PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2004/19

Micro-circuit NEC V-WAY 64 V3.0 (µPD79216000)

Paris, le 16 septembre 2004

Le Directeur central de la sécurité des systèmes d'information

Henri Serres

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.
Toutefois, 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.

Table des matières

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 selon les ITSEC et les Critères Communs 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 :

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.

L'accord du Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires de l'accord[2], des certificats délivrés dans le cadre du schéma Critères

[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 novembre 2003, 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 et la Turquie.

Communs. La reconnaissance mutuelle s'applique au niveau EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

Les sites des organismes nationaux de certification des pays signataires de l'accord Common Criteria Recognition Arrangement sont :

Pays	Organisme certificateur	Site web
France	DCSSI	www.ssi.gouv.fr
Royaume-Uni	CESG	www.cesg.gov.uk
Allemagne	BSI	www.bsi.bund.de
Canada	CSE	www.cse-cst.gc.ca
Australie-Nouvelle Zélande	AISEP	www.dsd.gov.au/infosec
Etats-Unis	NIAP	www.niap.nist.gov
Japon	IPA	www.ipa.go.jp

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est le micro-circuit Micro-circuit NEC V-WAY 64 V3.0 (µPD79216000) (référence : V01005V30054) développé par NEC. Il intègre un logiciel de test dédié ainsi que deux librairies livrées sous forme linkable :

- la librairie d'accès au crypto-processeur (Licrypt.a version 3.0),
- une librairie de calcul RSA (RSAlib.a version 2.0).

La référence du produit est : V01005V30054 mnnn vw ; où mnnn identifie le code logiciel USER ROMCODE et TEST ROMCODE, et vw identifie le programme de test.

1.2. Le développeur

Le développement du produit est réalisé par plusieurs acteurs qui interviennent dans sa conception et sa fabrication (cf. description du cycle de vie §1.3.2) :

Le produit est développé et testé par :

NEC Electronics Europe, Smart Card Application Center

4, avenue Morane Saulnier
78140 Vélizy
France.

NEC Micro Systems (Kumamoto)

2081-24 Tabaru Michiki-Machi
Kamimashiki-gun
Kumamoto 861-2202
Japon.

Les photomasks du micro-circuit sont fabriqués par :

Toppan printing Ltd

7-21-33 Nobidome Niiza-city
Saitama 252-8562
Japon.

La production des wafers est réalisée par :

NEC Electronics Sagamihara

1120 Shimokusawa Sagamihara-city
Kanagawa 229-1198
Japon.

Le test industriel et le sciage des wafers se fait à :

NEC Yamaguchi

192-3 Kamimoto, Haigashimagura
Kusunoki-cho, Asa-gun
Yamaguchi 757-0298
Japon.

1.3. Description du produit évalué

Le produit évalué est le V-WAY 64 V3.0 développé et fabriqué par NEC Electron Device.

Le produit a deux modes d'utilisation :

- mode «Test» : à la fin de sa fabrication, le micro-circuit est testé à l'aide d'un système externe et du logiciel de test présent en ROM. Les données de pré-personnalisation peuvent être chargées en EEPROM. Ce mode est ensuite bloqué de manière irréversible lors du passage en mode «User» ;
- mode «User» : mode final d'utilisation du micro-circuit qui fonctionne alors sous le contrôle du logiciel embarqué de la carte à puce. Le logiciel de test n'est plus accessible. Les utilisateurs finaux ne peuvent utiliser le micro-circuit que dans ce mode.

Le micro-circuit seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou des applications et à être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (applications bancaires, télévision à péage, transport, santé,...) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels n'ont pas fait partie de l'évaluation.

1.3.1. Architecture

Le micro-circuit V-WAY 64 fabriqué en technologie 0,25µm est constitué des éléments suivants :

- une partie matérielle :
  - un processeur RISC 32-bit,
  - des mémoires : 200 Ko de ROM (192 Ko USER_ROM, 8 Ko TEST_ROM), 64 Ko d'EEPROM, 64 octets d'OTP, zone de registres speciaux (User et Test), 4 Ko de RAM.
  - un cryptoprocesseur (NEC SuperMAP),
  - un accélérateur DES,
  - une horloge interne allant jusqu'à 36 MHz,
  - un générateur d'aléas de 16 bits,
  - deux compteurs de 16 bits,
  - 49 contrôleurs d'interruption,
  - une entrée/sortie couplée à une interface série compatible ISO7816 et EMV,

- un jeu complet de circuits de sécurité,
- un contrôleur de stand-by (HALT, IDLE, STOP),
- une circuit de contrôle de l'alimentation incluant un générateur de RESET et un régulateur de tension ;

- une partie logicielle :
  - librairie d'accès au crypto-processeur,
  - librairie de calcul RSA 1024bits,
  - programme de test et de gestion du micro-circuit.

Une description détaillée de l'architecture du produit se trouve dans le document [HLD].

1.3.2. Cycle de vie

Le cycle de vie du produit inspiré du cycle de vie décrit dans le PP/9806 [PP9806] est le suivant :

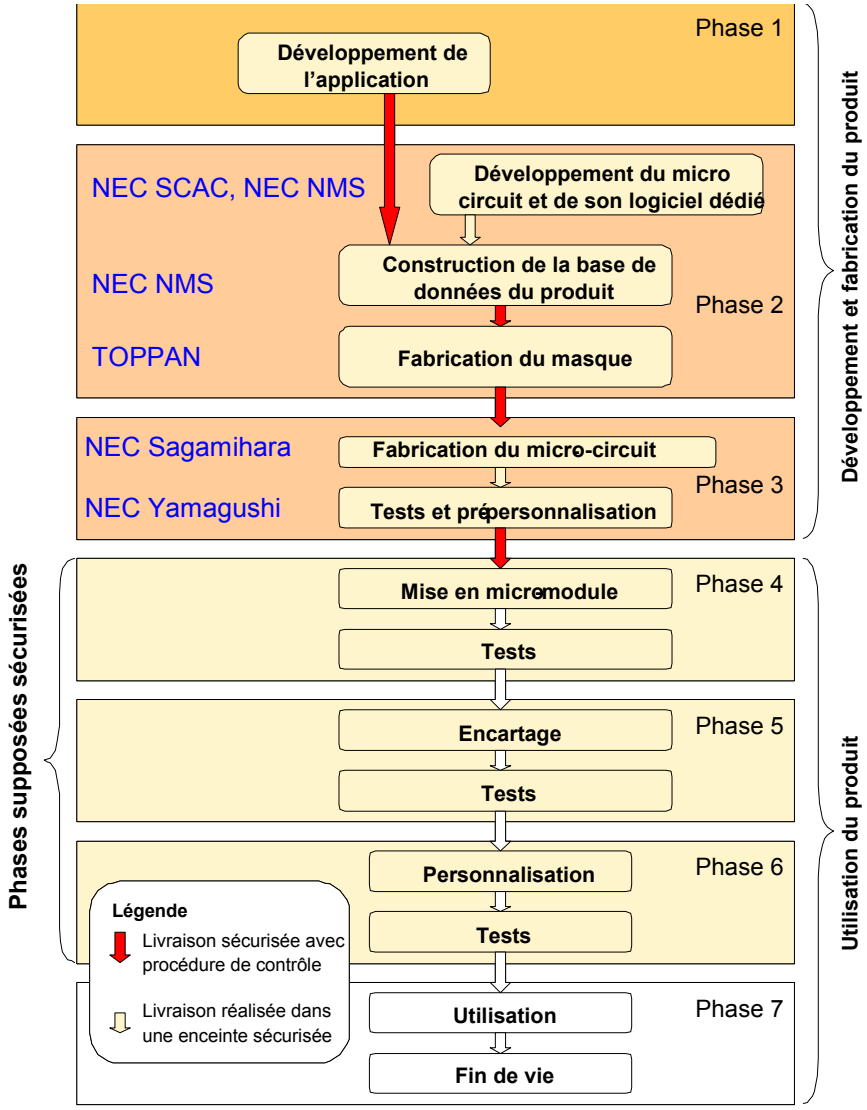

Figure 1 - Cycle de vie standard d'une carte à puce

1.3.3. Périmètre et limites du produit évalué

Ce rapport de certification présente les travaux d'évaluation relatifs au micro-circuit et aux librairies logicielle identifiés au §1.1 et décrits au §1.3.1. Toute autre application éventuellement embarquée, notamment les applications embarquées pour les besoins de l'évaluation, ne font donc pas partie du périmètre d'évaluation.
En regard du cycle de vie, le produit évalué est le produit qui sort de la phase de fabrication, tests et pré-personnalisation (phase 3).

1.4. Utilisation et administration

1.4.1. Utilisation

Le produit évalué n'est pas un produit mettant en œuvre une application particulière. Il s'agit d'une plate-forme matérielle et logicielle offrant différents services pour les logiciels embarqués dans l'optique d'une utilisation de type carte à puce. De fait, il n'y a pas réellement d'utilisation à proprement parler. Les utilisateurs du micro-circuit peuvent être vus comme étant les développeurs des applications ainsi que tous les acteurs intervenant dans les phases dites d'administration du micro-module et de la carte (phase 4 à 6) qui interviendront notamment dans la configuration et la personnalisation des applications embarquées.

Dans le cadre de l'évaluation du V-WAY 64 V3.0 : les utilisateurs sont définis comme étant les personnes pouvant mettre en œuvre les fonctionnalités du micro-circuit et de sa bibliothèque logicielle (il n'y a pas de logiciel applicatif). Cette définition comprend tous les utilisateurs utilisant le produit en mode « user » : l'émetteur de la carte mais également le développeur du logiciel embarqué, le responsable de l'encartage et la personne en charge d'intégrer la carte dans son système d'utilisation finale.

Les objectifs de sécurité sur l'environnement de développement et d'exploitation relatifs aux utilisateurs sont listés dans la cible de sécurité [ST].

1.4.2. Administration

Les phases 4 à 6 du produit, dites d'administration, sont couvertes par une hypothèse dans le profil de protection, qui suppose que les opérations associées à ces phases sont réalisées dans des conditions ne remettant pas en cause la sécurité du produit. Ces conditions n'ont pas été évaluées.

2. L'évaluation

2.1. Centre d'évaluation

CEACI (Thalès Microelectronics – CNES)

18, avenue Edouard Belin
31401 Toulouse Cedex 4
France

Téléphone : +33 (0)5 61 27 40 29

Adresse électronique : ceaci@cnes.fr

L'évaluation s'est déroulée de septembre 2002 à mars 2004.

2.2. Commanditaire

NEC Electronics (Europe) GmbH
Smart Card Application Center

9, rue Paul Dautier
B.P. 52
78142 Vélizy Cedex
France

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'ensemble des interprétations finales listées dans les rapports d'évaluation.

2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 des Critères Communs [CC].
La cible de sécurité répond aux exigences de la classe ASE.

2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation respectent les exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].

2.5.1. Développement du produit

La classe d'assurance ADV – développement – définit les exigences de raffinement pas à pas des fonctions de sécurité du produit depuis ses spécifications globales dans la cible de sécurité [ST] jusqu'à l'implémentation. Chacune des représentations des fonctions de sécurité du

produit qui résultent de ce processus fournit des informations qui aident l'évaluateur à déterminer si les exigences fonctionnelles du produit ont été satisfaites.
L'analyse des documents associés à la classe ADV montre que les exigences fonctionnelles sont correctement et complètement raffinées dans les différents niveaux de représentation du produit (spécifications fonctionnelles (FSP), sous-systèmes (HLD), modules (LLD) et implémentation (IMP)), jusqu'à l'implémentation de ses fonctions de sécurité.
Les documents fournis pour la classe ADV – développement – répondent aux exigences de la partie 3 des critères communs [CC] en termes de contenu et de présentation des éléments de preuve.

2.5.2. Documentation

Du point de vue de l'évaluation, il n'y a pas d'administrateur du micro-circuit pendant les phases d'utilisation (phases 4 à 7 du cycle de vie). En effet, l'administration dans ces phases d'utilisation est liée à une application particulière qui est en dehors du périmètre de l'évaluation. Du point de vue de l'évaluation, les utilisateurs sont les personnes pouvant mettre en œuvre les fonctionnalités « utilisateurs » du produit (notamment le développeur du logiciel embarqué).
Les guides utilisateur [USR] et administrateur [IGS] répondent aux exigences de la partie 3 des critères communs [CC] en termes de contenu et de présentation des éléments de preuve.

2.5.3. Livraison et installation

Conformément au guide pour l'évaluation « The application of CC to IC » [CC_IC], les livraisons considérées sont :

- la livraison du code des applications embarquées au fabricant du micro-circuit,
- la livraison des informations nécessaires au fabricant du masque,
- la livraison du masque au fabricant du micro-circuit,
- la livraison des micro-circuits au responsable de l'étape suivante (mise en micro-module, encartage).

Les différents sites impliqués sont identifiés au §1.2 du présent rapport. Ces sites ont été visités dans le cadre de l'évaluation pour s'assurer de l'application des procédures (cf. Annexes 1 à 5) .
La procédure [DEL] de livraison est suffisante pour répondre aux exigences demandées : elle permet de connaître l'origine de la livraison et de détecter une modification du produit pendant la livraison.
Le démarrage du produit correspond à un RESET, les procédures d'installation, de génération et de démarrage [IGS] permettent d'obtenir une configuration sûre.
Les documents fournis pour la classe ADO – livraison et opération – répondent aux exigences de la partie 3 des critères communs [CC] en termes de contenu et de présentation des éléments de preuve.

2.5.4. L'environnement de développement

Le système de gestion de configuration est utilisé conformément au plan de gestion de configuration [ACM].
Les listes de configuration [LGC] identifient les éléments tracés par le système de gestion de configuration. Les éléments de configuration identifiés dans la liste de configuration sont maintenus par le système de gestion de configuration. Les procédures de génération du produit sont efficaces pour s'assurer que les bons éléments de configuration sont utilisés pour générer le produit.

Les différents sites impliqués dans le développement sont identifiés au §1.2 du présent rapport.
Les mesures de sécurité décrites dans les procédures fournissent le niveau nécessaire de protection pour maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation.
La vérification de la mise en œuvre des procédures de développement et de gestion de configuration a été effectuée par des visites des sites (cf Annexe 1 à 5). Les rapports de visite se trouvent sous la référence [Visite].
Les documents fournis pour la classe ACM – gestion de la configuration – et ALC – support au cycle de vie – répondent aux exigences de la partie 3 des critères communs [CC] en termes de contenu et de présentation des éléments de preuve.

2.5.5. Tests fonctionnels

L'évaluateur a vérifié que toutes les fonctions de sécurité et les interfaces de la spécification fonctionnelle du produit sont reliées à au moins un test fonctionnel dans la documentation de test. Il a vérifié aussi que toutes les caractéristiques fonctionnelles de chaque fonction de sécurité, telles qu'elles sont décrites dans la conception de haut niveau [HLD], sont couvertes par les tests du développeur.

2.5.6. Estimation des vulnérabilités

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement prises en compte dans la conception du produit.
L'évaluateur a également réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités exploitables au niveau d'évaluation considéré.
Le produit dans son environnement d'exploitation est résistant à des attaquants disposant d'un potentiel d'attaque **élevé**.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation du produit **V-WAY 64 V3.0 (µPD79216000)**.

3.2. Niveau d'évaluation

Le produit **Micro-circuit V-WAY 64 V3.0 (µPD79216000)** a été évalué selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **EAL4**[1] **augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_IMP.2	Implementation of the TSF
ALC_DVS.2	Sufficiency of security measures
AVA_VLA.4	Highly resistant

Tableau 1 - Augmentations

Pour tous les composants, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
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
Class ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Class ADO	**Delivery and operation**	
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

[1] Annexe 8 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

Class ADV	**Development**	
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite
ADV_SPM.1	Informal TOE security policy model	Réussite
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite
Class ALC	**Life cycle support**	
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite
Class ATE	**Tests**	
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite
Class AVA	**Vulnerability assessment**	
AVA_MSU.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

Tableau 2 - Composants et verdicts associés

3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** suivantes[1]. Les opérations sur ces exigences sont décrites dans la cible de sécurité [ST].

- Potential violation analysis (FAU_SAA.1)
- Cryptographic operation (FCS_COP.1)
- Complete access control (FDP_ACC.2)
- Security attributes based access control (FDP_ACF.1)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- Stored data integrity monitoring and action (FDP_SDI.1)
- User attribute definition (FIA_ATD.1)
- User authentication before any action (FIA_UAU.2)
- User Identification before any action (FIA_UID.2)

[1] Annexe 7 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Static attribute initialisation (FMT_MSA.3)
- Security management roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)
- TOE Security Functions testing (FPT_TST.1)

3.4. Résistance des fonctions

Seules les fonctions d'authentification ont fait l'objet d'une estimation du niveau de résistance.
Le niveau de résistance des fonctions de sécurité est jugé **élevé** (**SOF-High**).

3.5. Analyse des mécanismes cryptographiques

Seul le générateur de nombres aléatoires a été analysé dans le cadre de l'évaluation (cf Annexe 6).

3.6. Conformité à un profil de protection

Le produit répond aux exigences de sécurité du profil de protection PP/9806 [PP9806].

3.7. Reconnaissance européenne (SOG-IS)

Ce certificat a été émis dans les conditions de l'accord du SOG-IS. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].

3.8. Reconnaissance internationale (CC RA)

Ce certificat a été émis dans les conditions de l'accord du CC RA. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].
Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA [CC RA] : ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4 (Tableau 1).

3.9. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement (§ 3.10) ainsi que les recommandations se trouvant dans les guides utilisateur [USR] et administrateur [IGS].
Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.
Ce rapport de certification donne une appréciation de la résistance du produit "Micro-circuit NEC V-WAY 64 V3.0 (µPD79216000)" à des attaques qui demeurent fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée qu'au travers de l'évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de cette évaluation.

3.10. Objectifs de sécurité sur l'environnement d'exploitation

Ces objectifs de sécurité concernent le système dans lequel sera utilisé le micro-circuit avec son application embarquée (extraits de la cible de sécurité [ST § 4.2.6]) :

- la communication entre un produit développé sur le micro-circuit sécurisé et d'autres produits doit être sécurisée (en termes de protocole et de procédure),
- le système (terminal, communication,…) doit garantir la confidentialité et l'intégrité des données sensibles qu'il stocke ou qu'il traite.

3.11. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le produit **V-WAY 64 V3.0 (µPD79216000)** identifié au paragraphe 1.1 et décrit au paragraphe 1.3 du présent rapport **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

Annexe 1. Rapport de visite du site de NEC à Vélizy

Le site de développement et de test de :

NEC Smart Card Application Center
4, avenue Morane Saulnier
78140 Vélizy
France

a fait l'objet, dans le cadre de l'évaluation du produit **V-WAY 64 V3.0**, d'une visite sur site, en **décembre 2003**, pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- la livraison : **ADO** (ADO_DEL.2) ;
- le support au cycle de vie : **ALC** (ALC_DVS.2).

La visite par le centre d'évaluation, accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site.

Annexe 2. Rapport de visite du site de NEC à Kumamoto

Le site de développement et de test de

NEC Micro Systems
2081-24 Tabaru Michiki-Machi
Kamimashiki-gun
Kumamoto 861-2202
Japon

a fait l'objet, dans le cadre de l'évaluation du produit **V-WAY 64 V3.0**, d'une visite sur site, en **octobre 2003**, pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- la livraison : **ADO** (ADO_DEL.2) ;
- le support au cycle de vie : **ALC** (ALC_DVS.2).

La visite par le centre d'évaluation a permis de conclure que les critères sont satisfaits sur ce site.

Annexe 3. Rapport de visite du site NEC à Sagamihara

Le site de production de wafers de

NEC UC line + G4
NEC Electronics Sagamihara
1120 Shimokusawa Sagamihara-city
Kanagawa 229-1198
Japon

a fait l'objet, dans le cadre de l'évaluation du produit **V-WAY 64 V3.0**, d'une visite sur site, en **octobre 2003**, pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- la livraison : **ADO** (ADO_DEL.2) ;
- le support au cycle de vie : **ALC** (ALC_DVS.2).

La visite par le centre d'évaluation a permis de conclure que les critères sont satisfaits sur ce site.

Annexe 4. Rapport de visite du site de NEC à Yamaguchi

Le site de test industriel et de sciage des wafers de

NEC Yamaguchi
192-3 Kamimoto, Haigashimagura
Kusunoki-cho, Asa-gun
Yamaguchi 757-0298
Japon

a fait l'objet, dans le cadre de l'évaluation du produit **V-WAY 64 V3.0**, d'une visite sur site, en **octobre 2003**, pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- la livraison : **ADO** (ADO_DEL.2) ;
- le support au cycle de vie : **ALC** (ALC_DVS.2).

La visite par le centre d'évaluation a permis de conclure que les critères sont satisfaits sur ce site.

Annexe 5. Rapport de visite du site de Toppan à Tokyo

Le site de fabrication des photomasks de

Toppan Printing
7-21-33 Nobidome Niiza-city
Saitama 252-8562
Japon

a fait l'objet, dans le cadre de l'évaluation du produit **V-WAY 64 V3.0**, d'une visite sur site, en **octobre 2003**, pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- la livraison : **ADO** (ADO_DEL.2) ;
- le support au cycle de vie : **ALC** (ALC_DVS.2).

La visite par le centre d'évaluation a permis de conclure que les critères sont satisfaits sur ce site.

Annexe 6. Analyse des mécanismes cryptographiques

Le Micro-circuit V-WAY 64 V3.0 (µPD79216000) offre un générateur de nombres aléatoires.

Ce service est fait pour être utilisé par le logiciel embarqué et a fait l'objet d'une analyse par la DCSSI. Cette analyse montre que dans le cas où le générateur d'aléas serait utilisé à des fins cryptographiques, il doit être utilisé conformément aux recommandations décrites dans les guides [USR].

Annexe 7. Exigences fonctionnelles de sécurité du produit évalué

Attention : les descriptions des composants fonctionnels suivants sont données à titre indicatif. Seule une lecture attentive de la cible de sécurité ([ST]) peut apporter la description exacte des exigences fonctionnelles du produit.

Class FAU	**Security audit**
Security audit analysis	
FAU_SAA.1	*Potential violation analysis* Le produit doit implémenter un seuil de détection élémentaire, défini selon une règle fixée (spécifiée dans la cible de sécurité [ST]).
Class FCS	**Cryptographic support**
Cryptographic operation	
FCS_COP.1	*Cryptographic operation* Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée (spécifiés dans la cible de sécurité [ST]).
Class FDP	**User data protection**
Access control policy	
FDP_ACC.2	*Complete access control* Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Information flow control policy	
FDP_IFC.1	*Subset information flow control* Le produit doit appliquer les politiques de sécurité de contrôle de flux d'information, lesquelles sont spécifiées dans la cible de sécurité [ST] pour un sous-ensemble des opérations possibles sur un sous-ensemble des flux d'informations.
Information flow control functions	
FDP_IFF.1	*Simple security attributes* Ce composant impose des attributs de sécurité aux informations, aux sujets qui déclenchent le transfert de ces informations ainsi qu'aux sujets qui reçoivent ces informations. Ce composant spécifie les règles qui doivent être appliquées par la fonction et décrit comment les attributs de sécurité sont choisis par la fonction.
Stored data integrity	
FDP_SDI.1	*Stored data integrity monitoring* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées.

Class FIA	**Identification and authentication**
User attribute definition	
FIA_ATD.1	*User attribute definition* Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.
User authentication	
FIA_UAU.2	*User authentication before any action* Les utilisateurs doivent s'authentifier avant que toute action ne soit autorisée.
User identification	
FIA_UID.2	*User identification before any action* Les utilisateurs doivent s'identifier avant que toute action ne soit autorisée.
Class FMT	**Security management**
Management of functions in TSF	
FMT_MOF.1	*Management of security functions behaviour* Le produit doit limiter la capacité à gérer le comportement des fonctions de sécurité du produit à des utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]).
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiés dans la cible de sécurité [ST]).
Class FPR	**Privacy**
Unobservability	
FPR_UNO.1	*Unobservability* Le produit n'autorise pas certains utilisateurs (spécifiés dans la cible de sécurité [ST]) à déterminer si certaines opérations (spécifiées dans la cible de sécurité [ST]) sont en cours d'exécution.
Class FPT	**Protection of the TSF**
TSF physical protection	
FPT_PHP.2	*Notification of physical attack* Le produit doit notifier automatiquement l'intrusion physique sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
FPT_PHP.3	*Resistance to physical attack* Le produit doit empêcher ou résister à certaines intrusions physiques (spécifiées dans la cible de sécurité [ST]) sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
TSF self test	
FPT_TST.1	*TSF testing* Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.

Annexe 8. Niveaux d'assurance prédéfinis ISO 15408 ou CC

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 9. Références documentaires du produit évalué

[ACM]	Configuration Management Smartcard Manual, réf: 81-00U0-00001, version 1.30 du 9/09/2003.
[Visite]	• Visit Report ARSIA (NEC SCAC Vélizy), réf: ARS_RDV_SCAC, version 1.0 du 12/12/2003; • ARSIA Audit Site : NEC NMS / Kumamoto October 01st & 02nd, 2003, réf: ARS_RDV_NMS, version a; • ARSIA Audit Site : Toppan Printing / Tokyo September 30th, 2003, réf: ARS_RDV_TOP, version a; • ARSIA Audit Site : NEC UC line + G4/ Sagamihara October 06th 2003, réf : ARS_RDV_SAG, version a; • ARSIA Audit Site : NEC / YAMAGUCHI October 01st & 02nd, 2003, réf: ARS_RDV_YAM, version a.
[DEL]	ADO_DEL: Delivery of the TOE, réf: 81-55w1-00001, version 1.01 du 13/01/2004.
[HLD]	Total Chip (TC) High Level Design, réf: 33-55Q1-10000, version 1.04 du 29/03/2004.
[IGS]	V-WAY64-V 3.0 [uPD79216000] Installation, Generation and Start-Up, réf 33-55F1-10000, version 1.10 du 12/11/2003.
[LGC]	VWAY 64 Configuration List, réf: 33-55U1-00001, version 1.04 du 26/04/2004. VWAY 64-V3.0 EAL4+ Document Navigator, réf: 33-5511-10002, version 1.23 du 17/06/2004.
[RTE]	Evaluation Technical Report of ARSIA project, réf: ARS_ETR, version 1.0 du 29/04/04.
[ST]	µPD79216000 V3.0 (V-WAY 64 V3.0) Security Target, Ref:33-55N1-10000, version 1.34 du 31/03/2004. µPD79216000 V3.0 (V-WAY 64 V3.0) Security Target Lite, Ref:33-55N1-10001, version 1.00 du 12/07/2004.
[USR]	V-WAY 64-V 3.0 [uPD79216000] User Guidance, réf: 33-65K1-10000, version 1.03 du 09/09/04.
[PP9806]	Common Criteria for Information Technology Security Evaluation - Protection Profile : Smart Card Integrated Circuit Version 2.0, Issue September 1998. Certifié par le centre de certification français sous la référence PP/9806.

Annexe 10. 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.	
[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, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, august 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, august 1999, version 2.1, réf: CCIMB-99-033.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.
[IS 15408]	Norme Internationale ISO/IEC 15408:1999, comportant 3 documents : ▪ ISO/IEC 15408-1: Part 1 Introduction and general model ; ▪ ISO/IEC 15408–2: Part 2 Security functional requirements ; ▪ ISO/IEC 15408–3: Part 3 Security assurance requirements ;
[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.

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