Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/04

Plate-forme Xaica-alpha version V150i_alpha7rs3_SM032 sur micro-circuit ST19XR34 F

Paris, le 8 mars 2005

Le Directeur central de la sécurité des systèmes d'information

Henri Serres
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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 2005/04

Produit : Plate-forme Xaica-alpha version V150i_alpha7rs3_SM032 sur micro-circuit ST19XR34 F

Développeurs : NTTDATA Corporation, TOPPAN, STMicroelectronics

Critères Communs version 2.1
(norme internationale ISO/IEC 15408:1999)

EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2)

Commanditaire : NTTDATA Corporation

Centre d'évaluation : Serma Technologies

Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA : ADV_IMP.2, ALC_DVS.2

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 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.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est la plate-forme Xaica-alpha version V150i_alpha7rs3_SM032 sur micro-circuit ST19XR34 F. Ce produit est spécifié et développé par la société NTTDATA Corporation. Le développement du masque est sous-traité à la société TOPPAN. Le micro-circuit est développé et fabriqué par STMicroelectronics.
Le micro-circuit seul a fait l'objet d'une évaluation ayant donné lieu au certificat [2004/31]

Le tableau suivant résume les différentes références des éléments de la plate-forme Xaica-alpha :

Elément	Type	Développeur
Xaica-alpha v1.50 / PQB ROM code	Système d'exploitation	NTTDATA / TOPPAN
Alpha7rs3v032.ccm	Softmask	TOPPAN
PQB ROM code	Masque du micro-circuit (ROM code)	TOPPAN / STMicroelectronics
ST19XR34 F	micro-circuit	STMicroelectronics

La référence complète du produit est : plate-forme Xaica-Alpha version V150i_alpha7rs3_SM32 sur le microcircuit ST19XR34K F RVU PQB ACA.

1.2. Développeur

Plusieurs acteurs interviennent pour la fabrication du produit :

La plate-forme Xaica-alpha est spécifiée, développée et testée par :

NTTDATA Corporation

Shin Kawasaki Mitsui Building
890-12 Kashimada, Saiwai-ku
Kawasaki-shi
Kanagawa
Japon

Une partie du développement de la plate-forme est réalisée par :

TOPPAN

1-3-3, Suido, Bunkyo-ku
Tokyo
Japon

Le micro-circuit est fabriqué par :

STMicroelectronics

ZI de Rousset – BP 2
F-13106 Rousset
France

1.3. Description du produit évalué

1.3.1. Architecture

Le produit évalué est la plate-forme Xaica-alpha. Il comprend :

- le système d'exploitation, offrant :
  - une interface en mode contact (ISO 7816 mode T=1) ou sans-contact (ISO 14443 type B),
  - un jeu de commandes APDU conforme aux spécifications JICSAP version 1.1, pour des applications embarquées,
  - le chargement d'applications
- l'application JUKI, pour les besoins spécifiques d'une carte d'identité, dans le cadre du programme de carte d'identité du gouvernement japonais. Cette application fait partie du même fichier en ROM que le système d'exploitation et est constituée en majeure partie de jeux de commandes du système d'exploitation ;
- le micro-circuit ST19XR34 F.

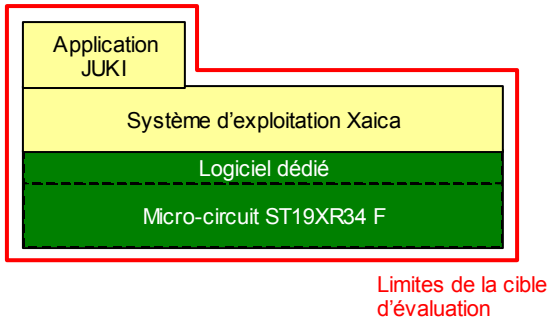

Figure 1 - Limites de la cible d'évaluation

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 :

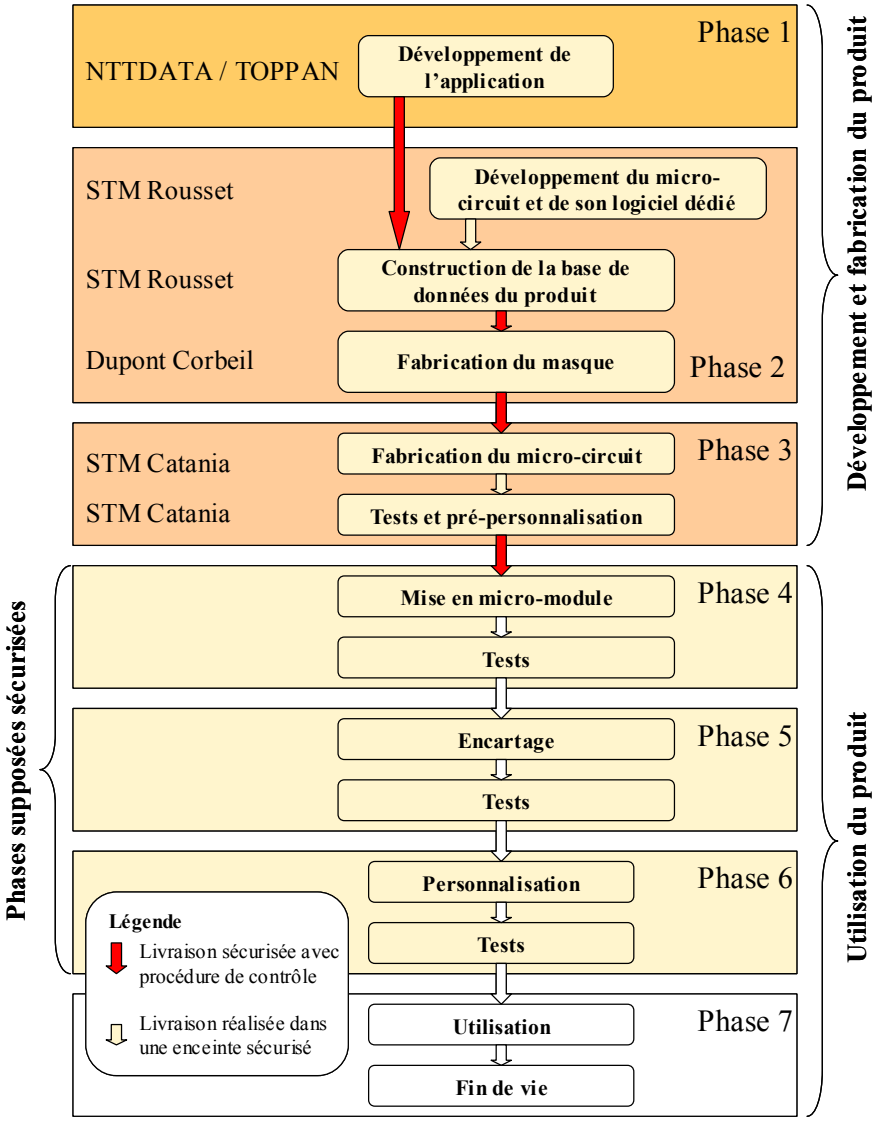

Figure 2 - Cycle de vie du produit

1.3.3. Périmètre et limites du produit évalué

Le périmètre d'évaluation est celui représenté sur la figure Figure 1. Il comprend la plate-forme Xaica-Alpha avec le Softmask 3 version 0.32 ainsi que le micro-circuit ST19XR34 F.
Le Softmask est installé sur la carte à puce par le *Card Manufacturer* TOPPAN.

Toutefois, il faut noter que les hypothèses suivantes ont été prises en compte durant l'évaluation :

- la fonction de chiffrement selon l'algorithme AES ne fait pas partie du périmètre d'évaluation ;
- la fonction de chiffrement selon l'algorithme simple DES ne fait pas partie du périmètre d'évaluation ;

- il a été considéré qu'aucune autre application n'était chargée, et notamment aucune application de type DLO (*Downloadable Objects*).

2. L'évaluation

2.1. Contexte

Le produit évalué est construit sur le micro-circuit ST19XR34F certifié en 2004 sous la référence [2004/31], et sous surveillance à la date d'émission de ce certificat.
Une partie des verdicts de la présente évaluation s'appuie donc sur les résultats des travaux menés lors de l'évaluation du micro-circuit.

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], et aux interprétations finales au 31 octobre 2003.

2.3. Commanditaire

NTTDATA Corporation

Shin Kawasaki Mitsui Building
890-12 Kashimada, Saiwai-ku
Kawasaki-shi
Kanagawa
Japon

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 du 19 décembre 2003 au 17 décembre 2004.

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 EAL4[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL4	Methodically designed, tested, and reviewed
+ ADV_IMP.2	Implementation of the TSF
+ ALC_DVS.2	Sufficiency of security measures

2.7.2. L'évaluation de l'environnement de développement

Le développement du produit implique l'ensemble des sites identifiés au §1.2 du présent rapport.

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 analysé le plan de gestion de configuration fourni par le développeur qui précise l'utilisation du système de gestion de configuration. Le système permet de générer notamment la liste de configuration [CONF] qui identifie tous les éléments gérés par le système.

Des procédures de génération permettent par ailleurs de s'assurer que les bons éléments sont utilisés pour générer le produit évalué.

[1] Annexe 3 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

La vérification de l'application des procédures analysées a été effectuée lors d'une visite des sites de NTTDATA et de TOPPAN (cf Annexe 1).

La vérification de l'application des procédures de développement et de gestion de configuration pour le micro-circuit a été effectuée lors de l'évaluation de ce dernier (cf. [2004/31]).

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_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
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

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), conception de haut-niveau (HLD), conception de bas-niveau (LLD), implémentation (IMP).

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

Exigences applicables au système d'exploitation Xaica-PF :

- Configuration generation (FAU_CFG.1)
- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key distribution (FCS_CKM.2)
- Cryptographic key destruction (FCS_CKM.4)
- Subset access control (FDP_ACC.1)
- Security attributes based access control (FDP_ACF.1)
- Import of user data without security attributes (FDP_ITC.1)
- Import of user data with security attributes (FDP_ITC.2)
- Authentication failures handling (FIA_AFL.1)
- User attribute definition (FIA_ATD.1)
- Timing of authentication (FIA_UAU.1)
- Single-use authentication mechanisms (FIA_UAU.4)
- Multiple authentication mechanisms (FIA_UAU.5)
- Re-authenticating (FIA_UAU.6)
- Timing of identification (FIA_UID.1)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)

- Static attribute initialisation (FMT_MSA.3)
- Management of TOE security functions data (FMT_MTD.1)
- Security management roles (FMT_SMR.1)
- TSF domain separation (FPT_SEP.1)
- Inter-TSF trusted channel (FTP_ITC.1)
- Inter-TSF basic TSF data consistency (FPT_TDC.1)

Exigences applicables à la plate-forme (système d'exploitation et micro-circuit) :

- Cryptographic operation (FCS_COP.1)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- TSF Generation of secrets (FIA_SOS.2)
- Failure with preservation of secure state (FPT_FLS.1)
- Automated recovery (FPT_RCV.2)
- Function recovery (FPT_RCV.4)
- TOE Security Functions testing (FPT_TST.1)

Exigences applicables au micro-circuit ST19XR34 :

- Potential violation analysis (FAU_SAA.1)
- Complete access control (FDP_ACC.2)
- Security attributes based access control (FDP_ACF.1)
- Limited illicit information flows (FDP_IFF.3)
- Partial elimination of illicit information flows (FDP_IFF.4)
- Basic internal transfer protection (FDP_ITT.1)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Management of security attributes (FMT_MSA.1)
- Static attribute initialisation (FMT_MSA.3)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)
- Unobservability (FPR_UNO.1)

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_SPM.1	Informal TOE security policy model	Réussite
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_IMP.2	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 la phase 4 (du cycle de vie décrit au paragraphe 1.3.2) et la phase 5. Le produit est livré au *Card Manufacturer* TOPPAN.

Ces procédures permettent de connaître l'origine de la livraison et de détecter une modification du produit au cours de cette livraison.

L'installation du produit correspond à la phase 5. 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.2	Detection of modification	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 administrateurs du produit le *Card Issuer* (cf §1.3.2 phase 6 et 7) et comme utilisateurs d'une part les porteurs de la carte pour ce qui est de l'application JUKI, et d'autre part les *Services Providers* voulant implémenter des applications sur la plate-forme Xaica-alpha.

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 plate-forme identifiée au paragraphe 1.1.

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

Classe ATE: Tests		**Verdicts**
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

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 (code PIN) ont fait l'objet d'une estimation du niveau de résistance intrinsèque. Le niveau de résistance de ces fonctions est jugé élevé : 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 sur la plate-forme identifiée au paragraphe 1.1.

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.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.2	Independent vulnerability analysis	Réussite

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] :

- La sécurité des données sensibles chargées dans la carte doit être garantie lorsqu'elles sont utilisées en dehors du produit. En particulier, la clé maître utilisée par le terminal doit être cohérente avec celle attendue et stockée dans la carte.
- Le terminal doit garantir la sécurité des données résidentielles de la carte lorsqu'il les manipule en phases d'authentification. Il doit les effacer intégralement après ces opérations.
- Le terminal doit implémenter des mécanismes pour prévenir une utilisation non autorisée.

Les exigences fonctionnelles pour l'environnement TI présente dans la cible devront également être respectées :

- Subset residual information protection (FDP_RIP.1)
- Subset access control (FDP_ACC.1)
- Security attributes based access control (FDP_ACF.1)
- Management of security attributes (FMT_MSA.1)
- Static attribute initialisation (FMT_MSA.3)
- Security roles (FMT_SMR.1)
- Timing of identification (FIA_UID.1)

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]. Toutefois, les augmentations suivantes n'entrent pas dans le cadre de l'accord : ADV_IMP.2, ALC_DVS.2.

Annexe 1. Visite du site de développement de la société NTTDATA Corporation à Kanagawa

Le site de développement de la société NTTDATA Corporation situé à Shin Kawasaki Mitsui Building, 890-12 Kashimada, Saiwai-ku, Kawasaki-shi, Kanagawa au Japon, a fait l'objet d'une visite par l'évaluateur du 31 mai au 3 juin 2004, et du 24 au 26 novembre 2004 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour la plate-forme Xaica-alpha version V150i_alpha7rs3_SM032 sur micro-circuit ST19XR34 F.

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

- ACM_AUT.1 et ACM_CAP.4 ;
- ALC_DVS.2 ;
- ADO_DEL.2.

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

Annexe 2. Visite du site de développement de la société TOPPAN à Tokyo

Le site de développement de la société TOPPAN situé au 1-3-3, Suido, Bunkyo-ku, Tokyo au Japon, a fait l'objet d'une visite par l'évaluateur du 31 mai au 3 juin 2004, et du 24 au 26 novembre 2004 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour la plate-forme Xaica-alpha version V150i_alpha7rs3_SM032 sur micro-circuit ST19XR34 F.

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

- ACM_AUT.1 et ACM_CAP.4 ;
- ALC_DVS.2 ;
- ADO_DEL.2.

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

Annexe 3. 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 4. Références documentaires du produit évalué

[2004/31]	Rapport de certification 2004/31 - Micro-circuit ST19XR34F, 8 octobre 2004, SGDN/DCSSI
[ST]	Cible de référence pour l'évaluation : • Xaica-alpha Security Target, Référence : NTTD-ST-XAICAALPHA-ST19, version 1.02 NTTDATA CORPORATION Pour les besoins de la reconnaissance internationale, la cible suivante a été fournie et validée dans le cadre de cette évaluation : • Xaica-alpha Security Target Lite, Référence : NTTD-STL-XAICAALPHA-ST19, version 1.02, February 17, 2005 NTTDATA CORPORATION
[RTE]	ALPHA project - Evaluation Technical Report, Référence : ALPHA_ETR_V1.1 Serma Technologies
[CONF]	Liste de configuration pour le micro-circuit : • ST19XR34 F configuration list, Référence : liste_config_XR34F_v1, STMicroelectronics Liste de configuration pour le logiciel embarqué : • Xaica-alpha softmask management document, Référence : ALPPUO-SMM-060_Ja TOPPAN
[INSTALL]	Les guides d'installation du produit sont constitués des documents suivants : • Xaica-alpha - Guidance for Card Issuer, référence : NTTD-GDI-XAICAALPHA-ST19, V1.0 NTTDATA CORPORATION, • Card Issue Process for Card Manufacturers, Référence : ALPCOP-IGS-030, V0.3, NTTDATA CORPORATION, • Installation guidance for 3rd vendor, Référence : ALPCOP-IG3, V0.1 NTTDATA CORPORATION.

[GUIDES]	Les guides d'utilisation et d'administration du produit sont constitués des documents suivants : • Xaica-alpha Guidance for Service Provider, Référence : NTTD-GDS-XAICAALPHA-ST19, V1.02 NTTDATA CORPORATION, • Guidance for Service Provider (Command APDU Specifications), Référence : NTTD-GDS-ADD.2-XAICAALPHA-ST19, V1.0 NTTDATA CORPORATION, • Xaica-alpha Guidance for Card Holder, Référence : NTTD-GDH-XAICAALPHA-ST19, V1.02 NTTDATA CORPORATION.
[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 9806. *Document publié sur le site : www.ssi.gouv.fr*
[Visite]	Alpha project evaluation report – classes ACM and ALC & family ADO_DEL, Référence : ALPHA_ACM-ADO_DEL-ALC_V2.1 Serma Technologies

Annexe 5. 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, 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. Le contenu des Critères Communs version 2.1 est identique à celui de la Norme Internationale ISO/IEC 15408:1999, comportant les trois documents suivants: 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.
[CEM]	Common Methodology for Information Technology Security Evaluation : Part 2: Evaluation Methodology, August 1999, version 1.0, ref CEM- 99/045.
[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.

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