PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

DIRECTION CENTRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Schéma Français
d'Évaluation et de Certification
de la Sécurité des Technologies de l'Information

Rapport de certification 2001/11

Ligne de production CZ6
du site NEC à Yamaguchi-Japon

Juin 2001

Ce document constitue le rapport de certification du système “Ligne de production CZ6 du site NEC à Yamaguchi-Japon”.

Ce rapport de certification est disponible sur le site internet de la Direction Centrale de la Sécurité des Systèmes d'Information à l'adresse suivante :

www.ssi.gouv.fr

Toute correspondance relative à ce rapport de certification doit être adressée au :

Secrétariat général de la défense nationale
DCSSI
Centre de Certification de la Sécurité des Technologies de l’Information
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

Mél: certification.dcssi@sgdn.pm.gouv.fr

Ce document est folioté de 1 à 24 et certificat.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

Schéma Français d'Évaluation et de Certification de la Sécurité des Technologies de l'Information

CERTIFICAT 2001/11

Ligne de production CZ6 du site NEC à Yamaguchi-Japon

Développeur : NEC Yamaguchi Ltd

EAL1 augmenté

Commanditaire : NEC SCAC

Le 28 juin 2001,

Commanditaire :
NEC Microcomputer Division General Manager
Yuichi KAWAKAMI

L'Organisme de certification :
Le Directeur chargé de la sécurité des systèmes d'information
Henri SERRES

Security Manager de NEC SCAC
Joël LEBIHAN

Ce système a été évalué par un centre d'évaluation de la sécurité des TI conformément aux critères communs pour l'évaluation de la sécurité des TI version 2.1 et à la méthodologie commune pour l'évaluation de la sécurité des TI version 1.0.

Ce certificat ne s'applique qu'à la version évaluée du système dans sa configuration d'évaluation et selon les modalités décrites dans le rapport de certification associé. L'évaluation a été conduite en conformité avec les dispositions du Schéma français d'évaluation et de certification de la sécurité des TI. Les conclusions du centre d'évaluation enregistrées dans le rapport technique d'évaluation sont cohérentes avec les éléments de preuve fournis.

Ce certificat ne constitue pas en soi une recommandation du système par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise. Ce certificat n'exprime directement ou indirectement aucune caution du système par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

Organisme de certification :
Secrétariat général de la défense nationale
DCSSI
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

Common Criteria

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du système “Ligne de production CZ6 du site NEC à Yamaguchi-Japon” ayant pour objet de produire des microcircuits destinés à être insérés dans des cartes à puces. Cette ligne de production se décompose en trois flux :

- le flux de production des microcircuits ;
- le flux des réticules ;
- le flux des programmes de tests.

2 Le niveau d’assurance atteint est le niveau EAL1 augmenté du composant d’assurance AVA_VLA.2 “Analyse de vulnérabilités indépendante” tel que décrit dans la partie 3 des Critères Communs [3].

3 La portée de la cible de sécurité et les limites de la cible d’évaluation ont été définies dans le respect des exigences pour l’environnement du profil de protection “Smartcard Integrated Circuit” enregistré auprès de la DCSSI dans le catalogue des profils de protection certifiés sous les références PP/9806 [7].

4 Pour l’évaluation d’un microcircuit fabriqué à travers cette ligne de production CZ6, les exigences d’assurance pour l’environnement de production ADO_DEL.2 “Détection de modifications” et ALC_DVS.2 “Caractère suffisant des mesures de sécurité” seront considérées comme couvertes par le présent rapport de certification.

Chapitre 2

Résumé

2.1 Contexte de l'évaluation

5 L'évaluation a été menée conformément aux Critères Communs ([1] à [3]) et à la méthodologie définie dans le manuel CEM [4].

6 Etant donné qu'il s'agit d'une évaluation de type système, elle s'est déroulée consécutivement au développement du système d'octobre 2000 à avril 2001. Un audit de trois jours a eu lieu pendant cette période.

7 La cible d'évaluation a été développée par la société suivante (ci-après le "développeur") :

- NEC Yamaguchi Ltd
  Jinga, Higashimagura, Kusunoki-Cho
  Asa-Gun, Yamaguchi 757-098
  Japon.

8 Le commanditaire de l'évaluation est la société suivante (ci-après le "commanditaire") :

- NEC SmartCard Application Center
  9, rue Paul Dautier
  BP 52
  78142 Vélizy
  France.

9 L'évaluation a été conduite par le centre d'évaluation de la sécurité des technologies de l'information (ci-après "CESTI") :

- AQL
  Rue de la Châtaigneraie
  BP 127
  35513 Cesson-Sévigné Cedex
  France.

2.2 Description de la cible d'évaluation

10 La cible d'évaluation est le système "Ligne de production CZ6 du site NEC à Yamaguchi-Japon" ayant pour objet de produire des microcircuits destinés à être insérés dans des cartes à puces.

11 Les circuits intégrés résultant de ce système de production sont les microcontrôleurs basés sur une technologie .35 microns utilisant des CPU 78KOS (8 bits CISC) et V850 (32 bits RISC) et incluant des mémoires (EEPROM, ROM et RAM) de différentes tailles en fonction de la version du produit.

12 Ces deux familles de microcircuits sont connues commercialement sous les noms suivants :

- famille 8 bits : µPD7898XX ;
- famille 32 bits : µPD7039XX.

2.3 Conclusions de l'évaluation

13 Le système soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [3].

14 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL1 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élémentaire tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.

15 La validité des résultats d'évaluation est soumise aux recommandations figurant au chapitre 6 du présent rapport.

Chapitre 3

Identification de la cible d'évaluation

3.1 Objet

16 La cible d'évaluation est le système "Ligne de production CZ6 du site NEC à Yamaguchi-Japon" ayant pour objet de produire des microcircuits destinés à être insérés dans des cartes à puces.

3.2 Historique du développement

17 La cible d'évaluation était déjà installée au moment du démarrage de l'évaluation. Cependant, pour corriger les problèmes identifiés dans le cadre de l'évaluation, le système a été modifié pendant la durée de l'évaluation ; l'arrêt bi-annuel du site de Yamaguchi a été l'occasion de mettre en place ces modifications.

18 Par ailleurs, dans le cadre du programme d'amélioration continue du site de Yamaguchi, certaines optimisations ont été envisagées ; les évolutions correspondantes sont prévues pour être implémentées d'ici la fin de l'année 2001et feront l'objet d'un programme de maintenance.

3.3 Composition de la cible d'évaluation

19 Etant donné que la cible d'évaluation est un système, il n'est pas fait de distinction entre sa partie matérielle et sa partie logicielle.

20 La cible d'évaluation intègre les aspects des technologies de l'information suivants :

- une application serveur de GPAO installée sur des serveurs UNIX sous le système d'exploitation HP-UX 10.2 ;
- une application cliente de GPAO installée sur des terminaux sous le système d'exploitation Windows NT4 ; ces terminaux sont destinés à l'acquisition des données de traçabilité des lots de wafers ;
- un système d'exploitation Windows NT4 installé sur une console de contrôle de l'équipement de test et sur un serveur destiné à l'acquisition et au traitement des résultats de test.

21 Elle intègre également des parties ne relevant pas des technologies de l'information telles que :

- les équipements utilisés pour la production,
- les programmes et les outils de tests.

22 Les aspects liés à l'environnement, tels que l'environnement physique et informatique dans lequel la cible d'évaluation est implantée ainsi que les personnels employés, sont également couverts par l'évaluation.

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

23 Les caractéristiques de sécurité évaluées sont consignées dans la cible de sécurité [5] qui est la référence pour l'évaluation. Les paragraphes ci-après reformulent les éléments essentiels de ces caractéristiques.

4.2 Biens

24 Les biens à protéger sont classés en deux catégories :

- les biens sensibles de la cible d'évaluation;
- les biens sensibles traités par la cible d'évaluation.

25 Les biens sensibles de la cible d'évaluation sont les données de traçabilité (identification, statut, localisation et quantité des lots de wafers) et les résultats de test.

26 Les biens sensibles traités par la cible d'évaluation sont les produits (wafers), les réticules (tous les réticules ne sont pas considérés comme critiques pour la sécurité, seuls sept d'entre eux sont pris en compte dans le cadre de l'évaluation), et les programmes de test.

4.3 Hypothèses

27 La cible d'évaluation doit être utilisée dans un environnement qui satisfait aux hypothèses décrites dans la cible de sécurité [5]. Ces hypothèses couvrent les aspects suivants :

- livraison sûre des réticules et des programmes de test entre les fournisseurs et la cible d'évaluation,
- les réticules et les programmes de test livrés sont considérés comme sûrs,
- compétence et expérience des personnels employés sur le site de Yamaguchi qui interagissent avec la cible d'évaluation.

28 Le détail de ces hypothèses est disponible dans la cible de sécurité [5].

4.4 Menaces

29 Les principales menaces portent sur :

- la divulgation non autorisée des programmes et des résultats de test,
- la modification non autorisée des données de traçabilité, des programmes et des résultats de test,
- le vol et l'utilisation non autorisée des réticules, des produits (wafers), des programmes et des résultats de test.

30 Le détail de ces menaces est disponible dans la cible de sécurité [5].

4.5 Politiques de sécurité organisationnelles

31 Les politiques de sécurité organisationnelles couvrent les aspects suivants :

- les règles à appliquer pour rédiger et émettre des procédures ;
- la définition et l'application de la politique de sécurité du site de Yamaguchi ; ceci implique en particulier la réalisation d'un audit annuel réalisé par le responsable sécurité de NEC Smartcard Application Center, l'utilisation de rapports d'anomalies qui identifient les problèmes rencontrés ainsi que les actions correctives à mettre en place et la gestion des modifications ;
- l'approbation du choix des sous-traitants pour les activités de production.

32 Le détail de ces politiques de sécurité organisationnelles est disponible dans la cible de sécurité [5].

4.6 Fonctions de sécurité évaluées

33 Les fonctions de sécurité évaluées sont décrites ci-dessous. Le détail de ces fonctions est disponible dans la cible de sécurité [5].

4.6.1 SF1 : Login

34 Cette fonction de sécurité du système d'exploitation HP-UX impose l'identification et l'authentification des utilisateurs avant toute autre action.

4.6.2 SF2 : Contrôle d'accès

35 Cette fonction de sécurité de l'application de GPAO impose l'identification et l'authentification des utilisateurs avant toute autre action.

4.6.3 SF3 : Administration des attributs

36 Cette fonction de sécurité du système d'exploitation HP-UX correspond à l'administration des attributs appartenant aux utilisateurs du système d'exploitation HP-UX et de l'application de GPAO.

4.6.4 SF4 : Administration

37 Cette fonction de sécurité du système d'exploitation HP-UX permet d'associer les utilisateurs à des rôles et de gérer les différents rôles en utilisant les informations fournies par SF1 et SF2.

4.6.5 SF5 : Propriété des commandes et des fichiers

38 Cette fonction de sécurité du système d'exploitation HP-UX définit les droits de propriété des utilisateurs sur les commandes qui s'exécutent pour leur compte et sur les fichiers qu'ils créent.

4.6.6 SF6 : Configuration des fichiers

39 Cette fonction de sécurité du système d'exploitation HP-UX garantit que toute opération exécutée pour le compte d'un utilisateur hérite de ses attributs et des droits de propriété de la commande et du fichier concernés.

4.6.7 SF7 : Administration des droits

40 Cette fonction de sécurité du système d'exploitation HP-UX garantit que les droits des utilisateurs leur sont effectivement attribués sur la base de leur identification et leur authentification.

4.6.8 SF8 : Alarme de temps de transfert

41 Cette fonction de sécurité de l'application de GPAO assure le déclenchement d'une alarme si le temps de transfert des produits entre deux étapes successives de fabrication excède une durée prédéfinie.

4.6.9 SF9 : Logon

42 Cette fonction de sécurité du système d'exploitation Windows NT impose l'identification et l'authentification des utilisateurs avant toute autre action.

4.6.10 SF10 : Identifiant de sécurité

43 Cette fonction de sécurité du système d'exploitation Windows NT correspond à l'administration des attributs appartenant aux utilisateurs du système d'exploitation Windows NT et des applications associées.

4.6.11 SF11 : Administration des comptes utilisateurs

44 Cette fonction de sécurité du système d'exploitation Windows NT permet d'associer les utilisateurs à des rôles et de gérer les différents rôles en utilisant les informations fournies par SF9.

4.6.12 SF12 : Propriétaire

45 Cette fonction de sécurité du système d'exploitation Windows NT définit les droits de propriété des utilisateurs sur les commandes qui s'éxécutent pour leur compte et les fichiers qu'ils créent.

4.6.13 SF13 : Administration sécuritaire des comptes

46 Cette fonction de sécurité du système d'exploitation Windows NT garantit que les droits des utilisateurs leur sont effectivement attribués sur la base de leur identification et leur authentification.

4.7 Mesures de sécurité pour la cible d'évaluation

47 En complément des fonctions de sécurité évaluées, la cible de sécurité définit des mesures de sécurité pour la cible d'évaluation qui contribuent à couvrir les objectifs pour la cible d'évaluation.

48 Ces mesures de sécurité qui ne relèvent pas des technologies de l'information et qui ont donc été auditées dans le cadre de l'évaluation, concernent les aspects suivants :

- stockage sûr des produits, des réticules, des programmes et résultats de test,
- identification unique des produits, des réticules et des programmes de test,
- disponibilité limitée des programmes de test sur les équipements de test (les programmes sont installés avant la réalisation des tests et sont effacés une fois les tests réalisés),
- gestion de la fin de vie des programmes de test et des réticules,
- remise en main propre des réticules, des programmes de test et des lots de wafers destinés à être testés,
- disponibilité d'un back-up des résultats de test,
- gestion des commandes de nouveaux réticules,
- contrôle en configuration des produits, des réticules, des outils et programmes de test,
- gestion et destruction des rebuts et des réticules défectueux,
- gestion des mots de passe.

49 Le détail de ces mesures de sécurité pour la cible d'évaluation est disponible dans la cible de sécurité [5].

4.8 Mesures de sécurité pour l'environnement

50 Afin de couvrir les objectifs de sécurité pour l'environnement, la cible de sécurité définit des mesures de sécurité pour l'environnement.

51 Ces mesures de sécurité qui ont été auditées dans le cadre de l'évaluation concernent les aspects suivants :

- signature d'un engagement de confidentialité par les personnels employés sur le site de Yamaguchi,
- gestion des embauches de nouveau personnel et des départs,
- contrôle d'accès des personnels (ce contrôle peut se baser sur une identification et une authentification),
- gestion des mots de passe,
- protection du réseau informatique du site de Yamaguchi contre les attaques et les intrusions externes,
- utilisation de rapports d'anomalies pour identifier les problèmes rencontrés ainsi que les actions correctives à mettre en place.

52 Le détail de ces mesures de sécurité pour l'environnement est disponible dans la cible de sécurité [5].

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

53 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [6] produit par le CESTI d'AQL.

5.2 Principaux résultats de l'évaluation

54 Le système répond aux exigences des Critères Communs pour le niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante".

5.2.1 ASE : Evaluation de la cible de sécurité

55 Les critères d'évaluation sont définis par les sections ASE_DES.1.iE, ASE_ENV.1.iE, ASE_INT.1.iE, ASE_OBJ.1.iE, ASE_PPC.1.iE, ASE_REQ.1.iE, ASE_SRE.1.iE et ASE_TSS.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des Critères Communs [3].

56 La cible d'évaluation est le système "Ligne de production CZ6 du site NEC à Yamaguchi-Japon".

57 La cible de sécurité décrit de façon claire la cible d'évaluation ainsi que son environnement. Elle distingue les fonctions de sécurité à évaluer des mesures de sécurité pour la cible d'évaluation et pour l'environnement à auditer.

5.2.2 ACM_CAP.1 : Numéros de version

58 Les critères d'évaluation sont définis par la section ACM_CAP.1.1E de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [3].

59 La référence de la cible d'évaluation est CZ6. Le nombre "6" correspond à la version de la ligne de production ; ce numéro de version est incrémenté lorsque la ligne de production subit une évolution technologique.

60 L'évaluateur a vérifié que la ligne de production est effectivement identifiée par cette référence ; en particulier, les éléments de preuve fournis à l'évaluateur utilisent cette référence afin de caractériser la cible d'évaluation.

5.2.3 ADO_IGS.1 : Procédures d'installation, de génération et de démarrage

61 Les critères d'évaluation sont définis par les sections ADO_IGS.1.iE de la classe ADO, telle que spécifiée dans la partie 3 des Critères Communs [3].

62 Le développeur a fourni les procédures d'installation, de génération et de démarrage pour les systèmes d'exploitation HP-UX et Windows NT.

63 Pour l'application serveur de GPAO, seules les procédures de génération et de démarrage ont été livrées car son installation ne relève par du développeur.

64 Pour l'application cliente de GPAO, les procédures complètes étant uniquement disponibles en japonais, le développeur a fourni un document général introduisant chacune des procédures existantes.

65 L'évaluateur a trouvé dans les documents produits les informations suffisantes pour installer, générer et démarrer la cible d'évaluation. Par ailleurs, il a vérifié que l'application des procédures d'installation, de génération et de démarrage permet une configuration sûre de la cible d'évaluation.

5.2.4 ADV_FSP.1 : Spécifications fonctionnelles informelles

66 Les critères d'évaluation sont définis par les sections ADV_FSP.1.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

67 Le développeur a fourni la documentation spécifiant les fonctions de sécurité des différentes composantes de la cible d'évaluation (HP-UX, Windows NT et application de GPAO) et leurs interfaces externes.

68 L'évaluateur a examiné ces spécifications et montré qu'elles représentent une description complète et homogène des fonctionnalités de sécurité du système.

5.2.5 ADV_RCR.1 : Démonstration de correspondance informelle

69 Les critères d'évaluation sont définis par la section ADV_RCR.1.1E de la classe ADV, telle que spécifiée dans la partie 3 des Critères Communs [3].

70 Le développeur a fourni une documentation qui indique la correspondance entre les deux niveaux de représentation des fonctions de sécurité de la cible d'évaluation, à savoir les spécifications globales de la cible d'évaluation décrites dans la cible de sécurité et les spécifications fonctionnelles.

71 L'évaluateur a donc pu s'assurer que les fonctions de sécurité de la cible d'évaluation exprimées dans la cible de sécurité sont correctement et complètement implémentées à travers les spécifications fonctionnelles de la cible d'évaluation.

5.2.6 AGD_ADM.1 : Guide de l'administrateur

72 Les critères d'évaluation sont définis par la section AGD_ADM.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des Critères Communs [3].

73 Le développeur a fourni la documentation d'administration des fonctions de sécurité du système. Lorsque cette documentation était uniquement disponible en japonais, le développeur a fourni un résumé décrivant la couverture de la documentation complète.

74 L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation et a vérifié qu'elle permet une administration sûre du système.

5.2.7 AGD_USR.1 : Guide de l'utilisateur

75 Les critères d'évaluation sont définis par la section AGD_USR.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des Critères Communs [3].

76 Le développeur a fourni la documentation d'utilisation des fonctions de sécurité du système. Les parties du système concernées sont l'application cliente de GPAO, les terminaux destinés à l'acquisition des données de traçabilité des lots de wafers et la console de contrôle de l'équipement de test.

77 L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation et a vérifié qu'elle permet une utilisation sûre du système.

5.2.8 ATE_IND.1 : Tests indépendants - Conformité

78 Les critères d'évaluation sont définis par les sections ATE_IND.1.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

79 L'évaluateur a effectué un ensemble de tests sur la cible d'évaluation pour démontrer que les fonctions de sécurité fonctionnent conformément à leurs spécifications. Ces tests ont été réalisés lors de l'audit du site de Yamaguchi.

5.2.9 AVA_VLA.2 : Analyse de vulnérabilités indépendante

80 Les critères d'évaluation sont définis par les sections AVA_VLA.2.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [3].

81 Le développeur a fourni une analyse des vulnérabilités potentielles du système. L'évaluateur a examiné cette fourniture et réalisé sa propre analyse de vulnérabilités indépendante.

82 Les tests de pénétration ont été réalisés lors de l'audit du site de Yamaguchi. L'objectif de ces tests de pénétration est de vérifier que la cible d'évaluation résiste aux attaques correspondant à un potentiel élémentaire de l'attaquant tel que défini par le composant AVA_VLA.2 "Analyse de vulnérabilités indépendante".

5.2.10 Audit

83 La cible d'évaluation étant un système, son évaluation a nécessité la réalisation d'un audit qui a été décomposé en deux parties :

- un audit technique qui a été l'occasion de réaliser les tests fonctionnels et de pénétration sur la cible d'évaluation ;
- un audit organisationnel qui a permis à l'évaluateur de vérifier que les mesures de sécurité pour la cible d'évaluation et pour l'environnement sont effectivement mises en œuvre par le développeur.

5.2.11 Verdicts

84 Pour tous les aspects des critères communs identifiés ci-dessus, un avis “réussite” a été émis.

Chapitre 6

Recommandations

85 Le système “Ligne de production CZ6 du site NEC à Yamaguchi-Japon” est soumis aux recommandations exprimées ci-dessous :

- les réticules et les programmes de test doivent être échangés de manière sûre entre leurs fournisseurs respectifs et la cible d’évaluation,
- les réticules et les programmes de test livrés doivent être sûrs,
- les personnels employés sur le site de Yamaguchi doivent être compétents et respectueux des règles de sécurité,
- le système doit être utilisé et administré conformément aux guides d’utilisation et d’administration validés.

86 Le respect de ces recommandations conditionne la validité du certificat.

Chapitre 7

Certification

7.1 Objet

87 Le système soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [3].

88 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL1 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élémentaire tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.

7.2 Portée de la certification

89 La certification ne constitue pas en soi une recommandation du système. Elle ne garantit pas que le système certifié est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle que des vulnérabilités exploitables n'aient pas été découvertes ; probabilité d'autant plus faible que le niveau d'assurance est élevé.

90 Le certificat ne s'applique qu'à la version évaluée du système identifiée au chapitre 3.

91 La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	L'addition d'un ou de plusieurs composants d'assurance de la Partie 3 des Critères Communs à un EAL ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou son environnement.
Cible d'évaluation	Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Evaluation	Estimation d'un profil de protection ou d'une cible d'évaluation par rapport à des critères définis.
Niveau d'assurance de l'évaluation	Un paquet composé de composants d'assurance tirés de la Partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des Critères Communs.
Objectif de sécurité	Une expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Politique de sécurité organisationnelle	Une ou plusieurs règles, procédures, codes de conduite ou lignes directrices de sécurité qu'une organisation impose pour son fonctionnement.
Profil de protection	Un ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

Acronymes

CISC	Complex Instruction Set Computer
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable and Programmable Read Only Memory
GPAO	Gestion de Production Assistée par Ordinateur
RAM	Random Access Memory
RISC	Reduced Instruction Set Computer
ROM	Read Only Memory
SOF	Strength of Function
TOE	Target of Evaluation
TSF	TOE Security Functions

Annexe B

Références

[1] [CC-1] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 1 : Introduction et modèle général CCIMB-99-031, version 2.1 Août 1999.

[2] [CC-2] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 2 : Exigences fonctionnelles de sécurité CCIMB-99-032, version 2.1 Août 1999.

[3] [CC-3] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 3 : Exigences d'assurance de sécurité CCIMB-99-033, version 2.1 Août 1999.

[4] [CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information Partie 2 : Méthodologie d'évaluation CEM-99/045, version 1.0 Août 1999.

[5] Cible de sécurité "Public Security Target - NEC Wafer Production - Japan", version 1.0 du 13 mai 2001 (document public).

[6] Rapport technique d'évaluation référencé NEC002-ETR01-1.01, version 1.00 du 20 avril 2001 (diffusion contrôlée).

[7] Profil de protection "Smartcard Integrated Circuit", version 2.0 de septembre 1998, enregistré sous la référence PP/9806 (document public).