Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2004/22

Micro-circuit ATMEL AT05SC1604R rev. K

Paris, le 6/12/2004

Le Directeur central de la sécurité des systèmes d'information

Henri Serres
[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.
Toutefois, 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.

Table des matières

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

[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 novembre 2003, 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 et la Turquie.

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. Le produit évalué

1.1. Contexte

Ce certificat porte sur une mise à jour du micro-circuit AT05SC1604R en révision H certifié sous la référence 2002/03 (cf. [2002/03]).
Sur la base des informations fournies par le développeur [SIA_DEV], l'évaluateur a estimé l'impact des évolutions sur la sécurité du micro-circuit AT05SC1604R en révision K et a mené les travaux d'évaluation requis. Les résultats de cette analyse sont disponibles dans les rapports d'analyse d'impact [SIA_CE].

1.2. Identification du produit

Le produit évalué est le micro-circuit AT05SC1604R (référence AT568C6 rev. K) développé par ATMEL Smart Card ICs.

1.3. Le développeur

Plusieurs acteurs interviennent dans la conception et fabrication du micro-circuit :

Le micro-circuit est développé et testé par :

Atmel East Kilbride

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

La base de données de fabrication du masque du micro-circuit ainsi que la fabrication du produit lui-même sont réalisées par :

Atmel Rousset

Z.I. Rousset Peynier
13106 Rousset Cedex
France.

Les réticules du micro-circuit sont fabriqués par :

Dupont Photomasks

224, bd John Kennedy
91100 Corbeil Essonnes
France

1.4. Description du produit évalué

Le micro-circuit AT05SC1604R Rev. K est développé et fabriqué par Atmel. En termes de description technique, le produit est identique à la version précédente certifiée sous la référence 2002/03 (cf. [2002/03]).

Seule une étape du développement a changé dans le cycle de vie puisque le fabricant de réticule « Dupont Photomask » a changé d'adresse et se trouve désormais à Corbeil Essonnes (cf. §1.3).
Le périmètre d'évaluation est également identique à celui de la version précédente (cf. [2002/03]).

1.5. Utilisation et administration

Les modes d'administration et d'utilisation du produit sont identiques à ceux de la version précédente (cf. [2002/03]).

2. L'évaluation

2.1. Centre d'évaluation

L'évaluation du produit a été réalisée par le centre d'évaluation :

CEA - LETI

17 rue des martyrs
38054 Grenoble Cedex 9
France

Téléphone : +33 (0)4 38 78 40 87

Adresse électronique : alain.merle@cea.fr

Cependant, les tâches environnementales relatives aux sites situés en France ont été réalisées par le centre d'évaluation :

CEACI (Thalès Microelectronics – CNES)

18 avenue Edouard Belin
31401 Toulouse Cedex 4

Téléphone : +33 (0)5 61 27 40 29

Adresse électronique : ceaci@cnes.fr

2.2. Commanditaire

ATMEL Smart Card ICs

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

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'ensemble des interprétations finales listées dans les rapports d'évaluation.

2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 des Critères Communs [CC].
La cible de sécurité répond aux exigences de la classe ASE.

2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation respectent les exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST]. Dans le cadre d'une ré-évaluation, les travaux consistent à analyser l'impact des évolutions du produit.
A l'issue de cette analyse d'impact, le centre d'évaluation peut réaliser à nouveau certaines tâches d'évaluation relatives aux composants d'assurance pour lesquels les changements ont un impact majeur sur la sécurité.

2.5.1. Développement du produit

La classe d'assurance ADV définit les exigences de raffinement des fonctions de sécurité du produit depuis les spécifications globales présentes dans la cible de sécurité [ST] jusqu'à l'implémentation de ces fonctions.

Dans le cadre de cette ré-évaluation, l'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT05SC1604R rev. K a permis de conclure qu'il n'y avait pas nécessité de réaliser de travaux pour la classe d'assurance ADV.

2.5.2. Documentation

Utilisation
Le produit évalué ne met pas en œuvre une application particulière. Il s'agit d'une plate-forme matérielle et logicielle offrant différents services pour les logiciels embarqués dans l'optique d'une utilisation de type « carte à puce ». De fait, il n'y a pas réellement d'utilisation à proprement parler. Les utilisateurs du micro-circuit peuvent être vus (cf. document [CC_IC]) comme étant les développeurs des applications ainsi que tous les acteurs intervenant dans les phases dites d'administration du micro-module et de la carte (phases 4 à 6) qui interviendront notamment dans la configuration et la personnalisation des applications embarquées.

Administration
Le guide « The application of CC to Integrated Circuits » [CC_IC] spécifie les administrateurs du produit comme étant les différents intervenants des phases 4 à 7 du cycle de vie et qui configurent (personnalisation) le produit final. Ces opérations sont en grande partie liées au type d'applications embarquées. Dans le cadre d'un micro-circuit, seules les interfaces d'administration propres au micro-circuit sont évaluées. Par ailleurs, les phases 4 à 6 dites « d'administration » sont couvertes par une hypothèse dans le profil de protection, qui suppose que les opérations associées à ces phases sont réalisées dans des conditions ne remettant pas en cause la sécurité du produit. Ces conditions n'ont pas été évaluées.

Dans le cadre de cette ré-évaluation, l'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT05SC1604R rev. K a permis de conclure qu'il n'y avait pas nécessité de réaliser de travaux pour la classe d'assurance AGD.

2.5.3. Livraison et installation

Concernant la classe ADO, une étape du développement a changé dans le cycle de vie : le fabricant de réticule « Dupont Photomask » a changé d'adresse depuis la précédente évaluation (cf. [2002/03]) et se trouve désormais à Corbeil Essonnes.

Les procédures de livraison avec le fabriquant de masque « Dupont Photomask » à Corbeil Essonnes ont donc fait l'objet d'une évaluation et d'une visite sur site pour vérifier l'application des procédures (cf. Annexe 1). Cette évaluation a été réalisée par le centre d'évaluation CEACI également chargé des évaluations de produit ATMEL.
Par ailleurs, le site d'East Kilbride identifié dans le cycle de vie du produit (cf. §1.3) a fait l'objet d'une visite par le centre d'évaluation CESTI LETI (cf. Annexe 2).

2.5.4. L'environnement de développement

Concernant la classe ALC, une étape du développement a changé dans le cycle de vie : le fabricant de réticule « Dupont Photomask » a changé d'adresse depuis la précédente évaluation (cf. [2002/20]) et se trouve désormais à Corbeil Essonnes. En conséquence, la documentation sécuritaire du fabriquant de masque « Dupont Photomask » à Corbeil Essonnes a fait l'objet d'une évaluation et d'une visite sur site pour vérifier l'application des procédures (cf. Annexe 1). Cette évaluation a été réalisée par le centre d'évaluation CEACI également chargé des évaluations de produit ATMEL.
Par ailleurs, le site d'East Kilbride identifié dans le cycle de vie du produit (cf. §1.3) a fait l'objet d'une visite par le centre d'évaluation CESTI LETI (cf. Annexe 2).
La liste de configuration du produit [LGC] a également changé. Les tâches relatives à la classe ACM ont été partiellement réalisées pour vérifier la mise à jour de la liste de configuration [LGC].

2.5.5. Tests fonctionnels

L'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT05SC1604R rev. K (cf. [SIA_CE]) a permis de conclure à la nécessité de réaliser partiellement les travaux associés à la classe d'assurance ATE : le développeur a réalisé les tests fonctionnels déjà menés sur la version précédente du produit. Le centre d'évaluation a vérifié que les résultats obtenus étaient conformes aux résultats attendus et a mené, à nouveau, certains tests indépendants (cf. [SIA_CE]).

2.5.6. Estimation des vulnérabilités

L'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT05SC1604R rev. K (cf. [SIA_CE]) a permis de conclure qu'il n'y avait pas nécessité de réaliser de travaux spécifiques pour la classe d'assurance AVA.
Le produit dans son environnement d'exploitation est résistant à des attaquants disposant d'un potentiel d'attaque **élevé**.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique de l'évaluation précédente [RTE_OLD] complété du rapport d'analyse d'impact [SIA_CE] et des rapports d'évaluation additionnels identifiés en annexe 5 décrivent les résultats de l'évaluation du micro-circuit AT05SC1604R rev. K identifié au paragraphe 1.2.

3.2. Niveau d'évaluation

Le micro-circuit AT05SC1604R rev. K a été évalué selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **EAL4**[1] **augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_IMP.2	Implementation of the TSF
ALC_DVS.2	Sufficiency of security measures
AVA_VLA.4	Highly resistant

Tableau 1 - Augmentations

Pour tous les composants, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
ASE_DES.1	TOE description	[2002/03]
ASE_ENV.1	Security environment	[2002/03]
ASE_INT.1	ST introduction	[2002/03]
ASE_OBJ.1	Security objectives	[2002/03]
ASE_PPC.1	PP claims	[2002/03]
ASE_REQ.1	IT security requirements	[2002/03]
ASE_SRE.1	Explicitly stated IT security requirements	[2002/03]
ASE_TSS.1	Security Target, TOE summary specification	[2002/03]
Class ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	[2002/03]
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	[2002/03]
Class ADO	**Delivery and operation**	
ADO_DEL.2	Detection of modification	Réussite

[1] Annexe 5 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

ADO_IGS.1	Installation, generation, and start-up procedures	[2002/03]
Class ADV	**Development**	
ADV_FSP.2	Fully defined external interfaces	[2002/03]
ADV_HLD.2	Security enforcing high-level design	[2002/03]
ADV_IMP.2	Implementation of the TSF	[2002/03]
ADV_LLD.1	Descriptive low-level design	[2002/03]
ADV_RCR.1	Informal correspondence demonstration	[2002/03]
ADV_SPM.1	Informal TOE security policy model	[2002/03]
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	[2002/03]
AGD_USR.1	User guidance	[2002/03]
Class ALC	**Life cycle support**	
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	[2002/03]
Class ATE	**Tests**	
ATE_COV.2	Analysis of coverage	[2002/03]
ATE_DPT.1	Testing: high-level design	[2002/03]
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	[2002/03]
Class AVA	**Vulnerability assessment**	
AVA_MSU.2	Validation of analysis	[2002/03]
AVA_SOF.1	Strength of TOE security function evaluation	[2002/03]
AVA_VLA.4	Highly resistant	Réussite

Tableau 2 - Composants et verdicts associés

3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** suivantes[1]. Les opérations sur ces exigences sont décrites dans la cible de sécurité [ST].

- User authentication before any action (FIA_UAU.2)
- User Identification before any action (FIA_UID.2)
- User attribute definition (FIA_ATD.1)
- TOE Security Functions testing (FPT_TST.1)
- Stored data integrity monitoring and action (FDP_SDI.1)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Security management roles (FMT_SMR.1)
- Static attribute initialisation (FMT_MSA.3)

[1] Annexe 4 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- Complete access control (FDP_ACC.2)
- Security attributes based access control (FDP_ACF.1)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- Potential violation analysis (FAU_SAA.1)
- Unobservability (FPR_UNO.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)
- Cryptographic operation (FCS_COP.1)

3.4. Résistance des fonctions

L'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT05SC1604R rev. K a permis de conclure qu'il n'y avait pas nécessité de réaliser de travaux de mise à jour pour la famille d'assurance SOF. Dans le cadre de l'évaluation initiale, seules les fonctions d'authentification avaient fait l'objet d'une estimation du niveau de résistance.
Le niveau de résistance des fonctions de sécurité était jugé **élevé** (**SOF-High**). Cette cotation fut réalisée conformément au guide « Application of attack potential to smart-card » (cf. [JIL_AP]).

3.5. Analyse des mécanismes cryptographiques

Aucun mécanisme cryptographique n'a été coté dans le cadre de l'évaluation (cf Annexe 3).

3.6. Conformité à un profil de protection

Le produit répond aux exigences de sécurité du profil de protection PP/9806 [PP/9806].

3.7. Reconnaissance européenne (SOG-IS)

Ce certificat a été émis dans les conditions de l'accord du SOG-IS. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].

3.8. Reconnaissance internationale (CC RA)

Ce certificat a été émis dans les conditions de l'accord du CC RA. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].
Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA [CC RA] : ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4 (Tableau 1).

3.9. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement (§ 3.10) ainsi que les recommandations se trouvant dans les guides utilisateur et administrateur [USR].
Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.
De plus, la présente évaluation donne une appréciation de la résistance du produit à des attaques qui demeurent fortement génériques du fait de l'absence d'application spécifique

embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée qu'au travers d'une évaluation du produit complet. Cette évaluation pourra être réalisée en ré-utilisant les résultats de la présente évaluation.

3.10. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité suivants sont extraits de la cible de sécurité du produit [ST § 4.2] :

Objectifs de sécurité sur l'environnement concernant le système en phase d'utilisation

Ces objectifs de sécurité concernent le système dans lequel sera utilisé le micro-circuit avec son application embarquée (extraits de la cible de sécurité [ST § 4.2.6]) :

- la communication entre un produit développé sur le micro-circuit sécurisé et d'autres produits doit être sécurisée (en terme de protocole et de procédure),
- le système (terminal, communication,…) doit garantir la confidentialité et l'intégrité des données sensibles qu'il stocke ou qu'il traite.

3.11. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le produit micro-circuit AT05SC1604R rev. K identifié au paragraphe 1.2 et décrit au paragraphe 1.4 du présent rapport **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique de l'évaluation précédente [RTE_OLD], le rapport d'analyse d'impact [SIA_CE] et les rapports d'évaluation additionnels identifiés en annexe (cf. Annexe 6).

Annexe 1. Rapport de visite du site de Dupont Corbeil

Le site du fabriquant de masque « Dupont Photomask » situé à l'adresse 224, bd John Kennedy, 91100 Corbeil Essonnes en France, a fait l'objet, dans le cadre de l'évaluation des produits ATMEL, et en particulier de l'évaluation du micro-circuit AT05SC1604R rev. K, d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la livraison : **ADO** (ADO_DEL.2) ;
- le support au cycle de vie : **ALC** (ALC_DVS.2).

La visite par le centre d'évaluation a permis de conclure que les critères sont satisfaits sur ce site (cf. [Visite]).

Annexe 2. Rapport de visite du site d'Atmel East Kilbride

Le site de développement de Atmel Smart Card Ics situé au Maxwell Building, Scottish Enterprise technology Park, East Kilbride SCOTLAND G75 0QR, a fait l'objet, dans le cadre de l'évaluation des produits ATMEL, et en particulier de l'évaluation du micro-circuit AT05SC1604R rev. K, d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- la livraison : **ADO** (ADO_DEL.2) ;
- le support au cycle de vie : **ALC** (ALC_DVS.2).

La visite par le centre d'évaluation a permis de conclure que les critères sont satisfaits sur ce site (cf. [Visite]).

Annexe 3. Analyse des mécanismes cryptographiques

Aucun mécanisme cryptographique spécifique n'a été coté dans le cadre de l'évaluation de ce produit.

Annexe 4. Exigences fonctionnelles de sécurité du produit évalué

Attention : les descriptions des composants fonctionnels suivants sont données à titre indicatif. Seule une lecture attentive de la cible de sécurité ([ST]) peut apporter la description exacte des exigences fonctionnelles du produit.

Class FAU	**Security audit**
Security audit analysis	
FAU_SAA.1	*Potential violation analysis* Le produit doit implémenter un seuil de détection élémentaire, défini selon une règle fixée (spécifiée dans la cible de sécurité [ST]).
Class FCS	**Cryptographic support**
Cryptographic operation	
FCS_COP.1	*Cryptographic operation* Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée (spécifiés dans la cible de sécurité [ST]).
Class FDP	**User data protection**
Access control policy	
FDP_ACC.2	*Complete access control* Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Information flow control policy	
FDP_IFC.1	*Subset information flow control* Le produit doit appliquer les politiques de sécurité de contrôle de flux d'information, lesquelles sont spécifiées dans la cible de sécurité [ST] pour un sous-ensemble des opérations possibles sur un sous-ensemble des flux d'informations.
Information flow control functions	
FDP_IFF.1	*Simple security attributes* Ce composant impose des attributs de sécurité aux informations, aux sujets qui déclenchent le transfert de ces informations ainsi qu'aux sujets qui reçoivent ces informations. Ce composant spécifie les règles qui doivent être appliquées par la fonction et décrit comment les attributs de sécurité sont choisis par la fonction.
Stored data integrity	
FDP_SDI.1	*Stored data integrity monitoring* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées.

Class FIA	**Identification and authentication**
User attribute definition	
FIA_ATD.1	*User attribute definition* Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.
User authentication	
FIA_UAU.2	*User authentication before any action* Les utilisateurs doivent s'authentifier avant que toute action ne soit autorisée.
User identification	
FIA_UID.2	*User identification before any action* Les utilisateurs doivent s'identifier avant que toute action ne soit autorisée.
Class FMT	**Security management**
Management of functions in TSF	
FMT_MOF.1	*Management of security functions behaviour* Le produit doit limiter la capacité à gérer le comportement des fonctions de sécurité du produit à des utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]).
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiés dans la cible de sécurité [ST]).
Class FPR	**Privacy**
Unobservability	
FPR_UNO.1	*Unobservability* Le produit n'autorise pas certains utilisateurs (spécifiés dans la cible de sécurité [ST]) à déterminer si certaines opérations (spécifiées dans la cible de sécurité [ST]) sont en cours d'exécution.
Class FPT	**Protection of the TSF**
TSF physical protection	
FPT_PHP.2	*Notification of physical attack* Le produit doit notifier automatiquement l'intrusion physique sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
FPT_PHP.3	*Resistance to physical attack* Le produit doit empêcher ou résister à certaines intrusions physiques (spécifiées dans la cible de sécurité [ST]) sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
TSF self test	
FPT_TST.1	*TSF testing* Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.

Annexe 5. Niveaux d'assurance prédéfinis IS 15408 ou CC

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 6. Références documentaires du produit évalué

[2002/03]	Rapport de certification 2002/03 Micro-circuit ATMEL AT05SC1604R (référence AT568C6 rev. H), Mars 2002 SGDN/DCSSI
[LGC]	Liste de configuration du produit en révision K : ▪ OLYMPIA Design Configuration List, Référence : OLYMPIA_DCL_V1.6, 26/01/2004, ATMEL ▪ OLYMPIA Manufacturing Configuration List, Référence : OLYMPIA_MCL_V1.4, 23/01/2004, ATMEL ▪ Mask List AT05SC1604R - OLYMPIA, Référence : v1.4, 23/01/2004, ▪ IO Maintenance Update, Référence : LETI_MU_V3.0, March 2004, ATMEL
[PP9806]	Common Criteria for Information Technology Security Evaluation - Protection Profile : Smart Card Integrated Circuit Version 2.0, Issue September 1998. Certifié par le centre de certification français sous la référence 9806. *Document publié sur le site : www.ssi.gouv.fr*
[RTE_OLD]	Rapport Technique d'Evaluation, Référence : LETI.CESTI.OLY.RTE.001, CEA/LETI
[SIA_DEV]	▪ OLYMPIA Security Impact Analysis, Référence : OLYMPIA_SIA_V1.0, 20/06/2003, ATMEL ▪ OLYMPIA Security Impact Analysis, Référence : OLYMPIA_SIA_V1.1, 20/08/2003, ATMEL ▪ OLYMPIA Security Impact Analysis, Référence : OLYMPIA_SIA_V1.2, 26/01/2004, ATMEL
[SIA_CE]	▪ IO Project - Internal/End of Task Report AMA_SIA.1, Référence : LETI.CESTI.IO.RI/RT.002_V1.0, 08/09/2003. CEA/LETI

	▪ IO Project - Internal/End of Task Report AMA_SIA.1, Référence : LETI.CESTI.IO.RI/RT.003_V1.0, 15/01/2004 CEA/LETI Synthèse sur l'historique du projet : ▪ IO Project: Security Impact Analysis of OLYMPIA Revision K, Référence : IO.CR.003 v1.1 CEA/LETI
[ST]	▪ EUROPA AT05SC1604R Security Target, Référence: AT05SC1604R_ST v1.1 - 29 novembre 2001, ATMEL ▪ EUROPA AT05SC1604R Security Target - Lite, Référence : AT05SC1604R_ST_LITE v1.2 – 22 février 2002, ATMEL
[USR]	Un document générique sert d'interface pour toute la documentation d'utilisation : ▪ AT05SC1604R CC Guidance (AGD Interface Document) Référence : AT05SC1604R_ GUID v1.0 ATMEL Les documents associés sont : ▪ Technical Data AT05SC1604R Référence : 1522BX, rev. 1.5, ATMEL ▪ AT05SC1604R Supplementary Security Application Note, Référence : AT05_APP_016 v1.0 ATMEL ▪ Europa Application Note for CRC, Référence : Euro_APP_016 v1.1, ATMEL ▪ Europa Application Note for RNG, Référence : Euro_APP_017 v1.1, ATMEL
[Visite]	Rapport de visite relatif aux sites situés au Royaume Uni : ▪ IO Project - ATMEL East Kilbride Audit, Référence : IO.CR.005 version 1.0 CEA/LETI Rapport de visite relatif aux sites situés en France : ▪ Audit Status for ATMEL, Référence : Audit Status for ATMEL version 1.0 CEACI

Annexe 7. 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.	
[CC]	Critères Communs pour l'évaluation de la sécurité des technologies de l'information: ▪ Part 1: Introduction and general model, august 1999, version 2.1, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, august 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, august 1999, version 2.1, réf: CCIMB-99-033.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.
[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
[IS 15408]	Norme Internationale ISO/IEC 15408:1999, comportant 3 documents : ▪ ISO/IEC 15408-1: Part 1 Introduction and general model ; ▪ ISO/IEC 15408–2: Part 2 Security functional requirements ; ▪ ISO/IEC 15408–3: Part 3 Security assurance requirements ;
[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
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr