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-2016/20

ID-One eIDAS v1.0 en configuration SSCD-5 sur les composants P60x080PVC/PVG

Paris, le 12/05/2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2016/20

Nom du produit

ID-One eIDAS v1.0 en configuration SSCD-5 sur les composants P60x080PVC/PVG

Référence/version du produit

SAAAAR 080031 : ID-One ePass V3 Full EACv2 on NXP

SAAAAR 082456 : Code r6.0 Generic

SAAAAR 082844 : Optional Code r4.0 Digitaly Blurred Image

Conformité à un profil de protection

Protection profiles for secure signature creation device – Part 5 : Extension for device with key generation and trusted communication with signature creation application, version 1.0.1,
certifié sous la référence [PP-SSCD-Part5].

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Oberthur Technologies

420 rue d'Estienne d'Orves
CS 40008
92705 Colombes, France

NXP Semiconductors

Box 54 02 40,
D-22502 Hamburg, Allemagne

Commanditaire

Oberthur Technologies

420 rue d'Estienne d'Orves
CS 40008
92705 Colombes, 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 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Identification du produit 6
1.2.3. Services de sécurité 7
1.2.4. Architecture 7
1.2.5. Cycle de vie 7
1.2.6. Configuration évaluée 8

2. L'EVALUATION 9

2.1. REFERENTIELS D'EVALUATION 9
2.2. TRAVAUX D'EVALUATION 9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 9
2.4. ANALYSE DU GENERATEUR D'ALEAS 10

3. LA CERTIFICATION 11

3.1. CONCLUSION 11
3.2. RESTRICTIONS D'USAGE 11
3.3. RECONNAISSANCE DU CERTIFICAT 11
3.3.1. Reconnaissance européenne (SOG-IS) 11
3.3.2. Reconnaissance internationale critères communs (CCRA) 11

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 13

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 14

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 16

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce « ID-One eIDAS v1.0 en configuration SSCD-5 sur les composants P60x080PVC/PVG », pouvant être en mode contact ou sans contact. Le produit est développé par *OBERTHUR TECHONOLOGIES* sur un composant *NXP SEMICONDUCTORS*.

Ce produit est destiné à être utilisé pour créer des signatures électroniques.

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 strictement conforme au profil de protection [PP-SSCD-Part5].

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 les éléments présents dans la réponse que donne le produit suite à la commande GET DATA (voir [GUIDES]).

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

- nom commercial : ID-One ePass Full EAC V2 ;
- code SAAAAR[1] du code ROM : 080031 ;
- code patch obligatoire : 412E4D1EC087005B56A9A2CAC0B6558F4CAAE041D8B5A69345559B562A6F4C8E ;
- code patch optionnel : E339C30BC6A81162413612FE2698284FA6CD28AA5CF5257A20B83611E58E9BEE ;
- code composant (sur 42 octets) : XXXXvvvvXX..XX où vvvv peut valoir :
  - '6C14' pour le composant P60D080PVC ;
  - '6014' pour le composant P60D080PVG ;
  - '6019' pour le composant P60C080PVG.

Il peut être décidé ou non de charger le *patch* optionnel et d'ainsi de disposer ou non de la fonction *Digitally Blurred Image*.

Les codes « SAAAAR et patch » peuvent être vérifiés par une commande GETDATA avec le tag DF66. Le code composant peut être vérifié par une commande GETDATA avec le tag 9F7F comme décrit dans [GUIDES].

[1] S : code site (0 pour la France), AAAA : article sur 4 chiffres, R : *release* ou version du logiciel.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la génération de la donnée de création de signature (*Signature Creation Data* ou SCD) et de la donnée de vérification de signature (*Signature-Verification Data* ou SVD) associée ;
- l'export du SVD pour une création de certificat électronique ;
- la réception et le stockage des informations du certificat électronique (seulement si le personnalisateur les créées) ;
- le passage de l'état non opérationnel à l'état opérationnel ;
- la création de signature électronique via un canal de confiance ;
- l'authentification de l'administrateur ;
- l'authentification du signataire par un code PIN ou des données biométriques.

Il existe une fonction optionnelle non évaluée de *Digitally Blurred Image* permettant de rendre illisible la photo en cas d'utilisation frauduleuse.

1.2.4. Architecture

Le produit est une carte à puce fermée constituée des éléments suivants :

- un microcontrôleur P60x080PVC/PVG de *NXP SEMICONDUCTORS*, en configuration P60D080PVC, P60D080PVG ou P60C080PVG ;
- un logiciel « *BIOS* » donnant l'accès aux fonctionnalités du microcontrôleur ;
- une librairie cryptographique dédiée ;
- une application de personnalisation « *Perso* » ;
- l'application eSign ;
- l'application MRTD - IDL en dehors du périmètre de l'évaluation ;
- l'application eIDL en dehors du périmètre de l'évaluation ;
- l'application Dauth en dehors du périmètre de l'évaluation

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

	Phase	Acteur	Couvert par
Etape 1	Développement	*OBERTHUR TECHNOLOGIES*	ALC
Etape 2	Développement	*NXP SEMICONDUCTORS*	Certification du composant
Etape 3	Fabrication	*NXP SEMICONDUCTORS*	Certification du composant
Point de livraison TOE			
Etape 4	Fabriquant SSCD (Pré-perso)	Fabriquant SSCD	AGD_PRE
Etape 5	Fabriquant SSCD (Pré-perso)	Fabriquant SSCD	AGD_PRE
Etape 6	Personnalisation	Personnalisateur	AGD_PRE
Etape 7	Utilisation opérationnelle	Utilisateur final	AGD_OPE

Le produit a été développé sur le site suivant :

***OBERTHUR TECHNOLOGIES* – Site de Colombes**
420 rue d'Estienne d'Orves
92700 Colombes
France

***OBERTHUR TECHNOLOGIES* – Site de Pessac**
Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus – Porte 2
33600 Pessac
France

Le microcontrôleur est développé et fabriqué par *NXP SEMICONDUCTORS*. Les sites de développement et de fabrication du microcontrôleur sont détaillés dans le rapport de certification dont la référence est [BSI-DSZ-CC-0837-V2-2014].

Les « administrateurs du produit » sont les nations ou les organisations émettrices de la carte ID-One eIDAS v1.0.
Les « utilisateurs du produit » sont les signataires qui font appel à l'application eSign pour réaliser une opération de signature.

1.2.6. Configuration évaluée

Le produit est une carte fermée qui peut être personnalisée selon différentes configurations.
Ce rapport de certification porte sur la configuration incluant le mécanisme *Secure Signature Creation Device* selon le profil de protection [PP-SSCD-Part5].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], 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 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 du microcontrôleur « P60x080PVC/PVG » au niveau EAL6 augmenté des composants ALC_FLR.1 et ASE_TSS.2, conforme au profil de protection [BSI-PP-0035-2007]. Ce microcontrôleur a été certifié le 24 octobre 2014 sous la référence [BSI-DSZ-CC-0837-V2-2014].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 14 avril 2016, 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 a été réalisée conformément aux référentiels techniques de l'ANSSI [REF].

Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] qui donne lieu aux conclusions suivantes :

- les mécanismes analysés sont conformes aux exigences des référentiels techniques de l'ANSSI ([REF]) sous réserve de prendre en compte les recommandations se trouvant dans les guides (voir [GUIDES]) ;
- la fonction de hachage SHA-1 ne doit pas être utilisée pour les applications de signature.

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.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI. 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.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 (voir [BSI-DSZ-CC-0837-V2-2014]).

Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.

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.

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 « ID-One eIDAS v1.0 en configuration SSCD-5 sur les composants P60x080PVC/PVG » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 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 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].

[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.

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 5+	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**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	Well-structured internals
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal 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	**5**	Development tools 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	**2**	Compliance with implementation standards
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**	**3**	Testing: modular 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 : - MINOS – ID-One eIDAS v1.0 in SSCD-5 configuration Security Target, version 4, référence : 110 7734, 2 mars 2015, Oberthur Technologies. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ID-One eIDAS v1.0 in SSCD-5 configuration Public Security Target, version 2, référence : 110 7795, Oberthur Technologies.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – MINOS-eSign, version : 2.2, référence : LETI.CESTI.MIN.RTE.002 v2.2, 14 avril 2016, LETI.
[ANA-CRY]	MINOS - Cotation des mécanismes cryptographiques, version : 2.0, référence : LETI.CESTI.MIN.RT.004, 1 avril 2016, LETI.
[CONF]	Liste de configuration du produit : - MINOS ID-One eIDAS v1.0 Configuration List, version 6, 4 mars 2016, reference 110 7817, Oberthur Technologies.
[GUIDES]	Guide d'installation du produit : - MINOS – MRTD FULL EAC V2 – Guidance Document – PREparative procedures, version 11, 2 mars 2016, référence : 110 7111, Oberthur Technologies ; - MINOS – ID-ONE EIDAS v1.0 in SSCD-5 – Guidance Document – PREparative procedures, version 5, 2 mars 2016, référence : 110 7776, Oberthur Technologies. Guide d'utilisation du produit : - MINOS – ID-One eIDAS v1.0 – Guidance Document – OPErational user guidance, version 1, 2 décembre 2015, reference 110 7822, Oberthur Technologies.
[PP-SSCD-Part5]	Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, référence : prEN 14169-5:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012.*
[BSI-PP-0035-2007]	Security IC Platform Protection Profile, version 1.0, août 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*

[BSI-DSZ-CC-0837-V2-2014]	NXP Secure Smart Card Controller P60x080/052/040PVC(Y/Z/A)PVG with IC Dedicated Software. *Certifié par le BSI le 24 octobre 2014 sous la référence BSI-DSZ-CC-0837-V2-2014.*

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, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, Septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[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 1.2, janvier 2012.
[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.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.

	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 (RGS_B3), 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.