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-2019/56

IDmove v4 on Infineon in EAC configuration with AA in option

Paris, le 20 décembre 2019

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

Guillaume POUPARD
[ORIGINAL SIGNÉ]

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-2019/56

Nom du produit

IDmove v4 on Infineon in EAC configuration with AA in option

Référence/version du produit

OS Commercial Version : 0x 09 08 04
OS Unique Identifier : 0x 3C 1D

Conformité à un profil de protection

Machine Readable Travel Document with ICAO application Extended Access Control, version 1.10

certifié BSI-CC-PP-0056-2009 le 25 mars 2009

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

IDEMIA
2 place Samuel de Champlain,
92400 Courbevoie, France

Infineon Technologies AG
AIM CC SM PS – Am Campeon 1-12,
85579 Neubiberg, Allemagne

Commanditaire

IDEMIA
2 place Samuel de Champlain,
92400 Courbevoie, France

Centre d'évaluation

Serma Safety & Security
14 rue Galilée, CS 10071, 33608 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat 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 à puce « IDmove v4 on Infineon in EAC configuration with AA in option », pouvant être utilisée en mode contact ou sans contact. Le produit est développé par *IDEMIA* et *INFINEON TECHNOLOGIES AG*.

Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit est destiné à permettre la vérification de l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels, dans une *eCover* ou dans une *eDatapage*.

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 EAC].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité des données du porteur stockées dans la carte : nations ou organisations émettrices, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait, autres données optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document de voyage ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- la protection, en intégrité et en confidentialité, des données lues à l'aide du mécanisme *Secure Messaging* ;
- l'authentification du microcontrôleur par le mécanisme optionnel *Active Authentication* (AA) ;
- le mécanisme *Extended Access Control* (EAC) d'authentification forte entre le microcontrôleur et le système d'inspection préalable à tout accès aux données biométriques, permettant l'établissement d'un canal sécurisé fort (*secure messaging*).

1.2.3. Architecture

Le produit est constitué, comme décrit au chapitre 2.3.1 de la cible :

- Du microcontrôleur IFX_CCI_000005h H13, développé par *INFINEON TECHNOLOGIES AG* et certifié sous la référence [CER_IC] ;
- d'un module « BIOS » qui fournit les fonctionnalités pour la gestion des accès vers la couche applicative. Il fournit également les fonctions de gestion des exceptions et de communication ;

- d'une librairie cryptographique qui fournit à la couche applicative, les fonctions de sécurité cryptographique ;
- d'un module *Secure Messaging* qui fournit les fonctionnalités pour protéger en intégrité, authenticité et confidentialité les données permettant ainsi de disposer d'un moyen de communication sécurisée durant les phases de fabrication, de personnalisation et d'utilisation opérationnelle ;
- de *Resident Application* (RA), qui fournit un jeu de commandes complet qui permet la gestion de la carte dans sa phase opérationnelle ;
- de l'*Application Creation Engine* (ACRE), qui fournit un jeu de commandes complet utilisé pour pré-personnaliser la carte et ses applications ;
- de l'application *Machine Readable Travel Document* (MRTD), un jeu de commandes complet qui permet la gestion des données MRTD durant la phase opérationnelle ;
- et d'un *boot* qui est en charge de gérer le démarrage des applications MRTD, RA et ACRE.

Tous ces éléments font partie de la cible d'évaluation (TOE).

1.2.4. 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, décrits dans le guide [AGD_PRE] :

- OS *commercial version* : 0x090804 ;
- OS *Unique Identifier* : 0x3C1D ;
- *Chip type* :
  - ID1 : 0x0013,
  - ID2 : 0xXXXX pouvant prendre des valeurs différentes selon la configuration du microcontrôleur,
  - ID3 : 0x0000 ;
- *Design step* : 0x070D (H13) ;
- IFX_CCI : 0x000005 ;
- *Firmware version identifier* : 0x80100173.

Ces valeurs peuvent être vérifiées en utilisant la commande GET DATA avec le tag DF50 comme indiqué dans [AGD_PRE].
Durant les phases de pré-personnalisation et de personnalisation, les commandes « WRITE LOCK » et « READ LOCK » (voir [AGD_PRE]) sont disponibles pour activer ou désactiver une configuration (BAC, EAC, PACE, etc.), ou pour consulter la(les) configuration(s) activée(s) de la TOE. A noter que ces commandes ne sont plus disponibles en phase d'utilisation.

1.2.5. Cycle de vie

Les trois cycles de vie du produit sont décrits au chapitre 1.11 de la cible de sécurité [ST].
Ils sont conformes au profil de protection [PP0084].

Le produit a été développé sur les sites suivants (voir [SITES]) :

***IDEMIA* – Courbevoie** [CRB] 2, place Samuel de Champlain 92400 Courbevoie, France	***IDEMIA* – Pessac** [PSC] Bâtiment Elnath, 11 avenue de Canteranne, 33600 Pessac, France
***IDEMIA* – Vitré** [VTR] Avenue d'Helmstedt BP 90308 35503 Vitré Cedex France	***IDEMIA* – Shenzhen** [SZN] 4F, Great wall technology building No 2, KeFa Rd Science and Technology park, Nanshan district Shenzhen, 518057 P. R. of CHINA
***IDEMIA* – Haarlem** [HAA] Oudeweg 32, 2031 CC Haarlem, The Netherlands	***IDEMIA* – Noida** [NOI-P] Syscom India Private Limited PLOT-1A, sector 73, Noida Uttar Pradesh 201307, India
***IDEMIA* – Ostrava** [OST] Jelinkova 1174/3A, 721 00 Ostrava-Svinov, Czech Republic	

Les sites de développement du composant sont couverts par le certificat [CER_IC].

1.2.6. Configuration évaluée

Le certificat porte sur la configuration incluant :

- le mécanisme EAC (*Extended Access Control*) - incluant entre autre le mécanisme CA (*Chip Authentication*) - enrichi avec les fonctionnalités suivantes par rapport au [PP_EAC] : (1) génération de tout type de *secure messaging* à l'issue du CA (DES, AES-128, AES-192 et AES-256), et (2) exigence d'un niveau minimum de *secure messaging* préalablement configuré pour accéder aux données biométriques sensibles (iris, empreinte biométrique), afin de garantir un niveau de confidentialité adéquate ;
- le mécanisme AA (*Active Authentication*) qui est optionnel et éventuellement désactivé ;
- les phases de pré-personnalisation et de personnalisation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [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 du microcontrôleur « IFX_CCI_000005h H13 » au niveau EAL6 augmenté des composants ALC_FLR.1, conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le 18 juin 2019 sous la référence « BSI-DSZ-CC-1110-V2-2019 », voir [CER_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 28 novembre 2019, 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. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ETR]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI ([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.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 [CER_IC]).

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 « IDmove v4 on Infineon in EAC configuration with AA in option », 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 1.2 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 lorsque les dépendances CC sont satisfaites. 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 EAL2 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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 : - IDmove v4 on Infineon in EAC configuration with AA in option – Security Target, FQR 110 8953, 18 juillet 2019, *IDEMIA*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - IDmove v4 on Infineon in EAC configuration with AA in option – Public Security Target, FQR 110 9126, 18 juillet 2019, *IDEMIA*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - QUANTUM Project, QUANTUM_ETR_v1.2, 28 novembre 2019, *SERMA SAFETY & SECURITY*.
[CONF]	Liste de configuration du produit : - QUANTUM - Configuration List, FQR 110 9030 Ed 4, Version 4, 26 août 2019, *IDEMIA*.
[GUIDES] [AGD_PRE]	Guide d'installation du produit : - IDmove v4 on Infineon MRTD/IDL Preparative Guidance Document, FQR 110 8997 Ed 2, Version 2, 18 juillet 2019, *IDEMIA*.
[AGD_OPE]	Guide d'utilisation du produit : - IDmove v4 on Infineon MRTD/IDL User Guidance Document, FQR: 110 8998 Ed 1, Version 1, 31 mars 2019, *IDEMIA* ; - Quantum QR Recommendations for crypto assessment compatibility, référence FRQ 110 9040, version 1, 1 février 2019, *IDEMIA*.

[SITES]	Rapports d'analyse documentaire : - [GEN17] o Oberthur Technologies Development Environment (Generic Documentary activities), référence 17-0232_ALC_GEN_v1.0, 25/08/2017, *SERMA SAFETY & SECURITY* ; - [GEN19] o IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence IDEMIA R&D site 2018_GEN_v1.1, 19/06/2019, *SERMA SAFETY & SECURITY ;* o IDEMIA Haarlem Development Environment - ALC Class Evaluation Report (Generic Documentary activities), référence SITE_IDEMIA_HAARLEM_ALC_GEN_v1.0, 24/08/2019, *SERMA SAFETY & SECURITY*. Rapports d'audit de site pour la réutilisation : - [CRB] o Site Technical Audit Report CRB, référence IDEMIA R&D site 2018_CRB_STAR_v1.3, 26/06/2019, *SERMA SAFETY & SECURITY* ; - [HAA] o Site Technical Audit Report IDEMIA Haarlem, référence SITE_IDEMIA_HAARLEM_STAR_v1.1, 03/01/2019, *SERMA SAFETY & SECURITY* ; - [PSC] o Site Technical Audit Report IDEMIA Pessac, référence IDEMIA R&D site2018_PSC_STAR_v1.1, 22/05/2019, *SERMA SAFETY & SECURITY* ; - [VTR] o Vitré Site Visit lite report, référence 17-0232_SVR-VTR_M_V1.0, 17/01/18, *SERMA SAFETY & SECURITY* ; - [SZN] o Shenzhen Site Visit lite report, référence 17-0232_SZN_SVR-M_v1.0, 08/02/18, *SERMA SAFETY & SECURITY* ; - [OST] o Site Technical Audit Report OST, référence IDEMIA-2019_OST_STAR_v1.0, 24/06/2019, *SERMA SAFETY & SECURITY* ; - [NOI] o Site technical Audit Report 2019 NOI-P, référence IDEMIA-2019_NOIP_STAR_v1.1, 17/07/19, *SERMA SAFETY & SECURITY*.

[CER_IC]	Infineon Technologies Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h H13 including the products from the second production line and optional software packages: Flash Loader, Asymetric Crypto Library, Symmetric Cryptographic Library, Hardware Support Layer, Hash Crypto Library, Mifare Compatible Software, and CIPURSE Crypto Library from Infineon Technologies AG. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik)* le 18 juin 2019 sous la référence BSI-DSZ-CC-1110-V2-2019.
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.*
[PP EAC]	Protection Profile, Machine Readable Travel Document with “ICAO Application”, Extended Access Control, version 1.10, 25 mars 2009. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0056.*

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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[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 1.5.1, mai 2018.
[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.