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 2005/05

Micro-circuit ATMEL AT90SC7272C rev. D

Paris, le 11 mars 2005

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.

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 2005/05

Micro-circuit ATMEL AT90SC7272C rev. D

Développeurs : Atmel SmartCard ICs

Critères Communs version 2.1
(norme internationale ISO/IEC 15408:1999)

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

conforme au profil de protection PP/9806

Commanditaire : Atmel SmartCard ICs

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 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.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est le micro-circuit AT90SC7272C, référence AT578B3 révision D. Ce micro-circuit inclut une librairie logicielle cryptographique stockée en ROM en version 2.2 dont seule une partie a été évaluée (cf. périmètre de l'évaluation, §1.3.3).
Ce micro-circuit appartient à la famille de produits AVR ASL4 développée par Atmel SmartCard Ics.

1.2. Développeur

Plusieurs acteurs interviennent dans la conception et la 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

1.3. Description du produit évalué

1.3.1. Architecture

L'architecture du micro-circuit AT90SC7272C est la suivante :

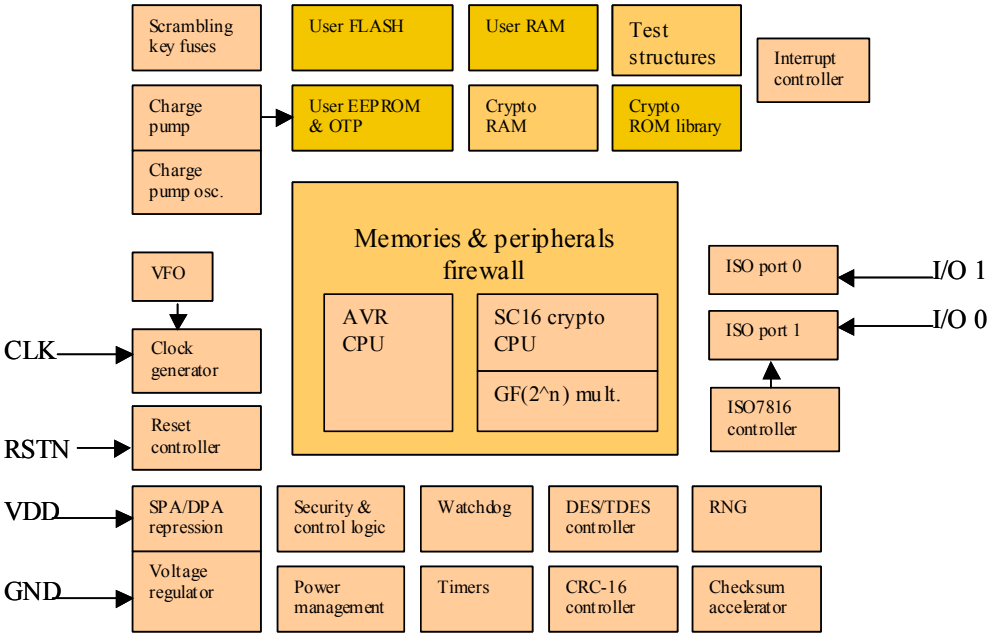

Figure 1 - micro-circuit ATMEL AT90SC7272C

Les caractéristiques techniques du produit sont les suivantes :

- CPU AVR Risc ;
- 72KB de mémoire Flash pour le stockage des programmes ;
- 72KB de mémoire EEPROM pour le stockage des programmes et des données avec 128 Bytes d'OTP (mémoire inscriptible, non effaçable en mode « utilisateurs », pour stocker les données sensibles par exemple, ou servir de verrous sur les phases du cycle de vie notamment) et 384 bytes accessibles par bit, une pompe de charge et ses oscillateurs ;
- 6KB de mémoire RAM ;
- des clés de brouillage pour les mémoires ;
- un accélérateur de calcul de checksum 32 bits (support à la détection d'erreurs sur les données ou programmes en mémoire) ;
- un périphérique CRC-16 (support à la détection d'erreurs sur les données ou programmes en mémoire) ;
- un générateur de nombres aléatoires ;
- un accélérateur de calcul cryptographique DES/3DES ;
- un coprocesseur cryptographique (SC16) incluant une librairie logicielle de 8KB en ROM (boîte à outils cryptographiques) permettant d'accélérer les calculs RSA (avec et sans CRT) et SHA-1. La librairie fournit également d'autres primitives, ainsi que des primitives permettant au logiciel embarqué de construire ses propres algorithmes mais ces primitives ne font pas partie du périmètre d'évaluation ;
- des détecteurs tension, fréquence, température et lumière ultraviolette ;
- un firewall protégeant l'accès à toutes les mémoires et périphériques, comportant trois modes d'utilisation ;
- un régulateur de tension (le micro-circuit fonctionne dans une gamme de tension de 3.0V à 5.0V) ;
- 2 Timers ;
- 2 ports série avec une interface et un contrôleur conforme au standard ISO7816 ;
- une structure de test dédiée, sciée lors de la mise en micro-module et accessible uniquement en mode test pour les tests de production.

Le micro-circuit comporte trois modes d'utilisation :

- Un mode « Test » dans lequel le micro-circuit fonctionne sous le contrôle d'un logiciel de test écrit en mémoire EEPROM à l'aide d'une interface de test, et utilisé sous le contrôle d'un système de test externe. Ce mode n'est utilisable que par le personnel autorisé de l'équipe du développement et dans un environnement sécurisé. Après la phase de test, le mode « test » est inhibé de façon irréversible par rupture de fusible. De plus, après découpage du « wafer », l'interface de test n'est plus accessible ;
- Un mode « utilisateur » dans lequel le micro-circuit fonctionne sous le contrôle du logiciel embarqué de la carte à puce. Les utilisateurs finaux ne peuvent utiliser le micro-circuit que dans ce mode ;
- Un mode « diagnostic » utilisé lors du retour de pièces défectueuses et permettant d'effectuer un sous-ensemble de tests à l'aide d'une interface de test utilisée sous le contrôle d'un système de test externe. Lors de l'activation de ce mode, le contenu des mémoires est effacé. Ce mode n'est utilisable que par le personnel autorisé de l'équipe du développement et dans un environnement sécurisé.

Le micro-circuit seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou des applications et à être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (applications bancaires, télévision à péage, transport, santé,...) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

1.3.2. Cycle de vie

Le cycle de vie du produit inspiré du cycle de vie décrit dans le PP/9806 [PP9806] est le suivant :

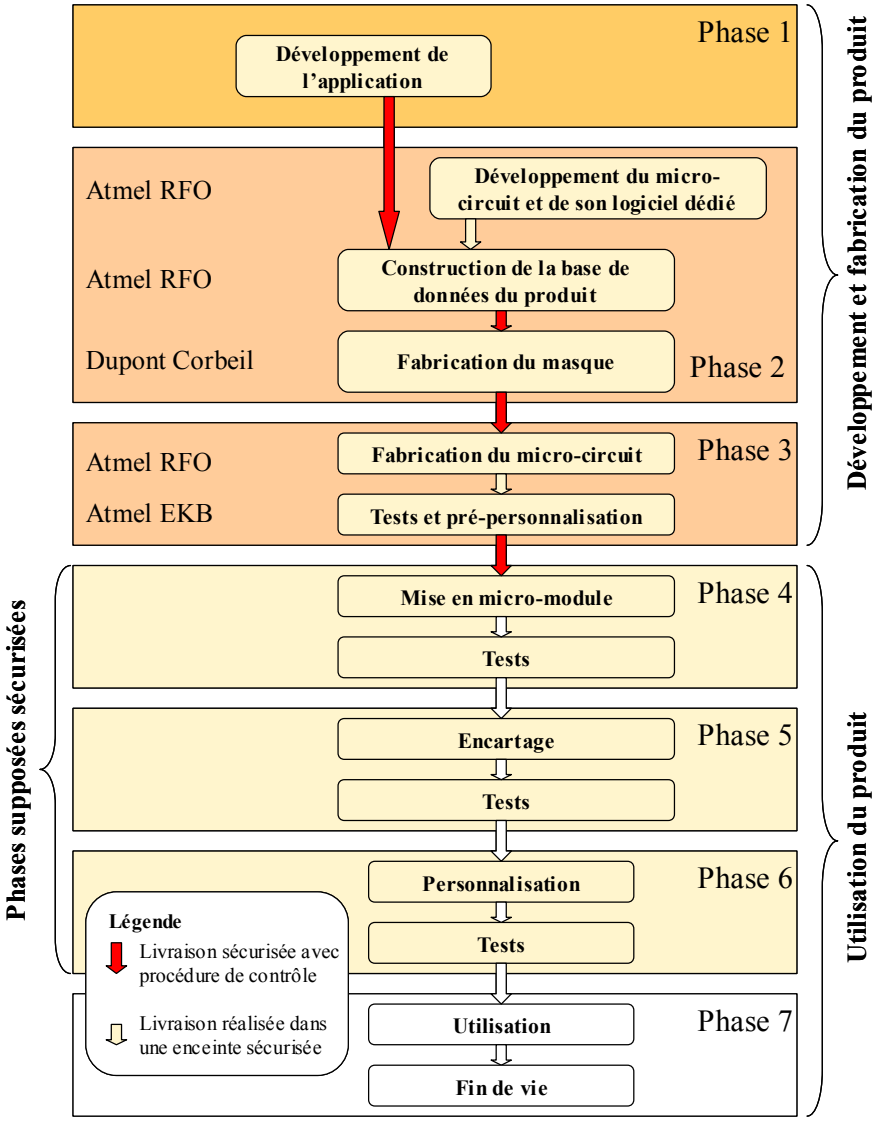

Figure 2 - Cycle de vie du produit

1.3.3. Périmètre et limites du produit évalué

Ce rapport de certification présente les travaux d'évaluation relatifs au micro-circuit seul et aux commandes de la librairie cryptographique relatives aux calculs RSA et SHA (commandes 02h, 08h, 09h et 0Bh). Les autres commandes de la librairie sont exclues du périmètre d'évaluation.

Toute application, éventuellement embarquée pour les besoins de l'évaluation, ne fait pas partie du périmètre d'évaluation.

En regard du cycle de vie, le produit évalué est le produit qui sort de la phase de fabrication, tests et pré-personnalisation (phase 3).

2. L'évaluation

2.1. Contexte

Le produit évalué est dérivé du micro-circuit AT90SC9608RC certifié en 2003 sous les références [2003/11] pour la révision D et [2003/28] pour la révision E, et en 2004 sous les références [2004/05] pour la révision F et [2004/35] pour la révision I.
Une partie des verdicts de la présente évaluation s'appuie donc sur les résultats des travaux menés lors des précédentes évaluations. Pour les tâches environnementales, une partie des verdicts provient de l'évaluation d'un produit similaire certifié sous la référence [2004/02].

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], et aux interprétations suivantes :

- RI013, RI038, RI043, RI064 et RI085 pour ASE,
- RI003, RI004, RI037, RI038 et RI095 pour ACM,
- RI074 et RI075 pour ATE,
- RI006 pour ADV,
- RI031 et RI051 pour VLA.

2.3. Commanditaire

ATMEL Smart Card ICs

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

2.4. Centre d'évaluation

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

CEACI (TES – CNES)

18 avenue Edouard Belin
31401 Toulouse Cedex 4

Téléphone : +33 (0)5 61 27 40 29

Adresse électronique : ceaci@cnes.fr

Cependant, les tâches environnementales relatives au site situé au Royaume-Uni ont été réalisées 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

2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée du 9 juillet 2004 au 8 décembre 2004.

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 9806 (cf. [PP9806]).

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

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

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

2.7.2. L'évaluation de l'environnement de développement

Le développement du micro-circuit implique l'ensemble des sites identifiés au §1.2.
Les environnements de développement des sites impliqués sont évalués et audités dans le cadre des différentes évaluations et ré-évaluations des produits ATMEL (voir en particulier le rapport de certification [2004/02]). Deux centres d'évaluation réalisent ces tâches : le CEA/LETI pour les sites situés au Royaume-Uni, et le CEACI pour les sites situés en France. Les conclusions des travaux associés sont satisfaisantes (cf. [Visite]). Les environnements de développement liés à ces sites n'ont donc pas fait l'objet d'une évaluation particulière au sein de ce projet.
Les tâches relatives à la classe ACM ont été à nouveau partiellement réalisées, notamment pour vérifier la mise à jour de la liste de configuration [CONF].

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	[2004/02]
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	[2004/02]
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 Generation (FCS_CKM.1)
- Cryptographic operation (FCS_COP.1)
- 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)
- Stored data integrity monitoring and action (FDP_SDI.1)
- User attribute definition (FIA_ATD.1)
- User authentication before any action (FIA_UAU.2)

- User Identification before any action (FIA_UID.2)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Static attribute initialisation (FMT_MSA.3)
- Security management roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)
- TOE Security Functions testing (FPT_TST.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

Conformément au guide pour l'évaluation « The application of CC to IC » (cf. [CC_IC]), les livraisons considérées sont :

- la livraison du code des applications embarquées au fabricant du micro-circuit,
- la livraison des informations nécessaires au fabricant de réticules,
- la livraison des réticules au fabricant du micro-circuit,
- la livraison des micro-circuits au responsable de l'étape suivante (mise en micro-module, encartage).

Les différents sites impliqués sont identifiés au §1.2 du présent rapport. Tous les flux relatifs à l'ensemble des sites sont évalués et audités régulièrement dans le cadre des différentes évaluations et ré-évaluations des produits ATMEL (voir en particulier le rapport de certification [2004/02]). Deux centres d'évaluation réalisent ces tâches : le CEA/LETI pour les sites situés au Royaume-Uni, et le CEACI pour les sites situés en France. Les conclusions des travaux associés sont satisfaisantes (cf. [Visite]). Ces flux n'ont donc pas fait l'objet d'évaluation pour ce projet.
Par ailleurs, le produit évalué ne comportant pas d'application embarquée spécifique, il ne nécessite pas de phases d'installation, génération et démarrage spécifiques.

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	[2004/02]
ADO_IGS.1	Installation, generation, and start-up procedures	[2004/02]

2.7.5. L'évaluation de la documentation d'exploitation

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.

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 sur la plate-forme suivante : micro-circuit AT90SC7272C, référence AT578B3 révision D, avec un OS de test, en mode « ouvert[1] ».

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

[1] mode permettant de charger et d'exécuter du code natif en EEPROM et de déconnecter les mécanismes sécuritaires paramétrables

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

Le micro-circuit AT90SC7272C est fonctionnellement similaire au micro-circuit déjà évalué AT90SC9608RC (cf. [2003/11], [2004/35]). L'analyse de l'évaluateur a permis de conclure qu'il n'y avait pas nécessité de réaliser de travaux de mise à jour pour la famille d'assurance MSU.

Seules les fonctions suivantes ont fait l'objet d'une estimation du niveau de résistance intrinsèque :
- authentification de l'administrateur en mode test et en mode package,
- protection de l'accès à la mémoire de test,
- audit des événements,
- non-observabilité.

Le niveau de résistance de ces fonctions est jugé élevé : **SOF-High**.
Cette cotation a été réalisée conformément au guide « Application of attack potential to smart-card » (cf. [CC_AP]).

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 plate-forme suivante : micro-circuit AT90SC7272C, référence AT578B3 révision D, avec un OS de test, en mode « ouvert[1] ».

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	[2004/35]
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

Le produit évalué offre les services cryptographiques suivants :
- accélérateur de calcul cryptographique DES/3DES,

[1] mode permettant de charger et d'exécuter du code natif en EEPROM et de déconnecter les mécanismes sécuritaires paramétrables

- accélérateur de calcul RSA (avec et sans CRT),
- accélérateur de calcul SHA-1.

Ces services ne peuvent cependant pas être analysés d'un point de vue cryptographique car ils ne concourent pas à la sécurité propre du produit ; leur résistance dépend de leur emploi par l'application embarquée sur le micro-circuit.

2.7.9. L'analyse du générateur d'aléas

Le produit évalué offre un générateur d'aléas qui peut être utilisé par le logiciel embarqué. Ce générateur a fait l'objet d'une analyse par la DCSSI.
Cette analyse n'a permis de mettre en évidence aucun biais statistique élémentaire. Ceci ne permet pas de dire que les données générées sont réellement aléatoires mais assure que le générateur ne souffre pas de défaut majeur de conception.

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.

Ce certificat donne une appréciation de la résistance du produit <*nom 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 de l'évaluation du produit complet, laquelle pourra être réalisée en utilisant les résultats de cette évaluation.

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 [GUIDES].
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]) :

- la communication entre un produit développé sur le micro-circuit sécurisé et d'autres produits doit être sécurisée (en termes 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.

3.3. 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 et AVA_VLA.4.

Annexe 1. 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 2. Références documentaires du produit évalué

[2003/11]	Rapport de certification 2003/11 Micro-circuit ATMEL AT90SC9608RC, 22 septembre 2003 SGDN/DCSSI
[2003/28]	Rapport de certification 2003/28 Micro-circuit ATMEL AT90SC9608RC rev. E, 18 décembre 2003 SGDN/DCSSI
[2004/02]	Rapport de certification 2004/02 Micro-circuit ATMEL AT90SC6404R rev. F, 19 février 2004 SGDN/DCSSI
[2004/05]	Rapport de certification 2004/02 Micro-circuit ATMEL AT90SC6404R rev. F, 19 février 2004 SGDN/DCSSI
[2004/35]	Rapport de certification 2004/05 Micro-circuit ATMEL AT90SC9608RC rev. F, 2 avril 2004 SGDN/DCSSI
[CONF]	Liste de configuration du design : • Archer Design Configuration List, Référence : Archer_DCL_V1.0_01Apr04, ATMEL Liste de configuration de la fabrication : • Archer Manufacturing Configuration List, Référence : Archer_MCL_V1.1_25May04, ATMEL Liste des patterns et des masques : • Archer Pattern and Mask List, Référence : Archer_PML_RevD_04Apr04, ATMEL Liste des fournitures ATMEL : • Archer Deliverables List, Référence : Archer EDL-11Oct04, ATMEL

[GUIDES]	Un document générique sert d'interface pour toute la documentation d'utilisation : • AT90SC Guidance Interface Document, Référence : AT90SC_GUID_V1.0_09Feb04 ATMEL Les documents associés sont : • AT90SC7272C Technical Data Sheet, Référence : TPR0110BX-09Feb04, ATMEL • Archer Wafer Saw Recommendations, Référence : Archer_WSR_V1.0_10Jun04, ATMEL • AT90SC Addressing Modes and Instruction Set, Référence : 1323, Rev. B, 26Feb01, ATMEL • Checksum Accelerator use on the AT90SC ASL4 products, Référence : TPR0065A-02Jul02, ATMEL • Security recommendation for AT90SC ASL4, Référence : TPR0066D-23Nov04 ATMEL • Generating unpredictable random numbers on AT90SC Family devices, Référence : 1573CX rev. C, 21/03/03 ATMEL • App note : Using the supervisor and user modes on the AT90SC ASL4 products, Référence : TPR0095A-11Mar03 ATMEL • Securing the DES/TDES on the AT90SC ASL 4, Référence : TPR0063D 27Feb04, ATMEL • Securing RSA Operation in AT90SC ASL4 products, Référence : TPR0062C-15May03 ATMEL
[RTE]	Rapport technique d'évaluation complet : • Evaluation technical report of ARCHER projects, Référence : ARC_RTE v2.0 CEACI Pour le besoin des évaluations en composition, une version diffusable du document a été validée :

	• ETR Lite for composition - AT90SC7272C revD, Référence : ARC_RTElite v2.0 CEACI
[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*
[ST]	Cible de référence pour l'évaluation : • Archer Security Target, Référence : Archer_ST_V1.2_17Nov04 ATMEL Pour les besoins de la reconnaissance internationale, la cible suivante a été fournie et validée dans le cadre de cette évaluation : • AT90SC7272C Security Target Lite, Référence : TPG0054A_08Dec04 ATMEL
[Visite]	Rapport de synthèse des visites relatives aux sites situés au Royaume Uni : • IO Project - ATMEL East Kilbride Audit, Référence : IO.CR.005 version 1.0 CEA/LETI Rapport de synthèse des visites relatives aux sites situés en France : • Audit Status for ATMEL, Référence : Audit Status for ATMEL version 1.0 CEACI

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, 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. Le contenu des Critères Communs version 2.1 est identique à celui de la Norme Internationale ISO/IEC 15408:1999, comportant les trois documents suivants: 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.
[CEM]	Common Methodology for Information Technology Security Evaluation : Part 2: Evaluation Methodology, August 1999, version 1.0, ref CEM- 99/045.
[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.
[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