



Liberté - Égalité - Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

SECRETARIAT 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 2001/04

Plate-forme ST19 (technologie 0.6 μ) :
Micro-circuit ST19SF16CCxyz

Mars 2001

Ce document constitue le rapport de certification du produit " Plate-forme ST19 (technologie 0,6μ) : micro-circuit ST19SF16CCxyz".

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.ssi.gouv.fr

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

Secrétariat général de la défense nationale
SCSSI
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

© SCSSI, France 2001.

La reproduction de tout ou partie de ce document, sans altérations ni coupures, est autorisée.

Tous les noms des produits ou des services de ce document sont des marques déposées de leur propriétaire respectif.

Ce document est folioté de 1 à 38 et certificat.



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

CERTIFICAT 2001/04

**Plate-forme ST19 (technologie 0.6 μ) :
Micro-circuit ST19SF 16CCxyz**

Développeur : STMicroelectronics SA

**EAL4 augmenté
conforme au profil de protection PP/9806**

Commanditaire : STMicroelectronics SA

Le 26 mars 2001,

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

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

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



Chapitre 1

Introduction

- 1 Ce document représente le rapport de certification du produit constitué du micro-circuit ST19SF16CCxyz, bâti sur la plate-forme ST19 de STMicroelectronics.
- 2 Le produit ST19SF16CCxyz présente des fonctionnalités de sécurité en tout point identiques aux fonctionnalités de sécurité du produit ST19SF16FFxyz, certifié et maintenu dans le cadre du programme de maintenance PM 2000/01 associé à la plate-forme ST19. Les produits se distinguent uniquement par la version des logiciels dédiés présents sur le micro-circuit.
- 3 Il a donc été procédé à la réévaluation du micro-circuit ST19SF16CCxyz, afin de réutiliser au mieux les résultats de l'évaluation du micro-circuit ST19SF16FFxyz (certificat 2000/13 [6]).
- 4 Le niveau d'assurance atteint est le niveau EAL4 augmenté des composants d'assurance suivants tels que 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",
 - ALC_FLR.1 "Correction d'anomalies élémentaire",
 - AMA_AMP.1 "Plan de maintenance de l'assurance",
 - AMA_CAT.1 "Rapport de classification des composants de la TOE".
- 5 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 [5].

Chapitre 2

Résumé

2.1 Contexte

7 Le produit soumis à cette évaluation est le micro-circuit ST19SF16CCxyz qui fait l'objet du certificat joint au présent rapport.

8 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

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

- le micro-circuit ST19SF16CCxyz et ses logiciels dédiés,
- l'environnement de développement tel que décrit dans le présent rapport.

10 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.

11 Ces logiciels d'application n'ont pas fait l'objet de la présente évaluation et certification.

2.3 Résumé des caractéristiques de sécurité

2.3.1 Menaces

12 Les principales menaces identifiées dans la cible de sécurité [7] 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.

13 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

14 L'annexe A donne les principales caractéristiques de sécurité telles qu'elles sont décrites dans la cible de sécurité [7], en particulier les hypothèses d'utilisation du produit.

2.3.3 Exigences fonctionnelles de sécurité

15 Les principales fonctionnalités de sécurité du produit décrites dans la cible de sécurité [7] 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

16 Les exigences d'assurance spécifiées dans la cible de sécurité [7] sont celles du niveau EAL4 augmenté des composants d'assurance suivants tels que 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",
- ALC_FLR.1 "Correction d'anomalies élémentaire",
- AMA_AMP.1 "Plan de maintenance de l'assurance",
- AMA_CAT.1 "Rapport de classification des composants de la TOE".

2.4 Acteurs dans l'évaluation

17 Le commanditaire de l'évaluation est :

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

18 La cible d'évaluation a été développée par la même société :

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

19 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 ST19SF16CCxyz :

Dupont Photomasks
ZI de Rousset
F- 13106 Rousset Cedex.

20 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
I- 20041 Agrate Brianza.

21 Le micro-circuit ST19SF16CCxyz qui a fait l'objet de cette certification, est fabriqué à Rousset et à Agrate.

2.5 Contexte de l'évaluation

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

23 L'évaluateur a procédé à une réévaluation basée sur les résultats de l'évaluation du micro-circuit ST19SF16FFxyz qui a fait l'objet du certificat 2000/13 [6].

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 réévaluation dont la cible de sécurité [7] est partiellement reprise dans l'annexe A du présent rapport, satisfait aux exigences du niveau EAL4 augmenté des composants d'assurance suivants tels que 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",
- ALC_FLR.1 "Correction d'anomalies élémentaire",
- AMA_AMP.1 "Plan de maintenance de l'assurance",
- AMA_CAT.1 "Rapport de classification des composants de la TOE".

26 Par ailleurs, la résistance des fonctions de sécurité est cotée au niveau élevée (SOF-high).

27 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 élevé tel qu'il est spécifié par le composant d'assurance AVA_VLA.4.

28 L'évaluation a également montré que le produit ST19SF16CCxyz est conforme aux exigences du profil de protection PP/9806 [5].

29 Enfin, 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

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

- le micro-circuit ST19SF16CCxyz et ses logiciels dédiés,
- l'environnement de développement tel que décrit dans le présent rapport.

29 Ce micro-circuit est destiné à recevoir les logiciels fournis par des développeurs 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.

30 Le micro-circuit est ensuite inséré dans une carte porteur de format carte de crédit ou tout autre support. Les phases d'encartage et de personnalisation sont hors du champ de l'évaluation.

31 Les modes d'utilisation du micro-circuit identifiés dans la cible de sécurité sont les suivants :

- mode TEST : mode utilisé pour les tests, uniquement actif en phase de fabrication du micro-circuit et dans un environnement sécurisé ;
- mode ISSUER : mode utilisé pour la pré-personnalisation et la personnalisation du micro-circuit ;
- mode USER : mode en utilisation finale du micro-circuit.

3.2 Historique du développement

32 Le composant ST19SF16CCxyz a été développé et testé par STMicroelectronics sur le site de Rousset. La production des micro-circuits est effectuée sur les sites de Rousset (France) et Agrate (Italie).

3.3 Description du matériel

33 Le micro-circuit électronique ST19SF16CCxyz 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 intégralement actives pendant la phase de test du micro-circuit (mode TEST) puis partiellement en mode ISSUER.

36 A l'issue de ces phases, 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 [7] 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 [7]. 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 [9].

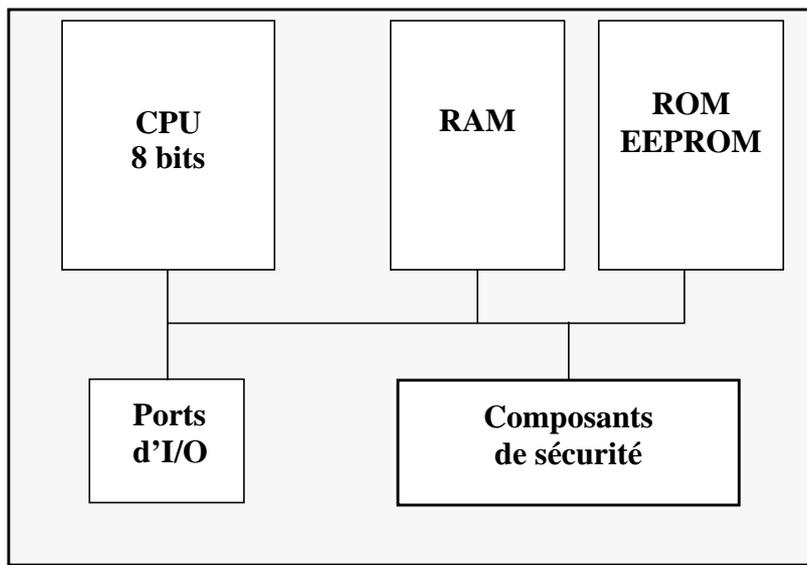
41 Les hypothèses d'utilisation et d'environnement du produit sont consignées dans le chapitre 3 de la cible de sécurité [7]. Celles-ci sont reprises en annexe A.2.

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 ST19SF16 est un micro contrôleur bâti sur la plateforme 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 16 Koctets (EEPROM). Il dispose également de différents composants de sécurité (une logique de matrice de contrôle d'accès, un générateur d'horloge, un générateur de nombres non-prédictibles). Le générateur de nombres non-prédictibles ne fait pas l'objet de cette évaluation.



Tab. 4.1 - Modèle d'architecture du micro-circuit ST19SF16

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 Configuration évaluée

45

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

46 Les résultats de l'évaluation sont exposés dans les rapports techniques d'évaluation [8].

5.2 Résultats de l'évaluation du produit

47 Le produit répond aux exigences des critères communs pour le niveau EAL4 augmenté des composants d'assurance suivants tels que 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",
- ALC_FLR.1 "Correction d'anomalies élémentaire",
- AMA_AMP.1 "Plan de maintenance de l'assurance",
- AMA_CAT.1 "Rapport de classification des composants de la TOE".

48 La cible de sécurité [7] constitue la référence de l'évaluation.

49 Les résultats de l'évaluation sont consignés dans les rapports techniques d'évaluation [8].

50 La version produit ST19SF16CCxyz ne diffère de la version ST19SF16FFxyz que par les logiciels dédiés présents sur le micro-circuit. L'analyse d'impact fournie par le développeur montre que cette caractéristique n'a pas d'incidence sur la sécurité du produit. Par ailleurs, les deux produits sont développés et fabriqués suivant les mêmes procédés et sur les mêmes sites de production. L'évaluateur a ainsi pu appuyer ses verdicts sur l'évaluation du composant ST19SF16FFxyz dont les résultats sont certifiés [6] et maintenus dans le cadre du programme de maintenance PM 2000/01.

51 Les travaux complémentaires effectués par l'évaluateur sont décrits ci-dessous.

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

52 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 [3].

53 L'évaluateur a vérifié la cohérence de la liste de configuration fournie pour le micro-circuit produit à Rousset et Agrate avec la référence du mask set inscrite sur

un échantillon. L'évaluateur a opéré cette vérification par inspection visuelle au moyen d'un microscope optique.

5.2.2 AVA_VLA.4 Résistance élevée

54 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 [3].

55 À partir de l'analyse d'impact fournie par STMicroelectronics, l'évaluateur a jugé nécessaire de réaliser à nouveau des tests de pénétration afin de pouvoir vérifier que le produit résiste aux attaques correspondant à un potentiel de l'attaquant élevé tel que défini par le composant AVA_VLA.4 "Résistance élevée".

5.3 Verdicts

56 Pour tous les aspects des Critères Communs identifiés ci-dessus, un avis "réussite" a été émis.

Chapitre 6

Recommandations d'utilisation

60

La cible d'évaluation "ST19SF16CCxyz", 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.

- a) le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [7].
- b) le produit doit être développé et utilisé conformément aux recommandations d'utilisation exprimées dans le document "Security Application Manual" [9]. Cette documentation contient des informations confidentielles et est disponible, de manière contrôlée, sur demande auprès de la société STMicroelectronics, Division Smartcard.
- c) des procédures de livraison sûre et des mesures de sécurité doivent impérativement être mises en place pour garantir la protection des micro-circuits en mode ISSUER ; et cela jusqu'à leur passage en mode USER.

Chapitre 7

Certification

7.1 Objet

61 Le produit dont les caractéristiques de sécurité sont définies dans la cible de sécurité [7], 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",
- ALC_FLR.1 "Correction d'erreurs élémentaire",
- AMA_AMP.1 "Plan de maintenance de l'assurance",
- AMA_CAT.1 "Rapport de classification des composants de la TOE".

62 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 [5].

63 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 élevé tel qu'il est spécifié par le composant d'assurance AVA_VLA.4.

7.2 Portée de la certification

64 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.

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

Annexe A

Caractéristiques de sécurité

- 66 Les caractéristiques de sécurité évaluées sont décrites dans la cible de sécurité [7] qui est la référence pour l'évaluation, et jointe au présent rapport de certification.
- 67 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

68 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	Divulgence non autorisée des informations délivrés par le concepteur du circuit au développeur des logiciels embarqués.
T.DIS_DEL	Divulgence 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 Divulgence non autorisée au cours des phases 2 à 7

T.DIS_DESIGN	Divulgence non autorisée de la conception du circuit.
T.DIS_SOFT	Divulgence non autorisée des logiciels embarqués.
T.DIS_DSOFT	Divulgence non autorisée des logiciels de tests dédiés.
T.DIS_TEST	Divulgence non autorisée des informations de tests du micro-circuit.
T.DIS_TOOLS	Divulgence non autorisée des outils de développement.
T.DIS_PHOTOMASK	Divulgence 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.

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.

Les **informations sensibles** désignent :

- les données applicatives chargées en EEPROM telles que les données de pré-personalisation,
- les logiciels dédiés.

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 micro-circuit 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 les phases en mode TEST et ISSUER**

Protection des données utilisateur	FDP_SDI.1	Contrôle de l'intégrité des données stockées.
Identification et authentification	FIA_UID.2	Identification de l'utilisateur préalablement à toute action.
	FIA_UAU.2	Authentification de l'utilisateur préalablement à toute action.
	FIA_ATD.1	Définition des attributs de l'utilisateur.
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	Administration du comportement des fonctions de sécurité.
	FMT_MSA.1	Administration des attributs de sécurité.
	FMT_SMR.1	Rôles de sécurité.
	FMT_MSA.3	Initialisation statique d'attributs.
Protection des données utilisateur	FDP_ACC.2	Contrôle d'accès complet.
	FDP_ACF.1	Contrôle d'accès basé sur les attributs de sécurité.
	FDP_IFC.1	Contrôle de flux d'informations partiel
	FDP_IFF.1	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	Notification d'une attaque physique.
	FPT_PHP.3	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 de haut niveau - identification des sous-systèmes dédiés à la sécurité.
	ADV_IMP.1	Sous-ensemble de l'implémentation de la TSF.
	ADV_LLD.1	Conception de bas niveau 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 de haut niveau.
	ATE_FUN.1	Tests fonctionnels.
	ATE_IND.2	Tests indépendants - 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 indépendante.	
Augmentation	ADV_IMP.2	Implémentation de la TSF.
	ALC_DVS.2	Caractère suffisant des mesures de sécurité.
	ALC_FLR.1	Correction d'anomalies élémentaire.
	AVA_VLA.4	Résistance élevée.
	AMA_AMP.1	Plan de maintenance de l'assurance.
AMA_CAT.1	Rapport de classification des composants de la TOE.	

Annexe B

Configuration de la cible d'évaluation

- 70 La cible d'évaluation, bâtie sur la plate-forme ST19, comporte :
- le micro-circuit ST19SF16CCxyz et ses logiciels dédiés,
 - l'environnement de développement tel que décrit dans le présent rapport.
- 71 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.
- 72 La configuration de test de la cible d'évaluation est la suivante :
- ST19SF16CC :
 - micro-circuit : ST19SF16C,
 - logiciels dédiés: TEC, UEC,
 - mask set K480A (site de fabrication de Rousset),
 - mask set K481A (site de fabrication d'Agrate).
- 73 La cible d'évaluation est livrée en mode ISSUER.
- 74 La documentation disponible pour le produit est la suivante :
- Documentation d'utilisation du produit : "ST19SFxx IC Data Sheet",
 - Documentation d'administration du produit : "Security Application Manual" [9].

Annexe C

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 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.
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.

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-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).
- [4] [CEM] Common Methodology for Information Technology Security Evaluation CEM-99/045, version 1.0, August 1999.
- [5] Profil de protection PP/9806, "Smartcard Integrated Circuit, version 2.0" de Septembre 1998.
- [6] Rapport de certification 2000/13, décembre 2000.
- [7] - "ST19SFxx Platform Security Target, version 1.4"
- "ST19SF16CCxyz Security Target Addendum rev. 1.0".
- [8] - Rapport technique d'évaluation, référencé AZUR_ETR version 1.0, 19 octobre 2000 (diffusion limitée).
- Rapport d'évaluation d'analyse d'impact, référencé AZUR2_AMA_SIA version 1.0, 27 février 2001 (diffusion limitée).
- Report on SIA_AZUR0012_001V1_0, version 2.1, 19 janvier 2001 (diffusion limitée).
- [9] Security Application Manual, Version 1.2, 30 juin 2000 (diffusion limitée).

