité de la cible d'évaluation, identifiées dans sa cible de sécurité.

6.56 **Politique de sécurité** (security policy - 6.61) : voir "politique de sécurité interne", "politique de sécurité d'un système", "politique de sécurité technique".

6.57 **Politique de sécurité d'un système** (system security policy - 6.70) : ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique.

6.58 **Politique de sécurité interne** (corporate security policy - 6.19) : ensemble des lois, règles et pratiques qui régissent la façon dont les biens, y compris les informations sensibles, sont gérés, protégés et distribués au sein d'un organisme utilisateur.

6.59 **Politique de sécurité technique** (technical security policy - 6.72) : ensemble des lois, règles et pratiques qui régissent le traitement des informations sensibles et l'utilisation des ressources par le matériel et le logiciel d'un système ou d'un produit TI.

6.60 **Procédure d'exploitation** (operating procedure - 6.43) : ensemble de règles définissant l'emploi correct d'une cible d'évaluation.

6.61 **Procédure de réception** (acceptance procedure - 6.2) : procédure utilisée pour prendre les objets produits au cours des processus de développement, production et maintenance d'une cible d'évaluation et les placer délibérément sous le contrôle d'un système de gestion de configuration.

6.62 **Processus de développement** (development process - 6.29) : ensemble des phases et des tâches par lesquelles une cible d'évaluation est construite et qui traduisent les spécifications en matériel et logiciel réels.

6.63 **Production** (production - 6.50) : processus par lequel des copies d'une cible d'évaluation sont générées pour être distribuées aux clients.

6.64 **Produit** (product - 6.48) : paquetage logiciel et/ou matériel TI qui assure une fonctionnalité conçue pour être utilisée ou incorporée au sein de multiples systèmes.

6.65 **Profil d'assurance** (assurance profile - 6.8) : exigence d'assurance pour une TOE dans laquelle différents degrés de confiance sont exigés pour différentes fonctions dédiées à la sécurité.

6.66 **Réalisation** (implementation - 6.40) : phase du processus de développement dans laquelle la spécification détaillée d'une cible d'évaluation est traduite en matériels et logiciels réels.

6.67 **Résistance des mécanismes** (strength of mechanism - 6.66) : aspect de l'estimation de l'efficacité d'une cible d'évaluation qui recouvre la capacité de ses mécanismes de sécurité à résister à une attaque directe contre des défauts dans les algorithmes, les principes et les propriétés sous-jacents.

6.68 **Sécurité** (security - 6.57) : combinaison de confidentialité, d'intégrité et de disponibilité.

6.69 **Sécurité du développeur** (developer security - 6.27) : ensemble des contrôles de sécurité physiques, organisationnels ou relatifs au personnel, imposés par un développeur à son environnement de développement.

6.70 **Spécification des besoins** (requirements - 6.53) : phase du processus de développement dans laquelle la cible de sécurité d'une cible d'évaluation est produite.

6.71 **Sujet** (subject - 6.67) : entité active, généralement une personne, un processus ou un équipement [TCSEC].

6.72 **Système** (system - 6.69) : installation spécifique de TI, avec un but et un environnement d'exploitation particuliers.

6.73 **Tâches de l'évaluateur** (evaluator actions - 6.36) : partie des critères d'évaluation pour une phase ou un aspect particulier de l'évaluation identifiant ce que l'évaluateur doit faire pour vérifier les informations fournies par le commanditaire de l'évaluation, et les actions complémentaires qu'il doit effectuer.

6.74 **Test de pénétration** (penetration testing - 6.47) : tests effectués par un évaluateur sur une cible d'évaluation pour confirmer si oui ou non les vulnérabilités connues sont réellement exploitables en pratique.

6.75 **Touchant à la sécurité** (security relevant - 6.62) : qui n'est pas dédié à la sécurité, mais qui doit fonctionner correctement pour que la cible d'évaluation puisse faire respecter la sécurité.

6.76 **Unité fonctionnelle** (functional unit - 6.38) : partie d'un composant élémentaire fonctionnellement distincte.

6.77 **Utilisateur final** (end-user - 6.33) : personne en contact avec une cible d'évaluation qui n'utilise que ses capacités opérationnelles.

6.78 **Vulnérabilité** (vulnerability - 6.76) : faiblesse de la sécurité d'une cible d'évaluation (due par exemple à des défauts dans l'analyse, la conception, la réalisation ou l'exploitation).

Références

6.79 (6.78) Dans ce document, il est fait référence aux ouvrages et articles suivants :

AND Computer Security Technology Planning Study
J.P. Anderson
ESD-TR-73-51, ESD/AFSC, US Air Force, Bedford, Mass., October 1972.

BLP Secure Computer Systems : Unified Exposition and Multics Interpretation
D.E.Bell and L.J. LaPadula
Report MTR-2997 Rev. 1, MITRE Corporation, Bedford, MASS, 1976

BNM The Chinese Wall Security Policy
D.F.C. Brewer and M.J. Nash
Proceedings of the IEEE Symposium on Security and Privacy,
Oakland, May 1989, p. 206-214

CESG3 UK Systems Security Confidence Levels, CESG Memorandum No. 3,
Communications-Electronics Security Group, United Kingdom, January 1989.

CWM A Comparison of Commercial and Military Computer Security Policies
D.D. Clark and D.R. Wilson
Proceedings of the IEEE Symposium on Security and Privacy, Oakland,
April 1987, pp. 184-194.

DTIEC DTI Commercial Computer Security Centre Evaluation Levels Manual, V22,
Department of Trade and Industry, United Kingdom, February 1989.

DTIFN DTI Commercial Computer Security Centre Security Functionality Manual, V21
Department of Trade and Industry, United Kingdom, February 1989.

EZBM Mandatory Policy : Secure Systems Model
G. Eizenberg
ONERA/CERT/DERI, Toulouse, France, undated

GYPSY Report on Gypsy 2.05
D.I. Good, R.L. Akers and L.M. Smith
Report ICSCA-CMP-48, University of Texas at Austin, February 1986

IJRM The Ina Jo Specification Language Reference Manual
Unisys Corporation
Culver City, California, United States of America, 1989.

JSD System Development
M.A. Jackson
Prentice-Hall International, 1983.

JSP Principles of Program Design
M.A. Jackson
Academic Press, New-York, 1975.

LOTOS Information Processing Systems - Open Systems Interconnection - LOTOS - A formal Description Technique Based On the Temporal Ordering of Observational Behaviour
International Standard ISO 8807
International Organization for Standardization, 1989.

LWM A Security Model for Military Message Systems
C.E. Landwehr, C.L. Heitmeyer and J. McLean
ACM Transactions on Computer Systems, Vol. 2 No. 3, August 1984, pp. 198-222.

OSI Information Processing Systems - Open Systems Interconnection - Basic Reference Model - part 2 : Security Architecture
International Standard ISO 7498-2
International Organization for Standardization, 1988.

RSL RAISE Specification Language Reference Manual
Raise/CRI/DOC/2/V1

Computer Resources International A/S
Birkerod, Denmark, 1990.

SADT An Introduction to SADT
Structured Analysis and Design Technique
Report 9022-78R
SofTech Inc, 460 Totten Pond Road
Waltham, MA 02154, USA, November 1976.

SCSSI Catalogue de Critères Destinés à évaluer le Degré de Confiance des Systèmes d'Information, 692/SGDN/DISSI/SCSSI
Service Central de la Sécurité des Systèmes d'Information, Juillet 1989.

SSADM The SSADM Manual, ISBN 085-012-527-X
National Computing Centre Limited
Manchester, United Kingdom, 1989.

SSVDM Systematic Software Development Using VDM
C.B. Jones
Prentice Hall International, 1990.

TCSEC Trusted Computer Systems Evaluation Criteria, DOD 5200.28-STD,
Department of Defense, United States of America, December 1985.

YSM A Note on the Yourdon Structured Method
A.J. Bowles
Yourdon Inc
ACM SIGSOFT Software Engineering Notes
Vol. 15 No. 2 April 1990, p. 27.

ZRM The Z Notation : A Reference Manual, ISBN-0-13-983768-X
J.M. Spivey
Prentice Hall International, 1988.

ZSIEC Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems, ISBN 3-88784-200-6,
German Information Security Agency (Bundesamt für Sicherheit in der Informationstechnik), Federal Republic of Germany, January 1989.

Annexe A - EXEMPLES DE CLASSES DE FONCTIONNALITE

Introduction

A.1 Cette annexe présente des exemples de classes prédéfinies, telles que définies au chapitre 2. Ces classes constituent une annexe à ces critères car elles sont données comme exemples, et non comme des classes définitives, à utiliser dans des évaluations réelles. On espère qu'elles vont stimuler le débat sur les exigences réelles des fonctionnalités de sécurité. De fait, le besoin de créer des classes prédéfinies définitives a été largement approuvé lors du processus de consultation qui a précédé la publication de cette version des critères.

A.2 Des travaux sont déjà en cours dans des organismes de normalisation et d'autres organisations industrielles pour développer des normes pour des fonctionnalités de sécurité dans des contextes spécifiques. On s'attend à ce que de tels travaux produisent des définitions de fonctionnalités de sécurité qui feront autorité et qui pourront être adaptées pour être utilisées avec ces critères et incluses ou mises en référence dans la prochaine version définitive de ce document.

A.3 Les présents exemples fournissent une référence de base et montrent comment des classes prédéfinies peuvent être tirées des critères existants : de fait, ces classes ont été adaptées avec un minimum de modification du [ZSIEC].

A.4 Chaque classe consiste en une présentation des objectifs, suivie par les exigences présentées dans des rubriques génériques appropriées. L'absence d'une rubrique générique dans la description d'une classe donnée signifie qu'il n'existe aucune exigence pour cette rubrique. Les classes F-B2 et F-B3 contiennent en outre des informations complémentaires qu'il est nécessaire d'inclure dans une cible de sécurité ; ces informations spécifient les mécanismes par mandats exigés pour la compatibilité avec le TCSEC.

A.5 Les cinq exemples de classes de fonctionnalité F-C1, F-C2, F-B1, F-B2, et F-B3 forment une hiérarchie puisqu'elles sont issues des exigences fonctionnelles des classes hiérarchiques du TCSEC. Dans la description de ces classes, les parties de chaque classe qui sont nouvelles ou qui ont été changées par rapport aux classes précédentes sont imprimées en gras.

A.6 D'autres classes de fonctionnalité basées sur une hiérarchie pourront être créées dans le futur, par des organismes de normalisation et des organisations industrielles, pour aborder d'autres types d'objectifs de sécurité (par exemple pour l'intégrité et la disponibilité). En attendant, les classes F-IN, F-AV, F-DI, F-DC, et

F-DX ont été incluses pour illustrer la large gamme d'exigences de sécurité qui peuvent être exprimées sous la forme d'une classe de fonctionnalité prédéfinie.

Exemple de classe de fonctionnalité : F-C1

Objectif

A.7 L'exemple de classe F-C1 est dérivé des exigences fonctionnelles de la classe C1 du TCSEC américain. Elle offre un contrôle d'accès discrétionnaire ("besoin d'en connaître").

Identification et authentification

A.8 La TOE doit identifier et authentifier les utilisateurs. L'identification et l'authentification doivent avoir lieu avant toute autre interaction entre la TOE et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies. Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles par des utilisateurs autorisés.

Contrôle d'accès

A.9 La TOE doit pouvoir distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur individuel, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. Il doit être possible de refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet. Il ne doit pas être possible à quelqu'un qui n'est pas un utilisateur autorisé d'accorder ou de retirer des droits d'accès à un objet.

A.10 Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande. Les tentatives d'accès non autorisé doivent être rejetées.

Exemple de classe de fonctionnalité : F-C2

Objectif

A.11 **L'exemple de classe F-C2 est dérivé des exigences fonctionnelles de la classe C2 du TCSEC américain. Elle offre un contrôle d'accès discrétionnaire plus fin que la classe C1, en rendant les utilisateurs individuellement responsables de leurs actions à travers des procédures d'identification, l'audit des événements relatifs à la sécurité et l'isolation des ressources.**

Identification et authentification

A.12 La TOE doit identifier et authentifier **de façon unique** les utilisateurs. L'identification et l'authentification doivent avoir lieu avant toute autre interaction entre la TOE et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies. Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles par des utilisateurs autorisés. **Pour chaque interaction, la TOE doit pouvoir établir l'identité de l'utilisateur.**

Contrôle d'accès

A.13 La TOE doit pouvoir distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur individuel, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. Il doit être possible de refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet. **Il doit également être possible de limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas cet objet. Il doit être possible d'accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel.** Il ne doit pas être possible à quelqu'un qui n'est pas un utilisateur autorisé d'accorder ou de retirer des droits d'accès à un objet. **L'administration des droits doit disposer de contrôles pour limiter la propagation des droits d'accès. De même, seuls des utilisateurs autorisés doivent pouvoir introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.**

A.14 Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande. Les tentatives d'accès non autorisé doivent être rejetées.

Imputabilité

A.15 **La TOE doit comporter un composant d'imputation qui soit capable, pour chacun des événements suivants, d'enregistrer cet événement avec les données exigées :**

a) **Utilisation du mécanisme d'identification et d'authentification :**

Données exigées : Date ; heure ; identité fournie par l'utilisateur ; identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé (par exemple identificateur du terminal) ; réussite ou échec de la tentative.

b) **Actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits :**

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de la tentative d'accès ; réussite ou échec de la tentative.

c) **Création ou suppression d'un objet soumis à l'administration des droits :**

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de l'action.

d) **Actions d'utilisateurs autorisés affectant la sécurité de la TOE :**

Données exigées : Date ; heure ; identité de l'utilisateur ; type de l'action ; nom de l'objet sur lequel porte l'action (de telles actions sont l'introduction ou la suppression (suspension) d'utilisateurs ; l'introduction ou le retrait de supports de stockage ; le démarrage ou l'arrêt de la TOE).

A.16 **Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation. Il doit être possible de mettre sélectivement en oeuvre l'imputation pour un ou plusieurs utilisateurs. Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.**

Audit

A.17 **Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.**

Réutilisation d'objet

A.18 **Tous les objets de stockage rendus à la TOE doivent, avant d'être réutilisés par d'autres sujets, être traités d'une manière telle qu'aucune conclusion ne puisse être tirée concernant leur contenu précédent.**

Exemple de classe de fonctionnalité : F-B1

Objectif

A.19 **L'exemple de classe F-B1 est dérivé des exigences fonctionnelles de la classe B1 du TCSEC américain. En plus du contrôle d'accès discrétionnaire, elle introduit des fonctions pour maintenir des marques de sensibilité et les utilise pour faire respecter un ensemble de règles de contrôle d'accès par mandats à tous les sujets et à tous les objets de stockage sous son contrôle. Il est possible d'attribuer de façon précise un label aux informations exportées.**

Identification et authentification

A.20 La TOE doit identifier et authentifier de façon unique les utilisateurs. L'identification et l'authentification doivent avoir lieu avant toute autre interaction entre la TOE et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies. Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles par des utilisateurs autorisés. Pour chaque interaction, la TOE doit pouvoir établir l'identité de l'utilisateur.

Contrôle d'accès

A.21 La TOE doit pouvoir distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur individuel, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux. Il doit être possible de refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet. Il doit également être possible de limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas cet objet. Il doit être possible d'accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel. Il ne doit pas être possible à quelqu'un qui n'est pas un utilisateur autorisé d'accorder ou de retirer des droits d'accès à un objet. L'administration des droits doit disposer de contrôles pour limiter la propagation des droits d'accès. De même, seuls des utilisateurs autorisés doivent pouvoir introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.

A.22 **En outre, la TOE doit donner des attributs à tous les sujets et à tous les objets de stockage sous son contrôle (par exemple les processus, les fichiers, les segments de mémoire, les dispositifs). Les valeurs de ces attributs doivent servir de base pour**

les droits d'accès par mandats. Des règles doivent spécifier quelles combinaisons de valeurs d'attributs d'un sujet et d'un objet sont nécessaires pour que l'accès à cet objet soit accordé au sujet.

A.23 **Lorsqu'un objet est exporté, ses attributs doivent être exportés d'une manière telle que celui qui les reçoit puisse reconstituer leur valeur sans ambiguïté.**

A.24 **Les droits d'accès par mandats doivent être conçus de telle manière que le cas spécial suivant puisse être réalisé :**

L'attribut comprend deux parties : la première peut prendre des valeurs ordonnées hiérarchiquement, la seconde représente un ensemble. (Dans le domaine gouvernemental, la première partie contient des classifications, par exemple non classifié, confidentiel, secret, très secret. La seconde contient des catégories.)

On dit qu'un attribut A domine un attribut B si :

la première partie de A est hiérarchiquement supérieure ou égale à la première partie de B, et la deuxième partie de B est un sous-ensemble de la deuxième partie de A ou lui est égale.

A.25 **Les règles suivantes doivent être imposées :**

a) **L'accès en lecture d'un sujet à un objet n'est autorisé que si l'attribut du sujet domine celui de l'objet ;**

b) **L'accès en écriture d'un sujet à un objet n'est autorisé que si l'attribut de l'objet domine celui du sujet.**

A.26 **Les attributs d'un sujet créé pour agir au nom d'un utilisateur doivent être dominés par l'habilitation et l'autorisation de cet utilisateur telles qu'elles ont été déterminées au moment de l'identification et de l'authentification. Si les données importées n'ont pas d'attribut, un utilisateur autorisé doit pouvoir leur en assigner.**

A.27 **Chaque canal d'exportation doit pouvoir être identifié comme étant soit à niveau unique, soit multi-niveau. Il doit être impossible de transmettre ou de recevoir des données par des canaux désignés comme étant à niveau unique, à moins que les attributs de ces données ne correspondent à un attribut préspécifié déterminé. Les données transmises ou reçues par un canal à niveau unique doivent être communiquées avec un attribut correspondant, sauf s'il est possible à un utilisateur autorisé de spécifier l'attribut du canal d'une façon qui ne puisse pas être imitée. Dans ce cas, l'attribut des données est implicitement spécifié par l'attribut du canal.**

A.28 **Pour les canaux multi-niveaux, le protocole de communication doit garantir que le destinataire pourra complètement et sans ambiguïté reconstituer et mettre en correspondance les données et les attributs reçus.**

A.29 **Des utilisateurs non autorisés ne doivent pas pouvoir modifier les attributs d'un canal qui touchent à la sécurité. Il ne doit pas être possible de modifier ces attributs sans que la modification soit effectuée explicitement.**

A.30 **La TOE doit marquer les sorties lisibles par l'homme avec des valeurs d'attribut. Les valeurs d'attribut doivent être déterminées suivant les règles établies dans la TOE. Des utilisateurs autorisés doivent pouvoir spécifier le libellé imprimable de chaque valeur d'attribut.**

A.31 Lors de toute tentative d'un utilisateur ou groupe d'utilisateurs pour accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande. Les tentatives d'accès sans autorisation doivent être rejetées. **Les valeurs des attributs doivent servir de base aux décisions concernant le contrôle d'accès par mandats. Les règles doivent spécifier sans ambiguïté quand un sujet est autorisé à avoir accès à un objet ainsi protégé. Si des droits d'accès discrétionnaires sont aussi attribués à un objet, l'accès ne doit être autorisé qu'à condition que les droits d'accès par mandats et discrétionnaires le permettent tous les deux.**

Imputabilité

A.32 La TOE doit comporter un composant d'imputation qui soit capable, pour chacun des événements suivants, d'enregistrer cet événement avec les données exigées :

a) Utilisation du mécanisme d'identification et d'authentification :

Données exigées : Date ; heure ; identité fournie par l'utilisateur ; identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé (par exemple identificateur du terminal) ; réussite ou échec de la tentative ; **autorisation de l'utilisateur**.

b) Actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits :

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de la tentative d'accès ; réussite ou échec de la tentative ; **attribut de l'objet**.

c) Création ou suppression d'un objet soumis à l'administration des droits :

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de l'action ; **attribut de l'objet**.

d) Actions d'utilisateurs autorisés affectant la sécurité de la TOE :

Données exigées : Date ; heure ; identité de l'utilisateur ; type de l'action ; nom **et attribut** de l'objet sur lequel porte l'action (de telles actions sont l'introduction ou la suppression (suspension) d'utilisateurs ; l'introduction ou le retrait de supports de stockage ; le démarrage ou l'arrêt de la TOE ; **l'assignation d'un attribut ; la modification des attributs, des marques ou de la classification d'un canal**).

A.33 Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation. Il doit être possible de mettre sélectivement en oeuvre l'imputation pour un ou plusieurs utilisateurs. Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

Audit

A.34 Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

Réutilisation d'objet

A.35 Tous les objets de stockage rendus à la TOE doivent, avant d'être réutilisés par d'autres sujets, être traités d'une manière telle qu'aucune conclusion ne puisse être tirée concernant leur contenu précédent.

Exemple de classe de fonctionnalité : F-B2

Objectif

A.36 **L'exemple de classe F-B2 est dérivé des exigences fonctionnelles de la classe B2 du TCSEC américain. Elle étend le contrôle d'accès par mandats à tous les sujets et objets et renforce les exigences d'authentification de la classe B1.**

Mécanismes obligatoires

A.37 **Cette classe exige que le contrôle d'accès soit implémenté à l'aide d'un mécanisme de validation à référence unique qui implémente le concept de moniteur de référence, c'est à dire que le mécanisme doit être résistant à l'intrusion, systématiquement utilisé et suffisamment petit (ayant une organisation suffisamment simple et une complexité suffisamment faible) pour être soumis à une analyse et à des tests dont la complétude puisse être assurée.**

Identification et authentification

A.38 La TOE doit identifier et authentifier de façon unique les utilisateurs. L'identification et l'authentification doivent avoir lieu avant toute autre interaction entre la TOE et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies. Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles par des utilisateurs autorisés. **L'identification et l'authentification doivent être traitées à travers un chemin de confiance entre l'utilisateur et la TOE initialisé par l'utilisateur.** Pour chaque interaction, la TOE doit pouvoir établir l'identité de l'utilisateur.

Contrôle d'accès

A.39 La TOE doit pouvoir distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur individuel, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. **Il doit être possible de regrouper des droits d'accès pour servir de base à des rôles. Au minimum, doivent pouvoir être définis les rôles d'opérateur de la TOE et d'administrateur de la TOE.** Il doit être possible de refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet. Il doit être également possible de limiter l'accès d'un utilisateur à un objet aux seules

opérations qui ne modifient pas cet objet. Il doit être possible d'accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel.

A.40 Il ne doit pas être possible à quelqu'un qui n'est pas un utilisateur autorisé d'accorder ou de retirer des droits d'accès à un objet. L'administration des droits doit disposer de contrôles pour limiter la propagation des droits d'accès. De même, seuls des utilisateurs autorisés doivent pouvoir introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.

A.41 En outre, la TOE doit donner des attributs à tous les sujets et à tous les **objets** (par exemple les processus, les fichiers, les segments de mémoire, les dispositifs). Les valeurs de ces attributs doivent servir de base pour les droits d'accès par mandats. Des règles doivent spécifier quelles combinaisons de valeurs d'attributs d'un sujet et d'un objet sont nécessaires pour que l'accès à cet objet soit accordé au sujet.

A.42 Lorsqu'un objet est exporté, ses attributs doivent être exportés d'une manière telle que celui qui les reçoit puisse reconstituer leur valeur sans ambiguïté.

A.43 Les droits d'accès par mandats doivent être conçus de telle manière que le cas spécial suivant puisse être réalisé :

L'attribut comprend deux parties : la première peut prendre des valeurs ordonnées hiérarchiquement, la seconde représente un ensemble. (Dans le domaine gouvernemental, la première partie contient des classifications, par exemple non classifié, confidentiel, secret, très secret. La seconde contient des catégories.)

On dit qu'un attribut A domine un attribut B si :

la première partie de A est hiérarchiquement supérieure ou égale à la première partie de B, et la deuxième partie de B est un sous-ensemble de la deuxième partie de A ou lui est égale.

A.44 Les règles suivantes doivent être imposées :

a) L'accès en lecture d'un sujet à un objet n'est autorisé que si l'attribut du sujet domine celui de l'objet ;

b) L'accès en écriture d'un sujet à un objet n'est autorisé que si l'attribut de l'objet domine celui du sujet.

A.45 Les attributs d'un sujet créé pour agir au nom d'un utilisateur doivent être dominés par l'habilitation et l'autorisation de cet utilisateur telles qu'elles ont été

déterminées au moment de l'identification et de l'authentification. Si les données importées n'ont pas d'attribut, un utilisateur autorisé doit pouvoir leur en assigner.

A.46 Chaque canal d'exportation doit pouvoir être identifié comme étant soit à niveau unique, soit multi-niveau. Il doit être impossible de transmettre ou de recevoir des données par des canaux désignés comme étant à niveau unique, à moins que les attributs de ces données ne correspondent à un attribut préspécifié déterminé. Les données transmises ou reçues par un un canal à niveau unique doivent être communiquées avec un attribut correspondant, sauf s'il est possible à un utilisateur autorisé de spécifier l'attribut du canal d'une façon qui ne puisse pas être imitée. Dans ce cas, l'attribut des données est implicitement spécifié par l'attribut du canal.

A.47 Pour les canaux multi-niveaux, le protocole de communication doit garantir que le destinataire pourra complètement et sans ambiguïté reconstituer et mettre en correspondance les données et les attributs reçus. **Pour les canaux multi-niveaux, il doit être possible de déclarer les attributs maximums et minimums. Aucune donnée ne doit être transmise par un canal multi-niveau à moins que l'attribut de cette donnée domine l'attribut minimum du canal et qu'il soit dominé par l'attribut maximum du canal.**

A.48 Des utilisateurs non autorisés ne doivent pas pouvoir modifier les attributs d'un canal qui touchent à la sécurité. Il ne doit pas être possible de modifier ces attributs sans que la modification soit effectuée explicitement.

A.49 La TOE doit marquer les sorties lisibles par l'homme avec des valeurs d'attribut. Les valeurs d'attribut doivent être déterminées suivant les règles établies dans la TOE. Des utilisateurs autorisés doivent pouvoir spécifier le libellé imprimable de chaque valeur d'attribut.

A.50 **Un utilisateur doit être informé immédiatement de toute modification apportée au niveau de sécurité qui lui est associé pendant une session interactive. L'utilisateur doit pouvoir à tout moment passer en revue tous les attributs du sujet.**

A.51 Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande. Les tentatives d'accès non autorisé doivent être rejetées. Les valeurs des attributs doivent servir de base aux décisions concernant le contrôle d'accès par mandats. Les règles doivent spécifier sans ambiguïté quand un sujet est autorisé à avoir accès à un objet ainsi protégé. Si des droits d'accès discrétionnaires sont aussi attribués à un objet, l'accès ne doit être autorisé qu'à condition que les droits d'accès par mandats et discrétionnaires le permettent tous les deux.

A.52 **Il ne doit exister aucun canal de stockage connu qui puisse transférer de l'information entre des processus sans vérification de droits d'accès (c'est à dire de façon cachée) et qui ait une bande passante maximum (déterminée par des mesures réelles ou par une estimation technique) d'un niveau inacceptable. (Se référer au guide pour les canaux cachés du TCSEC [TCSEC] pour les indications d'acceptabilité.)**

Imputabilité

A.53 La TOE doit comporter un composant d'imputation qui soit capable, pour chacun des événements suivants, d'enregistrer cet événement avec les données exigées :

a) Utilisation du mécanisme d'identification et d'authentification :

Données exigées : Date ; heure ; identité fournie par l'utilisateur ; identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé (par exemple identificateur du terminal) ; réussite ou échec de la tentative ; autorisation de l'utilisateur.

b) Actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits :

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de la tentative d'accès ; réussite ou échec de la tentative ; attribut de l'objet.

c) Création ou suppression d'un objet soumis à l'administration des droits :

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de l'action ; attribut de l'objet.

d) Actions d'utilisateurs autorisés affectant la sécurité de la TOE :

Données exigées : Date ; heure ; identité de l'utilisateur ; type de l'action ; nom et attribut de l'objet sur lequel porte l'action (de telles actions sont l'introduction ou la suppression (suspension) d'utilisateurs ; l'introduction ou le retrait de supports de stockage ; le démarrage ou l'arrêt de la TOE ; l'assignation d'un attribut ; la modification des attributs, des marques ou de la classification d'un canal).

A.54 Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation. Il doit être possible de mettre sélectivement en oeuvre l'imputation pour un ou

plusieurs utilisateurs. Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

Audit

A.55 Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs. **En outre, la TOE doit être capable d'auditer les événements connus qui pourraient être utilisés de façon malveillante pour permettre un flux non autorisé d'informations par exploitation de canaux cachés.**

Réutilisation d'objet

A.56 Tous les objets de stockage rendus à la TOE doivent, avant d'être réutilisés par d'autres sujets, être traités d'une manière telle qu'aucune conclusion ne puisse être tirée concernant leur contenu précédent.

Exemple de classe de fonctionnalité : F-B3

Objectif

A.57 **L'exemple de classe F-B3 est dérivé des exigences fonctionnelles des classes B3 et A1 du TCSEC américain. En plus des fonctions de la classe B2, elle fournit des fonctions pour permettre la mise en oeuvre de rôles distincts d'administration de la sécurité, et l'audit est étendu pour signaler les événements touchant à la sécurité.**

Mécanismes obligatoires

A.58 Cette classe exige que le contrôle d'accès soit implémenté à l'aide d'un mécanisme de validation à référence unique qui implémente le concept de moniteur de référence, c'est à dire que le mécanisme doit être résistant à l'intrusion, systématiquement utilisé et suffisamment petit (ayant une organisation suffisamment simple et une complexité suffisamment faible) pour être soumis à une analyse et à des tests dont la complétude puisse être assurée.

Identification et authentification

A.59 La TOE doit identifier et authentifier de façon unique les utilisateurs. L'identification et l'authentification doivent avoir lieu avant toute autre interaction entre la TOE et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies. Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles par des utilisateurs autorisés. L'identification et l'authentification doivent être traitées à travers un chemin de confiance entre l'utilisateur et la TOE initialisé par l'utilisateur **ou par la TOE**. Pour chaque interaction, la TOE doit pouvoir établir l'identité de l'utilisateur.

Contrôle d'accès

A.60 La TOE doit pouvoir distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur individuel, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. Il doit être possible de regrouper des droits d'accès pour servir de base à des rôles. Au minimum, doivent pouvoir être définis les rôles d'opérateur de la TOE et d'administrateur de la TOE. **Les rôles d'opérateur de la TOE, d'administrateur de la TOE et d'officier de sécurité de la TOE doivent être séparés.**

Il doit être possible de refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet. Il doit également être possible de limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas cet objet. Il doit être possible d'accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel. Il ne doit pas être possible à quelqu'un qui n'est pas un utilisateur autorisé d'accorder ou de retirer des droits d'accès à un objet.

A.61 **Pour chaque objet soumis à l'administration des droits, il doit être possible de fournir une liste d'utilisateurs et une liste de groupes d'utilisateurs avec leurs droits sur cet objet. De plus, pour chacun de ces objets, il doit aussi être possible de fournir une liste des utilisateurs et une liste des groupes d'utilisateurs auxquels l'accès à cet objet est interdit.** L'administration des droits doit disposer de contrôles pour limiter la propagation des droits d'accès. De même, seuls des utilisateurs autorisés doivent pouvoir introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.

A.62 En outre, la TOE doit donner des attributs à tous les sujets et à tous les objets (par exemple les processus, les fichiers, les segments de mémoire, les dispositifs). Les valeurs de ces attributs doivent servir de base pour les droits d'accès par mandats. Des règles doivent spécifier quelles combinaisons de valeurs d'attributs d'un sujet et d'un objet sont nécessaires pour que l'accès à cet objet soit accordé au sujet.

A.63 Lorsqu'un objet est exporté, ses attributs doivent être exportés d'une manière telle que celui qui les reçoit puisse reconstituer leur valeur sans ambiguïté.

A.64 Les droits d'accès par mandats doivent être conçus de telle manière que le cas spécial suivant puisse être réalisé :

L'attribut comprend deux parties : la première peut prendre des valeurs ordonnées hiérarchiquement, la seconde représente un ensemble. (Dans le domaine gouvernemental, la première partie contient des classifications, par exemple non classifié, confidentiel, secret, très secret. La seconde contient des catégories.)

On dit qu'un attribut A domine un attribut B si :

la première partie de A est hiérarchiquement supérieure ou égale à la première partie de B, et la deuxième partie de B est un sous-ensemble de la deuxième partie de A ou lui est égale.

A.65 Les règles suivantes doivent être imposées :

a) L'accès en lecture d'un sujet à un objet n'est autorisé que si l'attribut du sujet domine celui de l'objet ;

b) L'accès en écriture d'un sujet à un objet n'est autorisé que si l'attribut de l'objet domine celui du sujet.

A.66 Les attributs d'un sujet créé pour agir au nom d'un utilisateur doivent être dominés par l'habilitation et l'autorisation de cet utilisateur telles qu'elles ont été déterminées au moment de l'identification et de l'authentification. Si les données importées n'ont pas d'attribut, un utilisateur autorisé doit pouvoir leur en assigner.

A.67 Chaque canal d'exportation doit pouvoir être identifié comme étant soit à niveau unique, soit multi-niveau. Il doit être impossible de transmettre ou de recevoir des données par des canaux désignés comme étant à niveau unique, à moins que les attributs de ces données ne correspondent à un attribut préspécifié déterminé. Les données transmises ou reçues par un un canal à niveau unique doivent être communiquées avec un attribut correspondant, sauf s'il est possible à un utilisateur autorisé de spécifier l'attribut du canal d'une façon qui ne puisse pas être imitée. Dans ce cas, l'attribut des données est implicitement spécifié par l'attribut du canal.

A.68 Pour les canaux multi-niveaux, le protocole de communication doit garantir que le destinataire pourra complètement et sans ambiguïté reconstituer et mettre en correspondance les données et les attributs reçus. Pour les canaux multi-niveaux, il doit être possible de déclarer les attributs maximums et minimums. Aucune donnée ne doit être transmise par un canal multi-niveau à moins que l'attribut de cette donnée domine l'attribut minimum du canal et qu'il soit dominé par l'attribut maximum du canal.

A.69 Des utilisateurs non autorisés ne doivent pas pouvoir modifier les attributs d'un canal qui touchent à la sécurité. Il ne doit pas être possible de modifier ces attributs sans que la modification soit effectuée explicitement.

A.70 La TOE doit marquer les sorties lisibles par l'homme avec des valeurs d'attribut. Les valeurs d'attribut doivent être déterminées suivant les règles établies dans la TOE. Des utilisateurs autorisés doivent pouvoir spécifier le libellé imprimable de chaque valeur d'attribut.

A.71 Un utilisateur doit être informé immédiatement de toute modification apportée au niveau de sécurité qui lui est associé pendant une session interactive. L'utilisateur doit pouvoir à tout moment passer en revue tous les attributs du sujet.

A.72 Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la

demande. Les tentatives d'accès non autorisé doivent être rejetées. Les valeurs des attributs doivent servir de base aux décisions concernant le contrôle d'accès par mandats. Les règles doivent spécifier sans ambiguïté quand un sujet est autorisé à avoir accès à un objet ainsi protégé. Si des droits d'accès discrétionnaires sont aussi attribués à un objet, l'accès ne doit être autorisé qu'à condition que les droits d'accès par mandats et discrétionnaires le permettent tous les deux.

A.73 Il ne doit exister aucun canal connu de stockage **ou de séquencement** qui puisse transférer de l'information entre des processus sans vérification de droits d'accès (c'est à dire de façon cachée) et qui ait une bande passante maximum (déterminée par des mesures réelles ou par une estimation technique) d'un niveau inacceptable. (Se référer au guide pour les canaux cachés du TCSEC [TCSEC] pour les indications d'acceptabilité.)

Imputabilité

A.74 La TOE doit comporter un composant d'imputation qui soit capable, pour chacun des événements suivants, d'enregistrer cet événement avec les données exigées :

a) Utilisation du mécanisme d'identification et d'authentification :

Données exigées : Date ; heure ; identité fournie par l'utilisateur ; identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé (par exemple identificateur du terminal) ; réussite ou échec de la tentative ; autorisation de l'utilisateur.

b) Actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits :

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de la tentative d'accès ; réussite ou échec de la tentative ; attribut de l'objet.

c) Création ou suppression d'un objet soumis à l'administration des droits :

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de l'action ; attribut de l'objet.

d) Actions d'utilisateurs autorisés affectant la sécurité de la TOE :

Données exigées : Date ; heure ; identité de l'utilisateur ; type de l'action ; nom et attribut de l'objet sur lequel porte l'action (de telles actions sont

l'introduction ou la suppression (suspension) d'utilisateurs ; l'introduction ou le retrait de supports de stockage ; le démarrage ou l'arrêt de la TOE ; l'assignation d'un attribut ; la modification des attributs, des marques ou de la classification d'un canal).

A.75 Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation. Il doit être possible de mettre sélectivement en oeuvre l'imputation pour un ou plusieurs utilisateurs. Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

Audit

A.76 Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs. En outre, la TOE doit être capable d'auditer les événements connus qui pourraient être utilisés de façon malveillante pour permettre un flux non autorisé d'informations par exploitation de canaux cachés.

A.77 **De plus, il doit exister un mécanisme pour surveiller l'apparition d'événements qui, soit touchent particulièrement à la sécurité, soit, en raison de leur fréquence, peuvent devenir une menace critique pour la sécurité de la TOE. Ce mécanisme doit pouvoir notifier sans délai à un utilisateur particulier ou ayant un rôle particulier l'apparition de tels événements. Le mécanisme doit mettre en oeuvre l'action la moins perturbatrice pour mettre fin à de tels événements.**

Réutilisation d'objet

A.78 Tous les objets de stockage rendus à la TOE doivent, avant d'être réutilisés par d'autres sujets, être traités d'une manière telle qu'aucune conclusion ne puisse être tirée concernant leur contenu précédent.

Exemple de classe de fonctionnalité : F-IN

Objectif

A.79 L'exemple de classe de fonctionnalité F-IN concerne les TOE pour lesquelles il y a des exigences élevées d'intégrité pour les données et les programmes. De telles exigences peuvent être nécessaires par exemple pour des TOE bases de données.

Identification et authentification

A.80 La TOE doit identifier et authentifier de façon unique les utilisateurs. L'identification et l'authentification doivent avoir lieu avant toute autre interaction entre la TOE et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies. Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles pour consultation ou modification par des utilisateurs autorisés. Pour chaque interaction, la TOE doit pouvoir établir l'identité de l'utilisateur.

Contrôle d'accès

A.81 La TOE doit pouvoir distinguer et administrer les droits d'accès des utilisateurs, des rôles et des processus aux objets désignés explicitement (le terme rôle désigne des utilisateurs qui ont des attributs spéciaux). Il doit être possible de restreindre l'accès des utilisateurs à ces objets d'une façon telle que cet accès ne soit possible que par l'intermédiaire de processus établis spécialement. De plus, il doit être possible d'affecter des objets à un type prédéfini. Il doit aussi être possible de spécifier pour chaque type d'objet quels sont les utilisateurs, les rôles ou les processus qui peuvent disposer de certains types d'accès à ces objets. Cela devrait permettre de limiter l'accès des utilisateurs aux objets d'un certain type d'une façon telle que cet accès ne soit possible que par l'intermédiaire de processus définis et fixés. Il ne devrait être possible qu'aux utilisateurs autorisés de définir des types nouveaux, d'accorder ou de retirer des droits d'accès à des types. Ces actions doivent être initialisées explicitement par ces utilisateurs. Pour ces actions, toute communication entre l'utilisateur et la TOE doit se faire à travers un chemin de confiance.

A.82 Les droits d'accès minimum suivants doivent exister : lecture, écriture, ajout, suppression, renommage (pour tous les objets), exécution, suppression, renommage (pour les objets exécutables), création d'objets d'un certain type, suppression d'objets d'un certain type.

A.83 Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande. Les tentatives d'accès non autorisé doivent être rejetées.

Imputabilité

A.84 La TOE doit comporter un composant d'imputation qui soit capable, pour chacun des événements suivants, d'enregistrer cet événement avec les données exigées :

a) Utilisation du mécanisme d'identification et d'authentification :

Données exigées : Date ; heure ; identité fournie par l'utilisateur ; identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé (par exemple identificateur du terminal) ; réussite ou échec de la tentative.

b) Actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits :

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de la tentative d'accès ; réussite ou échec de la tentative.

c) Création ou suppression d'un objet soumis à l'administration des droits :

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de l'action.

d) Actions d'utilisateurs autorisés affectant la sécurité de la TOE :

Données exigées : Date ; heure ; identité de l'utilisateur ; type de l'action ; nom et attribut de l'objet sur lequel porte l'action (de telles actions sont l'introduction ou la suppression (suspension) d'utilisateurs ; l'introduction ou le retrait de supports de stockage ; le démarrage ou l'arrêt de la TOE).

e) Définition ou suppression de types :

Données exigées : Date ; heure ; identité de l'utilisateur ; type de l'action ; nom du type.

f) Assignation d'un type à un objet :

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; nom du type.

g) Attribution ou révocation de droits d'accès à un objet ou un type d'objet :

Données exigées : Date ; heure ; identité de l'utilisateur ; type de l'action ; type du droit d'accès ; nom du sujet ; nom de l'objet ou nom du type d'objet.

A.85 Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation. Il doit être possible de mettre sélectivement en oeuvre l'imputation pour un ou plusieurs utilisateurs. Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs. La structure des enregistrements d'imputation doit être décrite de façon complète.

Audit

A.86 Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

Exemple de classe de fonctionnalité : F-AV

Objectif

A.87 La classe de fonctionnalité F-AV impose des exigences élevées pour la disponibilité d'une TOE complète ou de fonctions particulières d'une TOE. De telles exigences sont importantes par exemple pour des TOE qui contrôlent des processus industriels.

Fiabilité de service

A.88 La TOE doit être capable de se rétablir à la suite d'une panne de certains composants matériels individuels (par exemple une carte d'un processeur particulier dans une TOE multiprocesseur) de façon telle que toutes les fonctions exigées en permanence restent constamment disponibles dans le reste de la TOE. Après réparation du composant défaillant, il doit être possible de le réintégrer dans la TOE de façon telle que la continuité de l'exploitation des fonctions exigées en permanence soit assurée. A la suite de cette réintégration, la TOE doit retrouver son degré originel de tolérance aux pannes. La durée maximum de tels processus de réintégration doit être déclarée.

A.89 A tout moment et quelle que soit sa charge, la TOE doit pouvoir garantir un temps de réponse maximum pour certaines actions spécifiées. De plus, pour certaines actions spécifiées, il doit être garanti que la TOE ne sera pas sujette à une étreinte fatale.

Exemple de classe de fonctionnalité : F-DI

Objectif

A.90 L'exemple de classe de fonctionnalité F-DI impose des exigences élevées en ce qui concerne la préservation de l'intégrité des données au cours de leur échange.

Identification et authentification

A.91 La TOE doit identifier et authentifier de façon unique les utilisateurs. L'identification et l'authentification doivent avoir lieu avant toute autre interaction entre la TOE et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies. Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles pour consultation ou modification par des utilisateurs autorisés. Pour chaque interaction, la TOE doit pouvoir établir l'identité de l'utilisateur.

A.92 Avant l'établissement d'une connexion, l'entité homologue (ordinateur, processus ou utilisateur) doit être identifiée et authentifiée de façon unique. Les données de l'utilisateur ne doivent être échangées qu'après que l'identification et l'authentification ont été effectuées avec succès. A la réception de données, il doit être possible d'identifier et d'authentifier de façon unique leur émetteur. Toutes les informations d'authentification doivent être protégées contre un accès non autorisé ou une contrefaçon.

Imputabilité

A.93 La TOE doit comporter un composant d'imputation qui soit capable, pour chacun des événements suivants, d'enregistrer cet événement avec les données exigées :

a) Utilisation du mécanisme d'identification et d'authentification :

Données exigées : Date ; heure ; initiateur de l'identification et de l'authentification ; nom du sujet à identifier ; réussite ou échec de l'action.

b) Erreurs identifiées pendant l'échange de données :

Données exigées : Date ; heure ; entité homologue dans l'échange de données ; nature de l'erreur ; réussite ou échec de la tentative de correction.

c) Echange de données :

Données exigées : Date ; heure ; identité de l'utilisateur initiateur ; nom de l'entité homologue (ordinateur, processus ou utilisateur) ; paramètres d'établissement de la connexion (s'ils varient).

A.94 Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation. Il doit être possible de mettre sélectivement en oeuvre l'imputation pour un ou plusieurs utilisateurs. Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs. La structure des enregistrements d'imputation doit être complètement décrite.

Audit

A.95 Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

Echange de données

Intégrité des données

A.96 Des méthodes de détection et de correction d'erreurs doivent être appliquées en cas d'échange de données. Ces mécanismes doivent être conçus de manière à permettre d'identifier les manipulations intentionnelles des champs d'adresse et des données de l'utilisateur. La connaissance des seuls algorithmes utilisés dans les mécanismes, sans connaissance supplémentaire particulière, ne doit pas permettre une manipulation non reconnue des données précitées. La connaissance supplémentaire indispensable pour le faire doit être protégée de telle façon que seul un nombre restreint d'utilisateurs autorisés puissent y avoir accès.

A.97 De plus, des mécanismes qui identifient de façon sûre et unique comme une erreur la réémission non autorisée de données doivent être utilisés.

Exemple de classe de fonctionnalité : F-DC

Objectif

A.98 L'exemple de classe de fonctionnalité F-DC est destiné aux TOE très exigeantes en matière de confidentialité des données au cours de leur échange. Un équipement cryptographique est un exemple de candidat pour cette classe.

Echange de données

Confidentialité des données

A.99 La TOE doit être dotée d'un dispositif destiné à chiffrer l'information de l'utilisateur avant l'échange et (côté réception) à la déchiffrer automatiquement. Un algorithme officiellement approuvé par une autorité de certification doit être utilisé. Il doit être assuré que les valeurs des paramètres (par exemple les clés) nécessaires au déchiffrement sont protégées de telle manière qu'aucune personne non autorisée ne puisse avoir accès à ces données.

Exemple de classe de fonctionnalité : F-DX

Objectif

A.100 L'exemple de classe de fonctionnalité F-DX est destiné aux réseaux très exigeants en matière de confidentialité et d'intégrité des informations à échanger. Par exemple, cela peut être le cas lorsque des informations sensibles doivent être échangées à travers des réseaux non protégés (par exemple des réseaux publics).

Identification et authentification

A.101 La TOE doit identifier et authentifier de façon unique les utilisateurs. L'identification et l'authentification doivent avoir lieu avant toute autre interaction entre la TOE et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies. Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles pour consultation ou modification par des utilisateurs autorisés. Pour toute interaction, la TOE doit pouvoir établir l'identité de l'utilisateur.

A.102 Avant l'échange de données de l'utilisateur, l'entité homologue (ordinateur, processus ou utilisateur) doit être identifiée et authentifiée de façon unique. Les données de l'utilisateur ne doivent être échangées qu'après que l'identification et l'authentification ont été effectuées avec succès. A la réception de données, il doit être possible d'identifier et d'authentifier de façon unique leur émetteur. Toutes les informations d'authentification doivent être protégées contre un accès non autorisé ou une contrefaçon.

Imputabilité

A.103 La TOE doit comporter un composant d'imputation qui soit capable, pour chacun des événements suivants, d'enregistrer cet événement avec les données exigées :

a) Utilisation du mécanisme d'identification et d'authentification :

Données exigées : Date ; heure ; initiateur de l'identification et de l'authentification ; nom du sujet à identifier ; réussite ou échec de l'action.

b) Erreurs identifiées pendant l'échange de données :

Données exigées : Date ; heure ; entités homologues dans l'échange de données ; type de l'erreur ; réussite ou échec de la tentative de correction.

c) Etablissement de la connexion :

Données exigées : Date ; heure ; identité de l'utilisateur initiateur ; nom de l'entité homologue (ordinateur, processus ou utilisateur) ; paramètres d'établissement de la connexion (s'ils varient).

d) Transactions d'échange de données spéciales :

Données exigées : Date ; heure ; identité de l'utilisateur émetteur ; identité de l'utilisateur récepteur ; informations de l'utilisateur transmises ; date et heure de la réception des données.

A.104 Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation. Il doit être possible de mettre sélectivement en oeuvre l'imputation pour un ou plusieurs utilisateurs. Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs. La structure des enregistrements d'imputation doit être complètement décrite.

Audit

A.105 Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

Echange de données

Contrôle d'accès

A.106 Toutes les informations transmises auparavant et pouvant être utilisées pour un déchiffrement non autorisé doivent être protégées de manière telle que seules puissent accéder à ces données les personnes qui en ont absolument besoin pour pouvoir remplir leur tâche.

Confidentialité des données

A.107 La TOE doit offrir la possibilité d'un chiffrement de bout en bout qui garantisse la confidentialité en ce qui concerne le destinataire sur de grandes sections du canal

de communication. En outre, la confidentialité du flux de trafic doit aussi être garantie sur des liaisons de données désignées.

Intégrité des données

A.108 La TOE doit être conçue de façon telle qu'une manipulation non autorisée des données des utilisateurs et des données d'imputation, et une réémission de données non autorisée soient identifiées de façon sûre comme des erreurs.

Annexe B - Le "Claims Language"

Introduction

B.1 Dans le contexte des critères d'évaluation de la sécurité des TI, il est commode de disposer d'un moyen pour décrire en style semi-formel les fonctions de sécurité annoncées par un produit de sécurité TI, mais encore exprimées en langage naturel. Le Claims Language défini dans la présente annexe a été développé pour satisfaire ce besoin.

B.2 Les avantages de l'utilisation de ce langage pour spécifier la fonctionnalité de sécurité sont les suivants :

a) il fournit un style semi-formel de spécification, mais qui, comme il est basé sur le langage naturel, peut être lu et compris sans connaissance particulière d'une notation ou d'un ensemble de règles ;

b) il indique les liaisons et les regroupements nécessaires entre les annonces ;

c) il réduit les risques d'ambiguïté dans l'interprétation des annonces ;

d) il permet d'exprimer les annonces concernant une TOE d'une manière adaptée au processus d'évaluation.

B.3 Le Claims Language facilite une extension contrôlée de la notation prédéfinie dans le maniement de concepts pour lesquels il n'existe pas d'élément adapté. Dans un Claims Document, le langage naturel normal peut être utilisé pour décrire des mécanismes et des hypothèses lorsqu'une approche plus formelle n'est pas nécessaire. Le Claims Language est assez souple pour permettre de définir tout ensemble d'annonces propre à une TOE spécialisée sans s'écarter aucunement des règles du langage : ainsi les commanditaires d'une évaluation ne sont nullement astreints à adapter leurs annonces au langage.

Vue d'ensemble

B.4 Dans l'utilisation du Claims Language, les fonctions de sécurité sont exprimées au moyen d'un ensemble de règles pour produire des Modèles d'Expression d'Action dont chacun fournit l'ossature d'un type particulier d'annonce. Chaque Modèle d'Expression d'Action est alors combiné avec un élément d'un ensemble d'Expressions de Cible pour créer l'ébauche d'une annonce. Des noms et des expressions spécifiques au produit, à la fonction ou au fournisseur sont alors

substitués dans cette ébauche pour créer une annonce réelle. Un exemple de génération d'une annonce figure dans les paragraphes B.30 à B.34 de la présente annexe.

B.5 Il est possible d'inclure dans la déclaration d'une annonce une référence au mécanisme qui l'implémente.

B.6 Il est permis d'omettre ou de modifier les mots de liaison utilisés dans les ébauches d'annonces afin d'en faciliter la lecture ou d'en améliorer la justesse grammaticale.

B.7 Voici des exemples de modifications autorisées :

a) remplacer le pluriel par le singulier et vice versa ;

b) insérer ou retirer les articles définis et indéfinis ;

c) modifier les prépositions.

B.8 Il est permis d'introduire de nouvelles expressions d'action ou de cible lorsqu'il n'existe pas d'expression appropriée, à condition qu'elles aient été discutées avec l'organisme de certification et approuvées par lui.

B.9 Une présentation normalisée doit être utilisée pour les Claims Documents contenant des annonces en Claims Language, comme il est indiqué dans les paragraphes B.38 à B.44 de la présente annexe. Les annonces doivent être regroupées sous une rubrique normalisée basée sur les rubriques génériques pour la fonctionnalité. Cela facilite la compréhension et la comparaison avec d'autres TOE.

Avertissements

B.10 Il faudra prendre des précautions pour formuler les annonces qui dépendent de la configuration. Il est peut-être possible de configurer une TOE d'une manière non sûre (c'est-à-dire que certaines annonces sont invalidées). Si c'est le cas, des restrictions propres à exclure de telles options ou combinaisons d'options non sûres devraient être présentées comme des contraintes d'environnement (voir le paragraphe B.41 plus loin dans cette annexe).

B.11 Il faudra aussi prendre des précautions pour que les annonces soient formulées au niveau voulu de granularité. Si une des annonces proposées semble englober plusieurs rubriques génériques ou si elle exige plus de substitutions que ne le permet l'emploi du modèle approprié, c'est que l'annonce est d'un niveau trop élevé et qu'elle a besoin d'être fragmentée en une série d'annonces plus simples.

Modèles d'Expression d'Action

B.12 Les Modèles d'Expression d'Action doivent être réalisés à partir de l'ossature ci-dessous, dans laquelle les caractères italiques indiquent des mots ou des expressions, dans le modèle, qui doivent être remplacés, dans l'annonce réelle, par des substitutions spécifiques en rapport avec l'annonce, [] désignant les parties facultatives et <> un choix parmi les options pertinentes de la liste qui suit.

This *TOE* [<qualifier>] <verb> <action> ... [time] [using the mechanism defined in paragraph *n*].

Où <qualifier> peut être :

contains a *function* that
ou must be used in an environment that

et <verb> peut être :

will
ou will not
ou can be configured to
ou can be configured to not
ou cannot be configured to

et <action> peut être :

establish
ou detect
ou control
ou permit
ou prevent
ou ensure
ou record in *object*

et <time> peut être :

before *security-relevant-event*
ou after *security relevant-event*

B.13 L'option "environment" de <qualifier> n'est utilisée que pour définir les contraintes d'environnement lorsqu'une grande précision est exigée.

B.14 Lorsque les détails de mécanismes spécifiques font partie de la cible de sécurité, ils doivent être définis comme faisant partie du Claims Document à l'aide d'un paragraphe associé de spécification du mécanisme. Si une telle association n'est pas incluse, c'est que les détails du mécanisme ne font pas partie de la cible de sécurité et seront traités comme une information interne. L'option "function" du <qualifier> est facultative. Elle sert à nommer le mécanisme particulier d'un produit qui implémente une annonce particulière. Ce nom n'est inclus que dans un but explicatif.

B.15 Voici quelques exemples de Modèles d'Expression d'Action :

This product will ensure ....

This product contains an audit utility that will establish ...

This product can be configured to permit ...

This add-in board will record in its audit trail ...

This product will prevent ... before completion of secure startup.

Expressions de Cible

B.16 L'ensemble autorisé d'Expressions de Cible est le suivant, [] désignant les parties facultatives de l'expression :

1 ... *audit-information* concerning *security-relevant-events*

2 ... the identity of a *process* requested

3 ... the identity of the *{user,process}* requesting a *process*

4 ... the identity of the *{user,process}* requesting *access-type* to an *object*

5 ... the identity of a *process* executed

6 ... the rejection of a *process* request

7 ... the identity of an *object* to which *access-type* was requested

8 ... the identity of an *object* to which *access-type* was granted

9 ... the identity of an *object* to which *access-type* was refused

10 ... the *access-set* of a *user*

11 ... the *access-set* of a *process*

12 ... the *access-set* of a *{user,process}*

13 ... the *access-set* of an *object*

14 ... the *access-type* granted to a *{user,process}* in respect of an *object*

15 ... *access-type* by *{user,process}* in respect of an *object*

16 ... the action performed by a *{user,process}* in respect of an *object*

17 ... the *factors* affecting the *access-set* of a *user*

18 ... the *factors* affecting the *access-set* of a *process*

19 ... the *factors* affecting the *access-set* of a *{user,process}*

20 ... the *factors* affecting the *access-set* of an *object*

21 ... clearing of information from an *object*

22 ... the *security-attributes* of an *object*

23 ... the correctness of the *security-attributes* of an *object*

24 ... the *security-attributes* of an *object* formed by combining a number of *objects*

25 ... the *security-attributes* of a set of *objects* formed by partitioning a single *object*

26 ... the granting of *access-type* to an *object* cannot cause deadlock through *{user,process}es* using *access-type* to *objects*

27 ... the *{user,process}es* using *access-type* to an *object* which has caused deadlock

28 ... the granting of *access-type* to an *object* cannot cause livelock through *{user,process}es* using *access-type* to *objects*

29 ... the *{user,process}es* using *access-type* to an *object* which has caused livelock

30 ... *security-attribute* of *object* is identical to that of *object*

31 ... *claim* [not] to become time-critical

32 ... *claim* [not] to become accelerated or delayed

33 ... *claim* [not] to become time-dependant

34 ... *claim* [not] to be by-passed

35 ... *claim* [not] to be deactivated

36 ... *claim* [not] to be corrupted

Substitutions

B.17 Des substitutions doivent être faites pour les noms et expressions ci-après *(mis en italique dans les Modèles d'Expression d'Action et les Expressions de Cible ci-dessus) :*

access-set ; access-type ; audit-information ; claim ; factors ; function ; n ; object ; product ; process ; security-attribute ; security-relevant-event ; use ; {user,process}

B.18 Toutes les substitutions doivent être expliquées en utilisant le langage naturel, soit dans une section séparée du Claims Document (voir le paragraphe B.39 de la présente annexe), soit aussitôt après l'annonce où la substitution est employée.

B.19 Voici quelques exemples de possibilités de substitution :

access-set	remplacé par	read/write access to IO ports
access-type	remplacé par	read permission
access-type	remplacé par	read/write/delete permission
audit-information	remplacé par	date and time
audit-information	remplacé par	terminal number
claim	remplacé par	(a cross-reference to another claim)

factors	remplacé par	number of incorrect responses
function	remplacé par	password system
n	remplacé par	(a paragraphe number)
object	remplacé par	file
object	remplacé par	resource control block
object	remplacé par	hard disc storage (i.e. a type of object)
TOE	remplacé par	operating system
TOE	remplacé par	PC security board
process	remplacé par	unprivileged task
security-attribute	remplacé par	integrity of data
security-attribute	remplacé par	actual destination
security-attribute	remplacé par	apparent source
security-relevant-event	remplacé par	attempted privilege violation
security-relevant-event	remplacé par	user logoff
security-relevant-event	remplacé par	change of security level
user	remplacé par	data entry clerk
user	remplacé par	security administrator
{user,process}	remplacé par	job (i.e. implying any user)

B.20 Certaines parties des Expressions d'Action et des Expressions de Cible sont mises entre crochets [] ; ce sont des expressions ou des mots facultatifs qui peuvent être inclus ou omis suivant les besoins dans l'annonce du fournisseur.

B.21 La plupart des substitutions de noms et d'expressions s'expliquent d'elles-mêmes. Toutefois il existe quelques conventions particulières qui sont expliquées ci-après.

B.22 La définition d'un domaine d'accès (access-set) varie suivant qu'il est en rapport avec :

a) un objet ; dans ce cas il représente la liste des utilisateurs (user), des processus (process) et des groupes {user,process} à chacun desquels est associé un type d'accès (access-type) et qui sont capables d'utiliser un objet (object) ;

b) un processus, un utilisateur ou un groupe {user, process} ; auquel cas il représente la liste des objets à chacun desquels est associé un type d'accès et qui sont à la disposition d'un utilisateur, d'un processus ou d'un groupe {user, process}.

B.23 Ainsi un domaine d'accès est une liste (conceptuelle) de tous les objets auxquels un utilisateur peut avoir accès, ainsi que de ce que cet utilisateur peut faire à chacun de ces objets et à travers quels processus, *ou* une liste (conceptuelle) de tous les

utilisateurs qui peuvent accéder à un objet, à travers quels processus et ce qu'ils peuvent faire à cet objet.

B.24 Le type d'accès (access-type) est la série des modes d'utilisation d'un objet et il est défini par le fournisseur. Les expressions *create*, *read*, *write*, *delete*, *execute* ou une combinaison de ces mots, ou encore *none*, en sont des exemples représentatifs.

B.25 Un exemple spécifique pourrait être donné par l'ensemble suivant :

a) "Amend" permet de mettre à jour un enregistrement, mais pas d'en ajouter un nouveau dans le fichier,

b) "Create" permet d'ajouter de nouveaux enregistrements au fichier, mais pas de modifier ceux qui existent,

c) "Delete" permet de retirer des enregistrements du fichier,

d) "Execute" permet de charger le fichier en mémoire, puis de le mettre en attente d'exécution en tant que programme,

e) "Read" permet de recopier dans la mémoire de travail des données contenues dans des enregistrements.

B.26 Beaucoup d'objets possèderont des attributs de sécurité identiques. Aussi lorsqu'une annonce s'appliquera à tous les objets d'un type particulier, c'est généralement en termes de type d'objet que la substitution sera le mieux exprimée plutôt qu'en énumérant tous les objets possibles de ce type.

Mécanismes

B.27 Il est possible d'inclure dans une annonce la description du mécanisme utilisé pour implémenter cette annonce. Cela se fait à l'aide de l'option "using" du Modèle d'Expression d'Action de l'annonce, en donnant une référence à un paragraphe du Claims Document qui spécifie ou explique le mécanisme employé. L'évaluation comportera alors la confirmation du fait que le mécanisme déclaré est bien le mécanisme utilisé.

B.28 Toute méthode appropriée pourra être utilisée pour définir ou décrire le mécanisme pourvu que les explications soient suffisantes pour que l'évaluation détermine, à un niveau de confiance correspondant au niveau d'évaluation visé, que :

a) le mécanisme annoncé est bien présent dans le produit,

b) son fonctionnement correspond à la spécification annoncée,

c) c'est le mécanisme réellement utilisé pour implémenter l'annonce.

B.29 Dans beaucoup de cas, il peut être plus facile et plus clair de définir un mécanisme en se référant à une norme publiée, ou de présenter un tableau des types d'entrée et des résultats correspondants, plutôt que de fournir des détails de l'algorithme utilisé en se servant soit du langage naturel, soit d'un langage de spécification ou de programmation.

Exemple

B.30 A titre d'exemple, le modèle d'Expression d'Action suivant peut être généré en se servant des règles spécifiées :

This *TOE* will establish ....

où le mot en italique peut être remplacé par un terme spécifique.

B.31 De même, une Expression de Cible peut être choisie, comme par exemple :

... the identity of an *object* to which *access-type* was requested.

B.32 La réunion des deux donne le texte :

This *TOE* will establish the identity of an *object* to which *access-type* was requested.

dans lequel des substitutions possibles sont :

add-in security board	pour	*TOE*
any file	pour	*object*
write or delete permission	pour	*access-type*

B.33 Ainsi une annonce complète pourra être :

This add-in security board will determine the identity of any file to which write or delete permission was requested.

B.34 Evidemment cet exemple est tout à fait artificiel. En pratique, pour les TOE réelles, on fait des annonces extrêmement spécifiques, souvent liées à un environnement particulier, réel ou supposé.

Structure du Claims Document

Utilisation des rubriques génériques relatives à la fonctionnalité

B.35 Les annonces doivent être regroupées sous les rubriques génériques exposées au chapitre 2 des présents critères. Toutes les TOE ne feront pas des annonces entrant dans toutes les rubriques ; lorsque cela se présente, le fait qu'il n'y a pas d'annonce dans telle rubrique particulière doit être déclaré. Des annonces doivent être incluses pour tous les événements ou actions qui doivent être empêchées.

B.36 Le tableau B.1 identifie les Expressions de Cible qui apparaîtront souvent dans certaines rubriques génériques particulières. Il est destiné seulement à servir de guide général ; la souplesse du Claims Language signifie que souvent d'autres Expressions de Cible seront également appropriées.

B.37 Le tableau B.2 fait correspondre les Expressions de Cible et les possibilités de substitution qu'elles comportent.

Plan du Claims Document

B.38 Une cible de sécurité utilisant le Claims Language doit être présentée suivant la structure suivante :

a) les objectifs de sécurité de la cible, y compris toute contrainte ou hypothèse concernant l'environnement réel ou présumé de la TOE, sous forme d'un argumentaire du produit (ou une politique de sécurité du système dans le cas d'un système) ;

b) une spécification informelle des annonces en langage naturel, ou une référence à un autre document contenant cette spécification informelle (ce peut être la référence à une classe de fonctionnalité définie en style informel), et une correspondance entre ces annonces informelles et les objectifs de sécurité ;

c) les substitutions globales ;

d) les annonces entrant successivement sous chaque rubrique générique ;

e) le détail des mécanismes de sécurité ;

f) la cotation annoncée de la résistance minimum des mécanismes ;

g) le niveau d'évaluation visé.

B.39 Dans la rubrique "Substitutions Globales", toutes les substitutions générales utilisées dans les Expressions d'Action ou de Cible d'une ou de plusieurs annonces doivent être définies et expliquées.

B.40 On ne doit pas tenir compte de ces substitutions lorsque des substitutions différentes (généralement plus spécifiques) sont données comme faisant partie d'annonces particulières.

B.41 Si une TOE compte sur certaines propriétés de son environnement réel ou supposé pour fonctionner correctement, ces propriétés doivent être spécifiées dans la section argumentaire ou politique du Claims Document. Le processus d'évaluation supposera que ces contraintes ou ces hypothèses existeront dans l'environnement réel.

B.42 Chacune de ces contraintes ou de ces hypothèses devront être exprimées soit en langage naturel soit en Claims Language (en utilisant le qualificatif d'environnement de l'Expression d'Action). Lorsqu'il existe une ambiguïté (parce que le langage naturel a été utilisé) les évaluateurs interpréteront de telles contraintes ou hypothèses de façon cohérente avec les autres hypothèses ou annonces.

B.43 Certaines annonces peuvent rester valides même si une assertion particulière est inexacte. Lorsque tel est le cas, le langage naturel doit être utilisé pour indiquer quelles sont les annonces qui restent exactes quand cette affirmation est erronée.

B.44 Voici un exemple d'affirmation (exprimée en langue naturelle) :

Il ne faut pas retirer la batterie de secours de la mémoire vive de la carte de sécurité ni la laisser se décharger au-dessous de sa tension minimale de fonctionnement.

Format des annonces individuelles

B.45 Chaque substitution, dans les Expressions d'Action ou de Cible, utilisée pour construire une annonce qui n'est pas identifiée et définie dans la section des substitutions globales du Claims Document doit être définie et exprimée en langage naturel immédiatement après l'annonce où elle apparaît.

Tableau B.1 - Expressions de Cible des annonces et rubriques génériques

		Identification et authentification	Contrôle d'accès	Imputabilité	Audit	Réutilisation d'objet	Fidélité	Fiabilité de service	Echange de données
1	Audit information	X	X	X	X	X	X	X	X
2	Identity of process requested	X	X	X	X			X	X
3	Identity of {u,p} requesting a process	X	X	X	X			X	X
4	Identity of {u,p} requesting an object	X	X	X	X			X	X
5	Identity of process executed	X	X	X	X			X	X
6	Rejection of process request	X	X	X	X			X	X
7	Identity of object requested	X	X	X	X			X	X
8	Identity of object granted	X	X	X	X		X	X	X
9	Identity of object refused	X	X	X	X			X	X
10	Access-set of user		X						X
11	Access-set of process		X						X
12	Access-set of {u,p}		X						X
13	Access-set of object		X						X
14	Object access granted to {u,p}	X	X	X	X				X
15	Object access by {u,p}	X	X	X	X				X
16	Object actions performed by {u,p}		X	X	X				X
17	Factors affecting user access-set		X						X
18	Factors affecting process access-set		X						X
19	Factors affecting {u,p} access-set		X						X
20	Factors affecting object access-set		X						X
21	Clearing information from object					X			X
22	Security-attributes of object	X	X	X	X	X	X	X	X
23	Correctness of security-attributes of object						X		X
24	Security-attributes of combinaison object		X				X		X
25	Security-attributes of partitioned object		X				X		X
26	Granting access causes no deadlock							X	X
27	Deadlock can be detected							X	X
28	Granting access causes no livelock							X	X
29	Livelock can be detected							X	X
30	Objects have identical security-attributes		X				X		X
31	Time-critical claim							X	
32	Accelerated or delayed claim							X	
33	Time-dependant claim							X	
34	By-pass claim	X	X	X	X	X	X	X	X
35	Deactivate claim	X	X	X	X	X	X	X	X
36	Corrupt claim	X	X	X	X	X	X	X	X

Tableau B.2 - Expressions de Cible des annonces et substitutions autorisées

		access-set	access-type	audit-information	claim	object	process	security-attribute	security-relevant-event	user	{user,process}
1	Audit information		X			X					
2	Identity of process requested						X				
3	Identity of {u,p} requesting a process						X				X
4	Identity of {u,p} requesting an object		X		X						X
5	Identity of process executed						X				
6	Rejection of process request						X				
7	Identity of object requested		X		X						
8	Identity of object granted		X		X						
9	Identity of object refused		X		X						
10	Access-set of user	X								X	
11	Access-set of process	X					X				
12	Access-set of {u,p}	X									X
13	Access-set of object	X			X						
14	Object access granted to {u,p}		X		X						X
15	Object access by {u,p}		X		X						X
16	Object actions performed by {u,p}				X						X
17	Factors affecting user access-set	X								X	
18	Factors affecting process access-set	X					X				
19	Factors affecting {u,p} access-set	X									X
20	Factors affecting object access-set	X			X						
21	Clearing information from object				X						
22	Security-attributes of object				X			X			
23	Correctness of security-attributes of object				X			X			
24	Security-attributes of combinaison object				X			X			
25	Security-attributes of partitionned object				X			X			
26	Granting access causes no deadlock		X		X						X
27	Deadlock can be detected		X		X						X
28	Granting access causes no livelock		X		X						X
29	Livelock can be detected		X		X						X
30	Objects have identical decurity-attributes				X			X			
31	Time-critical claim			X							
32	Accelerated or delayed claim			X							
33	Time-dependant claim			X							
34	By-pass claim			X							
35	Deactivate claim			X							
36	Corrupt claim			X							