



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-2019/38

Cryptosmart-SIM card (Version 5.1)

**Annule et remplace le rapport de certification ANSSI-CC-
2019/38 signé le 17 décembre 2019**

Paris, le 28 janvier 2020

*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 présumées 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-2019/38	
Nom du produit	Cryptosmart-SIM card	
Référence/version du produit	Version 5.1	
Conformité à un profil de protection	Aucun	
Critères d'évaluation et version	Critères Communs version 3.1 révision 5	
Niveau d'évaluation	EAL4 augmenté ALC_DVS.2, AVA_VAN.4	
Développeurs	Ercom 6, rue Dewoitine 78140 Vélizy France	Idemia 2 place Samuel de Champlain, 92400 Courbevoie, France
		Infineon Technologies AG AIM CC SM PS – Am Campeon 1-12, 85579 Neubiberg, Allemagne
Commanditaire	Ercom 6, rue Dewoitine 78140 Vélizy France	
Centre d'évaluation	Serma Safety & Security 14 rue Galilée, CS 10071, 33608 Pessac Cedex, France	
Accords de reconnaissance applicables		
	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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Services de sécurité</i>	6
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Identification du produit</i>	7
1.2.5. <i>Cycle de vie</i>	8
1.2.6. <i>Configuration évaluée</i>	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. <i>Reconnaissance européenne (SOG-IS)</i>	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	11
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	13
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	14
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	15

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Cryptosmart-SIM card, Version 5.1 » développé par *ERCOM*.

Ce produit conçu, développé et pré-personnalisé par les sociétés *INFINEON TECHNOLOGIES AG*, *IDEMIA* et *ERCOM*, est destiné à être utilisé pour établir un canal sécurisé (authentification et négociation de clés partagées) avec un autre produit distant contenant l'applet *CRYPTOSMART*, comme par exemple le produit *Cryptosmart Mobile Suite*. Ce produit propose également plusieurs fonctions de cryptographie et une zone de stockage sécurisée.

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.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'authentification d'une application *CRYPTOSMART* distante et la négociation d'une clé partagée avec cette dernière ;
- la mise à disposition de fonctions cryptographiques telles que :
 - o l'authentification de l'utilisateur en utilisant un code sécurisé ;
 - o le stockage sécurisé de clés AES 256 bits ou RSA 2048 bits ;
 - o l'export sécurisé de clés AES de 256 bits ou RSA de 2048 bits ;
 - o un sous-ensemble des fonctionnalités de PKCS#11 ;
 - o la génération de clés RSA 2048 bits ;
 - o la génération de clés AES 256 bits ;
 - o la gestion des propriétés d'extraction des clés RSA et AES ;
 - o la gestion des propriétés d'utilisation des clés AES ;
 - o l'obtention de clés locales de chiffrement en dérivant les clés internes ;
 - o la génération et exportation de clés de chiffrement de clés ;
 - o la génération de nombres aléatoires ;
- la mise à disposition d'une zone de stockage sécurisée.

1.2.3. Architecture

L'architecture du produit est la suivante :

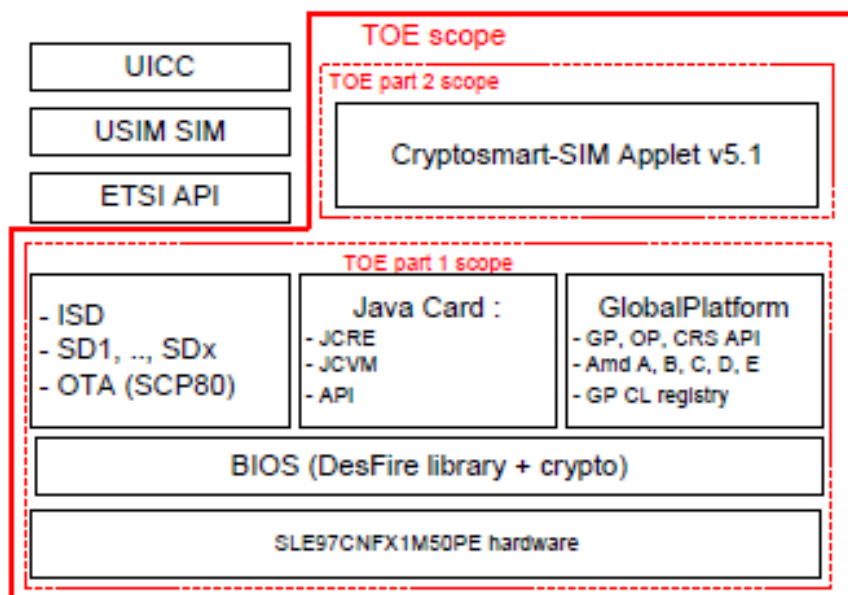


Figure 1 : Architecture du produit

Il n'y a pas d'application déjà chargée dans le produit autre que l'application Cryptosmart-SIM.

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 du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 1.1 « Security Target and TOE Identification ».

Eléments de configuration		Origine
Nom de la TOE	Cryptosmart-SIM	<i>ERCOM</i>
TOE identifier	Cryptosmart-SIM applet 5.1 on IDEMIA DRAGONFLY V4.0	
TOE version	5.1	
Applet Version	05 01 (5.1)	
Source version	00 03 92 (914)	
Build version	CA C7 FA 53	
SAAAAR code	41 26 91	<i>IDEMIA</i>
FAB_ID	48 30	
IC_ID	52 03	
OS_ID	82 31	
OS_Release_Date	53 17	
OS_Release_Level	32 78	

Card Manager version	47 4F 50 20 52 65 66 20 56 32 31 2E 30 36 2E 30 31 (in ASCII “GOP Ref V21.06.01”)
CM Install Parameter	xxxx xxx0 yyyy yyy1 (binary representation)

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans [GUIDES].

1.2.5. Cycle de vie

L'évaluation a couvert la conception, le développement, le chargement de l'application « Cryptosmart », la pré-personnalisation de la carte et la désactivation du *Java Card Manager* pour empêcher l'effacement de l'application « Cryptosmart » et interdire le chargement d'autres applications. Ces étapes se déroulent dans les locaux d'*ERCOM* ou dans les locaux d'*IDEMIA* couverts par le certificat [CER_PTF]. Elles correspondent à la phase 6 du cycle de vie. Une fois ces étapes effectuées, le produit est livré à l'utilisateur final.

Le produit a été développé sur le site suivant (voir [SITE]) :

Site de développement : Ercom Velizy

6 rue Dewoitine
78140 Vélizy-Villacoublay
France

Les sites de développement de la plateforme sont couverts par le certificat [CER_PTF].

Des applications peuvent être chargées en phase 6. Ces chargements doivent être protégés conformément au guide de la plateforme (voir [CER_PTF]).

Le guide [GUIDE-OPE] de [CER_PTF] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.

Par ailleurs dans [CER_PTF], les guides [GUIDE_Basic] et [GUIDE_Sec] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; le guide [GUIDE-OPE] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification.

Pour l'évaluation, l'évaluateur a considéré que les produits sont délivrés aux clients sans aucune clé installée. Charge à l'administrateur du client de personnaliser les cartes pour chacun des utilisateurs finaux, en utilisant le logiciel nommé « Card administration station » délivré par *ERCOM*. Ce logiciel permet notamment d'inscrire dans les cartes, les clés cryptographiques et les certificats nécessaires au bon fonctionnement des échanges sécurisés.

1.2.6. Configuration évaluée

Le certificat porte sur les configurations décrites au paragraphe 1.2.4.

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 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 de la plateforme « DragonFly v4.0 sur composant SLE97CNFX1M50PE » au niveau EAL4 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP (U)SIM]. Cette plateforme a été certifiée le 6 octobre 2016 sous la référence [CER_PTF]. Le niveau de résistance de cette plateforme au niveau AVA_VAN.4 a été confirmé le 5 novembre 2018 dans le cadre du processus de surveillance, voir [SUR_PTF].

L'évaluation s'appuie sur les résultats d'évaluation du produit « Cryptosmart Card applet V5.1 sur la plateforme OBERTHUR ID-ONE COSMO V7.0.1-R2, version 816 » certifié en 26 octobre 2016 sous la référence [CER].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 26 juin 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 conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI. 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.4 visé.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [ANA-CRY]. 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.4 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.4 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 « Cryptosmart-SIM card, Version 5.1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 augmenté des composants ALC_DVS.2 et AVA_VAN.4.

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'accord¹, 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].

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires¹, 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 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 4+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of TSF
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	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	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	1	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	4	4	Methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : <ul style="list-style-type: none"> - Cryptosmart-Sim Card Security Target, version 5.1, 15/09/2019, ERCOM.
[RTE]	Rapport technique d'évaluation : <ul style="list-style-type: none"> - Evaluation Technical Report Cryptosmart-SIM Project, référence : Cryptosmart-SIM_ETR_v1.0, 26/06/2019, SERMA.
[ANA-CRY]	Voir [RTE].
[CONF]	Liste de configuration du produit : <ul style="list-style-type: none"> - Evaluation configuration list for Cryptosmart Card, version : cryptosmartcard_documentation_config_list, 15/05/2019.
[GUIDES]	Guide d'administration du produit : <ul style="list-style-type: none"> - Cryptosmart Card Personalization Guide, version e9a4cd9, 12/03/2018, ERCOM. Guide de développement : <ul style="list-style-type: none"> - Cryptosmart-SIM Developer's guide, version 5.1, 15/05/2019, ERCOM. Guide de plateforme ouverte : <ul style="list-style-type: none"> - Voir [CER_PTF].
[CER_PTF]	DragonFly v4.0 sur composant SLE97CNFX1M50PE. <i>Certifié par l'ANSSI le 6 octobre 2016 sous la référence ANSSI-CC-2016/60.</i>
[SUR_PTF]	DragonFly v4.0 sur composant SLE97CNFX1M50PE. <i>Surveillé par l'ANSSI le 5 novembre 2018 sous la référence ANSSI-CC-2016/60-S01.</i>
[CER]	Cryptosmart Card applet V5.1 sur la plateforme OBERTHUR ID-ONE COSMO V7.0.1-R2, version 816 <i>Certifié par l'ANSSI le 26 octobre 2016 sous la référence ANSSI-CC-2016/69.</i>
[PP (U)SIM]	(U)SIM Java Card Platform Protection Profile - Basic Configuration, version 2.0.2. <i>Certifié par l'ANSSI le 10 juillet 2010 sous la référence ANSSI-CC-PP-2010/04.</i>

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 : <ul style="list-style-type: none"> - 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.