PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

SERVICE CENTRAL 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 2000/04

Plate-forme ST19 (technologie 0.6µ) :
Micro-circuit ST19SF08BDxyz

Mars 2000

Ce document constitue le rapport de certification du produit "Plate-forme ST19 (technologie 0,6µ) : micro-circuit ST19SF08BDxyz".

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

www.scssi.gouv.fr

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

SCSSI
Centre de Certification de la Sécurité des Technologies de l'Information
18, rue du docteur Zamenhof
F-92131 ISSY-LES-MOULINEAUX CEDEX.

mèl : ssi20@calva.net

Ce document est folioté de 1 à 44 et certificat.

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

CERTIFICAT 2000/04

Plate-forme ST19 (technologie 0.6µ) :
Micro-circuit ST19SF08BDxyz

Développeur : STMicroelectronics SA

EAL4 augmenté

conforme au profil de protection PP/9806

Commanditaire :

STMicroelectronics SA

Le 31 mars 2000,

Le Commanditaire :
Group Vice-President Memory Products
General Manager Smartcard Products Division
Mr. M. FELICI

L'organisme de certification :
Le chef du Service central de la sécurité
des systèmes d'information
Le Général Jean-Louis DESVIGNES

Ce produit 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 (conforme à la norme ISO 15408) 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 produit 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 produit 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 produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

Organisme de Certification
SCSSI
18, rue du docteur Zamenhof
F-92131 ISSY-LES-MOULINEAUX CEDEX.

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du produit constitué du micro-circuit ST19SF08BDxyz, bâti sur la plate-forme ST19 de STMicrolectronics.

2 Les fonctionnalités évaluées sont consignées en annexe A du présent rapport.

3 Le niveau d'assurance atteint est le niveau EAL 4 augmenté des composants d'assurance AVA_VLA.4 "Résistance élevée", ALC_DVS.2 "Caractère suffisant des mesures de sécurité", ADV_IMP.2 "Implémentation de la TSF" tel que décrits dans la partie 3 des critères communs [4].

4 Ce produit est conforme au profil de protection "Smartcard Integrated Circuit" enregistré auprès du SCSSI sous la référence PP/9806, version 2.0 de Septembre 1998 [6].

5 Le profil de protection a fait l'objet d'un rapport de certification PP/9806 [7].

Chapitre 2

Résumé

2.1 Contexte

6 Ce processus s'inscrit dans le programme d'évaluation et de maintenance de la sécurité de la plate-forme ST19. Il a pour but de faciliter la conception et la certification de la sécurité des produits bâtis sur cette plate-forme.

7 Le véhicule test utilisé pour cette évaluation est le ST19SF08BDxyz qui fait l'objet du premier certificat joint au présent rapport.

8 La certification de toute version ultérieure du véhicule test ST19SF08 nécessitera une analyse d'impact des modifications apportées. Ces modifications seront évaluées à travers le programme de maintenance de la plate-forme ST19.

9 La certification d'une nouvelle version produit de la plate-forme nécessitera une analyse d'impact des modifications apportées, par rapport au véhicule test ST19SF08. En fonction des modifications apportées, une réévaluation partielle pourra être réalisée.

10 Les résultats de certification de la plate-forme et des produits dérivés ainsi que les documentations d'administration et d'utilisation, serviront de base respectivement aux commanditaires et développeurs de logiciels d'application pour les produits qu'ils souhaiteront certifier.

2.2 Description de la cible d'évaluation

11 La cible d'évaluation, bâtie sur la plate-forme ST19, comporte :

- le micro-circuit ST19SF08BDxyz et ses logiciels dédiés,
- l'environnement de développement tel que décrit dans le présent rapport.

12 Les développeurs de logiciels d'application (système d'exploitation, application spécifique, ...) et les utilisateurs de ces applications devront se conformer aux recommandations recensées, respectivement, dans les guides d'utilisation et d'administration. Ces logiciels n'ont pas fait l'objet de la présente évaluation et certification.

2.3 Résumé des caractéristiques de sécurité

2.3.1 Menaces

13 Les principales menaces identifiées dans la cible de sécurité [8] peuvent être résumées comme suit :

- modification non autorisée de la conception du circuit et des logiciels dédiés,
- divulgation non autorisée de la conception du circuit et des logiciels dédiés, des informations de tests et des outils de développement,
- utilisation abusive du micro-circuit.

14 Les biens à protéger au sein de la cible d'évaluation sont définis comme étant les données applicatives du micro-circuit, les logiciels dédiés, les données de spécification et de conception du micro-circuit. Ces biens doivent être protégés en intégrité et en confidentialité.

2.3.2 Politiques de sécurité organisationnelles et hypothèses

15 L'annexe A donne les principales caractéristiques de sécurité telles qu'elles sont décrites dans la cible de sécurité [8], en particulier les hypothèses d'utilisation du produit.

2.3.3 Exigences fonctionnelles de sécurité

16 Les principales fonctionnalités de sécurité du produit décrites dans la cible de sécurité [8] sont les suivantes :

- authentification des acteurs au cours de la phase de test,
- contrôle d'accès,
- analyse des violations potentielles de sécurité,
- non-observabilité,
- administration des fonctions de sécurité,
- protection des fonctions de sécurité : notification et résistance aux attaques physiques.

2.3.4 Exigences d'assurance

17 Les exigences d'assurance spécifiées dans la cible de sécurité [8] sont celles du niveau d'évaluation EAL4 augmenté des composants d'assurance AVA_VLA.4 "Résistance élevée", ALC_DVS.2 "Caractère suffisant des mesures de sécurité",

ADV_IMP.2 “Implémentation de la TSF” tel que décrits dans la partie 3 des critères communs [4].

2.4 Acteurs dans l’évaluation

18 Le commanditaire de l’évaluation est :

STMicroelectronics SA
ZI de Rousset BP2
F- 13106 Rousset Cedex.

19 La cible d’évaluation a été développée par la même société :

STMicroelectronics SA
ZI de Rousset BP2
F- 13106 Rousset Cedex.

20 La société Dupont a également participé au développement de la cible d'évaluation en tant que développeur et fabricant des réticules servant à la fabrication du ST19SF08BDxyz :

Dupont Photomasks
ZI de Rousset
F- 13106 Rousset Cedex.

21 Les sites de production des produits bâtis sur la plate-forme ST19 sont les suivants :

- en France,

  STMicroelectronics
  ZI de Rousset BP2
  F- 13106 Rousset Cedex

- en Italie,

  STMicroelectronics
  Via C. Olivetti 2
  20041 Agrate Brianza - Italie

  Le micro-circuit ST19SF08BDxyz qui a fait l’objet de cette certification, a été fabriqué à Agrate.

2.5 Contexte de l’évaluation

22 L’évaluation a été menée conformément aux critères communs ([1] à [4]) et à la méthodologie définie dans le manuel CEM [5].

23 L’évaluation s’est déroulée simultanément au développement du produit.

24 L’évaluation a été conduite par le centre d’évaluation de la sécurité des technologies de l’information de Serma Technologies :

- Serma Technologies
  30, avenue Gustavel Eiffel
  F- 33608 Pessac Cedex.

2.6 Conclusions de l'évaluation

25 Le produit soumis à évaluation dont la cible de sécurité [8] est partiellement reprise dans l’annexe A du présent rapport, satisfait aux exigences du niveau d’évaluation EAL 4 augmenté des composants d’assurance AVA_VLA.4 “Résistance élevée”, ALC_DVS.2 “Caractère suffisant des mesures de sécurité”, ADV_IMP.2 “Implémentation de la TSF”. Il est conforme aux exigences du profil de protection PP/9806 [6]. Par ailleurs, la résistance des fonctions de sécurité est cotée au niveau élevée (SOF-high).

26 La recherche de vulnérabilités exploitables au cours de l’évaluation a été définie par la quantité d’informations disponibles pour le niveau EAL4 et par la compétence, l’opportunité et les ressources correspondant à un potentiel d’attaques tel qu’il est spécifié par le composant d’assurance AVA_VLA.4.

27 Les vulnérabilités connues du commanditaire de l’évaluation ont été toutes communiquées aux évaluateurs et au certificateur conformément au critère [AVA_VLA.4.4E].

28 L'utilisation de la cible d'évaluation de manière sûre est soumise aux recommandations figurant au chapitre 6 du présent rapport.

Chapitre 3

Identification de la cible d'évaluation

3.1 Objet

29 La cible d'évaluation, bâtie sur la plate-forme ST19, comporte :

- le micro-circuit ST19SF08BDxyz et ses logiciels dédiés,
- l'environnement de développement tel que décrit dans le présent rapport.

30 Ce micro-circuit est destiné à recevoir les logiciels fournis par le développeur d'applications, masqués dans la mémoire programme (ROM) au cours de la fabrication du micro-circuit. Ces logiciels applicatifs (le système d'exploitation de la carte ainsi que les applications éventuelles) ne font pas partie de l'évaluation. Le micro-circuit est ensuite inséré dans une carte porteur de format carte de crédit ou tout autre support. Par ailleurs, les phases d'encartage et de personnalisation de la cible d'évaluation sont hors du champ de l'évaluation.

31 Le micro-circuit électronique contient des logiciels dédiés développés par STMicroelectronics à des fins de tests du circuit.

3.2 Historique du développement

32 Le composant ST19SF08BDxyz a été développé et testé par STMicroelectronics sur le site de Rousset. La production des micro-circuits est effectuée sur les sites d'Agrate (Italie) et Rousset (France).

3.3 Description du matériel

33 Le micro-circuit électronique ST19SF08BDxyz est un micro contrôleur 8 bits, bâti sur la plate-forme ST19.

34 Il dispose de différents mécanismes de sécurité participant à la réalisation des fonctions dédiées à la sécurité pour lesquelles l'évaluation a été demandée.

3.4 Description du logiciel

35 La cible d'évaluation contient également les logiciels dédiés développés par STMicroelectronics ; ces logiciels contiennent des fonctionnalités de tests actives pendant la phase de test du micro-circuit. A l'issue de cette phase, ils ne sont plus accessibles.

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

36 Les caractéristiques de sécurité évaluées sont consignées dans la cible de sécurité [8] qui est la référence pour l'évaluation.

37 Les paragraphes ci-après reformulent les éléments essentiels de ces caractéristiques.

4.2 Politique de sécurité

38 La politique de sécurité de la cible d'évaluation dont le modèle figure dans la documentation disponible au titre des critères ADV_SPM repose principalement sur :

- le contrôle d'accès aux informations sensibles stockées par le micro-circuit,
- l'irréversibilité des phases de vie du micro-circuit (passage irréversible de la configuration de tests à la configuration d'utilisation),
- la détection des violations potentielles de sécurité.

4.3 Menaces

39 Les menaces effectivement couvertes par le produit sont décrites dans le chapitre 3 de la cible de sécurité [8]. Elles sont reprises en annexe A.1.

4.4 Hypothèses d'utilisation et d'environnement

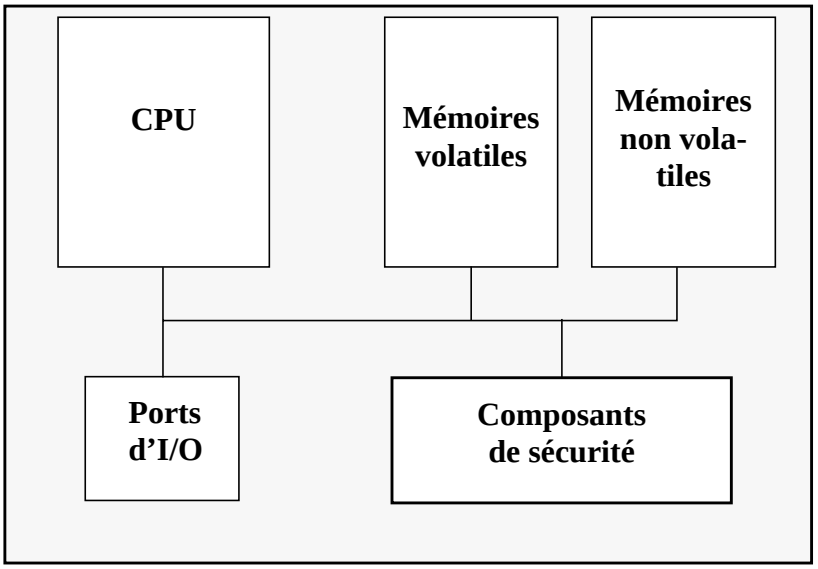
40 La cible d'évaluation doit être utilisée et administrée conformément aux exigences spécifiées dans la documentation d'utilisation et d'administration, et notamment dans le document Security Application Manual [10].

41 Les hypothèses d'utilisation et d'environnement du produit sont consignées dans le chapitre 3 de la cible de sécurité [8]. Celles-ci sont reprises en annexe A.2.

4.5 Architecture du produit

42 L'architecture du produit est décrite dans les documents de conception générale et détaillée exigibles pour les composants d'assurance ADV_HLD et ADV_LLD.

43 Le micro-circuit électronique ST19SF08 est un micro contrôleur bâti sur la plate-forme ST19. Il dispose d'une unité centrale de 8 bits associée à une mémoire de travail de 960 octets (RAM), d'une mémoire de programme de 32 Koctets (ROM), et d'une mémoire non volatile de 8Koctets (EEPROM). Il dispose également de différents composants de sécurité, d'une logique de matrice de contrôle d'accès, d'un générateur d'horloge ainsi que d'un générateur de nombres non-prédictibles. Ce dernier ne fait pas l'objet de cette évaluation.



Tab. 4.1 - Modèle d'architecture du micro-circuit ST19SF08B

4.6 Description de la documentation

44 La documentation disponible pour l'évaluation est décrite en annexe B du présent rapport de certification.

4.7 Tests de la cible d'évaluation

45 Plusieurs types de tests ont été passés sur le micro-circuit.

46 Les évaluateurs ont effectué un ensemble de tests sur le produit afin de vérifier par échantillonnage la conformité des fonctions de sécurité aux spécifications de sécurité. La procédure d'échantillonnage a été jugée conforme aux exigences du niveau d'évaluation EAL4.

47 De plus, dans le cadre du composant d'assurance AVA_VLA.4, les évaluateurs ont effectué de manière indépendante un ensemble de tests de pénétration sur le produit afin d'estimer l'efficacité des fonctions de sécurité offertes par le produit. Ces tests de pénétration sont adaptés à la nature du produit soumis à évaluation ainsi qu'à son environnement.

4.8 Configuration évaluée

48 La configuration de test de la cible d'évaluation est décrite en annexe B.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

49 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [9].

5.2 Résultats de l'évaluation de la cible de sécurité

50 La cible de sécurité répond aux exigences de la classe ASE, telle que définie dans la partie 3 des critères communs [4].

5.2.1 ASE_DES Description de la TOE

51 Les critères d'évaluation sont définis par les sections ASE_DES.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

52 La cible d'évaluation (TOE) est le micro-circuit ST19SF08BDxyz. Elle comporte les logiciels de tests dédiés. La description de la cible d'évaluation est précisée au chapitre 3 du présent rapport de certification.

5.2.2 ASE_ENV Environnement de sécurité

53 Les critères d'évaluation sont définis par les sections ASE_ENV.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

54 Les hypothèses d'utilisation et d'environnement du produit, ainsi que les menaces auxquelles doit faire face le produit sont décrites dans la cible de sécurité [8]. Ces caractéristiques de sécurité sont reprises en annexe A du présent rapport de certification.

5.2.3 ASE_INT Introduction de la ST

55 Les critères d'évaluation sont définis par les sections ASE_INT.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

56 L'introduction de la cible de sécurité [8] précise l'identification du produit et contient une vue d'ensemble de la cible de sécurité, ainsi qu'une annonce de conformité aux critères communs.

5.2.4 ASE_OBJ Objectifs de sécurité

57 Les critères d'évaluation sont définis par les sections ASE_OBJ.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

58 Les objectifs de sécurité pour la cible d'évaluation ainsi que pour l'environnement sont décrites dans la cible de sécurité [8]. Ces objectifs de sécurité sont repris en annexe A du présent rapport de certification.

5.2.5 ASE_PPC Annonce de conformité à un PP

59 Les critères d'évaluation sont définis par les sections ASE_PPC.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

60 L'évaluateur confirme l'annonce de conformité au profil de protection intitulé "Smartcard Integrated Circuit", référencé PP/9806 [6]. La cible de sécurité [8] constitue donc une instantiation correcte du profil de protection.

5.2.6 ASE_REQ Exigences de sécurité des TI

61 Les critères d'évaluation sont définis par les sections ASE_REQ.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

62 Les exigences de sécurité des TI fonctionnelles ou d'assurance sont décrites dans la cible de sécurité [8]. Ces exigences de sécurité sont reprises en annexe A du présent rapport de certification.

5.2.7 ASE_SRE Exigences de sécurité des TI déclarées explicitement

63 Les critères d'évaluation sont définis par les sections ASE_SRE.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

64 La cible de sécurité [8] ne contient pas d'exigences de sécurité des TI déclarées explicitement et ne faisant donc pas référence à la partie 2 des critères communs [2].

5.2.8 ASE_TSS.1 Spécifications de haut niveau de la TOE

65 Les critères d'évaluation sont définis par les sections ASE_TSS.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des critères communs [4].

66 La cible de sécurité [8] contient un résumé des spécifications des fonctions de sécurité du produit ainsi que les mesures d'assurance prises pour satisfaire les exigences d'assurance. L'évaluateur s'est assuré que ces fonctions de sécurité sont une représentation correcte des exigences fonctionnelles de sécurité et que les mesures d'assurance prises couvrent les exigences du niveau EAL4 augmenté.

5.3 Résultats de l'évaluation du produit

67 Le produit répond aux exigences des critères communs pour le niveau EAL4 augmenté des composants AVA_VLA.4 "Résistance élevée", ALC_DVS.2 "Caractère suffisant des mesures de sécurité", ADV_IMP.2 "Implémentation de la TSF" tel que décrits dans la partie 3 des critères communs [4].

5.3.1 ADV_FSP.2 : Spécifications fonctionnelles, définition exhaustive des interfaces externes

68 Les critères d'évaluation sont définis par les sections ADV_FSP.2.iE de la classe ADV, telle que définie dans la partie 3 des critères communs [4].

69 Le développeur a fourni la documentation spécifiant les fonctions de sécurité du produit. Les interfaces externes sont également décrites.

70 L'évaluateur a examiné ces spécifications et montré pour le niveau considéré qu'elles représentent une description complète et homogène des fonctionnalités de sécurité du produit.

5.3.2 ADV_SPM.1 : Modèle informel de politique de sécurité de la TOE

71 Les critères d'évaluation sont définis par les sections ADV_SPM.1.1E de la classe ADV, telle que définie dans la partie 3 des critères communs [4].

72 Le développeur a fourni un modèle de la politique de sécurité. L'évaluateur a examiné ce modèle et montré que toutes les fonctions de sécurité dans les spécifications fonctionnelles constituent une représentation complète et homogène du modèle de politique de sécurité.

5.3.3 ADV_HLD.2 : Conception générale de sécurité

73 Les critères d'évaluation sont définis par les sections ADV_HLD.2.iE de la classe ADV, telle que définie dans la partie 3 des critères communs [4].

74 Le développeur a fourni la conception générale du micro-circuit électronique et de ses logiciels de tests. Ce dossier présente la structure générale du produit pour chacun de ses sous-systèmes matériels et logiciels. L'ensemble des sous-systèmes principaux du microcircuit électronique et des logiciels de tests sont des sous-systèmes dédiés à la sécurité. La traçabilité entre les fonctions dédiées à la sécurité et les sous-systèmes a été vérifiée.

5.3.4 ADV_LLD.1 : Conception détaillée descriptive

75 Les critères d'évaluation sont définis par les sections ADV_LLD.1.iE de la classe ADV, telle que définie dans la partie 3 des critères communs [4].

76 Le développeur a fourni la conception détaillée du micro-circuit électronique comprenant la conception détaillée des logiciels de tests. Tous les composants élémentaires du microcircuit électronique et de ses logiciels dédiés sont spécifiés. La liste des mécanismes de sécurité est clairement établie. La traçabilité entre les fonctions dédiées à la sécurité et les mécanismes de sécurité puis les composants a été vérifiée. Une spécification ou une définition de chacun des mécanismes de sécurité est donnée.

5.3.5 ADV_IMP.2 : Implémentation de la TSF

77 Les critères d'évaluation sont définis par les sections ADV_IMP.2.iE de la classe ADV, telle que définie dans la partie 3 des critères communs [4].

78 Le développeur a fourni le code source des logiciels dédiés ainsi que les schémas descriptifs du micro-circuit. Une analyse détaillée du code source et des schémas a été effectuée par les évaluateurs afin de vérifier, d'une part, que ces éléments de réalisation constituent une représentation correcte et complète des fonctions de sécurité de la cible d'évaluation, et d'autre part, de rechercher des vulnérabilités potentielles.

5.3.6 ADV_RCR.1 : Démonstration de correspondance informelle

79 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 [4].

80 Le développeur a fourni une documentation de correspondance pour chaque représentation des fonctions de sécurité. Cette documentation indique la correspondance entre les fonctions de sécurité telles qu'elles sont définies dans deux niveaux adjacents de spécifications.

81 L'évaluateur a donc pu s'assurer de la conformité des spécifications fonctionnelles de sécurité à travers la conception générale, la conception détaillée du micro-circuit ainsi que son implémentation.

5.3.7 ACM_AUT.1 : Automatisation partielle de la CM

82 Les critères d'évaluation sont définis par la section ACM_AUT.1.1E de la classe ACM, telle que spécifiée dans la partie 3 des critères communs [4].

83 Le développeur a fourni la documentation du système de gestion de configuration utilisé pour le développement du micro-circuit électronique ainsi que ses logiciels dédiés.

84 Le système est fondé sur une gestion automatique de la configuration à travers un outil de gestion de configuration permettant de s'assurer que seuls les changements autorisés sur le produit sont possibles. L'évaluateur a analysé la documentation et vérifié au cours de l'audit du site de développement l'utilisation effective de l'outil de gestion de configuration, en accord avec les procédures du développeur.

5.3.8 ACM_CAP.4 : Aide à la génération et procédures de réception

85 Les critères d'évaluation sont définis par la section ACM_CAP.4.iE de la classe ACM, telle que spécifiée dans la partie 3 des critères communs [4].

86 Le développeur a fourni la documentation du système de gestion de configuration.

87 Ce système impose un contrôle des objets produits au cours du développement chez le développeur du micro-circuit. Des procédures permettent de prendre en compte

dans le système de gestion de configuration les objets composant la cible d'évaluation (procédure de réception). Des procédures gèrent également les révisions majeures et mineures de la cible d'évaluation. Pour le fondeur, la gestion de configuration passe par un système de suivi de toutes les modifications des niveaux de masque du produit. Le système de gestion de configuration énumère tous les composants élémentaires à partir desquels la cible d'évaluation a été construite. L'appellation commerciale de la cible d'évaluation (ST19SF08BDxyz) identifie les modifications majeures de ses constituants matériel ou logiciel.

88 Un système de gestion de configuration s'applique également chez le fabricant de réticules Dupont Photomasks. Les procédures utilisées sont en accord avec les principes du système de gestion de configuration du fondeur.

89 L'évaluateur s'est également assuré de l'absence d'incohérence dans la documentation fournie.

5.3.9 ACM_SCP.2 : Couverture du suivi des problèmes par la CM

90 Les critères d'évaluation sont définis par la section ACM_SCP.2.1E de la classe ACM, telle que spécifiée dans la partie 3 des critères communs [4].

91 Le système de gestion de configuration appliquée par le développeur couvre le produit ainsi que l'ensemble de sa documentation ; il couvre également toute erreur de sécurité qui pourrait être découverte : il contrôle donc la documentation de conception du produit, la documentation de test du produit, les éléments de réalisation du produit (schémas et code source), la documentation d'utilisation ainsi que la documentation d'administration.

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

92 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 [4].

93 Les procédures d'installation, de génération et de démarrage du produit concernent principalement la phase de fabrication du produit.

94 Elles définissent les exigences de sécurité que doit satisfaire le fondeur au cours de cette phase. L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation et a vérifié que ces procédures conduisent à une configuration sûre du produit.

5.3.11 ADO_DEL.2 : Détections de modification

95 Les critères d'évaluation sont définis par la section ADO_DEL.2.iE de la classe ADO, telle que spécifiée dans la partie 3 des critères communs [4].

96 Le développeur a fourni les procédures de livraison du produit. Celles-ci ont été vérifiées au cours d'une visite sur le site de production : en particulier, l'évaluateur s'est assuré que pendant la génération de la cible d'évaluation tout changement sera

audité afin de pouvoir a posteriori reconstituer exactement comment et quand la cible d'évaluation a été générée et livrée.

5.3.12 AGD_ADM.1 : Guide de l'administrateur

97 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 [4].

98 Le développeur a fourni la documentation d'administration des fonctions de sécurité du produit [10]. Ce guide d'administration est à usage :

- des développeurs de logiciels (Programming manual, Datasheet, User Manual, Security Application Manual) installés sur le micro-circuit qui administrent les fonctions de sécurité offertes par le micro-circuit électronique. En particulier, il contient un ensemble de recommandations sur le développement des logiciels applicatifs et sur l'utilisation sûre des fonctions de sécurité du micro-circuit.

- interne à STMicroelectronics,

- des fabricants et personnalisateurs (Datasheet, User Manual- Issuer, Die Description, Security Application Manual).

99 L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation et a vérifié que ces procédures permettent une administration sûre du produit.

5.3.13 AGD_USR.1 : Guide de l'utilisateur

100 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 [4].

101 Le développeur a fourni la documentation d'utilisation des fonctions de sécurité du produit [10]. Le guide d'utilisation est à usage :

- des développeurs de logiciels (Programming manual, Datasheet, User Manual- User, Security Application Manual) installés sur le micro-circuit qui administrent les fonctions de sécurité offertes par le micro-circuit électronique. En particulier, il contient un ensemble de recommandations sur le développement des logiciels applicatifs et sur l'utilisation sûre des fonctions de sécurité du micro-circuit.

- des fabricants et personnalisateurs (Datasheet).

102 L'évaluateur s'est assuré que cette documentation correspondait à une utilisation sûre du produit.

5.3.14 ALC_DVS.2 : Caractère suffisant des mesures de sécurité

103 Les critères d'évaluation sont définis par la section ALC_DVS.2.iE de la classe ALC, telle que spécifiée dans la partie 3 des critères communs [4].

104 Les évaluateurs ont analysé la sécurité du développement du micro-circuit électronique ainsi que la sécurité de la production au cours du processus de fabrication du micro-circuit (sites de Rousset et d'Agrate). La sécurité du développement et de la fabrication des réticules a également fait l'objet de l'évaluation.

105 Des procédures physiques, organisationnelles, techniques, liées au personnel assurent pour chaque organisme un niveau de protection de la cible d'évaluation, de ses constituants ainsi que de sa documentation qui répond aux exigences spécifiées par le composant ALC_DVS.2.

106 Des visites sur chacun des sites ont permis de vérifier l'application de ces procédures.

5.3.15 ALC_LCD.1 : Modèle de cycle de vie défini par le développeur

107 Les critères d'évaluation sont définis par la section ALC_LCD.1.1E de la classe ALC, telle que spécifiée dans la partie 3 des critères communs [4].

108 Le développeur a fourni le modèle de cycle de vie du micro-circuit électronique. Ce modèle est conforme au cycle de vie défini par le profil de protection PP/9806 [6].

109 L'évaluateur a analysé ce modèle et s'est assuré de l'absence d'incohérence dans ce modèle.

5.3.16 ALC_TAT.1 : Outils de développement bien définis

110 Les critères d'évaluation sont définis par la section ALC_TAT.1.iE de la classe ALC, telle que spécifiée dans la partie 3 des critères communs [4].

111 Le développeur a fourni la documentation relative aux outils de développement en ce qui concerne le développement du micro-circuit proprement dit (chaîne de développement du matériel) et le développement des logiciels de tests dédiés.

112 L'évaluateur a examiné cette documentation et s'est assuré de l'absence d'incohérences dans cette documentation. L'analyse de l'implémentation du produit (ADV_IMP.2) a également permis à l'évaluateur de confirmer la complétude de cette documentation.

5.3.17 ATE_FUN.1 : Tests fonctionnels

113 Les critères d'évaluation sont définis par la section ATE_FUN.1.iE de la classe ATE, telle que spécifiée dans la partie 3 des critères communs [4].

114 Le développeur a fourni la documentation de tests du produit. Les tests fournis par le développeur correspondent à un ensemble de tests matériels des fonctions de sécurité du micro-circuit, produits au cours de la caractérisation du micro-circuit et de sa production. En effet, deux types de tests sont réalisés sur le micro-circuit :

- des tests de l'ensemble des fonctionnalités de sécurité du micro-circuit au cours d'une phase dite de caractérisation du circuit, préalable à la mise en production des échantillons,

- des test de production effectués sur chaque micro-circuit à l'issue de sa fabrication, couvrant un sous-ensemble des fonctions de sécurité du produit.

115 Une documentation détaillée de tests a été fournie pour chacun des tests ; ces documentations décrivent le plan des tests, l'objectif des tests, les procédures de tests à réaliser ainsi que les résultats des tests.

116 L'évaluateur s'est assuré de la complétude de cette documentation.

5.3.18 ATE_COV.2 : Analyse de la couverture

117 Les critères d'évaluation sont définis par la section ATE_COV.2.iE de la classe ATE, telle que spécifiée dans la partie 3 des critères communs [4].

118 Le développeur a fourni une analyse de la documentation de tests justifiant la couverture de la spécification des fonctions de sécurité par les tests de caractérisation et de production.

119 L'évaluateur a confirmé cette analyse et procédé à des tests complémentaires

5.3.19 ATE_DPT.1 : Tests : conception générale

120 Les critères d'évaluation sont définis par la section ATE_DPT.1.iE de la classe ATE, telle que spécifiée dans la partie 3 des critères communs [4].

121 Le développeur a fourni une analyse de la documentation de tests justifiant la complétude des tests vis-à-vis de la conception générale du micro-circuit.

122 L'évaluateur a examiné cette documentation et s'est assuré de sa cohérence.

5.3.20 ATE_IND.2 Tests effectués de manière indépendante - échantillonnage

123 Les critères d'évaluation sont définis par les sections ATE_IND.2.iE de la classe ATE, telle que spécifiée dans la partie 3 des critères communs [4].

124 Les évaluateurs ont effectué un ensemble de tests sur le micro-circuit. Ils ont procédé à un échantillonnage des programmes de tests chez le développeur du micro-circuit électronique. La procédure d'échantillonnage a été jugée conforme aux exigences du niveau d'évaluation EAL4. Des tests complémentaires ont également été effectués par les évaluateurs.

5.3.21 AVA_MSU.2 : Validation de l'analyse

125 Les critères d'évaluation sont définis par la section AVA_MSU.2.iE de la classe AVA, telle que spécifiée dans la partie 3 des critères communs [4].

126 Le développeur a fourni une analyse de la documentation d'exploitation du produit permettant de vérifier l'absence d'utilisation impropre du circuit. Cette documentation identifie les modes d'exploitation de la cible d'évaluation ainsi que les conséquences et les implications de ces modes sur le maintien d'une exploitation sûre de la cible d'évaluation. Les évaluateurs ont réalisé des tests complémentaires afin de confirmer les résultats de cette analyse.

5.3.22 AVA_SOF.1 : Évaluation de la résistance des fonctions de sécurité de la TOE

127 Les critères d'évaluation sont définis par la section AVA_SOF.1.iE de la classe AVA, telle que spécifiée dans la partie 3 des critères communs [4].

128 Le développeur a fourni une analyse de la résistance des fonctions de sécurité du produit. Les évaluateurs ont analysé cette documentation et mené des analyses complémentaires. La cotation indépendante des mécanismes faite par les évaluateurs est en accord avec les analyses des développeurs. La résistance des fonctions de sécurité est considérée comme élevée. Les tests de pénétration ont permis de confirmer cette cotation.

5.3.23 AVA_VLA.4 : Résistance élevée

129 Les critères d'évaluation sont définis par les sections AVA_VLA.4.iE de la classe AVA, telle que spécifiée dans la partie 3 des critères communs [4].

130 Le développeur a fourni une documentation d'analyse des vulnérabilités potentielles du produit. L'évaluateur a examiné cette fourniture et réalisé sa propre analyse de vulnérabilités de manière indépendante.

131 L'évaluateur a réalisé des tests de pénétration, basés sur son analyse de vulnérabilités afin de pouvoir vérifier que le produit résiste aux attaques correspondant à un potentiel de l'attaquant tel que défini par le composant AVA_VLA.4 "Résistance élevée". Les attaques de nature évidente, incluant donc celles du domaine public, ont été également prises en compte dans cette analyse.

5.3.24 Verdicts

132 Pour tous les aspects des critères communs identifiés ci-dessus, un avis "réussite" a été émis.

Chapitre 6

Recommandations d'utilisation

133 La cible d'évaluation "ST19SF08BDxyz", bâtie sur la plate-forme ST19, est soumise aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

134 Le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [8].

135 Le produit doit être développé et utilisé conformément aux recommandations d'utilisation exprimées dans le document "Security Application Manual" [10]. Cette documentation contient des informations confidentielles et est disponible, de manière contrôlée, sur demande auprès de la société STMicroelectronics, Division Smartcard.

Chapitre 7

Certification

7.1 Objet

136 Le produit dont les caractéristiques de sécurité sont définies dans la cible de sécurité [8], satisfait aux exigences du niveau d'évaluation **EAL4 augmenté** des composants d'assurance suivants décrits dans la partie 3 des critères communs [3] :

- **AVA_VLA.4 "Résistance élevée"**,
- **ALC_DVS.2 "Caractère suffisant des mesures de sécurité"**,
- **ADV_IMP.2 "Implémentation de la TSF".**

137 Ce produit est conforme au profil de protection "Smartcard Integrated Circuit" enregistré auprès du SCSSI sous la référence PP/9806, version 2.0 de Septembre 1998 [6].

138 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour **le niveau EAL4** et **par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaques tel qu'il est spécifié par le composant d'assurance AVA_VLA.4.**

7.2 Portée de la certification

139 La certification ne constitue pas en soi une recommandation du produit. Elle ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle que des vulnérabilités exploitables n'aient pas été découvertes.

140 Le certificat ne s'applique qu'à la version évaluée du produit, telle qu'elle est définie en annexe B de ce rapport.

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

Annexe A

Caractéristiques de sécurité

142 Les caractéritiques de sécurité évaluées sont décrites dans la cible de sécurité [8] qui est la référence pour l'évaluation. Compte-tenu du caractère confidentiel de la cible de sécurité, un résumé public de la cible de sécurité a été rédigé [11], disponible sur demande.

143 La cible de sécurité étant rédigée en langue anglaise, les paragraphes ci-après sont une traduction française des hypothèses, des menaces ainsi que des objectifs et des exigences de sécurité.

A.1 Menaces

144 Le cycle de vie du produit est constitué des phases suivantes :

- phase 1 : développement des logiciels embarqués (systèmes d'exploitation, logiciels applicatifs),
- phase 2 : développement du micro-circuit et des logiciels dédiés,
- phase 3 : production du micro-circuit,
- phase 4 : mise en micro-modules (ateliers de micro-électronique),
- phase 5 : encartage,
- phase 6 : personnalisation,
- phase 7 : utilisation du produit final.

A.1.1 Clonage

T.CLON	Clonage fonctionnel de la cible d'évaluation.

A.1.2 Menaces sur la phase 1 (Développement des logiciels embarqués)

T.DIS_INFO	Divulgation non autorisée des biens délivrés par le concepteur du circuit au développeur des logiciels embarqués.
T.DIS_DEL	Divulgation non autorisée des logiciels embarqués pendant la phase de livraison au concepteur du circuit.
T.MOD_DEL	Modification non autorisée des logiciels embarqués pendant la phase de livraison au concepteur du circuit.
T.T_DEL	Vol des logiciels embarqués pendant la phase de livraison au concepteur du circuit.

A.1.3 Divulgation non autorisée au cours des phases 2 à 7

T.DIS_DESIGN	Divulgation non autorisée de la conception du circuit.
T.DIS_SOFT	Divulgation non autorisée des logiciels embarqués
T.DIS_DSOFT	Divulgation non autorisée des logiciels de tests dédiés.
T.DIS_TEST	Divulgation non autorisée des informations de tests du micro-circuit.
T_DIS_TOOLS	Divulgation non autorisée des outils de développement.
T_DIS_PHOTOMASK	Divulgation non autorisée des informations liées au réticule.

A.1.4 Vol ou utilisation abusive au cours des phases 2 à 7

T.T_SAMPLE	Vol ou utilisation abusive d'échantillons.
T.T_PHOTOMASK	Vol ou utilisation abusive des réticules du circuit.
T.T_PRODUCT	Vol ou utilisation abusive des produits cartes à puce.

A.1.5 Modification non autorisée au cours des phases 2 à 7

T.MOD_DESIGN	Modification non autorisée de la conception du circuit.
T.MOD_PHOTOMASK	Modification non autorisée des réticules du produit.
T.MOD_DSOFT	Modification non autorisée des logiciels de tests dédiés.
T.MOD_SOFT	Modification non autorisée des logiciels embarqués.

A.2 Hypothèses sur l'environnement

A.2.1 Hypothèses sur la phase 1

A.SOFT_ARCHI	Les logiciels embarqués doivent être développés de manière sûre, en veillant à assurer l'intégrité des programmes et des données.
A.DEV_ORG	Existence de procédures de sécurité traitant de la sécurité physique, liées au personnel, organisationnelles ou techniques au cours du développement des logiciels embarqués.

A.2.2 Hypothèses sur le processus de livraison de la cible d'évaluation (phases 4 à 7)

A.DLV_PROTECT	Existence de procédures assurant la protection de la cible d'évaluation au cours de la livraison.
A.DLV_AUDIT	Analyse et traitement des incidents.
A.DLV_RESP	Formation et qualification des personnels chargés de la livraison.

A.2.3 Hypothèses sur les phases 4 à 6

A.USE_TEST	Existence de tests fonctionnels adéquats des circuits intégrés au cours des phases 4 à 6.
A.USE_PROD	Existence de procédures de sécurité durant les phases de fabrication et de tests pour maintenir la confidentialité et l'intégrité de la cible d'évaluation.

A.2.4 Hypothèses sur la phase 7

A.USE_DIAG	Existence de protocoles de communication sûrs dans les échanges cartes et terminaux.
A.USE_SYS	L'intégrité et la confidentialité des données sensibles doivent être maintenues par le système.

145

A.3 Objectifs pour la cible d'évaluation

O.TAMPER	La TSF doit se prémunir contre les attaques physiques.
O.CLON	La TSF doit se prémunir contre le clonage fonctionnel.
O.OPERATE	La TSF doit assurer la continuité de ses fonctions de sécurité.
O.FLAW	La TSF ne doit pas contenir d'erreurs de conception, d'implémentation ou dans son exécution.
O.DIS_MECHANISM	La TSF doit se prémunir contre toute divulgation non autorisée de ces mécanismes de sécurité.
O.DIS_MEMORY	La TSF doit se prémunir contre toute divulgation non autorisée des informations sensibles contenues dans les mémoires.
O_MOD_MEMORY	La TSF doit se prémunir contre toute modification non autorisée des informations sensibles contenues dans les mémoires.

A.4 Objectifs pour l'environnement

A.4.1 Objectifs pour la phase 1

O.DEV_DIS	Maintien de l'intégrité et de la confidentialité des outils de développement fournis par le concepteur du circuit.
O.SOFT_DLV	Maintien de la sécurité au cours de la livraison des logiciels embarqués au concepteur du circuit.
O.SOFT_MECH	Utilisation par le développeur des logiciels embarqués des recommandations émises par le concepteur du circuit afin de garantir le niveau de sécurité du produit.
O.DEV_TOOLS	L'environnement de développement des logiciels embarqués doit permettre de garantir l'intégrité des programmes et des données.

A.4.2 Objectifs pour la phase 2

O.SOFT_ACS	Contrôle d'accès aux logiciels embarqués au sein du concepteur du microcircuit sur la base du besoin d'en connaître.
O.DESIGN_ACS	Contrôle d'accès aux informations relatives à la conception et à l'implémentation du micro-circuit.
O.DSOFT_ACS	Contrôle d'accès aux informations relatives à la conception et à l'implémentation des logiciels dédiés.
O.MASK_FAB	Existence de procédures de sécurité garantissant l'intégrité et la confidentialité de la cible d'évaluation au cours du processus de fabrication des réticules.
O.MECH_ACS	Contrôle de la diffusion des spécifications des mécanismes de sécurité du composant.
O.TI_ACS	Contrôle de la diffusion des informations liées à la technologie du composant.

A.4.3 Objectifs pour la phase 3

O.TOE_PRT	Protection de la cible d'évaluation au cours du processus de fabrication.
O.IC_DLV	Maintien de la confidentialité et de l'intégrité de la cible d'évaluation au cours des procédures de livraison des produits.

A.4.4 Objectifs pour les phases 4 à 7

O.DLV_PROTECT	Existence de procédures assurant la protection de la cible d'évaluation au cours de la livraison.
O.DLV_AUDIT	Analyse et traitement des incidents.
O.DLV_RESP	Formation et qualification des personnels chargés de la livraison.
O.TEST_OPERATE	Maintien de tests fonctionnels adéquats au cours des phases 4 à 6.
O.USE_DIAG	Existence de protocoles de communication sûrs dans les échanges cartes et terminaux au cours de la phase 7.
O.USE_SYS	L'intégrité et la confidentialité des données sensibles doivent être maintenues par le système au cours de la phase 7.

A.5 Exigences fonctionnelles de sécurité

A.5.1 Exigences fonctionnelles de sécurité pour la phase 3

Protection des données utilisateur	FDP_SDI.1	Contrôle de l'intégrité des données stockées.
Identification et authentification	FIA_UID.2 FIA_UAU.2 FIA_ATD.1	Identification de l'utilisateur préalablement à toute action. Authentification de l'utilisateur préalablement à toute action. Définition des attributs des utilisateurs.
Protection des fonctions de sécurité	FPT_TST.1	Test de la TSF.

A.5.2 Exigences fonctionnelles de sécurité pour la phase 3 à 7

Administration de la sécurité	FMT_MOF.1 FMT_MSA.1 FMT_SMR.1 FMT_MSA.3	Administration du comportement des fonctions de sécurité. Administration des attributs de sécurité. Rôles de sécurité. Initialisation statique d'attributs.
Protection des données utilisateur	FDP_ACC.2 FDP_ACF.1 FDP_IFC.1 FDP_IFF.1	Contrôle d'accès complet. Contrôle d'accès basé sur les attributs de sécurité. Contrôle de flux d'informations partiel Attributs de sécurité simple.
Audit de sécurité	FAU_SAA.1	Analyse de violation potentielle.
Protection de la vie privée	FPR_UNO.1	Non-observabilité
Protections des fonctions de sécurité	FPT_PHP.2 FPT_PHP.3	Notification d'une attaque physique. Résistance à une attaque physique.

A.6 Exigences d'assurance

Cible de sécurité	ASE	Évaluation de la cible de sécurité.
EAL4	ACM_AUT.1	Automatisation partielle de la CM.
	ACM_CAP.4	Aide à la génération et procédures de réception.
	ACM_SCP.2	Couverture du suivi des problèmes par la CM
	ADO_DEL.2	Détection de modifications
	ADO_IGS.1	Procédures d'installation, de génération et de démarrage.
	ADV_FSP.2	Définition exhaustive des interfaces externes.
	ADV_HLD.2	Conception générale de sécurité.
	ADV_IMP.1	Sous-ensemble de l'implémentation de la TSF.
	ADV_LLD.1	Conception détaillée descriptive.
	ADV_RCR.1	Démonstration de correspondance informelle.
	ADV_SPM.1	Modèle informel de politique de sécurité de la TOE.
	AGD_ADM.1	Guide de l'administrateur.
	AGD_USR.1	Guide de l'utilisateur.
	ALC_DVS.1	Identification des mesures de sécurité.
	ALC_LCD.1	Modèle de cycle de vie défini par le développeur.
	ALC_TAT.1	Outils de développement bien définis.
	ATE_COV.2	Analyse de la couverture.
	ATE_DPT.1	Tests : conception générale.
	ATE_FUN.1	Tests fonctionnels.
	ATE_IND.2	Tests effectués de manière indépendante - échantillonnage
	AVA_MSU.2	Validation de l'analyse
	AVA_SOF.1	Évaluation de la résistance des fonctions de sécurité de la TOE
	AVA_VLA.2	Analyse de vulnérabilités effectuée de manière indépendante.
Augmentation	ADV_IMP.2	Implémentation de la TSF.
	ALC_DVS.2	Caractère suffisant des mesures de sécurité.
	AVA_VLA.4	Résistance élevée.

Annexe B

Configuration de la cible d'évaluation

146 La cible d'évaluation, bâtie sur la plate-forme ST19, comporte :

- le micro-circuit ST19SF08BDxyz et ses logiciels dédiés,
- l'environnement de développement tel que décrit dans le présent rapport.

147 Afin de pouvoir être testé, le produit a été utilisé avec un logiciel embarqué développé par STMicroelectronics appelé "Card Manager". Ce logiciel ne fait pas partie de l'évaluation.

148 La configuration de test de la cible d'évaluation est la suivante :

- ST19SF08BDRZO :
  - micro-circuit : **ST19SF08B**,
  - logiciels enfouis : UH**D**,
  - logiciel "Card Manager" **RZO** (hors évaluation).

149 La documentation disponible pour le produit est la suivante :

- Documentation d'utilisation du produit : "ST19SF08 IC Data Sheet",
- Documentation d'administration du produit : "Security Application Manual", référencé [10].

Annexe C

Glossaire

C.1 Abréviations

CC	(Common Criteria) - Critères Communs, l'intitulé utilisé historiquement pour la présente norme à la place de l'intitulé officiel de l'ISO 15408: "Critères d'évaluation de la sécurité des technologies de l'information"
EAL	(Evaluation Assurance Level) - Niveau d'assurance de l'évaluation
PP	(Protection Profile) - Profil de protection
SF	(Security Function) - Fonction de sécurité
SFP	(Security Function Policy) - Politique d'une fonction de sécurité
ST	(Security Target) - Cible de sécurité
TI	(IT : Information Technology) - Technologie de l'Information
TOE	(Target of Evaluation) - Cible d'évaluation
TSF	(TOE Security Functions) - Ensemble des fonctions de sécurité de la TOE

C.2 Glossaire

Affectation	La spécification d'un paramètre identifié dans un composant.
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 à un EAL ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par les contre-mesures d'une TOE.
Cible d'évaluation (TOE)	Un produit ou un système TI et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité (ST)	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Classe	Un groupement de familles qui partagent un thème commun.
Composant	Le plus petit ensemble sélectionnable d'éléments qui peut être inclus dans un PP, une ST ou un paquet.
Évaluation	Estimation d'un PP, d'une ST ou d'une TOE par rapport à des critères définis.
Fonction de sécurité	Une partie ou des parties de la TOE sur lesquelles on s'appuie pour appliquer un sous-ensemble étroitement imbriqué de règles tirées de la TSP.
Informel	Qui est exprimé à l'aide d'un langage naturel.
Itération	L'utilisation multiple d'un composant avec des opérations différentes.
Niveau d'assurance de l'évaluation	Un paquet composé de composants d'assurance tirées de la Partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
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.

Plate-forme	Ensemble de technologies et de capacités pouvant être développées et appliquées afin de servir de base de croissance et d'innovation dans divers produits et services.
Politique de sécurité organisationnelle	Une ou plusieurs règles, procédures, codes de conduite ou lignes directrices de sécurité qu'une organisation impose pour son fonctionnement.
Produit	Un ensemble de logiciels, microprogrammes ou matériels TI qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.
Profil de protection	Un ensemble d'exigences de sécurité valables pour une catégorie de TOE, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.
Raffinement	L'addition de détails à un composant.
Sélection	La spécification d'une ou de plusieurs entités à partir d'une liste au sein d'un composant.
Utilisateur	Toute entité (utilisateur humain ou entité TI externe) hors de la TOE qui interagit avec elle.

Annexe D

Références

[1] [CC-1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIMB - 99-031, version 2.1, August 1999 (conforme à la norme ISO 15408),

[2] [CC-2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-99-032, version 2.1, August 1999 (conforme à la norme ISO 15408),

[3] [CC-2B] Common Criteria for Information Technology Security Evaluation Part 2 annexes CCIMB, version 2.1, August 1999 (conforme à la norme ISO 15408),

[4] [CC-3] Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIMB-99-033, version 2.1, August 1999 (conforme à la norme ISO 15408),

[5] [CEM] Common Methodology for Information Technology Security Evaluation CEM-99/045, version 1.0, August 1999.

[6] Profil de protection PP/9806, “Smartcard Integrated Circuit, Version 2.0” de Septembre 1998.

[7] Certificat PP/9806, Avril 1999.

[8] Cible de sécurité “ST19SF08B Security Target”, version 2.7, document confidentiel.

[9] Rapport technique d’évaluation, référencé PETRUS_ETR version 1.0, 15 mars 2000, document secret.

[10] Security Application Manual, Version 1, 17 february 2000, document confidentiel.

[11] Résumé de la cible de sécurité, “ST19SF08B Security Target”, document public.