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-2016/53

LEO V3
Référence PPD002-vwx-Axy
Version du Firmware PA01.02

Paris, le 6 septembre 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

Référence du rapport de certification

ANSSI-CC-2016/53

Nom du produit

LEO V3

Référence/version du produit

Référence PPD002-vwx-Axy
Version du Firmware PA01.02

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 3 augmenté

ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_FLR.3, ALC_TAT.1

Développeur

Ingenico

25 quai Gallieni, 92158 Suresnes Cedex

Commanditaire

Ingenico

25 quai Gallieni, 92158 Suresnes Cedex

Centres d'évaluation

Serma Safety & Security

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Oppida

4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, 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 le lecteur « LEO V3, référence PPDD002-vwx-Axy, version du Firmware PA01.02 » développé par *INGENICO*.

Il s'agit d'un lecteur de carte connecté à un PC via un câble USB. Il peut communiquer avec des cartes conformes à la norme ISO 7816 ou EMV2004 et permet de saisir un code confidentiel de manière sûre. Le lecteur possède également une application multi-signature : un utilisateur légitime peut signer plusieurs documents en entrant une seule fois le PIN sur le lecteur (pour un nombre limité de documents).

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.

La cible de sécurité s'inspire du profil de protection [PP LSCIHM].

1.2.2. Identification du produit

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

Le guide d'utilisation [GUIDES] intitulé « *Leo User Manual* » décrit la procédure permettant d'obtenir l'identification logicielle du produit (la version du *Firmware*). Cette procédure se déroule en quatre étapes :

- débrancher le connecteur USB du produit ;
- insérer une carte à puce à l'envers ;
- rebrancher le connecteur USB ;
- lire la version logicielle affichée sur le lecteur.

Le message affiché doit être : « SOTFTWARE VER PA01.02 ».

La référence générale du produit, appelée « *Identification number* », est « PPD002-vwx-Axy », elle est inscrite sur l'étiquette placée au dos du produit. Les lettres « vwx » et « xy » de la référence peuvent varier en fonction de paramètres non sécuritaires tels que la couleur des touches ou du boîtier.

1.2.3. Services de sécurité

Les services de sécurité fournis par le produit sont (voir [ST, section *8.1 TOE Security Functions*] pour plus de détails) :

- la vérification de la structure des commandes envoyées au lecteur ;
- l'effacement du PIN après son utilisation ou en cas de transaction inaboutie ;
- l'affichage sécurisé des messages.

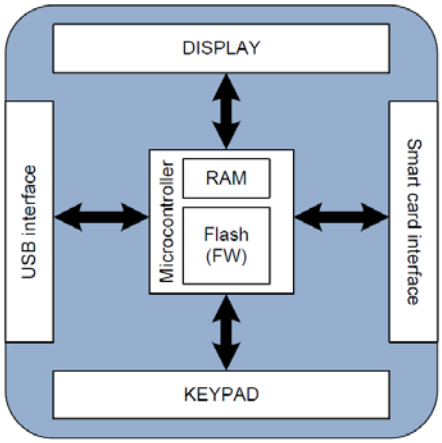
1.2.4. Architecture

Le produit est constitué d'un boîtier avec quatre interfaces :

- une liaison série vers une machine hôte (*USB interface*) ;
- un lecteur de carte à puce (*Smart Card Interface*) ;
- un écran (*Display*) ;
- un clavier (*Keyboard*).

Un microprocesseur gère ces différentes interfaces.

La figure ci-dessous représente l'architecture du produit :



1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

1. développement du boîtier et du logiciel par *INGENICO* en France ;
2. fabrication du boîtier et chargement du firmware par *KARCE COMPANY LTD* en Chine. Le point de livraison se situe une fois le firmware chargé ;
3. utilisation.

Le produit a été développé sur les sites suivants :

Centre de développement (*Firmware and Hardware design*) : *INGENICO*
River Seine, 25 quai Gallieni
92158 Suresnes, France.

***DataCenter* :** *OXYA*
1 rue de Londres
59120 Loos, France.

Centres de Fabrication : *KARCE COMPANY LIMITED*
(Dongguan Taida Electric Co,.Ltd)
3/Floor, Shenxiang lndustrial Park, Cuntou Administrative Division
Humen Town, Dongguan City
GuanDong Province, P.R. of China ;

(Guangxi Beiliu Taihongda Electronics Co., Ltd.)
Pijian, lndustrial Area, Gan Village, Beiliu City
GuanXi Province, P.R. of China.

1.2.6. Configuration évaluée

Le certificat porte sur le produit complet tel que décrit au paragraphe 1.2.2 Identification du produit. En particulier, l'i*dentification number* pour le produit évalué est PPD002-001-A10, où « 001-A10 » sont des paramètres non sécuritaires (la couleur des touches et du boîtier).

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 [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 équipements matériels avec boitiers sécurisés, les guides [JIWG SB] et [NOTE19] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG SB].

2.2. Travaux d'évaluation

L'évaluation s'appuie en partie sur les résultats d'évaluation du produit « LEO V2, référence : PPD001-003-AXY, version PK08.12 » certifié le 19 juillet 2012 sous la référence ANSSI-CC-2012/37 (voir [CER]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 18/07/2016, 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

Le produit ne comporte pas de mécanisme cryptographique.

2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas.

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 « LEO V3, référence PPDD002-vwx-Axy, version du Firmware PA01.02 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_FLR.3 et ALC_TAT.1.

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], notamment :

- s'assurer de l'intégrité physique du boîtier avant son utilisation ;
- utiliser le produit via un ordinateur à usage exclusif de l'utilisateur ou d'un ensemble restreint d'utilisateurs non hostiles.

Reconnaissance du certificat

3.2.1. 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 jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.2.2. 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 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 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, 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 3+	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	**3**	Authorisation controls
	ALC_CMS	1	2	3	4	5	5	5	**3**	Implementation representation CM coverage
	ALC_DEL		1	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			1	1	1	2	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	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	**2**	Vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Security Target – CC EAL 3+ - Leo V3, référence XRD-2014-2626, Confidential, version 1.5, 17/05/2016, Ingenico. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target lite – CC EAL 3+ - LeoV3, référence XRD-2015-3119, Public, version 1.0, 12/07/2016, Ingenico.
[RTE]	Rapport technique d'évaluation : Evaluation Technical Report - Leo V3 Project, référence LEO-V3_ETR_V1.2/1.2, 18/07/2016, Serma Technologies et Oppida.
[CONF]	Liste de configuration du produit : XRD-2014-2762-Configuration list (ID 2762), version 1.15, 12/07/2016, Ingenico.
[GUIDES]	- Leo User Manual, référence XRD-2014-2653, version DOC00909-rev B, Ingenico ; - Leo V3 Production test and Firmware Version access, référence XRD-2014-2691, version 1.3, 19/03/2015, Ingenico.
[CER]	Rapport de certification ANSSI-CC-2012/37, LEO V2 référence PPD001-003-AXY, version PK08.12. *Certifié par l'ANSSI le 19 juillet 2012*.
[PP LSCIHM]	Profil de protection – Lecteur sécurisé de carte avec interface homme machine, version v1.6 du 20 décembre 2011. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2012/01 le 5 avril 2012.*

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, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-004.
[JIWG SB]*	Mandatory Technical Document - Application of attack potential to hardware devices with security boxes, mai 2012, version 1.0 (for trial use).
[NOTE19]	Note d'application - Mise à jour de la table de cotation du document JIL "application of attack potential to hardware devices with security boxes", référence ANSSI-CC-NOTE-19, version 1.0.
[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.

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