PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/42

Applet CryptoSmart V2.0 sur base Oberthur COSMO64RSA D V5.2

Paris, le 1 décembre 2005

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2005/42

Produit : Applet CryptoSmart V2.0 sur base Oberthur COSMO64RSA D V5.2

Développeur : ERCOM SA.

Critères Communs version 2.2

EAL2 Augmenté

(ADV_HLD.2, ADV_IMP.1*, ADV_LLD.1*, ALC_DVS.1, ALC_TAT.1*, ALC_FLR.3, AVA_MSU.1, AVA_VLA.2)

*appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

Commanditaire : ERCOM SA.

Centre d'évaluation : Serma Technologies

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics. (article 7)
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (article 8)

Les procédures de certification sont publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)
Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.
[2] En mai 2005, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède, la Turquie, la République Tchèque, Singapour et l'Inde.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est l'applet CryptoSmart en version 2.0 (référence 2.0-000035-C37DB42C), chargée sur plate-forme Oberthur COSMO64RSA D V5.2. Le micro-circuit sous-jacent a pour référence : P5CT072.

1.2. Développeur

L'applet Cryptosmart est développée par la société :

ERCOM SA.

Immeuble Nungesser
13, avenue Morane Saulnier
78140 Vélizy
France

Pour information, la plate-forme COSMO64RSA est développée par la société :

Oberthur Card Systems

71-73, rue des Hautes Pâtures
92726 Nanterre Cedex
France

Pour information, le micro-circuit est développé par la société

Philips Semiconductors GmbH

Business Line Identification
P.O. Box 54 02 40
D-22502 Hamburg,
Germany

1.3. Description du produit évalué

1.3.1. Architecture

La carte constituée de l'applet Cryptosmart chargée sur la plate-forme Oberthur COSMO64RSA intervient dans un système de télécommunication de type :

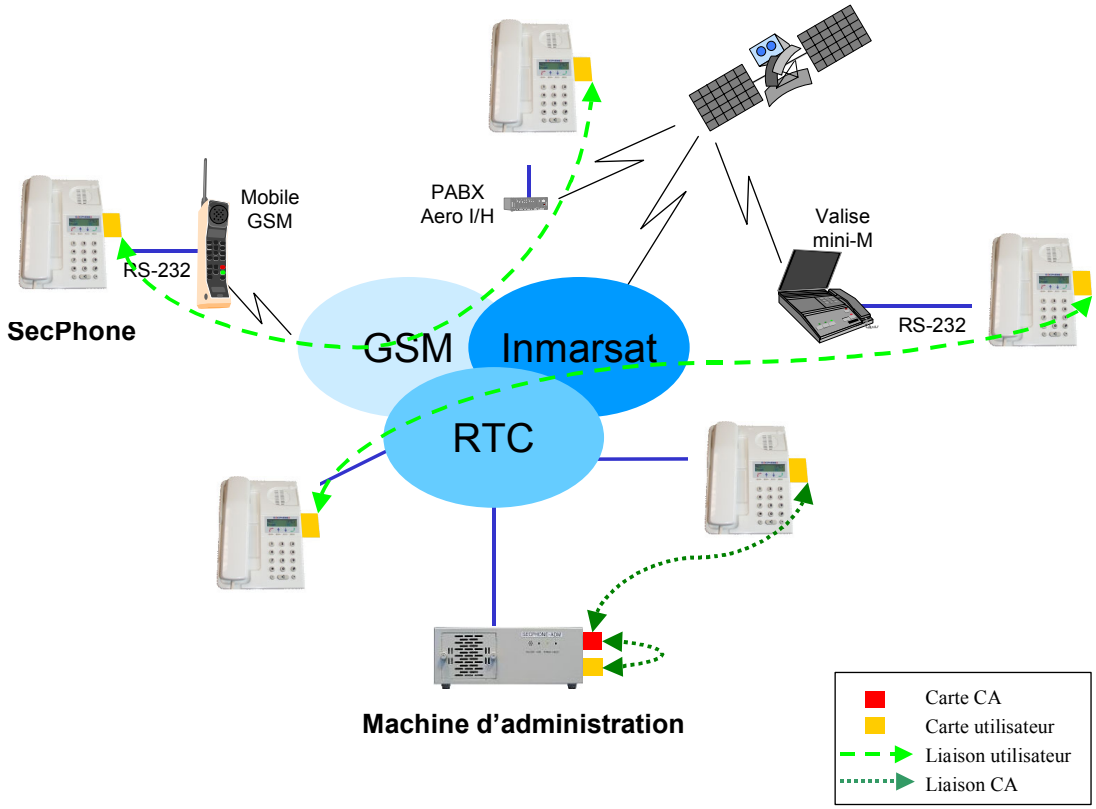

Figure 1 – Utilisation de la carte Cryptosmart

Insérée dans un téléphone SECPHONE, la carte Cryptosmart permet :

- d'authentifier l'utilisateur par un code PIN ;
- d'identifier et d'authentifier les correspondants entre eux ;
- de décider si la communication est autorisée ;
- de calculer une clé de session différente à chaque appel.

Les clés de session sont délivrées par la carte au téléphone SECPHONE qui chiffre alors les communications à l'aide d'un chiffrement symétrique (AES).

Les cartes à puce CryptoSmart sont regroupées en familles, dont une des cartes, dite « carte CA », a en charge la gestion des certificats pour l'ensemble de la famille. Les autres cartes sont dites « cartes utilisateur ». Seules des cartes à puce issues d'une même carte CA peuvent dialoguer ensemble. Une famille dispose d'un identifiant textuel « de famille », choisi par l'administrateur lors de la création de la carte CA.
La carte CA possède un bi-clé RSA dédié à la signature des clés publiques d'authentification des cartes de sa famille. Elle possède elle-même un bi-clé RSA d'authentification, comme une carte Utilisateur. Chaque carte Utilisateur connaît sans risque d'usurpation la clé publique de signature de la carte CA.
L'administration des cartes à puce est effectuée à l'aide d'une station d'administration, dispositif indépendant qui permet de créer les cartes localement, puis de les maintenir localement ou à distance.

L'architecture de la carte elle-même est présentée dans le schéma suivant :

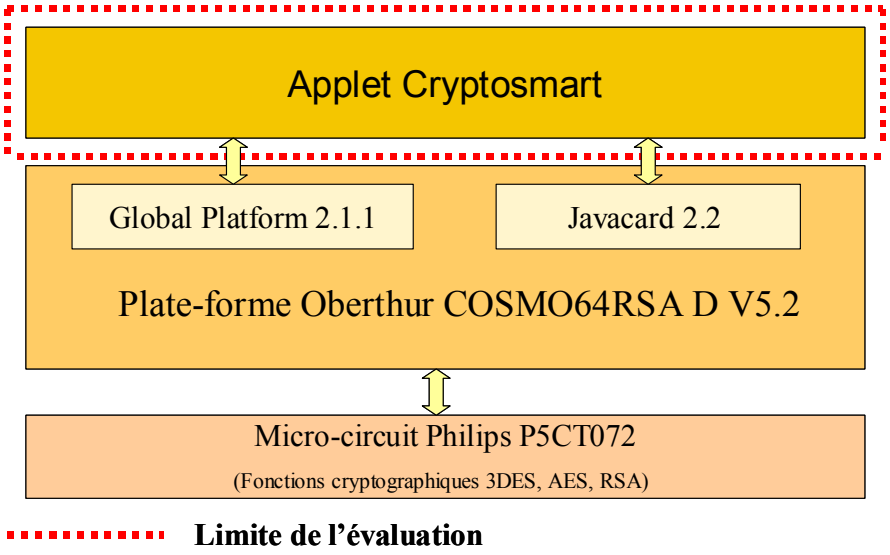

Figure 2 – Architecture de la carte Cryptosmart

L'applet met en œuvre des fonctionnalités d'audit, de cryptographie, de protection et de filtrage, d'identification et d'authentification, et de gestion de la sécurité (administration notamment). Ces fonctionnalités sont détaillées dans la cible de sécurité du produit (cf. [ST]).

1.3.2. Cycle de vie

Le cycle de vie du produit est le suivant :

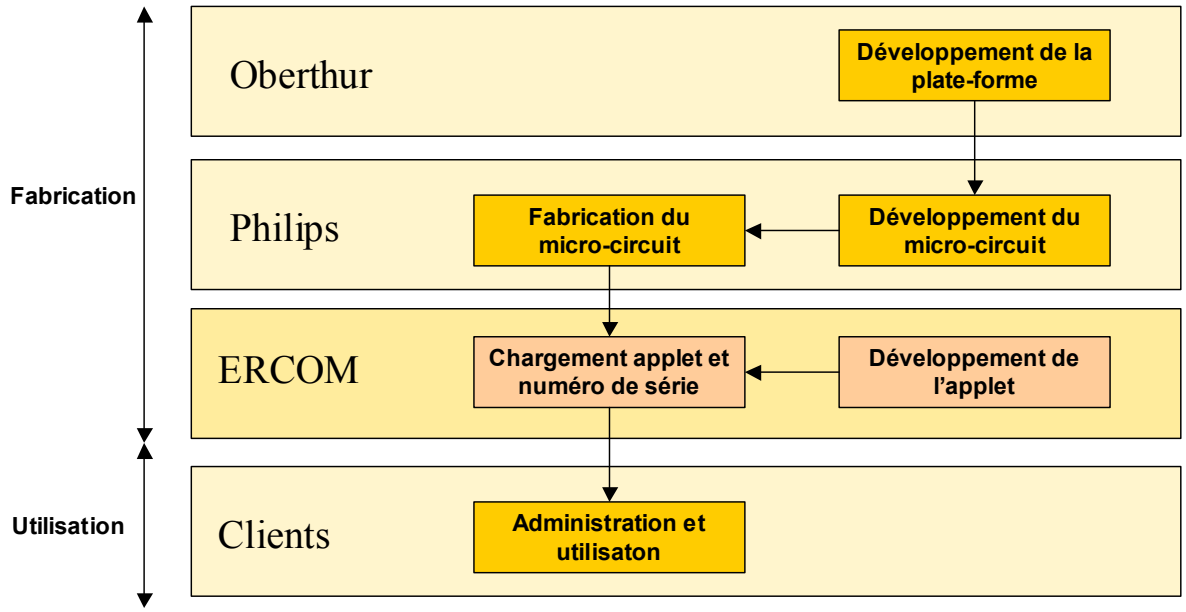

Figure 3 - Cycle de vie de la carte – fabrication

En phase d'utilisation la carte peut se trouver dans différents états résumés dans le schéma suivant :

Etat	Description
Non certifiée	Carte avec applet CryptoSmart et numéro de série chargés. C'est ainsi que la carte est fournie initialement au client.
CA non validée	Carte CA au repos
CA validée	Carte CA avec code PIN validé
CA bloquée	Carte CA bloquée suite à des erreurs répétées de code PIN
Utilisateur non validée	Carte Utilisateur au repos
Utilisateur validée	Carte Utilisateur avec code PIN validé
Utilisateur bloquée	Carte Utilisateur bloquée suite à des erreurs répétées de code PIN

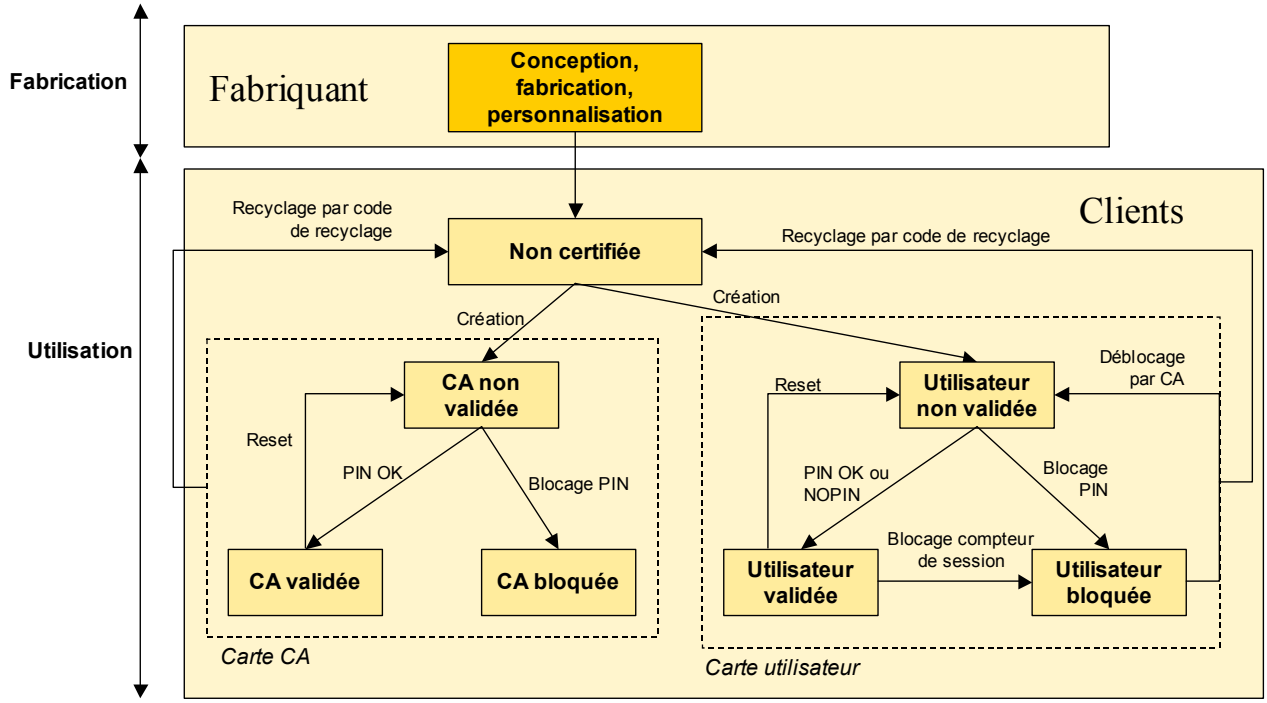

Figure 4 - Cycle de vie de la carte – utilisation

1.3.3. Périmètre et limites du produit évalué

Le produit évalué est l'applet Cryptosmart identifiée au §1.1.

Les éléments suivants ne font donc pas partie du périmètre d'évaluation :

- la plate-forme Oberthur COSMO64RSA D V5.2,
- le micro-circuit Philips,
- les téléphones Secphone v2.0 et le réseau les reliant,
- les stations d'administration SecPhone-ADM et leurs périphériques (ex : lecteur de carte).

2. L'évaluation

2.1. Contexte

Cette évaluation ne porte que sur l'applet Cryptosmart. La plate-forme Oberthur COSMO64RSA D V5.2 et le micro-circuit sont considérés comme étant dans l'environnement du produit. Il est cependant à noter que le micro-circuit utilisé a été évalué et certifié en Allemagne au niveau EAL5+ (cf. certificat [CERT-IC]) et qu'une version similaire de la plate-forme Oberthur a déjà fait l'objet d'une évaluation et certification en France au niveau EAL4+ (cf. [CERT-PF]).

2.2. Référentiels d'évaluation

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

2.3. Commanditaire

ERCOM SA.

Immeuble Nungesser
13, avenue Morane Saulnier
78140 Vélizy
France

2.4. Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Téléphone : +33 (0)5 57 26 08 64

Adresse électronique : m.dus@serma.com

2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée de décembre 2004 à octobre 2005.

Le rapport technique d'évaluation [RTE] détaille les travaux menés par l'évaluateur et présente les résultats obtenus. Les sections suivantes récapitulent les principaux aspects évalués.

2.6. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.

Pour les tâches d'évaluation de la cible de sécurité, les verdicts suivants ont été émis par l'évaluateur :

Classe ASE: Evaluation d'une cible de sécurité		**Verdicts**
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite

2.7. Evaluation du produit

2.7.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL2[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL2	Structurally tested
+ ADV_HLD.2	Security enforcing high-level design
+ ADV_LLD.1[2]	Descriptive low-level design
+ ADV_IMP.1[2]	Subset of the implementation of the TSF
+ ALC_DVS.1	Identification of security measures
+ ALC_FLR.3	Systematic flaw remediation
+ ALC_TAT.1[2]	Well-defined development tools
+ AVA_MSU.1	Examination of guidance
+ AVA_VLA.2	Independent vulnerability analysis

[1] Annexe 2 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].
[2] Appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

2.7.2. L'évaluation de l'environnement de développement

Le produit est développé sur le site de :

ERCOM SA.

Immeuble Nungesser
13, avenue Morane Saulnier
78140 Vélizy
France

Les mesures de sécurité analysées par l'évaluateur permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation lors du développement.

L'évaluateur a vérifié que :
- le produit évalué est identifié de façon unique ;
- cette identification est indiquée sur le produit ;
- les éléments constitutifs du produit évalué sont identifiés de façon unique.

Des procédures de correction d'anomalies décrivent la manière dont toute anomalie découverte sera suivie et corrigée, ainsi que la diffusion des informations et corrections relatives à ces anomalies, tant que le produit est maintenu par le développeur. Ces procédures ont été évaluées, bien que le respect de ces procédures ne puisse pas être déterminé au moment de l'évaluation.

La vérification de l'application des procédures analysées a été effectuée lors d'une visite du site de développement de ERCOM SA. à Vélizy (cf Annexe 1)

Pour les tâches d'évaluation liées à l'environnement de développement, les verdicts suivants ont été émis par l'évaluateur :

Classe ACM: Gestion de configuration		**Verdicts**
ACM_CAP.2	Configuration items	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.1	Identification of security measures	Réussite
ALC_FLR.3	Systematic flaw remediation	Réussite
ALC_TAT.1[1]	Well-defined development tools	Réussite

2.7.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit : spécifications fonctionnelles (FSP) et conception de haut-niveau (HLD). Pour la partie du produit réalisant des opérations cryptographiques (classe FCS), cette analyse a aussi porté sur la conception de bas-niveau (LLD) et la représentation de l'implémentation (IMP).

[1] Appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :

- Exigences extraites des [CC] :
  - Cryptographic Key Generation (FCS_CKM.1)
  - Cryptographic key destruction (FCS_CKM.4)
  - Cryptographic operation (FCS_COP.1)
  - Complete access control (FDP_ACC.2)
  - Security attributes based access control (FDP_ACF.1)
  - Authentication failures handling (FIA_AFL.1)
  - User attribute definition (FIA_ATD.1)
  - User authentication before any action (FIA_UAU.2)
  - User identification before any action (FIA_UID.2)
  - Management of security attributes (FMT_MSA.1)
  - Secure security attributes (FMT_MSA.2)
  - Static attribute initialisation (FMT_MSA.3)
  - Management of TOE security functions data (FMT_MTD.1)
  - Specification of management functions (FMT_SMF.1)
  - Security management roles (FMT_SMR.1)
  - Unlinkability (FPR_UNL.1)
  - Inter-TSF confidentiality during transmission (FPT_ITC.1)
  - Inter-TSF detection of modification (FPT_ITI.1)
  - Non-bypassability of the TSP (FPT_RVM)
  - TSF domain separation (FPT_SEP.1)
- Exigences de sécurité explicitement énoncées :
  - Limited specific audits (FAU_SPE).

Pour les tâches d'évaluation liées à la conception du produit, les verdicts suivants ont été émis par l'évaluateur :

Classe ADV: Développement		**Verdicts**
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1[1]	Descriptive low-level design	Réussite
ADV_IMP.1[1]	Subset of the implementation of the TSF	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite

2.7.4. L'évaluation des procédures de livraison et d'installation

L'évaluateur a analysé les procédures de livraison du produit entre :

- le fabricant des cartes (Oberthur Card systems) et ERCOM SA. (carte dans l'état « plate-forme ouverte »),
- ERCOM SA. et ses clients (carte avec l'applet Cryptosmart et son numéro de série chargée, dans l'état « non certifiée »).

L'installation du produit correspond à la phase de chargement de l'applet, de personnalisation de la carte et de verrouillage de la plate-forme. Les cartes obtenues après la phase

[1] Appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

d'installation sont dans l'état « non certifiées ». Les procédures analysées [INSTALL] permettent d'obtenir la configuration évaluée du produit.

Pour les tâches d'évaluation liées aux procédures de livraison et d'installation, les verdicts suivants ont été émis par l'évaluateur :

Classe ADO: Livraison et exploitation		**Verdicts**
ADO_DEL.1	Delivery procedures	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

2.7.5. L'évaluation de la documentation d'exploitation

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit la personne en possession de la carte CA et ayant accès aux fonctions d'administration relatives à un parc de carte utilisateur.
Pour l'évaluation, l'évaluateur a considéré comme utilisateurs les utilisateurs finaux des cartes Cryptosmart.
L'évaluateur a analysé les guides d'administration et d'utilisation [GUIDES] pour s'assurer qu'ils permettent d'exploiter le produit évalué d'une manière sécurisée.

Pour les tâches d'évaluation liées à la documentation d'exploitation, les verdicts suivants ont été émis par l'évaluateur :

Classe AGD: Guides		**Verdicts**
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite

2.7.6. L'évaluation des tests fonctionnels

L'évaluateur a analysé la documentation des tests réalisés par le développeur pour s'assurer que toutes les fonctionnalités du produit listées dans la cible de sécurité ont bien été testées.

L'évaluateur a également réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué.
L'évaluateur a réalisé ses tests fonctionnels indépendants sur la carte identifiée au §1.1, dans une configuration de tests à l'aide d'une station d'administration et d'un environnement associé.

Pour les tâches d'évaluation liées aux tests fonctionnels, les verdicts suivants ont été émis par l'évaluateur :

Classe ATE: Tests		**Verdicts**
ATE_COV.1	Evidence of coverage	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite

2.7.7. L'évaluation des vulnérabilités

L'évaluateur s'est assuré que la documentation fournie avec le produit [INSTALL] [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

Seules les fonctions d'authentification de l'administrateur et des utilisateurs par code PIN ont fait l'objet d'une estimation du niveau de résistance intrinsèque. Le niveau de résistance de ces fonctions est jugé élevé : SOF-High.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests menés dans une configuration de tests, et à l'aide d'une station d'administration et d'un environnement associé.

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à des attaques de niveau **élémentaire**.

Pour les tâches d'évaluation liées aux vulnérabilités, les verdicts suivants ont été émis par l'évaluateur :

Classe AVA : Estimation des vulnérabilités		**Verdicts**
AVA_MSU.1	Misuse	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.2	Independent vulnerability analysis	Réussite

2.7.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Ils sont reconnus comme étant compatibles avec le niveau standard de la qualification, conformément au référentiel cryptographique de la DCSSI (cf. [CRYPTO]).
Les résultats obtenus ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et décrits dans le rapport technique d'évaluation [RTE] permet la délivrance d'un certificat conformément au décret 2002-535.
Ce certificat atteste que l'exemplaire du produit soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST]. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (Art. 8 du décret 2002-535)

3.2. Restrictions d'usage

Les conclusions de l'évaluation ne sont valables que pour le produit spécifié au chapitre 1 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation résumés ci-dessous et suivre les recommandations se trouvant dans les guides fournis [INSTALL] [GUIDES] :

- le poste téléphonique doit réaliser sans défaut ses fonctions de sécurité ;
- le responsable de la TOE doit s'assurer que la station d'administration et la carte CA sont situées dans un environnement physiquement protégé (à l'exception d'une ligne téléphonique), où seul l'administrateur peut accéder ;
- la station d'administration doit réaliser sans défaut ses fonctions de sécurité ;
- le responsable de la TOE doit s'assurer que l'administrateur est une personne de confiance ;
- l'administrateur doit avoir été formé à l'utilisation de la machine d'administration ;
- le responsable de la TOE doit s'assurer que les utilisateurs ont été formés à l'utilisation de la TOE ;
- la plate-forme Javacard doit rendre impossible la lecture des éléments de la TOE sans passage par les fonctions prévues par la TOE ;
- la plate-forme Javacard doit rendre impossible l'installation d'une autre applet après verrouillage ;
- la plateforme Javacard doit réaliser sans défaut ses fonctions cryptographiques.

3.3. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

3.4. Reconnaissance internationale (CC RA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA].

Annexe 1. Visite du site de développement de la société ERCOM SA. à Vélizy

Le site de développement de la société ERCOM SA. situé Immeuble Nungesser, 13, avenue Morane Saulnier, 78140 à Vélizy en France, a fait l'objet d'une visite par l'évaluateur le 15 juin 2005 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour le produit « Applet CryptoSmart V2.0 sur base Oberthur COSMO64RSA D V5.2 ».

Ces procédures ont été fournies et analysées dans le cadre des tâches d'évaluation suivantes :

- ALC_DVS.1 ;
- ALC_FLR.3;
- ADO_DEL.1.

Un rapport de visite [Visite] a été émis par l'évaluateur.

Annexe 2. Niveaux d'assurance prédéfinis EAL

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Classe ADO Livraison et opération	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Classe AGD Guides d'utilisation	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Classe ATE Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Classe AVA Estimation des vulnérabilités	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Annexe 3. Références documentaires du produit évalué

[CERT-IC]	Philips P5CT072V0M und P5CC072V0M Secure Smart Card Controller, Référence : BSI-DSZ-CC-0227-2004 (16.09.2004) Bundesamt für Sicherheit in der Informationstechnik (BSI)
[CERT-PF]	Rapport de certification 2002/05 - COSMOPOLIC 2.1 V4 JavaCard Open Platform Embedded Software version 1, Mai 2002, SGDN/DCSSI
[CONF]	Liste de configuration, Référence : 2004I/401 v1.8 ERCOM SA.
[GUIDES]	• Cryptosmart – Manuel utilisateur, Référence : 2005R/51 version 1.3 ERCOM SA. • Notice d'utilisation de la Station d'Administration SECPHONE, Référence : 2003S/331 v3.3 ERCOM SA.
[INSTALL]	Procédure d'installation, Référence : 2005E/219 version 1.1 ERCOM SA.
[RTE]	Projet SECPHONE-CARD - Rapport Technique d'Evaluation, Référence : SECPHONE_RTE_V1.1 Serma Technologies
[ST]	Cible de sécurité Cryptosmart, Référence : Réf : 2004G/8 version 1.8 ERCOM SA.
[Visite]	Rapport d'évaluation - Classes ACM et ALC - Famille ADO_DEL – Annexe A, Référence : SECPHONE_ACM-ADO_DEL-ALC_V1.0 Serma Technologies

Annexe 4. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[CC AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[CRYPTO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, N° 2791/SGDN/DCSSI/SDS/Crypto, version 1.02 du 19/11/04, SGDN/DCSSI

Toute correspondance relative à ce rapport 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 cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr