Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2011/67

Carte VITALE 2 - Application VITALE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.1 avec correctif version 1

Paris, le 7 juin 2012

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Patrick Pailloux
[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 l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2011/67

Nom du produit

Carte VITALE 2 - Application VITALE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.1 avec correctif version 1

Référence/version du produit

- Version système d'exploitation : 1.0.1

- Version du correctif : 1

Conformité aux profils de protection

- [PP ESforSSD] certifié par l'ANSSI

Protection Profile Embedded software for Smart Secure Devices Basic and Extended configurations – Basic configuration, version 1.0

- [BSI-PP-0005-2002] : SSCD Type 2, version 1.04

- [BSI-PP-0006-2002] : SSCD Type 3, version 1.05

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Morpho	STMicroelectronics
18 Chaussée Jules César, 95520 Osny, France	**29 Boulevard Romain Rolland - 75669 Paris CEDEX 14**

Commanditaire

Morpho

18 Chaussée Jules César, 95520 Osny, France

Centre d'évaluation

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

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 modifié. Ce décret indique que :

- L'agence nationale 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 disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la « carte VITALE 2 - Application VITALE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.1 avec correctif version 1 » développée par Morpho et STMicroelectronics.

Suivant une règle de nommage interne de Morpho, la version du correctif (1) correspond au dernier digit de la version du système d'exploitation (1.0.1).

La cible d'évaluation (TOE – *Target Of Evaluation*) est l'application VITALE masquée. Elle fournit les services de signature électronique (SSCD type 2 et 3), c'est-à dire:

- générer les bi-clés de signature électronique ;
- détruire les bi-clés de signature électronique ;
- charger une clé privée de signature électronique ;
- créer une signature électronique.

De plus, l'application VITALE permet de fournir les services de santé VITALE 2 compatibles avec l'application VITALE 1.

Le produit embarque, outre l'application VITALE, d'autres applications dont la présence a été prise en compte lors de l'évaluation, notamment dans le cadre de la recherche de vulnérabilités :

- application ADELE (ADministration ELEctronique) qui est évaluée par ailleurs et qui comme l'application VITALE permet de fournir les services de signature électronique (SSCD type 2 et 3) ;
- application AIP (Application d'Initialisation et de Personnalisation) qui ne fait pas partie du périmètre de la TOE et qui est une application d'administration utilisée en phase de pré-personnalisation et de personnalisation. Elle est inactivée en phase "USER".

Ce produit est destiné à être utilisé dans le cadre de l'application SESAM VITALE ainsi que des applications de signature électronique.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.
Cette cible de sécurité est conforme de façon démontrable aux profils de protection [PP ESforSSD] (logiciel embarqué sur composant), [BSI-PP-0005-2002] (SSCD Type 2) et [BSI-PP-0006-2002] (SSCD Type 3).

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments suivants :

- par lecture de l'ATR. Les valeurs possibles en fonction de la phase de vie de la carte sont décrites dans [GUIDES] ; en phase d'utilisation, cet ATR est donné par le tableau suivant :

OCTET	VALEUR	EXPLICATION
TS	3B	Convention directe
T0	75	Octets système + nombre d'octets historique (de 0 à 15)
TA1	13	Voir ISO 7816-3
TB1	00	Voir ISO 7816-3
TC1	00	Voir ISO 7816-3
T1	XX	Déterminé par le GIE SESAM VITALE pour chaque produit • 46 : Vitale2 ST23
T2	09	Référence pour rétrocompatibilité Vitale1
T3	XX	Octet MCH
T4	90	Mot d'état SW1
T5	XX	Mot d'état SW2

- par lecture de la version contenue dans le CPLC (cf. [GUIDES], guide de préparation au chapitre « *3.1.1 CPLC description* »). Cette lecture s'effectue par la commande « GET DATA » (00 CA 9F 7F 2D). En retour, la carte émet le CPLC. La version du logiciel embarqué en ROM est codée sur deux octets en position 9 et 10. Leur contenu doit être égal aux valeurs hexadécimales « 10 10 » correspondant à la version « 1.0.1 » de l'OS de la TOE ;
- par lecture de la version du correctif contenue dans l'objet « *Optional code* » (cf. [GUIDES], guide de préparation au chapitre « *3.1.2 Optional code description* »). Cette lecture s'effectue par la commande « GET DATA » (80 CA DF 26 13). En retour, la carte émet les informations demandées. La signature du correctif en EEPROM est codée sur huit octets (les 8 derniers octets retournés par la commande précédente). Leur contenu doit être égal aux valeurs hexadécimales suivantes : « 7E 01 00 11 30 00 D9 EF » ;
- par vérification de l'intégrité des valeurs de sécurité du composant en lisant la valeur contenue dans l'objet « *Hardware security integrity* » (cf. [GUIDES], guide de préparation au chapitre « *3.1.3 Hardware security integrity* »). Cette lecture s'effectue par la commande « GET DATA » (80 CA DF 28 05). En retour, la carte émet les informations demandées. La signature des données en EEPROM est codée sur cinq octets. Leur contenu doit être égal aux valeurs hexadécimales suivantes : « DF 28 02 CD F0 ».

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit, détaillés dans la [ST] au chapitre « *9.1 TOE Summary Specification* », sont :

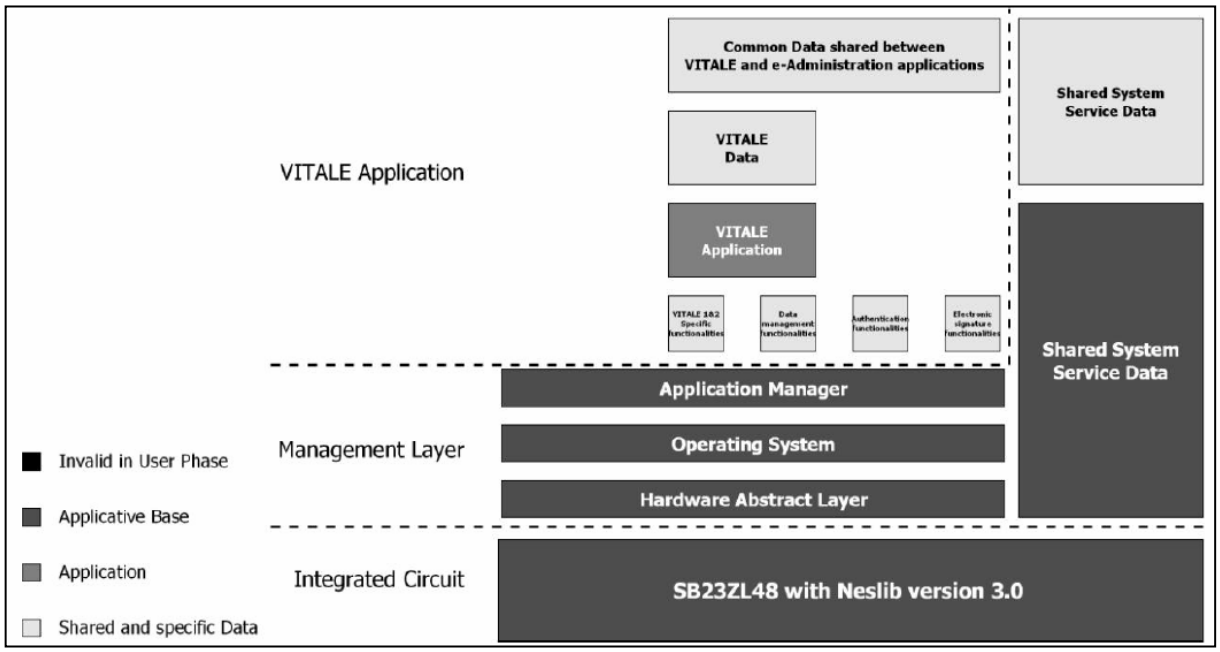
- ceux provenant du composant sous-jacent détaillés dans [ANSSI-CC-2010_08] ;
- ceux provenant de la TOE :
  - TSF_BOOT_AT_POWER_UP : initialisation sécurisée de la TOE ;
  - TSF_MONITORING : gestion des alarmes de sécurité ;
  - TSF_EXECUTION_ENVIRONMENT : gestion de l'environnement d'exécution ;
  - TSF_MEMORY_MANAGEMENT : gestion sécurisée des mémoires ;
  - TSF_IO_MANAGEMENT : gestion sécurisée des entrées/sorties ;
  - TSF_LIFE_CYCLE_MANAGEMENT : gestion sécurisée du cycle de vie de la TOE ;
  - TSF_RANDOM_NUMBERS : gestion sécurisée des aléas ;
  - TSF_ADMINISTRATION : gestion sécurisée de la création de l'arborescence pour l'administration de la TOE ;
  - TSF_AUTHENTICATION : gestion sécurisée des authentifications vis-à-vis de la TOE ;
  - TSF_CRYPTOGRAPHIC_OPERATIONS : gestion sécurisée des opérations cryptographiques ;
  - TSF_KEY_MANAGEMENT : gestion sécurisée des clés ;
  - TSF_ATOMIC_OPERATIONS : gestion des transactions atomiques (non interruptibles).

1.2.3. Architecture

Le produit, dont l'architecture est détaillée dans la [ST] au chapitre « *3 TOE description* », est constitué :

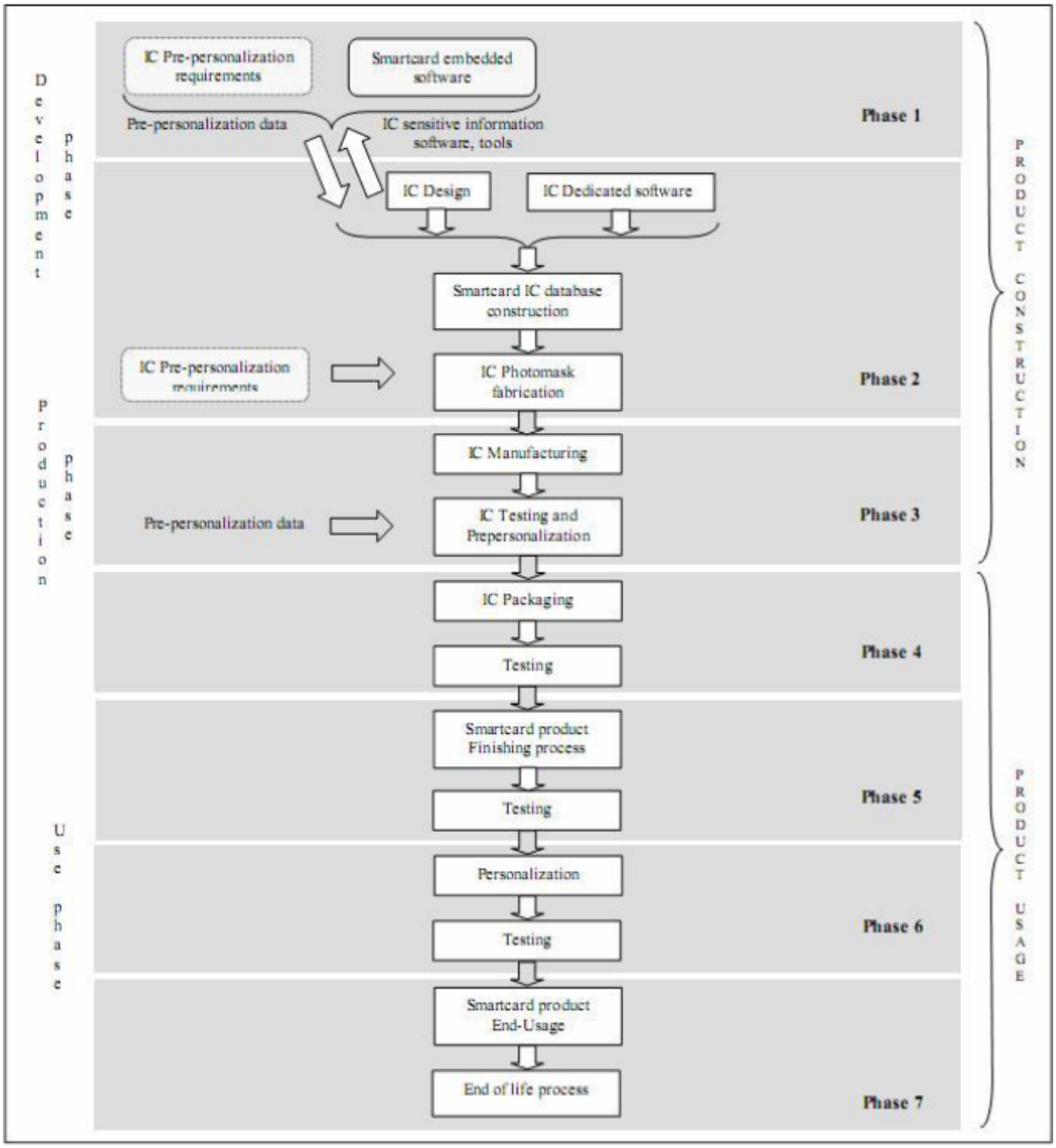
- d'un circuit intégré SB23ZL48 de la société STMicroelectronics ;
- d'un logiciel embarqué, développé par MORPHO, comprenant :
  - un système d'exploitation qui réalise :
    - la gestion des services d'administration (pré-personnalisation et personnalisation) ;
    - l'ensemble des fonctions pouvant être utilisées par les applications (gestion des fichiers en EEPROM, fonctions cryptographiques, gestion du bus d'Entrées-Sorties, gestion de la mémoire et des paramètres et traitements des erreurs et exceptions détectées par la carte) ;
  - un gestionnaire d'application qui est le point de passage obligé pour obtenir les services du système d'exploitation ;
  - des applications ;
  - des services partagés qui effectuent les contrôles relatifs à la sécurité et gèrent les mécanismes de *patch* ;
  - la gestion du composant (couche d'interface entre le composant et le système d'exploitation).

La figure suivante illustre l'architecture de la TOE :



1.2.4. Cycle de vie

Le cycle de vie du produit est celui d'une carte à puce et comprend 7 phases comme illustrées ci-après :



Le point de livraison est situé en fin de phase 3, marquant la fin de la phase de développement du produit, en particulier, le correctif est chargé en phase 3.

Toutes les étapes qui précèdent ce point de livraison ont été couvertes par la présente évaluation (au titre d'ALC), le cas échéant, en réutilisant les résultats obtenus lors de l'évaluation du composant sous-jacent qui a couvert les phases 2 et 3 (voir [ANSSI-CC-2010_08]).

Les phases 4 à 6 ont été prises en compte durant l'évaluation au travers des guides (au titre d'AGD).

Les tests ont porté sur les fonctionnalités du produit disponibles en phase 7 ou « *User Phase* » (au titre d'ATE et d'AVA).

L'application masquée a été développée sur le site suivant :

Site de Morpho pour le développement du logiciel :

18 Chaussée Jules César

95520 Osny
France

Pour l'évaluation, l'évaluateur a considéré comme :

- administrateurs du produit, les rôles suivants :
  - « *Embedder* » (encarteur) qui intervient en phase 4 et 5 ;
  - « *Personalizer* » (personnalisateur) qui intervient en phase 6 ;
  - « *Transmitter* » (transmetteur) qui intervient en phase 7 ;
  - « *Domain authority* » (autorité du domaine) qui intervient en phase 7 ;
- et comme utilisateurs du produit, les rôles suivants :
  - « *Health professional* » (professionnel de santé) qui intervient en phase 7 ;
  - « *Bearer* » (porteur) qui intervient en phase 7.

Ces rôles sont décrits dans [ST] au chapitre « *3.8.1 Generic users* ».

1.2.5. Configuration évaluée

Le certificat porte sur la configuration de la TOE obtenue en suivant le guide de préparation (cf. [GUIDES]). Ce guide décrit les options de personnalisation qui doivent être choisies afin d'obtenir la configuration évaluée de la TOE.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation des « microcontrôleurs sécurisés SA23ZL48/34/18A et SB23ZL48/34/18A, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [BSI-PP-0035-2007]. Ce microcontrôleur a été certifié par l'ANSSI (voir [ANSSI-CC-2010_08]).

Le niveau de résistance des microcontrôleurs ont été confirmés par l'ANSSI dans le cadre du processus de surveillance (cf. [SUR_IC]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 25 janvier 2012, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques (voir [SPEC-CRY-HYG]) a été réalisée conformément aux référentiels techniques de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Cette analyse n'a pas fait apparaître de vulnérabilités majeures. Il est cependant recommandé :

- d'utiliser la fonction de hachage SHA-2 en signature ;
- de dimensionner le module RSA et les paramètres Diffie-Hellman de façon conforme au référentiel technique [REF-CRY] de l'ANSSI.

Dans le cadre du processus de qualification renforcé, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI (cf. [RTE]). Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

L'analyse du générateur de nombres aléatoires a été réalisée conformément aux référentiels techniques de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT]. Ce générateur est reconnu conforme à ces référentiels.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « Carte VITALE 2 - Application VITALE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.1 avec correctif version 1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté de ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

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

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance 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] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	**1**	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedure
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Problem tracking CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ASE Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specifications
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**1**	Testing: basic design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independant testing, sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	**2**	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Security Target for VITALE application, référence 0000081294-06, date 14/12/11, Morpho. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - - Security Target Lite for VITALE application, référence 0000088820, date 24/01/12, Morpho.
[RTE]	Rapport technique d'évaluation : - HYGIE - Rapport Technique d'Evaluation / Evaluation Technical Report, référence LETI.CESTI.HYG.RTE.001 – v1.1, date 25/01/12, CEA-LETI.
[SPEC-CRY-HYG]	Spécification des mécanismes cryptographiques : - Analyse cryptographique, référence 0000079762, version 2, date 04/07/11, Morpho.
[ANA-CRY]	Rapport d'analyse cryptographique : - HYGIE - Cotation des mécanismes cryptographiques, référence LETI.CESTI.HYG.RT.01 - v3.0, date 02/12/2011, CEA-LETI.
[CONF]	Liste de configuration du produit telle qu'identifiée dans le RTE - - VITALE 2 3RD Software Release Sheet, référence SSE-0000083830-10, date 11/01/12, Morpho.
[GUIDES]	Guide de préparation du produit : - PREPARATIVE PROCEDURES FOR VITALE2, référence 0000086182-02, date 11/10/11, Morpho. Guide d'opération du produit : - OPERATIONAL USER GUIDANCE FOR VITALE2, référence 0000086181-02, date 11/10/11, Morpho.
[PP ESforSSD]	Profil de protection certifié par l'ANSSI le 1er décembre 2009, sous la référence ANSSI-CC-PP-2009_02 et portant le titre : « Protection Profile Embedded software for Smart Secure Devices Basic and Extended configurations –Basic configuration », version 1.0

[BSI-PP-0005-2002]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. Certifié par le BSI sous la référence BSI-PP-0005-2002T.
[BSI-PP-0006-2002]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. Certifié par le BSI sous la référence BSI-PP-0006-2002T.
[BSI-PP-0035-2007]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.
[ANSSI-CC-2010_08]	Certificat ANSSI délivré le 8 mars 2010 pour le produit : « Microcontrôleurs sécurisés SA23ZL48/34/18A et SB23ZL48/34/18A, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB ».
[SUR_IC]	Lettre de poursuite de la surveillance émise par l'ANSSI le 30 juin 2011, référence n°1677/ANSSI/SR/CCN, pour le produit : « Microcontrôleurs sécurisés SA23ZL48/34/18A et SB23ZL48/34/18A, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB » initialement certifiée par l'ANSSI (cf. [ANSSI-CC-2010_08]).

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié 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, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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 3.0, 8 Janvier 2010, Management Committee.

[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.