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 2002/05

COSMOPOLIC 2.1 V4 JavaCard Open Platform
Embedded Software version 1

Mai 2002

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

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

CERTIFICAT 2002/05

COSMOPOLIC 2.1 V4 JavaCard Open Platform Embedded Software version 1

Développeur : Oberthur Card Systems

Critères Communs
EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)

Commanditaire : Oberthur Card Systems
Centre d'évaluation : Serma Technologies

Le 30 mai 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.

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 logiciel de la plate-forme ouverte COSMOPOLIC 2.1 V4. Ce logiciel est développé par Oberthur Card Systems. Pour l'évaluation, ce logiciel est installé sur le micro-circuit P8WE5033 conçu et fabriqué par Philips Semiconducteurs. La référence interne du logiciel évalué est JPH33V4 version 1.

2 La carte, constituée de la plate-forme logicielle et du micro-circuit, est conçue pour accueillir des applications pour cartes à puce programmées en JavaCard. Elle se veut conforme aux spécifications Javacard 2.1.1 de Sun Microsystems [JC] et Open Platform 2.0.1' de Visa International [OP].

3 Cette plate-forme permet le chargement, l'installation et l'effacement des applications lors de sa phase d'utilisation.

4 Le développeur de la cible d'évaluation est Oberthur Card Systems :

- Oberthur Card Systems
  12bis, rue des Pavillons
  BP 133
  92804 Puteaux Cedex
  France

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

6 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 [CC] :

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

1.2 Contexte de l'évaluation

7 L'évaluation s'est déroulée d'avril 2001 à avril 2002.

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

- Oberthur Card Systems
  12bis, rue des Pavillons

BP 133
92804 Puteaux Cedex
France

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

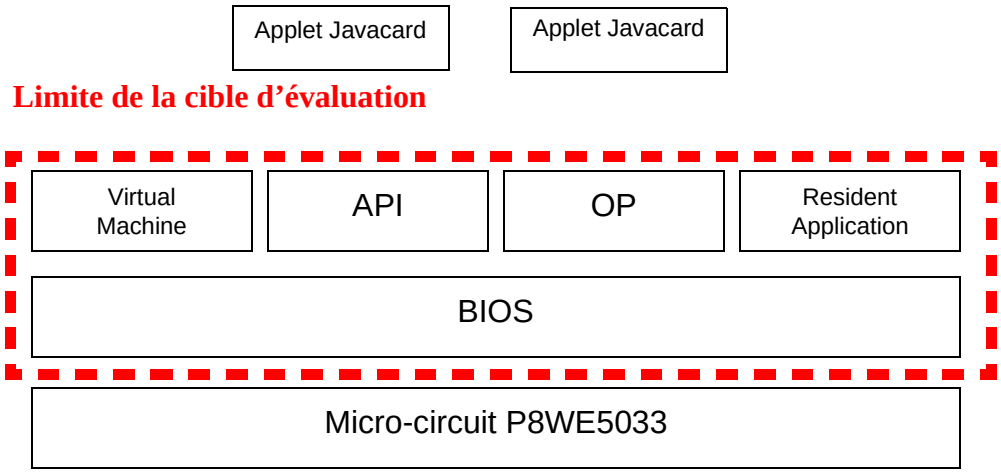
- Serma Technologies
  30 avenue Gustave Eiffel
  33608 Pessac Cedex
  France

Chapitre 2

Description de la cible d'évaluation

2.1 Périmètre de la cible d'évaluation

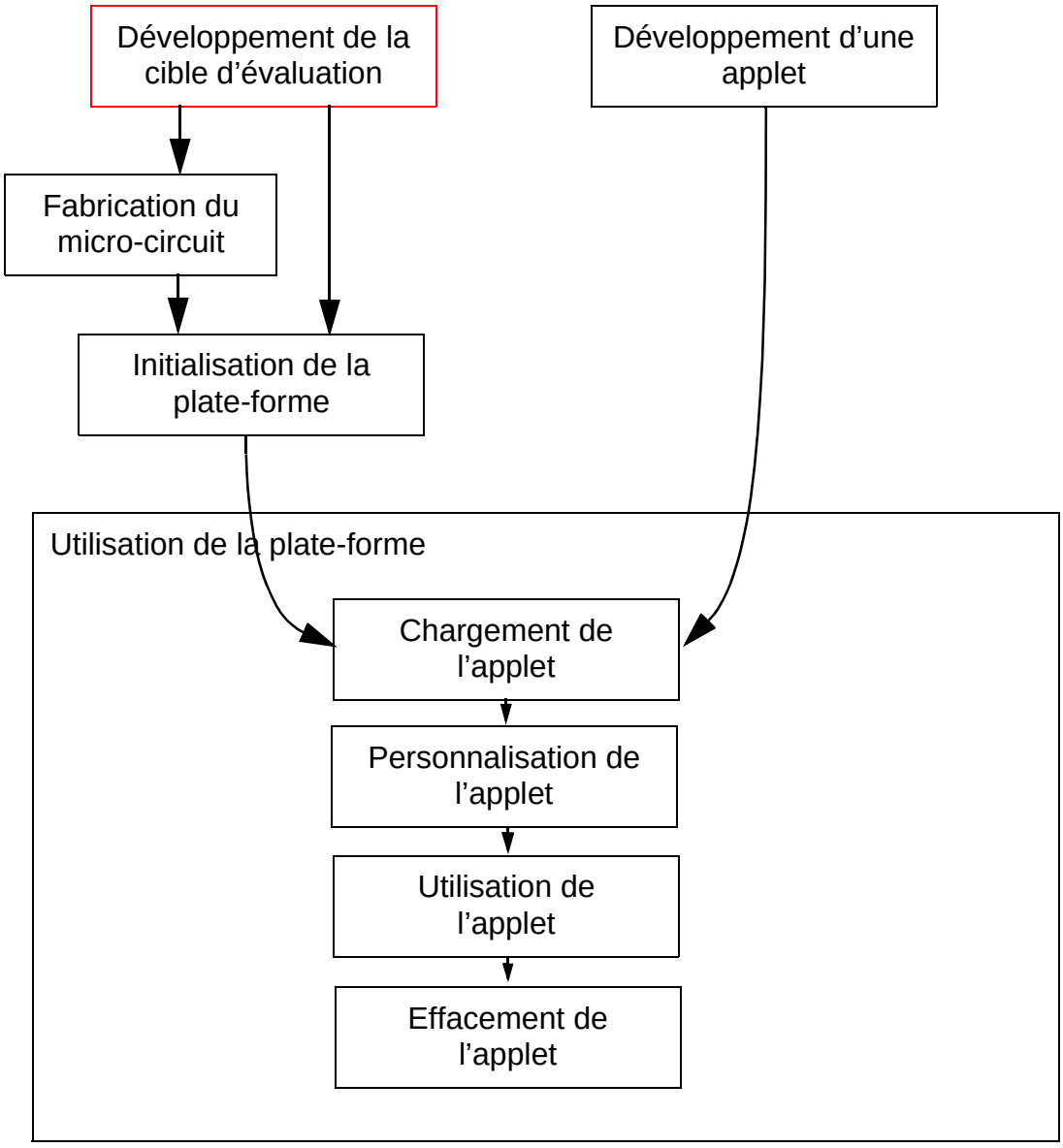
10 La cible d'évaluation est le logiciel de la plate-forme ouverte COSMOPOLIC 2.1 V4. Ce logiciel est développé par Oberthur Card Systems. Pour l'évaluation, ce logiciel est installé sur le micro-circuit P8WE5033.



11 La cible d'évaluation est plus précisément composée des logiciels suivants :

- BIOS (interface entre le composant matériel et les applications),
- Virtual Machine (machine virtuelle Javacard 2.1.1),
- API (interfaces d'applications Javacard 2.1.1,
- Open Platform OP 2.0.1' Configuration 1b (applications Card Manager, API OPSystem et Security Domain),
- Resident Application (répartiteur de commande).

2.2 Cycle de vie de la cible d'évaluation



2.3 Fonctions de sécurité évaluées

12 Les fonctions de sécurité évaluées sont de trois types :

- celles utilisées en interne par la plate-forme mais aussi fournies en tant que service pour les applets ;
- celles spécifiques à la plate-forme ;
- celles uniquement utilisées par les applets.

2.3.1 Fonctions internes et disponibles aux applets

- blocage de la carte en cas de détection d'attaque ;
- gestion des exceptions ;
- contrôle de l'intégrité et de la confidentialité des données transmises par Secure Channel ;
- contrôle de la confidentialité des données sensibles (PIN, clés, ...) avec suppression des données résiduelles ; suppression réalisée par le Garbage Collector ;
- contrôle de l'atomicité des transactions ;
- enregistrement des tentatives d'authentification ;
- contrôle d'intégrité des données sensibles (clés, PIN) ;
- contrôle d'intégrité de tous les objets java ;
- contrôle d'intégrité des packages java (Bytecode) chargés en EEPROM ;
- contrôle d'intégrité du code Rom ;
- contrôle d'intégrité de l'EEprom ;
- gestion des rôles internes des applets ;
- enregistrement des évènements liés à la sécurité et gestion du fichier d'audit (remplissage, exportation), blocage de la carte sur détection d'attaque ;
- contrôle de l'étanchéité entre les applets ;
- gestion de tableaux globaux («global arrays») ;
- gestion des objets partagés et contrôle du mécanisme de sharing ;
- gestion des clés ;
- contrôle d'accès aux clés DES et RSA ;
- gestion des «transient arrays» ;
- génération de secrets (nombres aléatoires, clés de session DES), (s'appuie sur le crypto-processeur du micro-circuit) ;
- calcul DES (s'appuie sur le crypto-processeur du micro-circuit).

2.3.2 Fonctions spécifiques à la plate-forme

- contrôle de l'intégrité des fichiers CAP lors de leur chargement,
- authentification des administrateurs de la plate-forme (émetteur, personnalisateur),
- contrôle de l'espace mémoire EEPROM utilisé par les applets,
- auto-test au démarrage,
- contrôle des commandes envoyées en phase de prépersonnalisation,
- contrôle des commandes envoyées au Card Manager,
- gestion du contexte du JCRE,

2.3.3 Fonctions spécifiques pour les applets

- génération de bi-clés RSA, (s'appuie sur le crypto-processeur du micro-circuit),
- calcul RSA, (s'appuie sur le crypto-processeur du micro-circuit).

13 Le détail des fonctions de sécurité est disponible dans la cible de sécurité [ST].

2.4 Documentation disponible

14 La documentation d'exploitation de la cible d'évaluation est la suivante :

- guide d'utilisation Oberthur Cosmopolic [GUIDE],
- guides JavaCard [JC],
- guides Open Platform [OP] et [VOP].

Chapitre 3

Résultats de l'évaluation

3.1 Exigences d'assurance

15 Le niveau visé pour l'évaluation est EAL4 augmenté des composants d'assurance ADV_IMP.2 "Implémentation de la TSF", ALC_DVS.2 "Caractère suffisant des mesures de sécurité", AVA_VLA.4 "Résistance élevée".

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

Classes d'Assurance	Composants d'Assurance
Guides	AGD_ADM.1 : Guide de l'administrateur AGD_USR.1 : Guide de l'utilisateur
Support au cycle de vie	ALC_DVS.2 : Caractère suffisant des mesures de sécurité ALC_FLR.1 : Correction d'anomalies élémentaire 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

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

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

18 L'évaluateur a examiné l'ensemble de la conception du logiciel jusqu'au code source pour s'assurer que les fonctions de sécurité sont bien implémentées dans la cible d'évaluation.

19 Un audit a été mené sur le site de développement d'Oberthur Card Systems à Puteaux (France) pour s'assurer de l'utilisation effective de systèmes de gestion de configuration et de l'application de mesures de sécurité suffisantes pour protéger les données sensibles utilisées.

3.2 Tests fonctionnels et de pénétration

3.2.1 Tests développeur

20 Le développeur a fourni la documentation de test fonctionnel du produit. Les tests ont été réalisés par Oberthur Card Systems sur son site de Puteaux.

3.2.2 Tests évaluateur

21 L'évaluateur a réalisé également des tests fonctionnels pour s'assurer par échantillonnage que les fonctions de sécurité identifiées dans la cible de sécurité sont bien réalisées par le produit en évaluation.

22 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 :

- Intégrité et confidentialité :
  - la cible d'évaluation doit détecter la perte d'intégrité des données en mémoires ROM et EEPROM ;
  - la cible d'évaluation doit assurer la confidentialité des données sensibles (PIN, clés) ;
  - les attributs de sécurité des applets doit être protégés en intégrité ;
- Chargement :
  - la cible d'évaluation doit vérifier lors du chargement d'une clé qu'elle est chiffrée et signée ;
  - le chargement, l'installation et l'effacement des applets ne peuvent être effectués qu'après authentification ;
  - la cible d'évaluation doit vérifier lors du chargement des applets qu'elles sont signées ;
  - la cible d'évaluation doit assurer l'intégrité et la confidentialité des applets lors de leur chargement ;
- Authentification :
  - les administrateurs de la cible d'évaluation doivent s'authentifier pour pouvoir exécuter des commandes administratives ;
- Etanchéité :
  - l'étanchéité entre les applets ainsi qu'entre les applets et le cible d'évaluation doit être assurée ;
- Gestion de la sécurité :
  - la cible d'évaluation doit gérer l'état du Card Manager ;
  - la cible d'évaluation doit contrôler les ressources utilisées par les applets ;
- Fourniture de services :
  - la cible d'évaluation doit fournir un ensemble de primitives cryptographiques sures aux applets.

3.3 Cotation des fonctions utilisant des mécanismes cryptographiques

23 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

24 Ce rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL4 augmenté des composants d'assurance suivants :

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

4.2 Recommandations

25 La cible d'évaluation "COSMOPOLIC 2.1 V4 JavaCard Open Platform Embedded Software version 1" est soumise aux recommandations d'utilisation ci-dessous :

- Environnement d'utilisation :
  - le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [ST] ;
  - toutes les données sensibles (clés, PIN, applets) doivent être protégées en intégrité et/ou confidentialité lors de leur stockage et de leur transmission hors de la cible d'évaluation, par exemple lors de la personnalisation du logiciel ou du chargement des applets ;
- Développement des applets :
  - les règles du guide de programmation [GUIDE] pour les applets qui seront installées sur la plate-forme comportant la cible d'évaluation doivent être impérativement respectées ;
  - les applets doivent être développées de manière à protéger de façon suffisante leurs données sensibles ;
  - le code de toutes les applets qui seront chargées doit être compilé, converti et vérifié au moyen d'outils conformes aux spécification Javacard. La signature DAP de ces applets est impératif pour s'assurer de ce passage ;
- Micro-circuit :
  - le micro-circuit sur lequel est installé la cible d'évaluation (Philips P8WE5033) doit fournir un ensemble de fonctionnalités de sécurité : primitives DES et RSA, génération de nombres aléatoires, effacement sûr des buffers utilisés lors des calculs cryptographiques ;

- le micro-circuit doit assurer la protection du code et des données de la cible d'évaluation contre les attaques physiques ;

- Utilisation du Secure channel :

  - 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

26 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.

27 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

Applet	Application développée en language JavaCard destinée à être chargée sur une plate-forme.
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.
EEPROM	«Electrically Erasable Programmable ROM» ROM programmable effaçable électriquement.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
JavaCard	Sous ensemble du langage de programmation Java appliqué aux systèmes embarqués, spécialement aux cartes à puces.
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.
PIN	«Personal Identification Number» Numéro personnel d'identification

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.
RAM	«Random Access Memory» Mémoire vive.
ROM	«Read Only Memory» Mémoire morte.
Sharing	Mécanisme JavaCard de partage d'objets entre différentes applets.

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] Security Target issue 4, réf. FQR 1101254, Oberthur Card Systems (document non public).
COSMOPOLIC2.1 V4 Java Card Open Platform Security Target, Oberthur Card Systems, réf: 057681-03-UDD-AA (version publique).

[RTE] Rapport Technique d'Evaluation, réf. RTE_HARRY_V1.0 (diffusion contrôlée).

[GUIDE] Cosmopolic 2.1 version 4, Open Platform Card, Reference Guide, réf. 057681-01-UDD ed. AC, Oberthur Card Systems.

[OP] Open Platform Card Specification V2.0.1, décembre 1999, Visa International.

[VOP] Visa Open Platform Circuit Card Implementation Specification, mars 1999, Visa International (new specifications, octobre 2000).

[JC] Java Card 2.1.1 : Application Programming Interfaces, JCRE, Virtual Machine Specifications, mai 2000, Sun Microsystems.

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