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-2013/29

Plateforme Java Card en configuration ouverte de la carte à puce MultiApp ID V2.1 masquée sur composant P5CC145V0A

Version : MPH119 avec filtre v2.4

Paris, le 15 mai 2013

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

[Original signé]

Patrick Pailloux

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-2013/29

Nom du produit

Plateforme Java Card en configuration ouverte de la carte à puce MultiApp ID V2.1 masquée sur composant P5CC145V0A

Référence/version du produit

Référence MultiApp ID V2.1, Version MPH119 avec filtre v2.4

Conformité à un profil de protection

[ANSSI-CC-PP-2010-03], version v2.6
PP-JCS Open Configuration

Critères d'évaluation et version

CC version 3.1 révision 3

Niveau d'évaluation

EAL5 Augmenté
ALC_DVS.2 et AVA_VAN.5

Développeurs

GEMALTO	NXP
La Vigie Avenue du Jujubier, ZI Athélia IV BP 90, 13702 La Ciotat, France	101 Stresemanallee, D-22502 Hambourg Allemagne

Commanditaire

GEMALTO
La Vigie Avenue du Jujubier, ZI Athélia IV BP 90, 13702 La Ciotat, France

Centre d'évaluation

SERMA Technologies
30 Avenue Gustave Eiffel, 33608 Pessac, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

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. Identification du produit 6
1.2.2. Services de sécurité 7
1.2.3. Architecture 7
1.2.4. Cycle de vie 8
1.2.5. Configuration évaluée 9

2. L'EVALUATION 10

2.1. REFERENTIELS D'EVALUATION 10
2.2. TRAVAUX D'EVALUATION 10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 10
2.4. ANALYSE DU GENERATEUR D'ALEAS 11

3. LA CERTIFICATION 12

3.1. CONCLUSION 12
3.2. RESTRICTIONS D'USAGE 12
3.3. RECONNAISSANCE DU CERTIFICAT 13
3.3.1. Reconnaissance européenne (SOG-IS) 13
3.3.2. Reconnaissance internationale critères communs (CCRA) 13

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 14

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 15

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 16

1. Le produit

1.1. Présentation du produit

Le produit évalué est la « plateforme Java Card en configuration ouverte de la carte à puce MultiApp ID V2.1 masquée sur composant P5CC145V0A, référence MultiApp ID V2.1, en version MPH119 avec filtre v2.4 », développé par GEMALTO et NXP.

La plateforme ouverte Java Card est destinée à fournir des services de sécurité aux applets qui seront installées et chargées sur la carte.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité est conforme au profil de protection [ANSSI-CC-PP-2010-03]. La conformité est démontrable.

1.2.1. 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 (cf. [GUIDES]).

Sur les produits utilisés lors de l'évaluation, sans application, la commande GET DATA pour le tag 01 03 a donné la réponse suivante :

- B0 85 37 39 10 24 47 90 51 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Cette réponse se décomposera comme indiqué dans le tableau ci-dessous, une fois les applications IAS Classic ou IAS XL personnalisées.

Nom de la famille	Java Card	B0h
Nom du système d'exploitation	MultiApp ID	85h
Numéro du masque	MPH119	37h
Nom du produit	Generic MPH119 product	39h
Configuration du produit	IAS Classic personnalisée / non personnalisée IAS XL personnalisées / non personnalisée	14h / 15h 16h / 17h
Version du filtre	version 2.4	24h
Fabricant du microcontrôleur	NXP	47 90h
Version du microcontrôleur	P5CC145	51 45h

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection de la confidentialité et de l'intégrité des clés cryptographiques et des données applicatives pendant l'exécution des opérations cryptographiques ;
- la protection de la confidentialité et de l'intégrité des données d'authentification et des données applicatives pendant l'exécution des opérations d'authentification ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications ;
- l'intégrité de l'exécution du code applicatif.

1.2.3. Architecture

La plateforme Java Card de la carte MultiApp v2.1, présentée figure 1, est constituée des éléments suivants :

- des fonctionnalités matérielles du composant (CPU, RAM, ROM, EEPROM, I/O, coprocesseurs cryptographiques) ;
- d'une partie native composée elle-même :
  - d'un gestionnaire de mémoire *Memory Manager* ;
  - d'un gestionnaire de communication *Communication* ;
  - de librairies cryptographiques *Crypto libs* ;
- d'un système Java Card (JCS : Java Card System) composée :
  - d'un environnement *runtime* (JCRE) ;
  - d'une machine virtuelle Java (VM) ;
  - d'une interface de programmation (Java API) ;
  - d'un gestionnaire d'applications (Card Manager).

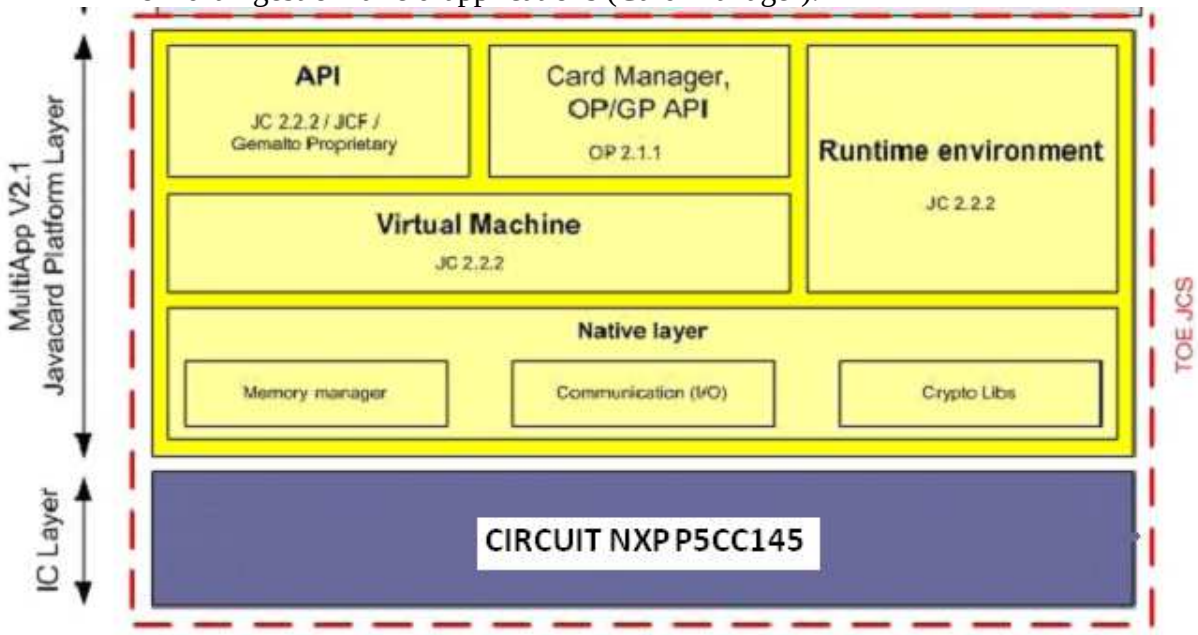

Figure 1 – Architecture et périmètre de la TOE

1.2.4. Cycle de vie

Le composant est fabriqué chez NXP. Il est ensuite envoyé sur le site de Gemalto où il est initialisé et pré-personnalisé. Le produit est ensuite verrouillé par une clé diversifiée et envoyé au personnalisateur.

Le produit a été développé sur les sites suivants :

Développement	**Gemalto** Meudon **Gemalto** La Ciotat **Gemalto** Gémenos
Fabrication du micromodule, initialisation et encartage	**Gemalto** Gémenos **Gemalto Pte Ltd** Singapore
Pré-personalisation	**Gemalto** Gémenos **Gemalto Pte Ltd** Singapore **Gemalto** Vantaa

GEMALTO

6 Rue de la verrerie
92190 Meudon
France

GEMALTO

La Vigie Avenue du Jujubier, ZI Athélia IV BP 90
13702 La Ciotat
France

GEMALTO

525 Avenue du Pic de Bertagne
13420 Gémenos
France

Gemalto Pte Ltd

Turvalaaksonkaari 2
12 Ayer Rajah Crescent, Singapore 139941
Singapore

Gemalto

Turvalaaksonkaari 2
FI-01741 Vantaa
Finlande

Les sites de développement et de fabrication du microcontrôleur sont identifiés dans le rapport de certification [BSI-DSZ-CC-0645-2010].

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit le pré-personnalisateur, le personnalisateur et le gestionnaire de la carte chargé de l'administration de la carte, et comme utilisateurs du produit les développeurs des applications à charger dans la plateforme.

1.2.5. Configuration évaluée

L'évaluateur a testé la plateforme Java Card masquée sur le composant P5CC145V0A.

Les applets présentes sur la plateforme ont été analysées dans le cadre de cette évaluation au titre de l'environnement de la cible de sécurité. Elles ne dégradent pas la sécurité de la plateforme.

Le certificat porte sur la plate-forme ouverte Java Card seule, telle que présentée au paragraphe 1.2.1, et configurée conformément au guide de personnalisation (cf. [GUIDES]).

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 cartes à puce, les guides [CC 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 « NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software » au niveau EAL5 augmenté des composants ASE_TSS.2, ALC_DVS.2 et AVA_VAN.5,, conforme au profil de protection [BSI-CC-PP-0035-2007]. Ce microcontrôleur a été certifié le 23 juillet 2010 sous la référence [BSI-DSZ-CC-0645-2010].

Le niveau de résistance du microcontrôleur a été confirmé le 30 septembre 2011 dans le cadre du processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 8 janvier 2013, 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 selon les référentiels techniques de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit était dans le périmètre de l'évaluation et a été analysé par le centre d'évaluation. L'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN 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 « Plateforme Java Card en configuration ouverte de la carte à puce MultiApp ID V2.1 masquée sur composant P5CC145V0A, référence MultiApp ID V2.1, version MPH119 avec filtre v2.4 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5 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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

La cible de sécurité prévoit un autre cycle vie que celui qui a été évalué. N'ayant pas été évalué il ne fait pas partie du périmètre de cette certification.

Plus particulièrement, toutes les applications qui seront chargées sur la carte (qu'elles soient certifiées ou non) devront satisfaire l'ensemble des contraintes et exigences relatives aux propriétés de cloisonnement d'applications, imposées par la plateforme, avant leur installation effective.

3.3. Reconnaissance du certificat

Ce certificat fait l'objet d'une reconnaissance internationale.

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].

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 EAL4 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, Singapour, 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 : - MultiAppID V2.1Sofware - Security Target - JCS part référence R0A21037_003_CCD_ASE_JCS, version v0.1 du 14 janvier 2011. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - MultiAppID V2.1- Security Target – JavaCard System- Public version référence R0A21037_003_CCD_ASE-JCS, version v1.1 du 9 février 2012.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - CALLISTO Project référence CALLISTO_ETR_JCS_v2.0, version v2.0 du 8 janvier 2013.
[CONF]	Liste de configuration : - MultiApp v2.1 platform - Configuration list du 12 juin 2012.
[GUIDES]	Guide d'installation du produit : - MultiApp ID V2.1 Software Javacard Platform Preparative Procedures référence R0A21037_018_CC D_PRE-JCS, version v0.1 du 6 mai 2012 ; Guide d'utilisation du produit : - MultiApp ID V2.1 Software Javacard Platform Operational User Guide référence R0A21037_017_CC D_OPE-JCS, version v1.0 du 9 mars 2012 ; - MultiApp ID Operating System Reference Manual référence DOC118572B, du 22 octobre 2009.
[BSI-DSZ-CC-0645-2010]	NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software certifié le 23 juillet 2010 sous la référence BSI-DSZ-CC-0645-2010.
[ANSSI-CC-PP-2010-03]	Protection Profile - PP-JCS Open Configuration, version v2.6 du 25 juin 2010. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010-03.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 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, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[COMP]	Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, version 1.2, Jaunuary 2012.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[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 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité (RGS_B_2), voir www.ssi.gouv.fr.