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 2002/07

JavaCard 32K CRISTAL
(référence M256LCAC2)

SÉCURITÉ CERTIFICATION

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 2002/07

JavaCard 32K CRISTAL
(référence M256LCAC2)

Développeurs : SchlumbergerSema, Infineon Technologies AG

Critères Communs
EAL4 Augmenté

conforme aux profils de protection BSI-PP-0005-2002 et BSI-PP-006-2002

Commanditaire : SchlumbergerSema
Centre d'évaluation : Serma Technologies

Le 17 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 représente le rapport de certification du produit JavaCard 32K CRISTAL (référence: M256LCAC2). Ce produit est désigné par deux noms commerciaux : CYBERFLEX et ICITIZEN.

2 Ce produit est composé du micro-circuit SLE66CX322P, du système d'exploitation GEOS et d'une applet Cristal ; la référence du produit est M256LCAC2. Le produit est conforme aux exigences des profils de protection [SSCD/Type2] et [SSCD/ Type3].

3 Le certificat de ce produit s'appuie sur le certificat du micro-circuit «Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a23» émis par le BSI le 7 mai 2002 sous la référence : BSI-DSZ-CC-0169-2002 [BSI].

4 Ce certificat atteste que le micro-circuit SLE66CX322P atteint le niveau EAL 5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 et qu'il est conforme au profil de protection référencé PP/BSI-0002 «Smartcard Integrated Circuit Protection Profile v2.0» [SSVG]. La validité de ce certificat est reconnue par le schéma français en vertu de l'accord de reconnaissance du SOG-IS [SOG-IS].

5 Les développeurs de la cible d'évaluation sont les sociétés suivantes :

- SchlumbergerSema pour la partie applicative :

  SchlumbergerSema
  50, avenue Jean Jaurès
  BP 620-12
  92542 Montrouge Cedex
  France;

- Infineon Technologies AG pour le micro-circuit :

  Infineon Technologies AG
  Postfach 80 17 60
  81617 München
  Allemagne.

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, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4,

conformément à la partie 3 des Critères Communs [CC]. Le niveau de résistance des fonctions réalisées par des mécanismes probabilistiques et permutationnels est élevé (SOF-high).

1.2 Contexte de l'évaluation

8 L'évaluation s'est déroulée parallélement au développement du produit de décembre 2000 à mai 2002.

9 Le micro-circuit étant certifié par le schéma allemand, les travaux effectués dans le cadre de cette évaluation ont porté sur l'évaluation du masque et sur son intégration sûre dans le micro-circuit conformément aux interprétations sur la composition d'un circuit intégré et d'un logiciel embarqué [JIL-Comp] émis par la JIL (Joint Interpretation Library).

10 Le commanditaire de l'évaluation est la société SchlumbergerSema :

- SchlumbergerSema
  50, avenue Jean Jaurès
  BP 620-12
  92542 Montrouge Cedex
  France.

11 L'évaluation a été conduite par le Centre d'Evaluation de la Sécurité des Technologies de l'Information Serma Technologies :

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

Chapitre 2

Description de la cible d'évaluation

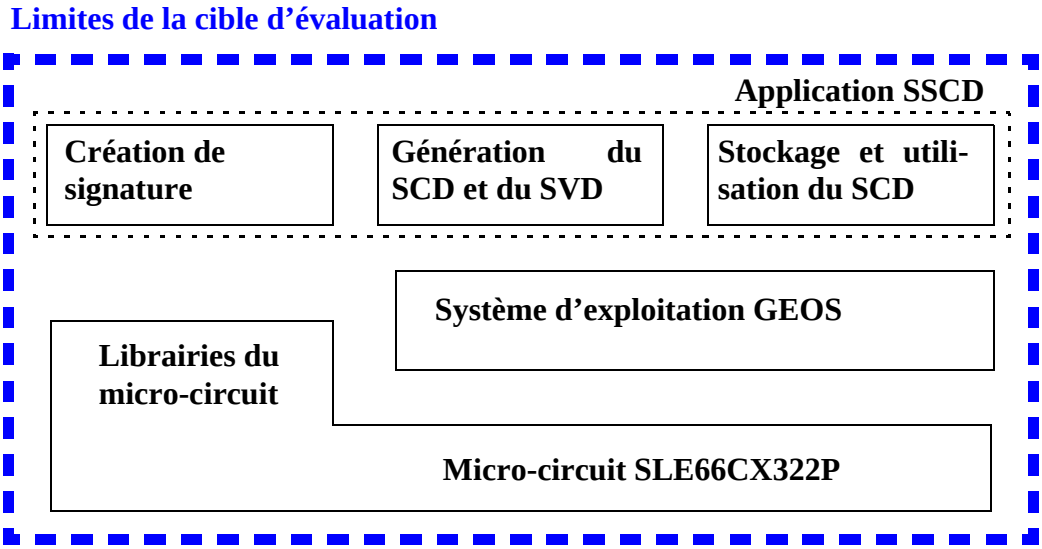
2.1 Périmètre de la cible d'évaluation

12 La cible d'évaluation est composée par :

- le micro-circuit SLE66CX322P (version GC A23) avec ses librairies RMS version 0.7 et ACE version 0.44 certifié EAL 5 augmenté et conforme au profil de protection PP/BSI-0002 [SSVG];
- le système d'exploitation générique GEOS version SC_V3.0.0 (système logiciel générique et machine virtuelle Java Card);
- l'application de création de signature CRISTAL version AC_V1.0.0.

13 La version du masque en ROM est SB80. Celle du masque logiciel est SM01_V3.0.0.

14 Ce produit permet de générer la clé secrète de l'utilisateur (SCD) et la clé publique correspondante (SVD) et de créer une signature sécurisée. La création d'une signature sécurisée nécessite l'utilisation d'une application de création de signature (SCA) permettant d'importer les données à signer sur la carte. La vérification de la signature par une tierce partie est possible grâce au transfert de la clé publique (SVD) par une application de génération de certificat (CGA). Ces deux applications sont hors du cadre de l'évaluation.



2.2 Cycle de vie

15 Le produit suit le cycle de vie d'une carte à puce suivant:

Phase 1 : le développement des applications logicielles qui sont masquées sur le circuit a été examiné 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 par TüV-IT qui a fait l'objet du certificat BSI-DSZ-CC-0169-2002 [BSI].

Phase 4 et 5 : la mise en micro-module et l'encartage des composants, réalisés à Orléans, ont été audités au cours de l'évaluation.

Phase 6 : cette phase sert à la personnalisation des cartes. Lors de cette phase, le personnalisateur (administrateur) importe le code PIN du porteur et éventuellement les clés de signature (SCD, SVD).

Phase 7 : la phase d'utilisation du produit par le porteur de la carte (utilisateur).

16 Les phases 1 à 5 correspondent au développement et à la fabrication de la cible d'évaluation, les phases 6 à 7 à son utilisation.

2.3 Fonctions de sécurité

17 Les fonctions de sécurité évaluées sont les suivantes :

- autotest de la carte;
- détection des événements de sécurité;
- effacement de la mémoire de travail;
- contrôle de l'intégrité des données;
- non-observabilité des données et des opérations;
- gestion de la carte;
- génération de clés;
- création de signature;
- hachage des données;
- génération et vérification de MAC;
- établissement d'un canal sécurisé;
- gestion du PIN;
- contrôle d'accès;
- contrôle du cycle de vie;
- définition des attributs;
- gestion des caractéristiques de sécurité;
- retour à un état sûr.

2.4 Documentation disponible

18 Le produit doit être accompagné de ses guides d'utilisation.

19 Ces guides s'adressent aux utilisateurs et aux administrateurs afin de permettre une utilisation sûre du produit ; ils sont décrits dans la fourniture d'évaluation «AGD - Guidance documents» [GUIDE].

20 Les guides administrateur décrivent les opérations qui garantissent une utilisation sûre du produit :

- par le personnalisateur en phase 6, spécialement en ce qui concerne l'initialisation de chacune des applications ;
- par l'émetteur de la carte en phase 7.

21 Le guide utilisateur explique comment l'utilisateur (phase 7) doit utiliser la carte spécialement en ce qui concerne le code PIN.

Chapitre 3

Résultats de l'évaluation

3.1 Exigences d'assurance

Classes d'Assurance	Composants d'Assurance
Cible de sécurité	Introduction de la ST (ASE_INT.1) Description de la TOE (ASE_DES.1) Environnement de sécurité (ASE_ENV.1) Objectifs de sécurité (ASE_OBJ.1) Annonce de conformité à un PP (ASE_PPC.1) Exigences de sécurité des TI (ASE_REQ.1) Exigences de sécurité des TI explicitement énoncées (ASE_SRE.1) Spécifications globales de la TOE (ASE_TSS.1)
Gestion de configuration	Automatisation partielle de la gestion de configuration (ACM_AUT.1) Aide à la génération et procédures de réception (ACM_CAP.4) Couverture du suivi des problèmes par la gestion de configuration (ACM_SCP.2)
Livraison et exploitation	Détection de modifications (ADO_DEL.2) Procédures d'installation, de génération et de démarrage (ADO_IGS.1)
Développement	Définition exhaustive des interfaces externes (ADV_FSP.2) Conception de haut niveau - identification des sous-systèmes dédiés à la sécurité (ADV_HLD.2) Implémentation de la TSF (ADV_IMP.2) Conception de bas niveau descriptive (ADV_LLD.1) Démonstration de correspondance informelle (ADV_RCR.1) Modèle informel de politique de sécurité de la TOE (ADV_SPM.1)
Guides	Guide de l'administrateur (AGD_ADM.1) Guide de l'utilisateur (AGD_USR.1)

Classes d'Assurance	Composants d'Assurance
Cycle de vie	Caractère suffisant des mesures de sécurité (ALC_DVS.2) Modèle de cycle de vie défini par le développeur (ALC_LCD.1) Outils de développement bien définis (ALC_TAT.1)
Tests	Analyse de la couverture (ATE_COV.2) Tests : conception de haut niveau (ATE_DPT.1) Tests fonctionnels (ATE_FUN.1) Tests indépendants - échantillonnage (ATE_IND.2)
Estimation des vulnérabilités	Analyse et tests des états non sûrs (AVA_MSU.3) Évaluation de la résistance des fonctions de sécurité de la TOE (AVA_SOF.1) Résistance élevée (AVA_VLA.4)

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

23 Le détail des travaux d'évaluation menés est disponible dans le Rapport Technique d'Evaluation [RTE].

24 Des audits sur les sites de Montrouge (développement), de Limère (mise en micro-modules) et de Sologne (encartage et pré-personnalisation) ont été menés afin de vérifier que les mesures d'assurance mises en place sont suffisantes.

3.2 Tests fonctionnels et de pénétration

3.2.1 Tests développeur

25 Le développeur a fourni la documentation de tests développeur du produit. Les tests ont été basés sur les fonctions reposant sur des mécanismes cryptographiques et sur les contrôles d'accès aux opérations.

3.2.2 Tests évaluateur

26 Les tests fonctionnels indépendants réalisés par l'évaluateur ont été basés sur les fonctions de sécurité impliquant des mécanismes cryptographiques.

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), conformément au potentiel d'attaque défini par la JIL [JIL-Cot], ne peut pas remettre en cause la politique de sécurité de la TOE, confirmant que les objectifs de sécurité de la cible d'évaluation (listés ci-après) sont respectés.

- limitation des émanations;
- sécurité du cycle de vie;
- confidentialité des données de création de signature (SCD);
- correspondance entre les données de création (SCD) et de vérification (SVD) de signature;
- authenticité des données de vérification de signature (SVD);
- détection d'intrusion physique;
- résistance à l'intrusion;
- transfert sûr des données de création de signature (SCD) entre dispositifs sécurisés de création de signature;
- génération de données de création et de vérification de signature;
- unicité des données de création de signature;
- vérification de l'intégrité des données à signer;
- génération de signature pour le signataire légitime;
- sécurité cryptographique de la signature.

3.3 Cotation des mécanismes cryptographiques

28 Les mécanismes de nature cryptographique ont été évalués par la Direction Centrale de la Sécurité des Systèmes d'Information. Ils sont compatibles avec le niveau de résistance élevé.

Chapitre 4

Certification

4.1 Verdict

29 Ce présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL4 augmenté des composants d'assurance ADV_IMP.2 "Implémentation de la TSF", ALC_DVS.2 "Caractère suffisant des mesures de sécurité", AVA_MSU.3 "Analyse et tests des états non sûrs" et AVA_VLA.4 "Analyse de vulnérabilités indépendante" tels que décrits dans la partie 3 des Critères Communs [CC].

4.2 Recommandations

30 La cible d'évaluation du produit JavaCard 32K CRISTAL (référence: M256LCAC2) est soumise aux recommandations d'utilisation exprimées ci-dessous.

- Les guides (utilisateur et administrateur) doivent être appliqués;
- Les hypothèses définies dans la cible de sécurité [ST] doivent être respectées lors de l'utilisation du produit;
- Pour assurer l'intégrité des données importées lors de l'utilisation d'un Secure channel, la fonction de chiffrement des données doit être utilisée.

4.3 Certification

31 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.

32 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	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	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.
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.
SSCD	Dispositif sécurisé de création de signature.
SCD	Données de création de signature (clé secrète).
SVD	Données de vérification de signature (clé publique).

SCA	Application de création de signature.
CGA	Application de génération de certificats.

Annexe B

Références

[CC] 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.
- Partie 2 : Exigences fonctionnelles de sécurité CCIMB-99-032, version 2.1 Août 1999.
- 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] Version complète : «JavaCard 32K security target», référence MRD06SBG003007 v2.1.
Version publique : «JavaCard 32K security target - public version - EAL4+», référence MRD06SBG023034 v1.1.

[RTE] «Evaluation Technical Report», référence ETR_RUBIS_V2.0 (diffusion contrôlée).

[GUIDE] «Administrator manual : RUBIS», référence MRD06GUI003072 v1.3.
«User manual : RUBIS», référence MRD06GUI003073 v1.4.

[SSCD/ Type2] Profil de protection «Secure Signature Creation Device Type 2, version 1.04», référence BSI-PP-0005-2002.

[SSCD/ Type3] Profil de protection «Secure Signature Creation Device Type 3, version 1.05», référence BSI-PP-0006-2002.

[BSI] Rapport de certification du produit «Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a23», référence BSI-DSZ-CC-0169-2002.

[SSVG] Profil de protection «Smartcard Integrated Circuit Protection Profile v2.0», référence BSI-PP-0002.

[JIL-Comp] «ETR-lite for composition: Annex A Composite smartcard evaluation : Recommended best practice», version 1.2, mars 2002.

[JIL-Cot] «Application of Attack Potential to Smartcards», version 1.0, mars 2002.

[SOG-IS] «Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Commitee of Agreement Group.

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