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-2015/35

Carte VITALE 2 - Application ADELE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.4 avec correctif version 4

Paris, le 23 octobre 2015

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

Contre-amiral Dominique RIBAN
[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-2015/35

Nom du produit

Carte VITALE 2 - Application ADELE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.4 avec correctif version 4

Référence/version du produit

Référence VITALE2/SB23ZL48/1.0.40

Conformité aux profisl de protection

- **[PP-ESforSSD], version 1.0, Protection Profile Embedded software for Smart Secure Devices Basic and Extended configurations – Basic configuration**
- **[PP-SSCD2], version 1.04, Protection Profile Secure Signature-Creation Device Type 2**
- **[PP-SSCD3], version 1.05, Protection Profile Secure Signature-Creation Device Type 3**

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

18 Chaussée Jules César, 95520 Osny, France

STMICROELECTRONICS

190 avenue Celestin Coq, ZI de Rousset, 13106 Rousset Cedex, France

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 EAL2.

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 ADELE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.4 avec correctif version 4, référence VITALE2/SB23ZL48/1.0.40 » développée par *MORPHO* et *STMICROELECTRONICS*.

La cible d'évaluation (TOE – *Target Of Evaluation*) est l'application ADELE (ADministration ELEctronique) 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.

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

- l'applicationVITALE qui est évaluée par ailleurs et qui comme l'application ADELE permet de fournir les services de signature électronique (SSCD type 2 et 3) ;
- l'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 utilisateur.

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

1.2.1. Introduction

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) ;
- [PP-SSCD2] (SSCD Type 2) ;
- [PP-SSCD3] (SSCD Type 3).

1.2.2. Identification du produit

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

La version certifiée du produit est identifiable par l'ensemble des 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 « 3B 75 13 00 00 XX 09 YY », où XX est déterminé par le GIE-SESAM VITALE en fonction du composant, YY = EA en phase utilisateur ou FA si l'application est invalidée ;

- par lecture de la version contenue dans le CPLC[1] (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 phase utilisateur. 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 40 », correspondant à la version « 1.0.4 » de l'OS de la TOE ;
- par vérification de l'intégrité des valeurs de sécurité du composant en lisant la valeur contenue dans l'objet h*ardware security integrity* (cf. [GUIDES], guide de préparation au chapitre 3.1.3 *Hardware security integrity*). Cette lecture s'effectue par la commande « 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 ».

1.2.3. Services de sécurité

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

- ceux provenant du composant sous-jacent détaillés dans [CER-IC] ;
- 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 l'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 nombre aléatoires ;
  - 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 (génération, destruction et vérifications de clés, exécution des opérations cryptographiques) ;
  - TSF_KEY_MANAGEMENT : gestion sécurisée des clés ;
  - TSF_ATOMIC_OPERATIONS : gestion des transactions atomiques (non interruptibles).

1.2.4. Architecture

Le produit, dont l'architecture est détaillée dans la cible de sécurité [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 :

[1] *Card Production Life Cycle* : Cycle de vie de production carte

- 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 du produit:

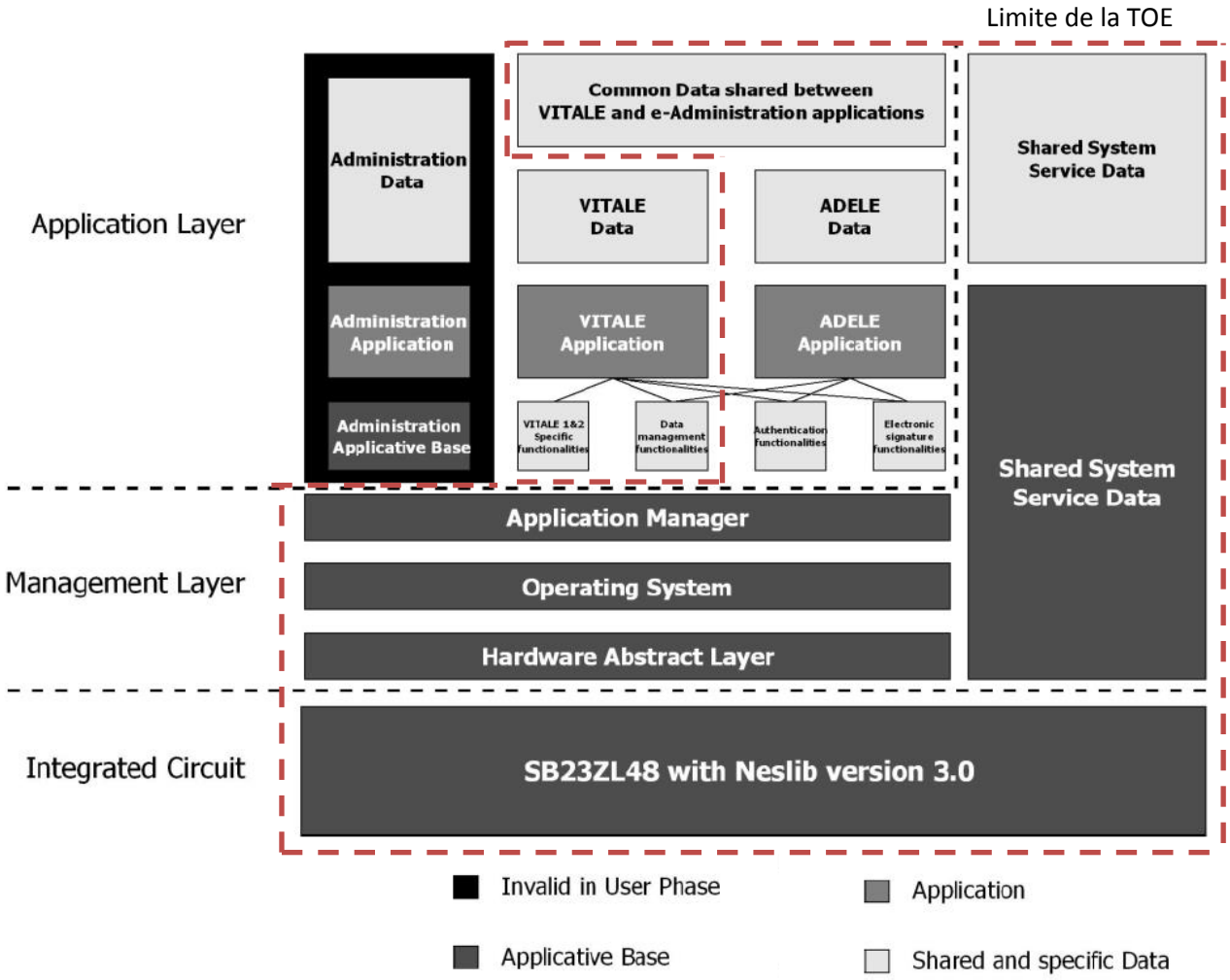

Figure 1 : Architecture du produit

1.2.5. Cycle de vie

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

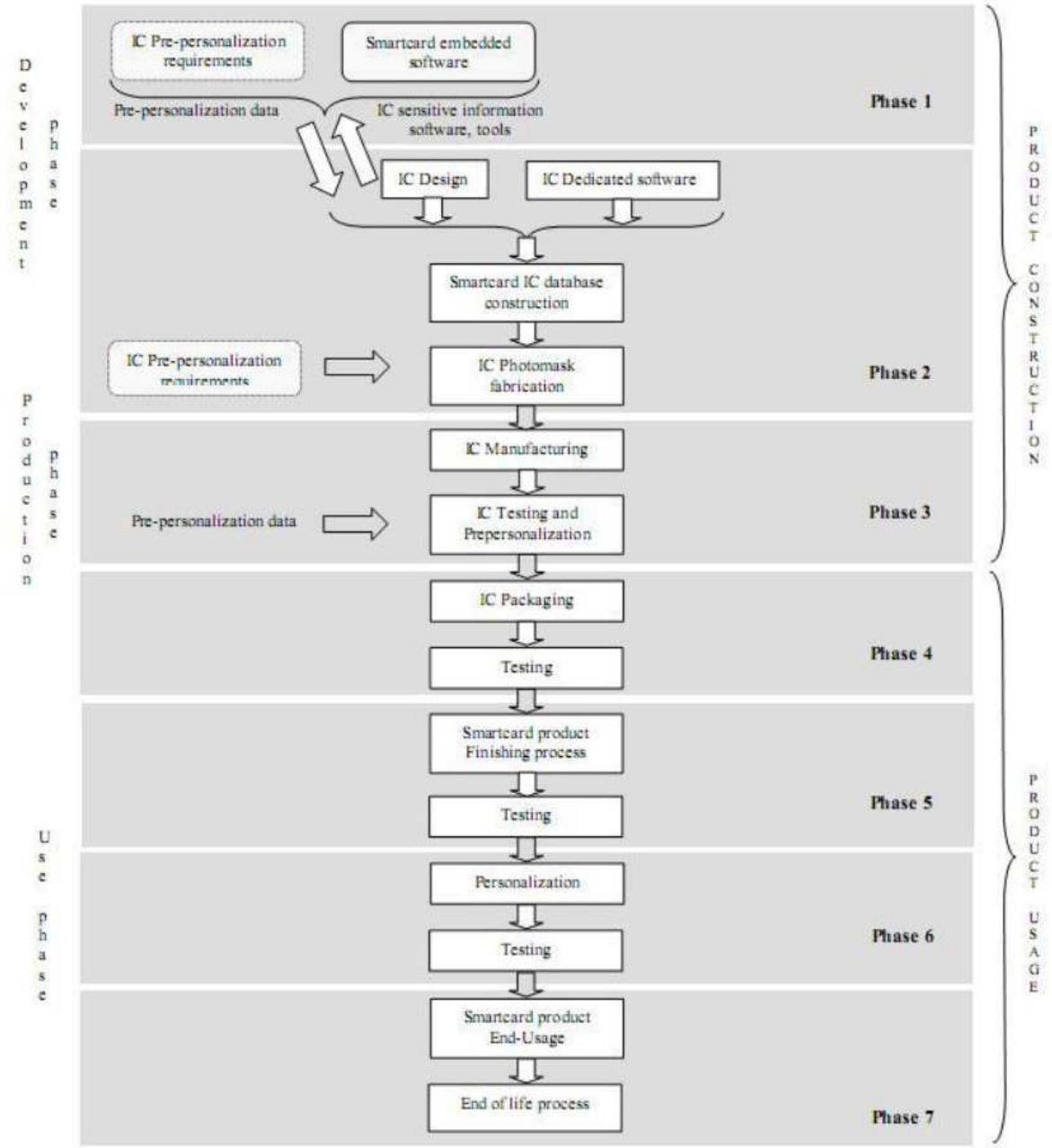

Figure 2 : Cycle de vie du produit

Les phases 1 à 3 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 (cf. [CER-IC]).
Le point de livraison est situé en fin de phase 3, marquant la fin de la phase de développement du produit. En particulier, le *patch* en EEPROM est intégré, dans la TOE, chez le fondeur durant les phases 1 à 3.
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).

Le produit a été développé sur le site suivant :

Site *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 ;
- 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 la cible de sécurité [ST] au chapitre 3.8.1 *Generic users*.

1.2.6. 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 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel [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 [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

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 [PP-0035]. Ce microcontrôleur a été certifié le 08 mars 2010 sous la référence ANSSI-CC-2010/08 (cf. [CER-IC]) et maintenu le 05 avril 2011 et le 26 février 2013 (cf. [CER-IC_M01] et [CER-IC_M02]). Le niveau de résistance du microcontrôleur a été confirmé le 20 novembre 2014 dans le cadre du processus de surveillance.

L'évaluation s'appuie sur les résultats d'évaluation du produit « carte VITALE 2 - Application ADELE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.1 avec correctif version 1 » certifié le 07 juin 2012 sous la référence ANSSI-CC-2011/68 (cf. [CER]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 9 octobre 2015, 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

L'analyse des mécanismes cryptographiques a été réalisée par le CESTI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI [REF], les recommandations suivantes doivent être suivies :

- dans la fonction d'authentification mutuelle asymétrique :
  - l'état interne du générateur de nombres aléatoires ne doit pas être compromis ;

  - les paramètres DIFFIE-HELLMAN doivent être tels que le module premier p a une taille d'au moins 2048 bits et l'ordre q du sous-groupe est multiple d'un nombre premier d'au moins 200 bits ;
  - la taille du module et de l'exposant privé RSA doit être d'au moins 2048 bits ;
- dans la fonction d'authentification mutuelle symétrique, les clés de confidentialité et d'intégrité doivent être utilisées pour au plus 2^{27} blocs (1 Go) ;
- dans la fonction d'authentification interne symétrique, les clés de confidentialité et d'intégrité doivent être utilisées pour au plus 2^{27} blocs (1 Go) ;
- dans la fonction d'authentification externe symétrique, les clés de confidentialité et d'intégrité doivent être utilisées pour au plus 2^{27} blocs (1 Go) ;
- dans la fonction d'authentification interne asymétrique :
  - la taille minimale du module et de l'exposant privé RSA doit être d'au moins 2048 bits ;
  - la bi-clé de signature doit être utilisé pour au plus 2^{27} signatures ;
  - la bi-clé de signature doit être dédié à l'authentification interne asymétrique ;
- dans la fonction d'authentification externe asymétrique :
  - la taille minimale du module et de l'exposant privé RSA doit être d'au moins 2048 bits ;
  - la bi-clé de signature doit être utilisé pour au plus 2^{27} signatures ;
- dans la fonction de *Secure Messaging*, les clés de confidentialité et d'intégrité doivent être utilisées pour au plus 2^{27} blocs (1 Go) ;
- dans la fonction de calcul de signature :
  - la taille minimale du module et de l'exposant privé RSA doit être d'au moins 2048 bits ;
  - la bi-clé de signature doit être dédié au calcul de signature ;
  - la fonction de hashage SHA-2 doit être utilisée ;
- dans la fonction de calcul de signature VITALE 1 et VITALE 2, les clés de signature doivent être utilisées pour au plus 2^{27} blocs de données à signer (1 Go) ;
- dans la fonction de chiffrement symétrique de données, la clé de confidentialité doit être utilisée pour au plus 2^{27} blocs (1 Go) ;
- dans la fonction de déchiffrement de données asymétrique, la taille minimale du module et de l'exposant privé RSA doit être d'au moins 2048 bits.

Quoi qu'il en soit, les 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.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (cf. [CER-IC]).

La sortie du générateur physique d'aléas subit un retraitement de nature cryptographique basé sur l'ANSI X9.31 qui n'est pas reconnu conforme au référentiel cryptographique de l'ANSSI [REF].

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 ADELE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.4 avec correctif version 4, référence VITALE2/SB23ZL48/1.0.40 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants 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 puce 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 :

[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.

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[1], des certificats Critères Communs.
La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 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 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, 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 TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	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 procedures
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 Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components 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 specification
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**	Independent 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 ADELE application, référence 0000081295, version 09, 02/10/2015. 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 ADELE application, référence 0000088819, version 03, 02/10/2015.
[RTE]	Rapport technique d'évaluation : Rapport Technique d'Evaluation/ Evaluation Technical Report, référence LETI.CESTI.HYR.RTE.001, version 1.1, 06/10/2015.
[ANA-CRY]	Cotation des mécanismes cryptographiques, référence LETI.CESTI.HYR.RT.01, version 1.0, 02/07/2015.
[CONF]	Liste de configuration du produit telle qu'identifiée dans [RTE] : VITALE 2 3RD Software Release Sheet, référence SSE-0000083830-16, version 1.16, 05/10/2015.
[GUIDES]	Guide de préparation du produit : – Prepartative Procedures for VITALE2, référence 0000086182-06, version 06, 07/08/15 ; Guide d'opération du produit : – Operational user guidance for VITALE2, référence 0000086181-03, version 03, 11/01/12.
[PP-ESforSSD]	Protection Profile - Protection Profile Embedded software for Smart Secure Devices Basic and Extended configurations – Basic configuration, version 1.0, 1er décembre 2009. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2009_02.*
[PP-SSCD2]	Protection Profile - Secure Signature-Creation Device Type 2, version 1.04, 25 juillet 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0005-2002T.*
[PP-SSCD3]	Protection Profile - Secure Signature-Creation Device Type 3, version 1.05, 25 juillet 2001. *Certifié par le BSI sous la référence BSI-PP-0006-2002T.*
[PP-0035]	Protection Profile, Security IC Platform Protection Profile, version 1.0, juin 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*

[CER-IC]	Rapport de certification « Microcontrôleurs sécurisés SA23ZL48/34/18A et SB23ZL48/34/18A, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB ». *Certifié par l'ANSSI le 7 mars 2010 sous la référence ANSSI-CC-2010/08.*
[CER-IC_M01]	Rapport de maintenance ANSSI-CC-2010/08-M01 émis le 05 avril 2011.
[CER-IC_M02]	Rapport de maintenance ANSSI-CC-2010/08-M02 émis le 26 février 2013.
[CER]	Rapport de certification « Carte VITALE 2 - Application ADELE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.1 avec correctif version 1 ». *Certifié par l'ANSSI le 7 juin 2012 sous la référence ANSSI-CC-2011/68.*

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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-001 ; Part 2 : Security functional components, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-002 ; Part 3 : Security assurance components, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, version 3.1, révision 3 Final, référence CCMB-2009-07-004, juillet 2009.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.4, août 2015.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.