PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

DIRECTION CENTRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

Rapport de certification 2001/16

Composant masqué CT2000
(référence ST16RF58HD50/RSG-A)

Septembre 2001

Ce document constitue le rapport de certification du produit “Composant masqué CT2000 (référence ST16RF58HD50/RSG-A)”.

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

www.ssi.gouv.fr

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

Secrétariat général de la Défense nationale
DCSSI
Bureau de Certification
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

certification.dcssi@sgdn.pm.gouv.fr

Ce document est folioté de 1 à 20 et certificat.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

CERTIFICAT 2001/16

Composant masqué CT2000
(référence ST16RF58HD50/RSG-A)

Développeur : ASK

EAL1 Augmenté

Commanditaire : ASK

Le 6 septembre 2001,

Le Commanditaire :
Le Directeur d'ASK

Georges Kayanakis

L'Organisme de certification :
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 Latour-Maubourg
F-75700 PARIS 07 SP.

Common Criteria

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du produit “Composant masqué CT2000 (référence ST16RF58HD50/RSG-A)”.

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

3 La cible d’évaluation est le composant masqué CT2000 consituté du micro-circuit ST16RF58HD50 fabriqué par STMicroelectronics et de son masque dévéloppé par ASK.

4 La cible d’évaluation est un composant masqué destiné à être inséré dans un support plastique pour être utilisé comme carte de transport, pouvant fonctionner soit en insertion (mode contact) soit en télé-alimentation (mode sans contact).

Chapitre 2

Résumé

2.1 Contexte de l'évaluation

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

6 Elle s'est déroulée consécutivement au développement du produit de décembre 2000 à juillet 2001.

7 Le commanditaire de l'évaluation et développeur de l'application est (ci-après "le commanditaire" ou "le développeur") :

- ASK
  15, traverse des Brucs
  F-06560 Sophia Antipolis.

8 Le fabricant du micro-circuit est :

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

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

- Serma Technologies
  30, avenue Gustave Eiffel
  F-33608 Pessac.

2.2 Description de la cible d'évaluation

10 La cible d'évaluation est le produit "Composant masqué CT2000" (référence ST16RF58HD50/RSG-A).

11 Les fonctions de sécurité de la cible d'évaluation telles que décrites dans la cible de sécurité [ST] ont été évaluées :

- Contrôle d'accès,
- Authentification de données externes,
- Authentification de données internes,
- Intégrité des données internes,
- Détection d'une utilisation anormale,
- Détection du rejeu,

- Contrôle de certificat d'intégrité,
- Authentification du porteur,
- Déchiffrement des clés.

2.3 Conclusions de l'évaluation

12 Le produit soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 tel que décrit dans la partie 3 des Critères Communs [CC-3].

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

14 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

15 La cible d'évaluation est un composant masqué destiné à être inséré dans un support plastique pour être utilisé comme carte de transport, pouvant fonctionner soit en insertion (mode contact) soit en télé-alimentation (mode sans contact).

16 La cible d'évaluation est constituée des éléments suivants :

- Le micro-circuit intégré comportant le logiciel applicatif,
- L'interface sans contact (l'antenne elle-même n'est pas identifiée comme un élément de la cible d'évaluation) et les composants associés qui permettent la communication sans contact.

17 Le cycle de vie d'une carte de transport CT2000 comporte les phases suivantes:

- Phase de fabrication pendant laquelle le logiciel embarqué est masqué sur le composant,
- Encartage,
- Phase de pré-personnalisation pendant laquelle des informations spécifiques (complément de code, architecture mémoire, numéro de série, clé de fabrication) sont insérés dans la carte,
- Phase opérationnelle pendant laquelle la carte est utilisée.

3.2 Historique du développement

18 L'application billetique a été développée par ASK. Cette application a été fournie à STMicroelectronics pour être masquée sur le micro-circuit.

3.3 Description des matériels

19 Le micro-circuit est fabriqué par STMicroelectronics sous la référence ST16RF58HD50, référence de masquage RSG-A.

3.4 Description des logiciels

20 L'application de billetique a été développée par ASK et est constituée des deux éléments suivants:

- L'application installée en ROM, version 1.0 référencée CT2000_MASK_000821,
- Le correctif applicatif chargé en EEPROM, version 2.0 référencée CT2000_PATCH_001110_V02.

3.5 Description de la documentation

21 Les documentations d'utilisation de la cible d'évaluation sont:

- Le guide administrateur [GUIDE_ADM] à destination de l'administrateur qui intervient dans un équipement pour la réalisation de transactions. Il existe plusieurs types d'équipements en fonction des fonctionnalités définies pour le système (validation, rechargement,...).
- Le guide utilisateur [GUIDE_USR] à destination du porteur pour la saisie du PIN uniquement.

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

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

4.2 Hypothèses

23 La cible d'évaluation (TOE) doit être utilisée dans un environnement qui satisfait aux hypothèses énoncées dans la cible de sécurité.

24 Ces hypothèses couvrent les aspects suivants :

- Connaissance par les utilisateurs des responsabilités envers le produit,
- Utilisation d'équipements de confiance pendant le développement de la TOE.

25 Le détail de ces hypothèses est disponible dans la cible de sécurité [ST].

4.3 Menaces

26 Les biens à protéger au sein de la cible d'évaluation sont les suivants :

- les traitements,
- les informations de gestion de la structure,
- les paramètres applicatifs,
- les informations sur le porteur,
- les éléments secrets (clés, PIN).

27 Les menaces couvertes par la cible d'évaluation ou par son environnement sont celles définies dans la cible de sécurité [ST]. Elles peuvent être résumées comme suit :

- Clonage de la cible d'évaluation,
- Divulgation non autorisée d'informations ayant un besoin de confidentialité et d'intégrité,
- Divulgation interdite d'éléments secrets,
- Modification non autorisée d'informations sensibles
- Modification non autorisée de traitements sensibles,
- Rejeu d'une authentification ou d'une transaction.

4.4 Politiques de sécurité organisationnelles

28 Les politiques de sécurité organisationnelles que doit respecter la cible d'évaluation et son environnement sont celles définies dans la cible de sécurité [ST]. Elles peuvent être résumées comme suit :

- La TOE doit, en phase opérationnelle, donner à l'équipement avec lequelle elle dialogue, la possibilité de vérifier l'intégrité de certaines informations,
- La TOE doit déchiffrer les clés qui lui sont transmises avant de les stocker,
- La TOE doit s'authentifier auprès d'un équipement,
- La TOE doit pouvoir vérifier l'intégrité de certaines informations qui lui sont transmises,
- La TOE doit pouvoir notifier à l'équipement avec lequel elle dialogue des violations de sécurité.

4.5 Fonctions de sécurité évaluées

29 La liste des fonctions de sécurité évaluées est disponible dans la cible de sécurité [ST]. Ces fonctions de sécurité peuvent être résumées comme suit :

- Contrôle d'accès,
- Authentification de données externes,
- Authentification de données internes,
- Intégrité des données internes,
- Détection d'une utilisation anormale,
- Détection du rejeu,
- Contrôle de certificat d'intégrité,
- Authentification du porteur,
- Déchiffrement des clés.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

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

5.2 Principaux résultats de l'évaluation

31 Le produit répond aux exigences des Critères Communs pour le niveau EAL1 augmenté du composant suivant tel que décrit dans la partie 3 des Critères Communs [CC-3] :

- AVA_VLA.2 : Analyse de vulnérabilités indépendante.

5.2.1 ASE : Evaluation de la cible de sécurité

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

33 La cible de sécurité [ST] fournie par le développeur décrit de manière suffisamment claire la cible d'évaluation, l'environnement supposé d'exploitation ainsi que les fonctions de sécurité évaluées. La cible de sécurité démontre que la liste des fonctions de sécurité répond aux objectifs de sécurité et par conséquent permet de contrer les menaces sur la TOE définies dans cette même cible.

5.2.2 ACM_CAP.1 : Numéro de version

34 Les critères d'évaluation sont définis par la section ACM_CAP.1.iE de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [CC-3].

35 La TOE et ses différents éléments sont correctements identifiés par une unique référence, ce qui est établi de la manière suivante :

- version 1.0 pour la version du logiciel en ROM (étiquette CT2000_MASK_000821) et version 2.0 pour le code en EEPROM (CT2000_PATCH_001110_V02),
- ST16RF58 HD50 -220pF pour le micro-circuit avec un masque RSG-A.

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

36 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 [CC-3].

37 La seule procédure de démarrage de la TOE est la mise sous tension de la carte (reset).

5.2.4 ADV_FSP.1 : Spécifications fonctionnelles informelles

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

39 L'évaluateur a examiné l'ensemble des spécifications et des interfaces. Il a vérifié qu'elles représentent une description complète et homogène des fonctionnalités de sécurité du produit.

5.2.5 ADV_RCR.1 : Démonstration de correspondance informelle

40 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 [CC-3].

41 L'évaluateur s'est assuré de la correspondance entre les différentes représentations des fonctions de sécurité de la cible d'évaluation.

5.2.6 AGD_ADM.1 : Guide de l'administrateur

42 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 [CC-3].

43 La documentation d'administration contient les informations relatives aux commandes d'administration de la carte (validation, rechargement, ...).

44 L'évaluateur s'est assuré que cette documentation permet une administration sûre du produit.

5.2.7 AGD_USR.1 : Guide de l'utilisateur

45 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 [CC-3].

46 La documentation d'utilisation contient les informations relatives à la mise en oeuvre des fonctions de sécurité de la cible d'évaluation pour l'utilisateur final (utilisation du code PIN).

47 L'évaluateur s'est assuré que cette documentation permet une utilisation sûre du produit.

5.2.8 ATE_IND.1 : Tests indépendants - conformité

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

49 L'évaluateur a effectué des tests fonctionnels sur le produit afin de vérifier la conformité des fonctions de sécurité par rapport aux spécifications de sécurité.

5.2.9 AVA_VLA.2 : Analyse de vulnérabilité indépendante

50 Les critères d'évaluation sont définis par les sections AVA_VLA.2.iE de la classe AVA, telles que spécifiées dans la partie 3 des Critères Communs [CC-3].

51 L'évaluateur a réalisé des tests de pénétration indépendants, basés sur son analyse de vulnérabilité afin de pouvoir vérifier que la cible d'évaluation résiste aux attaques correspondant à un potentiel de l'attaquant élémentaire tel que défini par le composant AVA_VLA.2.

5.2.10 Verdicts

52 Pour tous les aspects des Critères Communs identifiés ci-dessus, un avis "réussite" est émis.

Chapitre 6

Recommandations d’utilisation

53 La cible d’évaluation “Composant masqué CT2000” (référence ST16RF58HD50/RSG-A) 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 [ST].

b) Les procédures d’administration et d’utilisation de la TOE décrites par le développeur du composant masqué dans ses procédures d’administration [GUIDE_ADM] et d’utilisation [GUIDE_USR] doivent être respectées.

Chapitre 7

Certification

7.1 Objet

54 Le produit soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA.VLA.2 tels que décrit dans la partie 3 des Critères Communs [CC-3].

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

7.2 Portée de la certification

56 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.

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

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

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	L'addition d'un ou de plusieurs composants d'assurance de la Partie 3 à un EAL ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou son environnement.
Cible d'évaluation (TOE)	Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Niveau d'assurance de l'évaluation (EAL)	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.
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 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 cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

Annexe B

Références

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

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

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

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

[ST] Cible de sécurité : Security Target ASE, ASK, version 1.21, 4.04.2001, référencée STE000010. Version publique disponible sur demande auprès du commanditaire.

[RTE] Rapport technique d'évaluation, CESTI de SERMA Technologies, version 1.2, 16.07.2001, référencé RTE_ONTARIO_V1.2.fm (diffusion contrôlée).

[GUIDE_ADM] Manuel administrateur : Administrator Guidance, ASK, version 1.1, 4.04.2001, référencé STE010005 (diffusion contrôlée)

[GUIDE_USR] Manuel utilisateur : User Guidance, ASK, version 1.1, 4.04.2001, référencé STE010006 (diffusion contrôlée)