Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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 2002/06

Composant ST19SF02AD
masqué par l'application O.C.S. B0'V3
(référence ST19SF02AD/RRR)

Juin 2002

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma Français

d'Évaluation et de Certification

de la Sécurité des Technologies de l'Information

CERTIFICAT 2002/06

Composant ST19SF02AD masqué par l'application O.C.S. B0'V3

(référence ST19SF02AD/RRR)

Développeurs : STMicroelectronics, Oberthur Card Systems

Critères Communs

EAL4 Augmenté

conforme au profil de protection PP/9911

Commanditaire : Oberthur Card Systems

Centre d'évaluation : CEA LETI

Le 4 juin 2002,

Le Directeur central de la sécurité
des systèmes d'information
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 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, Direction centrale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Chapitre 1

Résumé

1.1 Objet

1 Ce document est le rapport de certification du composant ST19SF02AD masqué par l'application O.C.S. B0' V3 (référence ST19SF02AD/RRR).

2 L'application O.C.S. B0' V3 est l'application bancaire B4/B0' V3 et son système d'exploitationqui est masquée sur le micro-circuit ST19SF02. Le micro-circuit a été certifié sous la référence 2000/11 ; il est conforme au profil de protection PP/9806 ; la validité de ce certificat est assurée par le programme de maintenance PM 2000/ 01.

3 Le produit est conforme aux exigences du profil de protection PP/9911 «Smart Card Integrated Circuit with Embedded Software V2.0».

4 Le développeur du micro-circuit est STMicroelectronics :

- STMicroelectronics
  ZI de Rousset
  BP 2
  13106 Rousset Cedex
  France.

5 Le développeur du masque est Oberthur Card Systems :

- Oberthur Card Systems SA
  25, rue Auguste Blanche
  BP 133
  92804 Puteaux Cedex
  France.

6 L'évaluation a été menée conformément aux Critères Communs [CC] et à la méthodologie définie dans le manuel CEM [CEM].

7 Le niveau atteint par cette évaluation est le niveau d'assurance EAL 4 augmenté des composants :

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

8 L'évaluation du produit a été conduite par le Centre d'Evaluation de la Sécurité des Technologies de l'Information du CEA LETI :

- CEA Grenoble
  CESTI LETI
  17, rue des Martyrs
  38054 Grenoble Cedex 9
  France.

9 L'évaluation et la maintenance du micro-circuit est conduite par le Centre d'Evaluation de la Sécurité de l'Information de Serma Technologies :

- Serma Technologies
  30, rue Gustave Eiffel
  33608 Pessac Cedex
  France.

1.2 Contexte de l'évaluation

10 L'évaluation s'est déroulée parallèlement au développement du produit de septembre 2000 à avril 2002.

11 Le commanditaire de l'évaluation est Oberthur Card Systems :

- Oberthur Card Systems
  25, rue Auguste Blanche
  BP 133
  92804 Puteaux Cedex
  France.

Chapitre 2

Description de la cible d'évaluation

2.1 Périmètre de la cible d'évaluation

12 La cible d'évaluation est le composant ST19SF02AD masqué par l'application B4/ B0' V3 (référence ST19SF02AD/RRR) tel que décrit dans la cible de sécurité [ST]

13 Le produit évalué est constitué d'une partie matérielle :

- un micro-circuit ST19SF02, déjà évalué et certifié ;

14 et d'une partie logicielle ;

- le masque HOST V6.4 avec le système d'exploitation OS V6,
- et l'application carte bancaire B4/B0' V3.

2.2 Cycle de vie

15 Le produit suit le cycle de vie d'une carte à puce tel que décrit dans les profils de protection PP/9806 [PP9806] et PP/9911 [PP9911].

Phase 1 : Le développement de l'application logicielle qui est masquée sur le circuit a été examinée au cours de cette évaluation.

Phases 2 et 3 : Ces phases qui correspondent au développement et à la fabrication du micro-circuit ont été examinées au cours de l'évaluation du micro-circuit.

Phase 4 et 5 : Ces phases correspondent à la mise en micro-module et l'encartage des composants.

Phase 6 : Cette phase sert à la personnalisation des cartes.

Phase 7 : La phase d'utilisation du produit par le porteur.

16 Les phases 1 à 3 correspondent au développement et à la fabrication de la cible d'évaluation, les phases 4 à 7 à son utilisation.

17 Le produit a été évalué tel qu'il sort de la phase 3, il appartient ensuite à l'utilisateur de personnaliser le produit (phase 6) pour le faire fonctionner.

2.3 Fonctions de sécurité évaluées

18 Les fonctions de sécurité évaluées sont les suivantes :

- Intégrité des données des mémoires,
- Authentification des utilisateurs et administrateurs,
- Authentification de la carte,
- Authentification (certification) des transactions,
- Inhibition du mode tests,
- Cloisonnement des zones de mémoire à l'issue de la phase de fabrication,
- Contrôle d'accès aux zones de mémoire,
- Irréversibilité des phases,
- Enregistrement de l'autorité qui a écrit,
- Enregistrement de l'autorité qui a bloqué,
- Hyperviseur de sécurité,
- Lecture des données en phase d'invalidation,
- Réinitialisation,
- Disponibilité des services rendus par le composant masqué.

2.4 Documentation disponible

19 Des guides d'administration et d'utilisation fournis avec le produit permettent d'en assurer une utilisation sûre.

20 Ces guides [GUIDE] concernent :

- l'administration du composant masqué,
- les spécifications techniques de personnalisation,
- le protocole de pré-personnalisation,
- la pré-personnalisation client,
- l'utilisation du composant masqué.

Chapitre 3

Résultats de l'évaluation

3.1 Exigences d'assurance

Le produit a été évalué au niveau EAL 4 augmenté des composants ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4.

Classes d'Assurance	Composants d'Assurance
Cible de sécurité	ASE_INT.1 : Introduction de la ST ASE_DES.1 : Description de la TOE ASE_ENV.1 : Environnement de sécurité ASE_OBJ.1 : Objectifs de sécurité ASE_PPC.1 : Annonce de conformité à un PP ASE_REQ.1 : Exigences de sécurité des TI ASE_SRE.1 : Exigences de sécurité des TI explicitement énoncées ASE_TSS.1 : Spécifications globales de la TOE
Gestion de configuration	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
Livraison et exploitation	ADO_DEL.2 : Détection de modifications ADO_IGS.1 : Procédures d'installation, de génération et de démarrage
Développement	ADV_FSP.2 : Définition exhaustive des interfaces externes ADV_HLD.2 : Conception de haut niveau - identification des sous-sytèmes dédiés à la sécurité ADV_IMP.2 : 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
Guides	AGD_ADM.1 : Guide de l'administrateur AGD_USR.1 : Guide de l'utilisateur

Classes d'Assurance	Composants d'Assurance
Support au cycle de vie	ALC_DVS.2 : Caractère suffisant des mesures de sécurité ALC_LCD.1 : Modèle de cycle de vie défini par le développeur ALC_TAT.1 : Outils de développement bien définis
Tests	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
Estimation des vulnérabilités	AVA_MSU.2 : Validation de l'analyse AVA_SOF.1 : Évaluation de la résistance des fonctions de sécurité de la TOE AVA_VLA.4 : Résistance élevée

21 Pour tous les composants d'assurance ci-dessus, un verdict «réussite» a été émis par l'évaluateur.

22 Les travaux d'évaluation menés sont décrits dans le Rapport Technique d'Evaluation [RTE].

23 Dans le cadre des travaux d'évaluation, un audit organisationnel a été réalisé sur le site de développement de l'application à Puteaux ; cet audit a permis de s'assurer de l'application de mesures de sécurité suffisantes pour protéger les données sensibles utilisées.

24 La résistance des fonctions utilisant un mécanisme de type probabilistique ou permutationnel a été évalué au niveau élevé (SOF-high) exigé dans la cible de sécurité [ST].

3.2 Tests fonctionnels et de pénétration

3.2.1 Tests développeurs

25 Le développeur a effectué une campagne de test complète pour les deux applications pour vérifier la conformité avec les spécifications de Cartes Bancaires.

26 Les tests sur le micro-circuit ont été faits par STMicroelectronics.

3.2.2 Tests évaluateur

27 L'évaluateur a également mené une analyse de vulnérabilités, confirmée par des tests de pénétration, pour s'assurer qu'un attaquant disposant d'un potentiel

d'attaque élevé (composant AVA_VLA.4) ne peut pas remettre en cause les objectifs de sécurité de la cible d'évaluation suivants :

- la cible d'évaluation doit empêcher la manipulation des données sécuritaires,
- la cible d'évaluation doit permettre l'authentification de ses utilisateurs autorisés et de la carte,
- la cible d'évaluation doit assurer la continuité d'opération de ses fonctions de sécurité,
- la cible d'évaluation doit s'assurer que les données utilisateur ne sont accessibles qu'à des utilisateurs autorisés,
- la cible d'évaluation doit s'assurer que les informations sensibles en mémoires sont protégées contre toute modification non-autorisée.

3.3 Cotation des fonctions utilisant des mécanismes cryptographiques

28 La résistance des fonctions s'appuyant sur des mécanismes de nature cryptographique a été évaluée par la Direction Centrale de la Sécurité des Systèmes d'Information. Le niveau de ces fonctions est élevé.

Chapitre 4

Certification

4.1 Verdict

29 Ce présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL 4 augmenté des composants ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4, tels que décrits dans la partie 3 des Critères Communs [CC] :

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

30 De plus, la cible d'évaluation répond aux exigences du profil de protection «Smart Card Integrated Circuit with Embedded Software v2.0» [PP9911].

4.2 Recommandations

31 La cible d'évaluation "Composant ST19SF02AD masqué par l'application B4/ B0'V3 (référence ST19SF02AD/RRR)" est soumise aux recommandations d'utilisation ci-dessous :

a) le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [ST] ;

b) l'utilisation du produit doit être faite conformément aux guides d'administration et d'utilisation du produit [GUIDE].

4.3 Certification

32 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 ; probabilité d'autant plus faible que le niveau d'assurance est élevé.

33 Le certificat ne s'applique qu'à la version évaluée du produit identifiée au chapitre 2. 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	Addition d'un ou de plusieurs composants d'assurance de la partie 3 des CC à une échelle prédéfinie d'assurance ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou par son environnement.
Cible d'évaluation	Produit ou système et documentation associée pour (administrateur et utilisateur) qui est l'objet d'une évaluation.
Cible de sécurité	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 PP ou d'une cible d'évaluation par rapport à des critères définis.
Niveau d'assurance de l'évaluation (EAL)	Paquet de composants d'assurance extraits de la partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Produit	Ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.
Profil de protection	Ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

Annexe B

Références

[CC] Critères Communs pour l'évaluation de la sécurité des technologies de l'information :
- Part 1 : Introduction and general model, august 1999, version 2.1, réf : CCIMB-99-031 ;
- Part 2 : Security functional requirements, august 1999, version 2.1, réf : CCIMB-99-032 ;
- Part 3 : Security assurance requirements, august 1999, version 2.1, réf : CCIMB-99-033.

[CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information :
- Part 2 : Evaluation Methodology, august 1999, version 1.0, réf : CEM-99/045.

[ST] HOST Security Target - B0', Oberthur Card Systems, réf: PMEIGK/ADM/SEME/MDS-6O/B, version 3.06, décembre 2001. (document non public)
O.C.S. B0' V3 Security Target, version 1.0, réf: FQR 110 1932. (document public)

[RTE] Rapport Technique d'évaluation, CEA LETI, réf: LETI.CESTI.KHE.RTE.001, version 1.0 de mars 2002. (document non public)

[GUIDE]
- Evaluation de la sécurité du composant masqué B4/B0' V3, Documentation d'administration, Réf. GIE CB DET/DS/CBGEN6 V1.0, 09/2000,
- Spécification technique de la personnalisation du masque B4-B0' V3, Réf. DET/ES/SPE/2000-01 ver. 4 du 20/06/2000,
- Protocole de pré-pesonnalisation générique, Réf. 054762 00 POL Ed. 2-AA du 06/03/01,
- Pré-personnalisation client, Réf. 054762 00 PRP Ed. 2-AA du 02/03/01,
- Evaluation de la sécurité du composant masqué B4/B0' V3, Document d'utilisation, Ref: GIE CB DET/DS/CBGEN4 V1.0, 09/2000.

[PP9806] “Smartcard Integrated Circuit, Version 2.0”, septembre 1998, enregistré au catalogue des profils de protection certifiés sous la référence PP/9806.

[PP9911] “Smartcard Integrated Circuit with Embedded Software”, version 2.0, juin 1999, enregistré au catalogue des profils de protection certifiés sous la référence PP/9911.

[2000/11] Rapport de Certification 2000/11 «Plate-forme ST19 (technologie 0.6µ) : Micro-circuit ST19SF02ADxyz», décembre 2000, Schéma Français d’Evaluation et de Certification de la Sécurité des Technologies de l’Information.

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
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau Certification
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

certification.dcssi@sgdn.pm.gouv.fr