
PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

# Rapport de certification 2004/05

# Micro-circuit ATMEL AT90SC9608RC rev. F

*Paris, le 2 avril 2004*

*Le Directeur central de la sécurité des systèmes d'information*

*Henri Serres*
[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 terme 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 est 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 selon les ITSEC et les Critères Communs sont publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

Le site international concernant la certification selon les Critères Communs est accessible à l'adresse Internet :

www.commoncriteria.org

## 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 :


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

[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.

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.

L'accord du Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires de l'accord[1], des certificats délivrés dans le cadre du schéma Critères Communs. La reconnaissance mutuelle s'applique au niveau EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

Les sites des organismes nationaux de certification des pays signataires de l'accord Common Criteria Recognition Arrangement sont :

| Pays | Organisme certificateur | Site web |
|---|---|---|
| France | DCSSI | www.ssi.gouv.fr |
| Royaume-Uni | CESG | www.cesg.gov.uk |
| Allemagne | BSI | www.bsi.bund.de |
| Canada | CSE | www.cse-cst.gc.ca |
| Australie-Nouvelle Zélande | AISEP | www.dsd.gov.au/infosec |
| Etats-Unis | NIAP | www.niap.nist.gov |
| Japon | NITE | www.nite.go.jp |

[1] 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.

# 1. Le produit évalué

## 1.1. Contexte

Ce certificat porte sur une mise à jour du micro-circuit AT90SC9608RC rev. E certifié sous la référence 2003/28 (cf. [2003/28]), lui-même étant une mise à jour du micro-circuit AT90SC9608RC rev. D certifié sous la référence 2003/11 (cf. [2003/11). L'évaluation de cette mise à jour a été réalisée dans le cadre du programme de maintenance PM 2003/03 relatif aux micro-circuits ATMEL.
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 AT90SC9608RC en révision F. Les résultats de cette analyse sont disponibles dans le rapport d'analyse d'impact [SIA_CE].

## 1.2. Identification du produit

Le produit évalué est le micro-circuit AT90SC9608RC référence AT578A7 révision F. Ce micro-circuit inclut une librairie logicielle cryptographique stockée en ROM en version 2.1.

## 1.3. Le développeur

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

Le micro-circuit AT90SC9608RC 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 AT90SC9608RC est préparée par :

**Atmel Rousset**

Z.I. Rousset Peynier
13106 Rousset Cedex
France.

Les réticules du micro-circuit AT90SC9608RC sont fabriqués par :

**Compugraphics International Ltd**

Newark Road North
Eastfield industrial Estate
Glenrothes
Fife, KY7 4NT
Ecosse.

Le micro-circuit AT90SC9608RC est fabriqué par :

**Atmel North Tyneside**

Middle Engine Lane
Silverlink business Park
North Tyneside, NE28 9N2
Royaume Uni.

## 1.4. Description du produit évalué

Le micro-circuit AT90SC9608RC rev. F est développé et fabriqué par Atmel. En terme de description technique, le produit est identique aux versions précédentes certifiées sous les référence 2003/11 (cf. [2003/11]) et 2003/28 (cf. [2003/28]).
Le périmètre d'évaluation est également identique à celui des versions précédentes (cf. [2003/11] et [2003/28]).

## 1.5. Utilisation et administration

Les modes d'administration et d'utilisation du produit sont identiques à ceux des versions précédentes (cf. [2003/11] et [2003/28]).

# 2. L'évaluation

## 2.1. 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

L'évaluation s'est déroulée de février à mars 2004.

## 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'un programme de maintenance, l'évaluation consiste à analyser l'impact des évolutions du produit en maintenance.
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*

L'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT90SC9608RC rev. F (cf. [SIA_CE]) 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*

L'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT90SC9608RC rev. F (cf. [SIA_CE]) 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*

L'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT90SC9608RC rev. F (cf. [SIA_CE]) a permis de conclure qu'il n'y avait pas nécessité de réaliser de travaux pour la classe d'assurance ADO.

### *2.5.4. L'environnement de développement*

L'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT90SC9608RC rev. F (cf. [SIA_CE]) a permis de conclure qu'il n'y avait pas nécessité de réaliser de travaux pour la classe d'assurance ALC.
Concernant la classe ACM, la liste de configuration du produit [LGC] a changé. En conséquence, les tâches relatives à la classe ACM ont été partiellement réalisées pour vérifier la mise à jour de la liste de configuration (cf. [RTE]).

### *2.5.5. Tests fonctionnels*

L'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT90SC9608RC rev. F (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. [RTE]).

### *2.5.6. Estimation des vulnérabilités*

L'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT90SC9608RC rev. F (cf. [SIA_CE]) a permis de conclure à la nécessité de réaliser partiellement les travaux associés à la classe d'assurance AVA : le développeur a mis à jour son analyse de vulnérabilité indépendante. Les résultats ne montrent pas de vulnérabilités exploitables au niveau d'évaluation considéré. Le produit AT90SC9608RC rev. F identifié au §1.2 est donc résistant à des attaquants disposant d'un potentiel d'attaque **élevé** dans son environnement d'exploitation.

# 3. Conclusions de l'évaluation

## 3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation du micro-circuit AT90SC9608RC en révision F.

## 3.2. Niveau d'évaluation

Le micro-circuit AT90SC9608RC en révision F 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 | [2003/11] |
| ASE_ENV.1 | Security environment | [2003/11] |
| ASE_INT.1 | ST introduction | [2003/11] |
| ASE_OBJ.1 | Security objectives | [2003/11] |
| ASE_PPC.1 | PP claims | [2003/11] |
| ASE_REQ.1 | IT security requirements | [2003/11] |
| ASE_SRE.1 | Explicitly stated IT security requirements | [2003/11] |
| ASE_TSS.1 | Security Target, TOE summary specification | [2003/11] |
| **Class ACM** | **Configuration management** | |
| ACM_AUT.1 | Partial CM automation | [2003/11] |
| ACM_CAP.4 | Generation support and acceptance procedures | Réussite |
| ACM_SCP.2 | Problem tracking CM coverage | Réussite |
| **Class ADO** | **Delivery and operation** | |
| ADO_DEL.2 | Detection of modification | [2003/11] |
| ADO_IGS.1 | Installation, generation, and start-up procedures | [2003/11] |

[1] Annexe 4 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

| | | |
|---|---|---|
| **Class ADV** | **Development** | |
| ADV_FSP.2 | Fully defined external interfaces | [2003/11] |
| ADV_HLD.2 | Security enforcing high-level design | [2003/11] |
| ADV_IMP.2 | Implementation of the TSF | [2003/11] |
| ADV_LLD.1 | Descriptive low-level design | [2003/11] |
| ADV_RCR.1 | Informal correspondence demonstration | [2003/11] |
| ADV_SPM.1 | Informal TOE security policy model | [2003/11] |
| **Class AGD** | **Guidance** | |
| AGD_ADM.1 | Administrator guidance | [2003/11] |
| AGD_USR.1 | User guidance | [2003/11] |
| **Class ALC** | **Life cycle support** | |
| ALC_DVS.2 | Sufficiency of security measures | [2003/11] |
| ALC_LCD.1 | Developer defined life-cycle model | [2003/11] |
| ALC_TAT.1 | Well-defined development tools | [2003/11] |
| **Class ATE** | **Tests** | |
| 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 |
| **Class AVA** | **Vulnerability assessment** | |
| AVA_MSU.2 | Validation of analysis | [2003/11] |
| AVA_SOF.1 | Strength of TOE security function evaluation | [2003/11] |
| 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)
- Complete access control (FDP_ACC.2)

[1] Annexe 3 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- 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)
- Cryptographic Key Generation (FCS_CKM.1)

## 3.4. Résistance des fonctions

L'analyse de l'impact des évolutions sur la sécurité du micro-circuit AT90SC9608RC rev. F (cf. [SIA_CE]) 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 (cf. [2003/11]), les fonctions suivantes avaient fait l'objet d'une estimation du niveau de résistance :

- Authentification de l'administrateur en mode test,
- Protection de l'accès à la mémoire de test,
- Audit des événements,
- Non-observabilité.

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 de la révision F du micro-circuit AT90SC9608RC n'a été coté.

## 3.6. Conformité à un profil de protection

Le produit évalué est conforme au 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 par 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 [USR] et administrateur [ADM et IGS].
Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.

## 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 micro-circuit AT90SC9608RC en révision F identifié au paragraphe 1.2 **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 initiale [RTE_OLD] et le rapport technique de cette évaluation [RTE] dans le cadre du programme de maintenance PM 2003/03.

# Annexe 1. Rapport de visite de site

Aucune visite n'a été réalisée dans le cadre de cette évaluation.

# Annexe 2. Analyse des mécanismes cryptographiques

Aucun mécanisme cryptographique spécifique n'a été coté dans le cadre de l'évaluation de cette version du micro-circuit.

# Annexe 3. 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*<br>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 key management | |
| **FCS_CKM.1** | *Cryptographic key generation*<br>Le produit doit générer des clés cryptographiques conformément à un algorithme et des tailles de clés spécifiées qui peuvent être basés sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST]. |
| Cryptographic operation | |
| **FCS_COP.1** | *Cryptographic operation*<br>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*<br>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*<br>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*<br>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'information. |

| | |
|---|---|
| Information flow control functions | |
| **FDP_IFF.1** | *Simple security attributes*<br>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*<br>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*<br>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<br>Les utilisateurs doivent s'authentifier avant que toute action ne soit autorisée. |
| User identification | |
| **FIA_UID.2** | User identification before any action<br>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*<br>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*<br>Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés. |
| **FMT_MSA.3** | *Static attribute initialisation*<br>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<br>Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiées dans la cible de sécurité [ST]). |
| **Class FPR** | **Privacy** |
| Unobservability | |
| **FPR_UNO.1** | *Unobservability*<br>Le produit n'autorise pas certains utilisateurs (spécifiées 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*<br>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*<br>Le produit doit empêcher ou résister à certaines intrusion physique (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*<br>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 4. 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 5. Références documentaires du produit évalué

| | |
|---|---|
| [2003/11] | Rapport de certification 2003/11<br>Micro-circuit ATMEL AT90SC9608RC,<br>22 septembre 2003<br>SGDN/DCSSI |
| [2003/28] | Rapport de certification 2003/28<br>Micro-circuit ATMEL AT90SC9608RC rev. E,<br>18 décembre 2003<br>SGDN/DCSSI |
| [LGC] | Liste de configuration du produit en revision F :<br>▪ ARIEL Design Configuration List<br>Référence : Ariel_DCL_V1.3 – 26Jan04<br>ATMEL<br>▪ ARIEL Manufacturing Configuration List,<br>Référence : Ariel_MCL_V1.2 – 6Jan04<br>ATMEL<br>▪ ARIEL CC deliverables,<br>Référence : Ariel_EDL_03Feb04<br>ATMEL |
| [PP9806] | Common Criteria for Information Technology Security Evaluation - Protection Profile : Smart Card Integrated Circuit Version 2.0, Issue September 1998.<br>Certifié par le centre de certification français sous la référence 9806.<br>*Document publié sur le site : www.ssi.gouv.fr* |
| [RTE] | EVALUATION TECHNICAL REPORT OF ARIEL revF Project,<br>Référence : ARIF_RTE version 1.0 |
| [RTE_OLD] | EVALUATION TECHNICAL REPORT OF ARIEL Project,<br>Référence : ARI_RTE, version 1.0L<br>CEACI |
| [SIA_CE] | EVALUATION OF the security impact analysis of ARIEL revF Project,<br>Référence : ARIF_RFT_SIA, version 1.0 du 11/03/2004<br>CEACI |
| [SIA_DEV] | Ariel Security Impact Analysis AT90SC9608RC (Rev E to F)<br>Référence : Ariel_SIA_V1.2E - 02Feb04 |
| [ST] | ARIEL Security target<br>Référence : Ariel_ST_V1.1 (16 jun 03)<br>ATMEL |

| | |
|---|---|
| [USR] | Un document générique sert d'interface pour toute la documentation d'utilisation :<br>▪ Ariel Guidance AGD interface document<br>Référence : Ariel_GUID_v1.0, 16/04/03<br>Atmel<br>Les documents associés sont :<br>▪ Technical Data AT90SC9608R Data sheet,<br>Référence : 1581BX, rev. B, 01/06/03,<br>Atmel<br>▪ AT90SC technical data (preliminary) Addressing Modes & Instruction Set,<br>Référence : 1323, rev. B, 26 Feb 2001<br>Atmel<br>▪ Toolbox v2.1 SC16 crypto-coprocessor library,<br>Référence : TPR0096A – 12/03/03 – ARCP, rev A,<br>Atmel<br>▪ ARIEL Wafer Sawing Recommendation,<br>Référence : Ariel_WSR_V1.0, 17/04/03<br>Atmel<br>▪ Securing the RSA operations on the AT 90SC ASL 4,<br>Référence : TPR0062B, rev. B, 17/03/03<br>Atmel<br>▪ Securing the DES/TDES on the AT90SC ASL 4,<br>Référence : TPR0063C, rev. C, 21/03/03,<br>Atmel<br>▪ Checksum Accelerator use on the AT90SC ASL4 products,<br>Référence : TPR0065-02July02/ARCP, rev. A,<br>Atmel<br>▪ Security recommendation for AT90SC ASL4,<br>Référence : TPR0066C rev. C, 30/04/03<br>Atmel<br>▪ Generating unpredictable random numbers on AT90SC Family devices,<br>Référence : 1573CX rev. C, 21/03/03<br>Atmel |

# Annexe 6. 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:<br>▪ Part 1: Introduction and general model, august 1999, version 2.1, ref CCIMB-99-031 ;<br>▪ Part 2: Security functional requirements, august 1999, version 2.1, ref CCIMB-99-032 ;<br>▪ 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:<br>▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045. |
| [IS 15408] | Norme Internationale ISO/IEC 15408:1999, comportant 3 documents :<br>▪ ISO/IEC 15408-1: Part 1 Introduction and general model ;<br>▪ ISO/IEC 15408–2: Part 2 Security functional requirements ;<br>▪ 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. |
| [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 |

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