PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/38

Application ITSO SAM (référence 00_06_13) embarquée sur le micro-circuit ATMEL AT90SC3232CS (référence AT568D9 révision K)

Paris, le 24 novembre 2005.

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[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 le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2005/38

Application ITSO SAM (référence 00_06_13) embarquée sur le micro-circuit ATMEL AT90SC3232CS (référence AT568D9 révision K)

Développeurs : Ecebs, ATMEL

Critères Communs version 2.2

EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)

conforme au profil de protection PP/9911

Commanditaire : Ecebs

Centre d'évaluation : CEACI

Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA :
ADV_IMP.2, ALC_DVS.2, AVA_VLA.4

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 :

- La direction centrale 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 publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)
Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle 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] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.
[2] En mai 2005, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède, la Turquie, la République Tchèque, Singapour et l'Inde.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est l'application ITSO SAM (référence 00_06_13) embarquée sur le micro-circuit ATMEL AT90SC3232CS (référence AT568D9 révision K) développé par Ecebs et ATMEL.

1.2. Développeurs

Pour le micro-circuit :

Atmel East Kilbride

Maxwell Building
Scottish Enterprise technology Park
East Kilbride
SCOTLAND G75 0QR

Pour le logiciel embarqué :

Ecebs

The James Watt Building
Scottish Enterprise technology Park
East Kilbride
SCOTLAND G75 0QD

1.3. Description du produit évalué

Le produit ITSO SAM est un élément du système de billettique par cartes à puce sans contact spécifié par l'organisation ITSO (Integrated Transport Smartcard Organisation). Cette organisation, fondée en 1998, est soutenue par les principales organisations de transport par bus et par train en Grande-Bretagne.

Le produit ITSO SAM est destiné à être introduit dans des bornes d'achat, des équipements de validation et des terminaux de gestion.

1.3.1. Architecture

Le produit est constitué du micro-circuit ATMEL AT90SC3232CS (référence AT568D9 révision K) certifié sous la référence 2003/20 [2003/20] dans lequel est chargée l'application ITSO SAM.

La partie applicative ITSO SAM est constituée :

- d'un système d'exploitation MFOS ;

- de l'application ITSO ;
- et d'une couche d'abstraction du matériel (HAL).

1.3.2. Cycle de vie

Le cycle de vie du produit est le suivant :

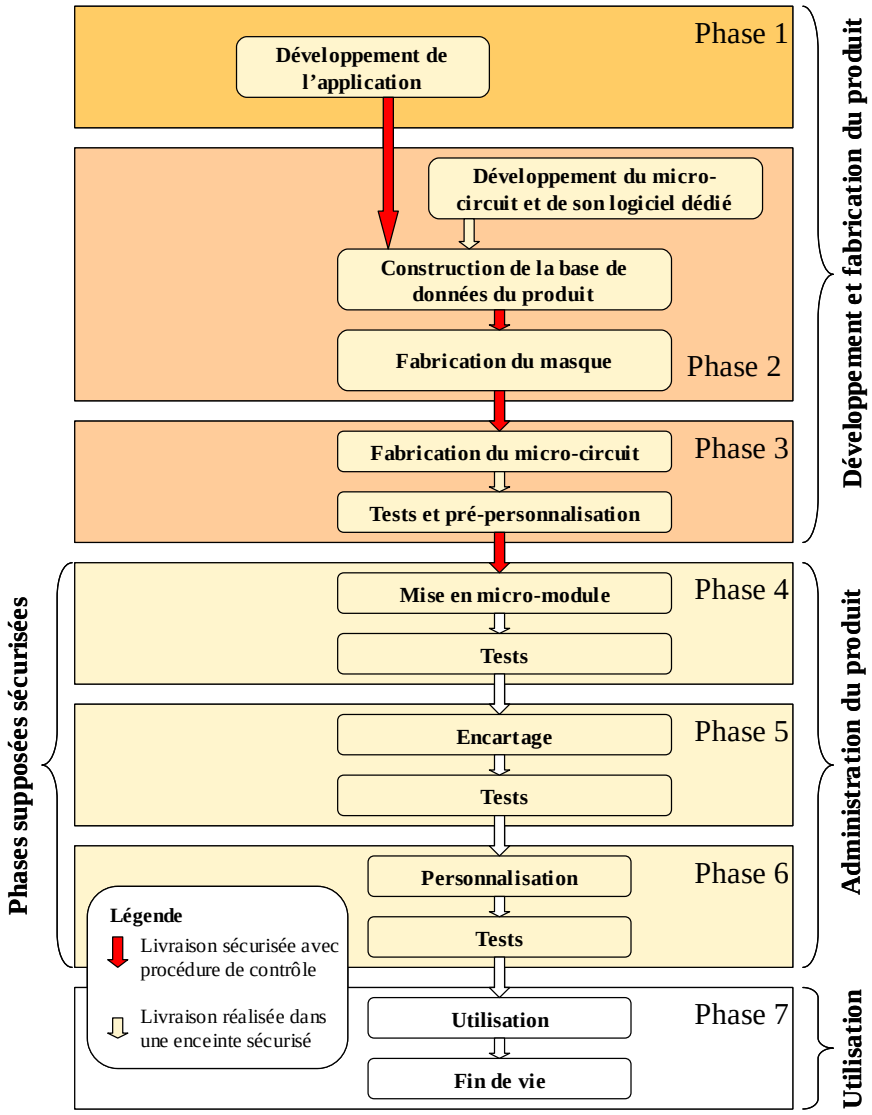

Figure 1 - Cycle de vie du produit

1.3.3. Périmètre et limites du produit évalué

Ce produit offre des fonctionnalités d'audit, d'auto-test, d'opérations cryptographiques (DES, RSA, SHA-1), de gestion de clés (génération, destruction), de contrôle d'accès et d'authentification.

Le produit ITSO SAM comporte une mémoire Flash de 32 Mégaoctets (ATMEL AT45DB321B) qui n'a pas été évaluée.

2. L'évaluation

2.1. Contexte

L'évaluation a été effectuée selon le schéma de composition défini dans le document [COMP]. La composition consiste à réaliser l'évaluation d'un composant masqué en évaluant d'une part le micro-circuit, et d'autre part la partie logicielle en vérifiant qu'aucune faiblesse n'est introduite par l'intégration du logiciel sur le micro-circuit.

Cette évaluation a été réalisée sur la base des résultats de l'évaluation du micro-circuit ATMEL AT90SC3232CS au niveau EAL4 augmenté des composants ADV_IMP.2, ALC_DVS.2, et AVA_VLA.4, conforme au profil de protection PP9806. Ce micro-circuit a été certifié le 13 novembre 2003 sous la référence 2003/20 [2003/20].

Le niveau de résistance du produit aux attaques a été confirmé le *28 octobre 2005* dans le cadre du processus de surveillance.

2.2. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.3. Commanditaire

Ecebs

The James Watt Building
Scottish Enterprise technology Park
East Kilbride
SCOTLAND G75 0QD

2.4. Centre d'évaluation

CEACI (Thales Security Systems – CNES)

18 avenue Edouard Belin
31401 Toulouse Cedex 9
France

Téléphone : +33 (0)5 61 27 40 29

Adresse électronique : ceaci@cnes.fr

2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée du 1er août 2002 au 9 novembre 2005.

Le rapport technique d'évaluation [RTE] détaille les travaux menés par l'évaluateur et présente les résultats obtenus. Les sections suivantes récapitulent les principaux aspects évalués.

2.6. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Cette cible de sécurité est conforme au profil de protection PP/9911.

Pour les tâches d'évaluation de la cible de sécurité, les verdicts suivants ont été émis par l'évaluateur :

Classe ASE: Evaluation d'une cible de sécurité		**Verdicts**
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite

2.7. Evaluation du produit

2.7.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL4[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL4	Methodically designed, tested, and reviewed
+ ADV_IMP.2	Implementation of the TSF
+ ALC_DVS.2	Sufficiency of security measures
+ AVA_VLA.4	Highly resistant

[1] Annexe 2 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

2.7.2. L'évaluation de l'environnement de développement

Le produit est développé sur le site de :

Ecebs

The James Watt Building
Scottish Enterprise technology Park
East Kilbride
SCOTLAND G75 0QR

Les mesures de sécurité analysées par l'évaluateur permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation lors du développement.

L'évaluateur a analysé le plan de gestion de configuration fourni par le développeur qui précise l'utilisation du système de gestion de configuration. Le système permet de générer notamment la liste de configuration [CONF] qui identifie tous les éléments gérés par le système.

Des procédures de génération permettent par ailleurs de s'assurer que les bons éléments sont utilisés pour générer le produit évalué.

La vérification de l'application des procédures analysées a été effectuée lors d'une visite du site de East Kilbride. (cf Annexe 1)

Pour les tâches d'évaluation liées à l'environnement de développement, les verdicts suivants ont été émis par l'évaluateur :

Classe ACM: Gestion de configuration		**Verdicts**
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite

2.7.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit : spécifications fonctionnelles (FSP), conception de haut-niveau (HLD), conception de bas-niveau (LLD), implémentation (IMP).

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :
- Potential violation analysis (FAU_SAA.1)
- Cryptographic key access (FCS_CKM.3)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)
- Complete access control (FDP_ACC.2)

- Security attributes based access control (FDP_ACF.1)
- Basic data authentication (FDP_DAU.1)
- Export of user data without security attributes (FDP_ETC.1)
- Import of user data without security attributes (FDP_ITC.1)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Authentication failures handling (FIA_AFL.1)
- User attribute definition (FIA_ATD.1)
- Timing of authentication (FIA_UAU.1)
- Unforgeable authentication (FIA_UAU.3)
- Single-use authentication mechanisms (FIA_UAU.4)
- Timing of identification (FIA_UID.1)
- User-subject binding (FIA_USB.1)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Management of TOE security functions data (FMT_MTD.1)
- Security management roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Resistance to physical attack (FPT_PHP.3)
- TSF domain separation (FPT_SEP.1)
- Inter-TSF basic TSF data consistency (FPT_TDC.1)
- TSF testing (FPT_TST.1)
- Non-bypassability of the TSP (FPT_RVM.1)

Pour les tâches d'évaluation liées à la conception du produit, les verdicts suivants ont été émis par l'évaluateur :

Classe ADV: Développement		**Verdicts**
ADV_SPM.1	Informal TOE security policy model	Réussite
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite

2.7.4. L'évaluation des procédures de livraison et d'installation

L'évaluateur a analysé les procédures de livraison du produit entre le développeur de l'application (Ecebs) et le développeur du micro-circuit (Atmel).

Ces procédures permettent de connaître l'origine de la livraison et de détecter une modification du produit au cours de cette livraison.

L'installation du produit correspond à la phase 7. Les procédures analysées [INSTALL] permettent d'obtenir la configuration évaluée du produit.

Pour les tâches d'évaluation liées aux procédures de livraison et d'installation, les verdicts suivants ont été émis par l'évaluateur :

Classe ADO: Livraison et exploitation		**Verdicts**
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

2.7.5. L'évaluation de la documentation d'exploitation

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit les intervenants des phases 4 à 6 et comme utilisateurs ceux de la phase 7.

L'évaluateur a analysé les guides d'administration et d'utilisation [GUIDES] pour s'assurer qu'ils permettent d'exploiter le produit évalué d'une manière sécurisée.

Pour les tâches d'évaluation liées à la documentation d'exploitation, les verdicts suivants ont été émis par l'évaluateur :

Classe AGD: Guides		**Verdicts**
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite

2.7.6. L'évaluation des tests fonctionnels

L'évaluateur a analysé la documentation des tests réalisés par le développeur pour s'assurer que toutes les fonctionnalités du produit listées dans la cible de sécurité ont bien été testées.

L'évaluateur a également réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué.

L'évaluateur a réalisé ses tests fonctionnels indépendants principalement sur les versions 00_06_11 et 00_06_12 de l'application ITSO SAM. Les modifications entre ces versions et la version 00_06_13 n'ont pas nécessité de nouveaux tests.

Pour les tâches d'évaluation liées aux tests fonctionnels, les verdicts suivants ont été émis par l'évaluateur :

Classe ATE: Tests		**Verdicts**
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite

2.7.7. L'évaluation des vulnérabilités

L'évaluateur s'est assuré que la documentation fournie avec le produit [INSTALL] [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

Les fonctions RAM Security Counter (SF13), EEPROM Security Counter (SF14), Delete Parameter (SF19) et Verify_ISAM_ID (SF20) ont fait l'objet d'une estimation du niveau de résistance intrinsèque. Le niveau de résistance de ces fonctions est jugé élevé : SOF-HIGH.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests sur la version 00_06_11 de l'application ITSO SAM. Les modifications entre cette version et la version 00_06_13 n'ont pas nécessité de nouveaux tests.

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à des attaques de niveau élevé.

Pour les tâches d'évaluation liées aux vulnérabilités, les verdicts suivants ont été émis par l'évaluateur :

Classe AVA : Estimation des vulnérabilités		**Verdicts**
AVA_MSU.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

2.7.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et décrits dans le rapport technique d'évaluation [RTE] permet la délivrance d'un certificat conformément au décret 2002-535.
Ce certificat atteste que l'exemplaire du produit soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST]. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (Art. 8 du décret 2002-535).

3.2. Restrictions d'usage

Les conclusions de l'évaluation ne sont valables que pour le produit spécifié au chapitre 1 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation résumés ci-dessous et suivre les recommandations se trouvant dans les guides fournis [INSTALL] [GUIDES] :

- la communication entre la carte et le terminal doit être sécurisée (en termes de protocole et de procédure).

3.3. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

3.4. Reconnaissance internationale (CC RA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA]. Toutefois, les augmentations suivantes n'entrent pas dans le cadre de l'accord : ADV_IMP.2, ALC_DVS.2, AVA_VLA.4.

Annexe 1. Visite du site de développement de la société Ecebs à East Kilbride

Le site de développement de la société Ecebs situé à East Kilbride, a fait l'objet d'une visite par l'évaluateur le 5 juin 2003 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour le produit Application ITSO SAM (référence 00_06_13) embarquée sur le micro-circuit ATMEL AT90SC3232CS (référence AT568D9 révision K).

Ces procédures ont été fournies et analysées dans le cadre des tâches d'évaluation suivantes :

- ACM_AUT.1 et ACM_CAP.4 ;
- ALC_DVS.2 ;
- ADO_DEL.2.

Un rapport de visite [Visite] a été émis par l'évaluateur.

Annexe 2. Niveaux d'assurance prédéfinis EAL

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 3. Références documentaires du produit évalué

[CONF]	Configuration List, Acceptance and Signoff - ISAM, référence TEN_06_13_ISAM_SEQ_02
[GUIDES]	- Les guides d'utilisation du produit sont constitués des documents suivants :HOPS ISAM User Guidance, référence ITSO-USR-002-L3E, version 2.4 - POST ISAM User Guidance, référence ITSO-USR-001-L3E, version 2.4 - Project ITSO: Administrator Guidance Manual, référence ITSO-ADM-001-L3E, version 1.5 - Secret Personnalisation Data, version 0.16 - Project ITSO: ISAM Manufacturing Data, référence ITSO-MANU-0001-L3E, version 2.0 - ISAM Personnalisation User Guide, référence ITSO-PERG-001-L3E, version 2.5 - ISAM Installation, Generation and Start-up Procedures at the terminal, référence ITSO-IGS-001-L3E, version 1.5
[INSTALL]	ISAM Installation, Generation and Start-up Procedures at the terminal, référence ITSO-IGS-001-L3E, version1.5
[RTE]	Evaluation Technical Report of Haggis Project, référence HAG_RTE, version 3.0
[ST]	- Ecebs ISAM/MFOS (Multefile) Security Target, référence ITSO-STR-001-L3E, version 6.5 du 20 avril 2005 - Ecebs ISAM/MFOS (Multefile) Security Target Lite, référence ITSO-STR-002-L2, version 6.5 Lite du 31 octobre 2005
[Visite]	Visit Report HAGGIS Project, référence HAG_RDV_EA, version 1.0
[PP/9911]	Profil de protection « Smartcard integrated circuit with embedded software v2.0, juin 1999 » certifié sous la référence PP/9911 le 16/07/99
[2003/20]	Rapport de certification 2003/20 « Micro-circuit ATMEL AT90SC3232CS » du 13 novembre 2003.

Annexe 4. 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, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[CC AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002.
[COMP]	Common Criteria supporting documentation – ETR-lite for composition: Annex A - Composite smartcard evaluation : Recommended best practice, Version 1.2, March 2002.
[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 2.0, April 1999, Management Committee of Agreement Group.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr