PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2006/20

Microcontrôleur sécurisé ATMEL AT90SC320288RCT/AT90SC144144CT rev. G

Paris, le 16 novembre 2006

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2006/20

Microcontrôleur sécurisé ATMEL AT90SC320288RCT/AT90SC144144CT rev. G

Développeur : Atmel SmartCard ICs

Critères Communs version 2.2

EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4)

conforme au profil de protection PP/9806

Commanditaire : Atmel SmartCard ICs

Centre d'évaluation : CESTI LETI

Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA :
ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, 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] 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 septembre 2006, 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, le Japon, la Norvège, les Pays-Bas, la Corée du Sud et l'Espagne ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Suède, la Turquie, la République Tchèque, Singapour, l'Inde et le Danemark.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est le microcontrôleur sécurisé AT90SC320288RCT, référence AT58807 révision G.
Ce microcontrôleur inclut une bibliothèque logicielle cryptographique optionnelle, stockée en mémoire ROM : Toolbox 3.x en version 00.03.01.04.
La référence AT90SC144144CT identifie le même composant matériel, mais embarquant un logiciel de configuration en mémoire ROM : « Embedded ROM Rev. 1.0 ». Il peut alors être considéré comme un composant « flash », le logiciel embarqué étant alors chargé après fabrication en mémoire EEPROM.
Ce microcontrôleur 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 microcontrôleur:

Le microcontrôleur est développé et testé par :

Atmel East Kilbride

Maxwell Building
Scottish Enterprise technology Park
East Kilbride, G75 0QR
Ecosse, Royaume-Uni.

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

Atmel Rousset

Z.I. Rousset Peynier
13106 Rousset Cedex
France.

Les réticules du microcontrôleur sont fabriqués par :

Toppan Photomasks France

224, bd John Kennedy
91100 Corbeil Essonnes
France.

1.3. Description du produit évalué

Le microcontrôleur comporte trois modes d'utilisation :

- un mode « Test », dans lequel le microcontrôleur 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 requiert une authentification de l'administrateur. Il 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 découpage du « wafer ». L'interface de test n'est alors plus accessible ;
- un mode « utilisateur », dans lequel le microcontrôleur fonctionne sous le contrôle du logiciel embarqué de la carte à puce. Les utilisateurs finaux ne peuvent utiliser le microcontrôleur que dans ce mode ;
- un mode « diagnostic », utilisé lors du retour de pièces défectueuses et permettant d'effectuer des 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 requiert une authentification de l'administrateur et n'est utilisable que par le personnel autorisé de l'équipe du fabricant et dans un environnement sécurisé.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, 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.

1.3.1. Architecture

Le microcontrôleur AT90SC320288RCT / AT90SC144144CT est constitué des éléments suivants :
- CPU AVR Risc ;
- 320ko de mémoire ROM en configuration « classique » (AT90SC320288RCT) pour le stockage des programmes ;
- 288ko de mémoire EEPROM pour le stockage des programmes et des données en configuration « classique », et en configuration « flash » (AT90SC144144CT), 144ko de mémoire « flash » pour le stockage des programmes, 144ko de mémoire EEPROM pour le stockage des programmes et des données ;
- La mémoire EEPROM comprend 128 octets 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 octets accessibles par bit, une pompe de charge et ses oscillateurs ;
- 8ko de mémoire RAM statique ;
- un accélérateur de calcul de checksum 32 bits (support à la détection d'erreurs sur les données ou programmes en mémoire) ;
- un périphérique CRC-16/32 (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 32-bits (AdvX) incluant sa librairie logicielle de 32ko en ROM (boîte à outils cryptographique) permettant d'accélérer les calculs RSA (avec et sans CRT), SHA-1 et de générer des nombres premiers ;
- des détecteurs tension, fréquence, température et lumière ultraviolette ;
- un firewall protégeant l'accès à toutes les mémoires et tous les périphériques, comportant cinq modes d'utilisation ;

- un régulateur de tension (le microcontrôleur fonctionne dans une gamme de tension de 3.0V à 5.0V) ;
- 2 Timers ;
- 1 port série SPI et 1 port 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.

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 :

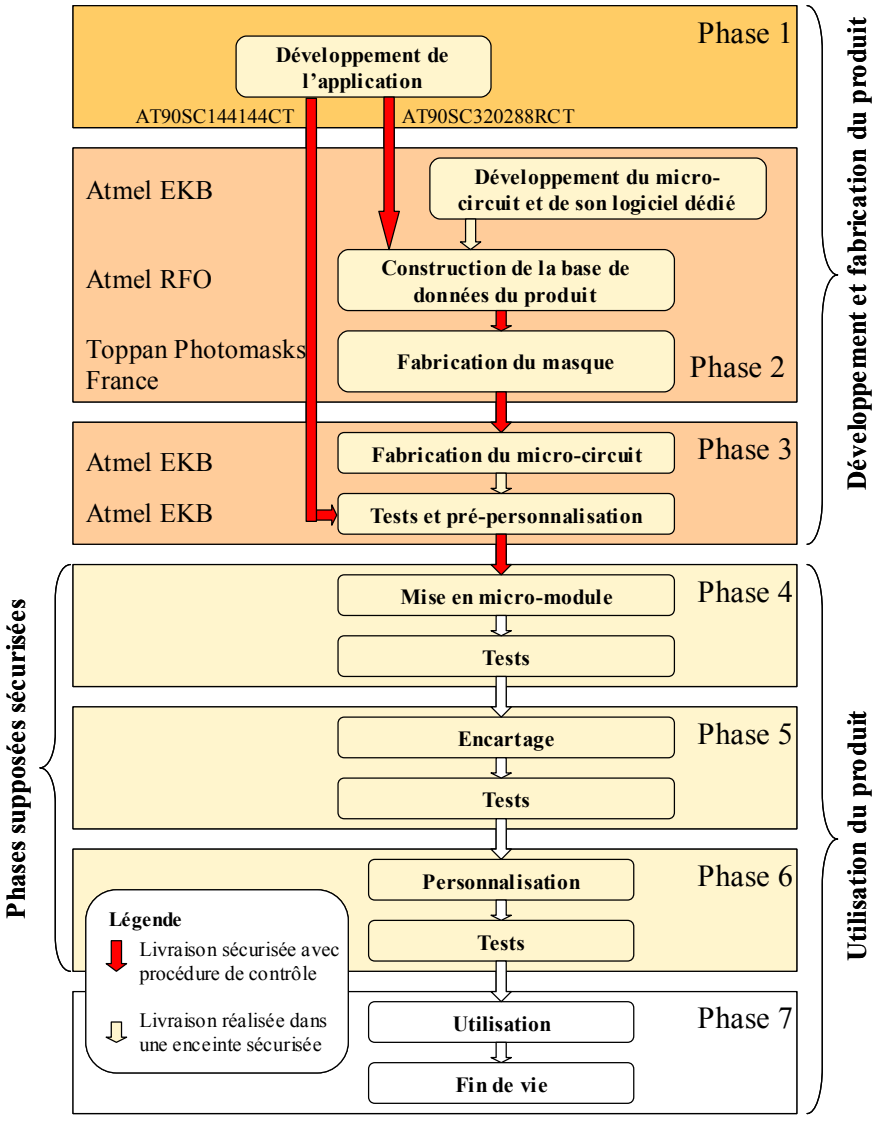

Figure 1 - Cycle de vie du produit

1.3.3. Périmètre et limites du produit évalué

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur seul et à la bibliothèque cryptographique, cette dernière étant optionnelle.

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).
Ce microcontrôleur comporte une spécificité en configuration « flash » (AT90SC144144CT) : le logiciel applicatif n'est pas embarqué en mémoire ROM (logiciel figé lors de la phase de fabrication) mais en mémoire Flash. Il peut donc être chargé ultérieurement à la phase de fabrication du microcontrôleur. Pour la présente évaluation, il est considéré que le logiciel applicatif est embarqué dans le microcontrôleur dans les locaux d'Atmel et sous sa responsabilité.

2. L'évaluation

2.1. Contexte

Le produit évalué est une évolution du microcontrôleur ATMEL AT90SC12836RCT rev. E certifié en 2005 sous la référence 2005/20 (cf. [2005/20]).
Une partie des verdicts de la présente évaluation s'appuie donc sur les résultats des travaux menés lors de la précédente évaluation.

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].
Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au CESTI, validées par la DCSSI et compatibles avec le document [AIS34] ont été utilisées.

2.3. Commanditaire

ATMEL Smart Card ICs

Maxwell Building
Scottish Enterprise technology Park
East Kilbride, G75 0QR
Ecosse, Royaume-Uni

2.4. 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 : cesti.leti@cea.fr

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

CEACI (Thales Security Systems – CNES)

18 avenue Edouard Belin
31401 Toulouse Cedex 9
France

Téléphone : +33 (0)5 61 27 40 29

Adresse électronique : ceaci@cnes.fr

2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée de mars 2006 à septembre 2006.

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
+ ADV_IMP.2	Implementation of the TSF
+ ALC_DVS.2	Sufficiency of security measures
+ AVA_MSU.3	Analysis and testing for insecure state
+ AVA_VLA.4	Highly resistant

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

2.7.2. L'évaluation de l'environnement de développement

Le développement du microcontrôleur implique l'ensemble des sites identifiés au §1.2.

Les environnements de développement des sites impliqués sont évalués et audités de façon continue dans le cadre des différentes évaluations et réévaluations des produits ATMEL. 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 associées à ces travaux sont satisfaisantes.

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

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

2.7.3. L'évaluation de la conception du produit

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

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :

- Potential violation analysis (FAU_SAA.1)
- Cryptographic Key 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)
- Specification of management functions (FMT_SMF.1)
- Security management roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)
- TSF 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 Integrated Circuits » (cf. [CC_IC]), les livraisons considérées sont :

- la livraison du code des applications embarquées au fabricant du microcontrôleur;
- la livraison des informations nécessaires au fabricant du masque ;
- la livraison du masque au fabricant du microcontrôleur;
- la livraison des microcontrôleurs 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 de façon continue dans le cadre des différentes évaluations et réévaluations des produits ATMEL. 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 associées à ces travaux sont satisfaisantes.

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

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

2.7.5. L'évaluation de la documentation d'exploitation

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 microcontrôleur 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.

Dans le cadre de cette évaluation, ces rôles sont rappelés dans la cible de sécurité [ST] : les utilisateurs sont définis comme étant les personnes pouvant mettre en œuvre les fonctionnalités du microcontrôleur, sa bibliothèque logicielle et son logiciel applicatif. Cette définition comprend tous les utilisateurs utilisant le produit en mode « user » : l'émetteur de la

carte mais également le développeur du logiciel embarqué, le responsable de l'encartage et la personne chargée d'intégrer la carte dans son système d'utilisation finale.

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 microcontrôleur, seules les interfaces d'administration propres au microcontrôleur 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 : microcontrôleur AT90SC320288RCT / AT90SC144144CT, référence AT58807 révision G 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 :

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

2.7.7. L'évaluation des vulnérabilités

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

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

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 : microcontrôleur AT90SC320288RCT / AT90SC144144CT, référence AT58807 révision G 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** (AVA_VLA.4). Cette cotation est réalisée conformément au guide « Application of attack potential to smart-card » (cf. [CC AP]).

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.3	Analysis and testing for insecure state	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

2.7.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

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

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 AT90SC320288RCT / AT90SC144144CT, référence AT58807 révision G 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 microcontrôleur ne pourra être appréciée qu'au travers de l'évaluation du produit complet, laquelle pourra être réalisée en se basant sur 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 microcontrôleur avec son application embarquée (extraits de la cible de sécurité [ST]) :

- la communication entre un produit développé sur le microcontrôleur 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, AVA_MSU.3, 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

[2005/20]	Rapport de certification 2005/20 Micro-circuit ATMEL AT90SC12836RCT rev. E, 9 août 2005 SGDN/DCSSI
[CONF]	Liste de configuration du design : • Longbow Design Configuration List, Référence : Longbow_DCL_V1.4_25Sep06 ATMEL Liste de configuration de la fabrication : • Longbow Manufacturing Configuration List, Référence : Longbow_MCL_V1.4_25Sep06 ATMEL Liste des patterns et des masques : • Longbow Pattern and Mask List, Référence : AT58807_PML_Design rev G, 25Sep06 ATMEL Liste de configuration de la librairie cryptographique : • Toolbox 3.x Crypto Toolbox Configuration List Référence : TPR0150DX_06Sep05 Liste de configuration du ROM code pour la configuration « flash » : • AT90SC144144CT ROM Configuration List, Référence : TPR0239AX_09Jun06 ATMEL Liste des fournitures ATMEL : • Longbow CC Deliverables List, Référence : Longbow_ EDL_24May06. ATMEL
[GUIDES]	Un document générique sert d'interface pour toute la documentation d'utilisation : • AT90SC CC AGD Interface, Référence : AT90SC_GUID_V1.4_05Jul05 ATMEL Les documents associés sont : • AT90SC320288RCT Technical Datasheet, Référence : TPR0115AX_03Jun04 ATMEL • AT90SC320288RCT 58807 Errata, Référence : TPR0151BX_30May05 ATMEL

	• AT90SC144144CT Configuration of AT90SC320288CT, Référence : TPR0143BX_04Jun06 ATMEL • Full NVM Erase Errata (AT90SC320288RCT/ AT90SC144144RCT), Référence : TPR0254AX_03Oct06 ATMEL • Toolbox 3.x on AT90SCxxxxC Family with AdvX, Référence : TPR0133CX-26Jul05 ATMEL • AT90SC Addressing Modes and Instruction Set, Référence : 1323C-03May04 ATMEL • Security Recommendations for AT90SC ASL4 Products, Référence : TPR0066G-05Jul05 ATMEL • Generating unpredictable random numbers on the AT90SC family devices, Référence : 1573CX_SMIC_21mar03 ATMEL • Using the supervisor and user modes on the AT90SC ASL4 products, Référence : TPR0095A-11Mar03 ATMEL • Secured Hardware DES/TDES on AT90SC ASL4 Products, Référence : TPR0063E-05Aug04 ATMEL • Securing Cryptographic Operations on AT90SC Products with Toolbox 3.x, Référence : TPR0141CX_03Apr06 ATMEL • AdvX for AT90SC Family, Référence : TPR0116AX-26Apr04 ATMEL • Efficient use of AdvX for Implementing Cryptographic Operations, Référence : TPR0142CX_14Jun05 ATMEL • Checksum Accelerator use on the AT90SC ASL4 products, Référence : TPR0065A-02Jul02 ATMEL

	• Wafer Saw Recommendations, Référence : TPG0079A_13Jun05 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]	Rapport technique d'évaluation complet : • LONGBOW Project - Evaluation Technical Report, Référence : LETI.CESTI.LON.RTE.003, Version:1.1 CEA/LETI Pour le besoin des évaluations en composition, une version diffusable du document a été validée : • LONGBOW Project - Evaluation Technical Report Lite, Référence : LETI.CESTI.LON.RTE.004, Version:1.1 CEA/LETI
[ST]	Cible de référence pour l'évaluation : • Longbow Security Target, Référence : Longbow_ST_v1.3_03Aug06 ATMEL Pour les besoins de la reconnaissance internationale, la cible suivante a été fournie et validée dans le cadre de cette évaluation : • AT90SC320288RCT / AT90SC144144CT Security Target Lite, Référence : TPG0132B_25Sep06 ATMEL

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, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[CC AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002.
[COMP]	Common Criteria supporting documentation – ETR-lite for composition: Annex A - Composite smartcard evaluation : Recommended best practice, Version 1.2, March 2002.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[AIS34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004

Toute correspondance relative à ce rapport doit être adressée au :

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

certification.dcssi@sgdn.pm.gouv.fr