Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2009/42

Carte à puce SafeAccess TV Card Application SAFEACCESS v2.0 Rev 67 embarquée sur le composant ST19NA18F

Paris, le 26 octobre. 2009

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

Patrick Pailloux
[ORIGINAL SIGNE]

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 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-2009/42

Nom du produit

Carte à puce SafeAccess TV Card

Application SAFEACCESS v2.0 Rev 67 embarquée sur le composant ST19NA18F

Référence/version du produit

Version 2.0 Rev 67

Conformité à un profil de protection

[PP/9911]

Protection Profile Smart Card Integrated Circuit With Embedded Software , version 2.0, June 1999certifié par l'ANSSI sous la reference PP/9911

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur(s)

LogiWays

Paris R&D site, 24-26 rue Louis Armand, 75015 Paris, France

ST Microelectronics

190 Avenue Célestin COQ, 13106 Rousset Cedex, France

Commanditaire

LogiWays

Paris R&D site, 24-26 rue Louis ARMAND. 75015 Paris

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com

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, publié au Journal officiel de la République française. 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

Table des figures

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce « *SafeAccess TV Card* », munie de l'application SAFEACCESS dans sa version 2.0 Révision 67, développée par LogiWays et embarquée sur le microcontrôleur ST19NA18F, développé par STMicroelectronics. Ce composant ST19NA18, en révision C, a été certifié par l'ANSSI sous la référence DCSSI-2007/07 et maintenu en révision F sous la référence DCSSI-2007/07-M01, cf. [CERT].

La carte à puce « *SafeAccess TV Card* » est chargée de gérer les droits d'accès d'un système de télévision à péage.

1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation. Elle s'inspire ici du profil de protection [PP/9911] adapté au CC v3.1 par le choix de composants complémentaires ADV_IMP.1 et ATE_DPT.2.

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration contenu dans le manuel [CONF].
La version certifiée du produit est identifiée par les éléments suivants :

- par des informations gravées sur le composant :
  - la référence du microcontrôleur : K7L0A ;
  - la référence du logiciel dédié du microcontrôleur : ZSD ;
  - la référence générique de l'application SAFEACCESS : NVB ;

- par des informations fournies à la mise sous tension (*Answer to Reset* ou ATR) :

Type	Taille	Valeur	Description
<Version>	1	0x91	ROMCODE Version 2
<Copyright>	11	0x28 0x43 0x29 0x4C 0x6F 0x67 0x69 0x77 0x61 0x79 0x73	Chaîne de caractères ASCII '(C)Logiways'
<Lock>	2	0x33 0x33	

La valeur 0x91 qui identifie la version 2.0 de l'application SAFEACCESS est le septième octet de l'ATR.

Pour connaître le numéro de révision d'une carte à puce (révision 67 pour la version évaluée), il est nécessaire de la fournir à LogiWays.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'utilisation d'un canal sécurisé en confidentialité et en intégrité pour les échanges de données avec le désembrouilleur (*descrambler*) du système de télévision à péage ;
- la protection en confidentialité et en intégrité des données de désembrouillage (*control* words) destinées au décodeur pour les différents modes d'utilisations (*live, recorded, pay-per-view*) ;
- la protection en confidentialité et en intégrité des données sensibles stockées (ex : clés) ;
- la mise à jour sécurisée des différents codes de protection.

1.2.3. Architecture

Le produit composite évalué est constitué par :

- le microcontrôleur et ses logiciels spécifiques dont le détail est disponible dans le rapport propre au microcontrôleur [RTE].
  Le microcontrôleur fournissant des services de calculs cryptographiques élémentaires (AES, TDES, RSA, SHA, CRC) via des APIs (*Application Programming Interfaces*).
- le « logiciel embarqué », dont l'un des modules est l'application de télévision à péage (ci-après nommée « application ») tandis que l'autre est constitué de services (ci-après nommée « services »). Une illustration des applications et services est faite dans la figure ci-dessous ;

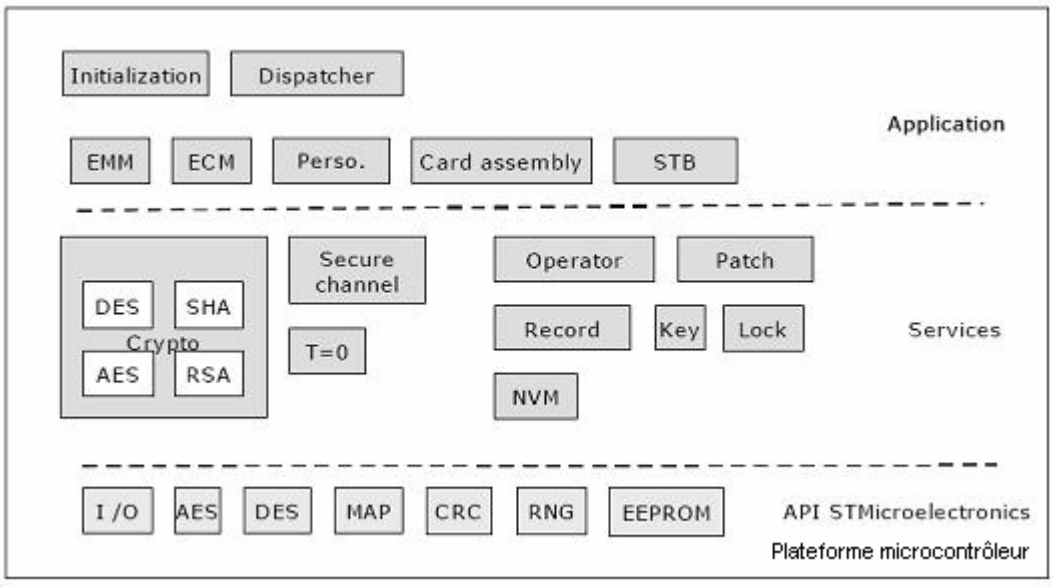
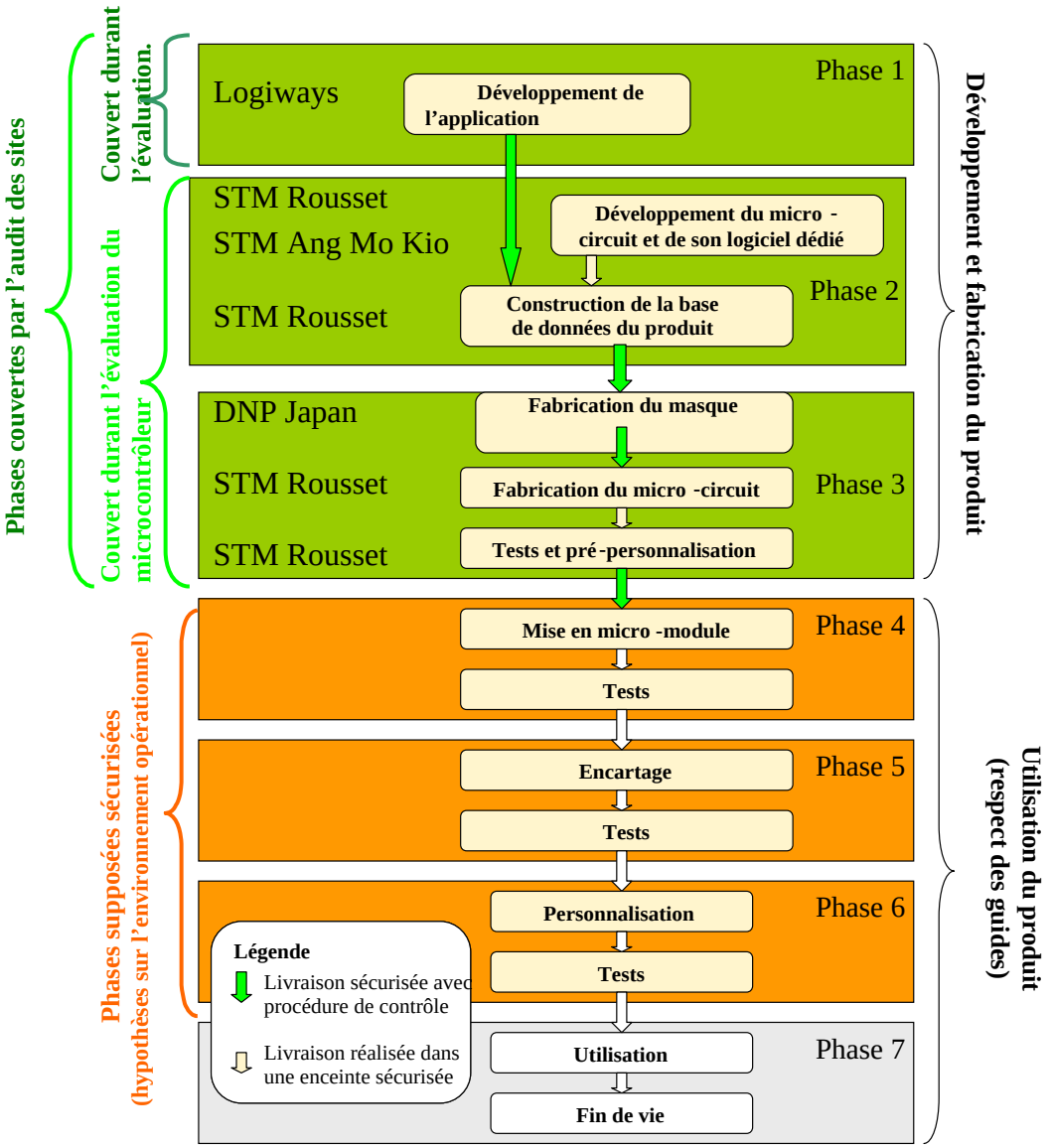


Figure 1 : Structure générale de la TOE

1.2.4. Cycle de vie

Le cycle de vie du produit comporte 7 phases comme précisé dans [ST], chapitre 1.4.2.

L'application de télévision à péage est masquée par le fabricant du microcontrôleur. Celui-ci est fourni aux industriels en charge de la fabrication et de la personnalisation des cartes dans la configuration « utilisateurs ».
Les évaluations de la phase 2 (développement du microcontrôleur) et de la phase 3 (test et fabrication du microcontrôleur) ont été réalisées durant l'évaluation du microcontrôleur.
La phase 1 (développement de logiciel embarqué sur le microcontrôleur) et la phase 7 (utilisation finale du produit) sont couvertes par la présente évaluation de la carte SafeAccess TV Card. Les autres phases (4 à 6) ne sont pas couvertes par l'évaluation, mais sont assujetties à satisfaire des hypothèses sur l'environnement opérationnel, de manière en outre à garantir le verdict de l'évaluation en phase 7.



Le produit a été développé sur les sites suivants :

Site de développement et de tests de l'ensemble des composants logiciels embarqués dans la TOE

LogiWays

Paris R&D site
24-26 rue Louis ARMAND
75015 Paris
France

Site de fabrication et de conception du microcontrôleur

STMicroelectronics SAS voir détails dans [DCSSI-2007/07]

Smartcard IC division
190 Avenue Célestin Coq, ZI de Rousset, BP2
13106 Rousset Cedex
France

Trois rôles sont à distinguer :

- le gestionnaire (*manager*) gère les cartes en créant/supprimant les opérateurs ; il gère les mises à jour des codes (patches en EEPROM) et la personnalisation des cartes. Ce rôle est tenu par LogiWays ;
- l'opérateur (*operator*) gère les droits des abonnés et attribue les accès aux différents services de télévision à péage ;
- le décodeur (ou *set-top-box*) assure le dialogue à travers le canal de confiance *trusted channel* et fournit des informations sur les droits de l'opérateur. Le décodeur est généralement associé à un abonné.

1.2.5. Configuration évaluée

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur, aux logiciels dédiés et,à l'application embarquée, identifiés au §1.1 et au §1.2.1.

Toute autre application éventuellement embarquée, notamment les routines développées et embarquées pour les besoins de l'évaluation, ne fait donc pas partie du périmètre d'évaluation.

L'évaluation a été réalisée en utilisant le principe de composition tel que décrit dans [COMP] La cible d'évaluation est donc la composition du microcontrôleur évaluée par ailleurs (ST19NA18F, certificat [DCSSI-2007/07]) et de l'application de télévision à péage.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et aux interprétations suivantes : ALC_DVS.2 et AVA_VAN.5.

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 « **ST19NA18 révision C**» au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 en CC 2.3 conforme aux profils de protection [PP/9806] et [PP0002]. Ce microcontrôleur a été certifié le 28 mars 2007 sous la référence DCSSI-2007/07 et une maintenance a été réalisée sur ce microcontrôleur dans sa révision actuelle « **ST19NA18 révision F » ou ST19NA18F** sous la référence DCSSI-2007/07-M01, cf. [CERT].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 17 juin 2009 et ses compléments détaillent les travaux menés par le centre d'évaluation et attestent que toutes les tâches d'évaluation sont à « **réussite »**.

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

A la demande du commanditaire, la cotation des mécanismes cryptographiques selon le référentiel technique [REF-CRY] n'a pas été réalisée par l'ANSSI. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction liées à la cryptographie pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le produit n'offre pas de service de génération d'aléas.

Néanmoins, pour ses besoins internes, le produit utilise directement le générateur physique d'aléas offert par le composant sous-jacent (voir rapport de certification du certificat DCSSI-2007/07, [CERT]).

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 l'application de télévision à péage « SAFEACCESS » dans la version 2.0 Rev 67 embarquée sur le composant ST19NA18F de ST Microelectronics répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

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].

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**	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
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	TOE 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**	CM capabilities
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	CM scope
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery
	ALC_DVS			**1**	1	1	**2**	2	**2**	Development security
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Life cycle Definition
	ALC_TAT				**1**	**2**	**3**	3	**1**	Tools and techniques
ASE Security Target Evaluation	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**	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**	Coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**2**	Depth
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional tests
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Vulnerabilty analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - LOGIWAYS TV CARD Security Target Référence : TWSTVC-002-ST, v1.3 du 25/09/2008 Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - LOGIWAYS TV CARD Security Target Référence : LWSTVC-004-ST, v1.5 du 15/10/2009
[RTE]	Rapport technique d'évaluation : - SAFEACCESS v2.0 embedded on ST19NA18 v1.0 Complément au RTE : - Réponses à questions des certificateurs de l'ANSSI du 15/07/2009 Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été utilisé : - ST19NA18C (Evaluation EAL5+) v1.1 Référence : YQUEM_ETRLite_ST19NA18C_v1.1
[CERT]	Rapports de certification et de maintenance - Rapport de certification DCSSI-2007/07 « Microcontrôleur sécurisé ST19NA18C » du 28 mars 2007 - Rapport de maintenance 2007/07-M01 « Microcontrôleur sécurisé ST19NA18F » du 4 mai 2009
[CONF]	Manuel de fabrication du logiciel de la carte à puce v1.2 du 30/04/2009
[GUIDES]	Guide de personnalisation de la carte fille : (Usage exclusif des « personnalisateurs » de cartes à puces) - PERS-FILLE V5.1R3 du 22/10/2008 Guide Interface Carte-Terminal : (Usage exclusif des fabricants de « décodeurs ») - MSD-STBV2.6 du 22/10/2008 Guide « Spécification du générateur d'EMM »: (Usage exclusif du fabricant du dispositif dit EMM_Générateur) - V1.0 du 11/01/2009 Guide « Spécification du générateur d'ECM » : (Usage exclusif du fabricant du dispositif dit ECM_Générateur) - V2.1 du 19/12/2008
[PP/9911]	Protection Profile Smart Card Integrated Circuit With Embedded Software , version 2.0, June 1999. *Certifié par l'ANSSI sous la référence PP/9911.*
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certifié par l'ANSSI sous la référence PP/9806.*

[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié sous la référence BSI-PP-002-2001*.

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, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.11 du 24 octobre 2008, voir www.ssi.gouv.fr