PREMIER MINISTRE

Secrétariat général de la Défense nationale

Direction centrale de la sécurité des systèmes d'information

Schéma Français

d'Évaluation et de Certification

de la Sécurité des Technologies de l'Information

Rapport de certification 2002/03

Micro-circuit ATMEL AT05SC1604R

(référence AT568C6 rev. H)

Mars 2002

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma Français
d'Évaluation et de Certification
de la Sécurité des Technologies de l'Information

CERTIFICAT 2002/03

Micro-circuit ATMEL AT05SC1604R

(référence AT568C6 rev. H)

Développeur : ATMEL Smart Card ICs

Critères Communs
EAL4 Augmenté
conforme au profil de protection PP/9806

Commanditaire : ATMEL Smart Card ICs
Centre d'évaluation : CEA LETI

Le 25 mars 2002,

Le Directeur central de la sécurité
des systèmes d'information
Henri Serres

Ce produit a été évalué par un centre d'évaluation de la sécurité des TI conformément aux Critères Communs pour l'évaluation de la sécurité des TI version 2.1 et à la méthodologie commune pour l'évaluation de la sécurité des TI version 1.0.

Ce certificat ne s'applique qu'à la version évaluée du produit dans sa configuration d'évaluation et selon les modalités décrites dans le rapport de certification associé. L'évaluation a été conduite en conformité avec les dispositions du Schéma français d'évaluation et de certification de la sécurité des TI. Les conclusions du centre d'évaluation enregistrées dans le rapport technique d'évaluation sont cohérentes avec les éléments de preuve fournis.

Ce certificat ne constitue pas en soi une recommandation du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise. Ce certificat n'exprime directement ou indirectement aucune caution du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

Organisme de certification :
Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Chapitre 1

Résumé

1.1 Objet

1 Ce document représente le rapport de certification du micro-circuit ATMEL AT05SC1604R (référence AT568C6 rev. H) développé par ATMEL Smart Card ICs.

2 Le micro-circuit est destiné à être inséré dans un support plastique pour constituer une carte à puce. Les usages de cette carte sont ensuite 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.

3 Le développeur de la cible d'évaluation est ATMEL Smart Card ICs :

- ATMEL Smart Card ICs
  Maxwell Building
  Scottish Enterprise Technology Park
  East Kilbride, G75 0QF
  Ecosse.

4 La cible d'évaluation est produite sur le site d'ATMEL à Rousset :

- ATMEL
  Z.I. Rousset Peynier
  13106 Rousset Cedex
  France.

5 La société DuPont Photomasks a également participé à la production de la cible d'évaluation en tant que fabricant des réticules :

- DuPont Photomasks
  Avenue Victoire, Z.I.
  13106 Rousset Cedex
  France.

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

7 Le niveau d'assurance atteint est le niveau EAL4 augmenté des composants d'assurance suivants tels que décrits dans la partie 3 des Critères Communs [CC] :

- ADV_IMP.2 "Implémentation de la TSF",
- ALC_DVS.2 "Caractère suffisant des mesures de sécurité",

- ALC_FLR.1 “Correction élémentaire d’anomalies”,
- AVA_VLA.4 “Résistance élevée”.

8 De plus, la cible d’évaluation répond aux exigences du profil de protection “Smartcard Integrated Circuit” enregistré auprès de la DCSSI [PP/9806].

1.2 Contexte de l’évaluation

9 L’évaluation s’est déroulée de mai 2001 à janvier 2002.

10 La cible d’évaluation est un produit directement dérivé du micro-circuit AT05SC3208R ayant fait l’objet d’un certificat en 2001 [2001/02]. Les produits se distinguent uniquement par la taille de leurs mémoires ROM et EEPROM. Une partie des verdicts de la présente évaluation s’appuie donc sur les résultats des travaux menés lors de la précédente évaluation.

11 Le commanditaire de l’évaluation est la société ATMEL Smart Card ICs :

- ATMEL Smart Card ICs
  Maxwell Building
  Scottish Enterprise Technology Park
  East Kilbride, G75 0QF
  Ecosse.

12 L’évaluation a été conduite par le Centre d’Evaluation de la Sécurité des Technologies de l’Information du CEA Leti (ci-après «l’évaluateur») :

- CESTI LETI
  CEA Grenoble
  17, rue des Martyrs
  38054 Grenoble Cedex 9
  France.

13 Les tâches d’évaluation associées à l’environnement de production de ATMEL Rousset ont été réalisées par le CEACI :

- CEACI (THALES Microelectronics-CNES)
  18 avenue Edouard Belin
  31441 Toulouse Cedex
  France.

Chapitre 2

Description de la cible d'évaluation

2.1 Périmètre de la cible d'évaluation

14 La cible d'évaluation est le micro-circuit ATMEL AT05SC1604R (référence AT568C6 rév. H). L'identification du micro-circuit est possible par inspection optique.

15 Le micro-circuit AT05SC1604R est bâti autour du micro-contrôleur Motorola M68HC05SC. Il embarque 16Ko de mémoire ROM et 4Ko de mémoire EEPROM. Il dispose également d'un générateur de nombres aléatoires.

16 Les modes d'utilisation de la cible d'évaluation identifiés dans la cible de sécurité sont les suivants :

- mode Test : mode de test uniquement actif en phase de production du micro-circuit et dans un environnement sécurisé.
- mode User : mode normal d'utilisation.

2.2 Cycle de vie

17 Le cycle de vie d'une carte à puce est constitué des phases suivantes :

- phase 1 : développement des logiciels embarqués (systèmes d'exploitation, logiciels applicatifs),
- phase 2 : développement du micro-circuit,
- phase 3 : production du micro-circuit,
- phase 4 : mise en micro-modules (ateliers de micro-électronique),
- phase 5 : encartage,
- phase 6 : personnalisation,
- phase 7 : utilisation du produit final.

18 Les phases 2 et 3 constituent les phases de construction de la cible d'évaluation.

19 Les phases 4 à 7 sont les phases d'exploitation de la cible d'évaluation.

2.3 Fonctions de sécurité évaluées

20 Les fonctions de sécurité évaluées sont les suivantes :

- Contrôle du passage en mode TEST,
- Contrôle d'accès aux mémoires en mode TEST,
- Blocage du mode TEST,

- Test du micro-circuit,
- Détection d'erreurs mémoire,
- Contrôle d'accès aux mémoires en exploitation,
- Détection d'évènements de sécurité,
- Réaction aux évènements de sécurité,
- Non-observabilité des opérations réalisées par le micro-circuit,
- Génération de nombres aléatoires.

2.4 Documentation disponible

21 La documentation disponible pour l'utilisation du micro-circuit est la suivante :

a) la «technical Datasheet» : AT05SC1604R technical data, réf. 1522BX, 12/10/00.

b) les notes d'applications (Application Notes) :

- Europa Application Note for CRC, réf. Euro_APP_016 v1.1,
- Europa Application Note for RNG, réf. Euro_APP_017 v1.1,
- AT05SC1604R Supp. Security Application Note, AT05_APP_016, V1.5.

Chapitre 3

Résultats de l'évaluation

3.1 Exigences d'assurance

Classes d'Assurance	Composants d'Assurance
Cible de sécurité	ASE_INT.1 : Introduction de la ST ASE_DES.1 : Description de la TOE ASE_ENV.1 : Environnement de sécurité ASE_OBJ.1 : Objectifs de sécurité ASE_PPC.1 : Annonce de conformité à un PP ASE_REQ.1 : Exigences de sécurité des TI ASE_SRE.1 : Exigences de sécurité des TI explicitement énoncées ASE_TSS.1 : Spécifications globales de la TOE
Gestion de configuration	ACM_AUT.1 : Automatisation partielle de la CM ACM_CAP.4 : Aide à la génération et procédures de réception ACM_SCP.2 : Couverture du suivi des problèmes par la CM
Livraison et exploitation	ADO_DEL.2 : Détection de modifications ADO_IGS.1 : Procédures d'installation, de génération et de démarrage
Développement	ADV_FSP.2 : Définition exhaustive des interfaces externes ADV_HLD.2 : Conception de haut niveau - identification des sous-sytèmes dédiés à la sécurité ADV_IMP.2 : Implémentation de la TSF ADV_LLD.1 : Conception de bas niveau descriptive ADV_RCR.1 : Démonstration de correspondance informelle ADV_SPM.1 : Modèle informel de politique de sécurité de la TOE
Guides	AGD_ADM.1 : Guide de l'administrateur AGD_USR.1 : Guide de l'utilisateur

Classes d'Assurance	Composants d'Assurance
Support au cycle de vie	ALC_DVS.2 : Caractère suffisant des mesures de sécurité ALC_FLR.1 : Correction d'anomalies élémentaire ALC_LCD.1 : Modèle de cycle de vie défini par le développeur ALC_TAT.1 : Outils de développement bien définis
Tests	ATE_COV.2 : Analyse de la couverture ATE_DPT.1 : Tests : conception de haut niveau ATE_FUN.1 : Tests fonctionnels ATE_IND.2 : Tests indépendants - échantillonnage
Estimation des vulnérabilités	AVA_MSU.2 : Validation de l'analyse AVA_SOF.1 : Évaluation de la résistance des fonctions de sécurité de la TOE AVA_VLA.4 : Résistance élevée

22 Pour tous les composants d'assurance ci-dessus, un verdict «Réussite» a été émis par l'évaluateur.

23 Les travaux d'évaluation menés sont décrits dans le Rapport Technique d'Evaluation [RTE].

24 L'évaluateur a examiné l'ensemble de la conception du micro-circuit jusqu'aux schémas descriptifs et au langage VHDL pour s'assurer que les fonctions de sécurité sont bien implémentées dans la cible d'évaluation.

25 Des audits ont été menés sur les sites suivants pour s'assurer de l'utilisation effective de systèmes de gestion de configuration et l'application de mesures de sécurité suffisantes pour protéger les données sensibles utilisées :

- ATMEL East Kilbride (Ecosse) pour la conception du micro-circuit,
- DuPont Photomasks Rousset (France) pour la fabrication des réticules,
- ATMEL Rousset (France) pour la production des microcircuits.

26 La seule fonction identifiée dans la cible de sécurité réalisée au moyen d'un mécanisme faisant appel à un calcul probabilistique ou permutationel est la fonction d'entrée en mode Test. L'évaluateur a analysé les documents fournis par le développeur et a mené sa propre analyse pour confirmer que cette fonction satisfait bien la résistance SOF-high exigée dans la cible de sécurité.

3.2 Tests fonctionnels et de pénétration

3.2.1 Tests développeur

27 Le développeur a fourni la documentation de test fonctionnel du produit. Les tests ont été réalisés par ATMEL sur son site de Eastkilbride (Ecosse).

28 Les tests fournis par le développeur sont des tests matériels des fonctions de sécurité réalisés au cours de la caractérisation du micro-circuit (avant sa production à grande échelle) puis de sa production.

3.2.2 Tests évaluateur

29 L'évaluateur a réalisé également des tests fonctionnels pour s'assurer par échantillonnage que les fonctions de sécurité identifiées dans la cible de sécurité sont bien réalisées par le produit en évaluation.

30 L'évaluateur a également mené une analyse de vulnérabilités, confirmée par des tests de pénétration, pour s'assurer qu'un attaquant disposant d'un potentiel d'attaque élevé (composant AVA_VLA.4) ne peut pas remettre en cause les objectifs de sécurité de la cible d'évaluation suivants :

- la cible d'évaluation doit se prémunir contre les attaques physiques,
- la cible d'évaluation doit se prémunir contre le clonage fonctionnel,
- la cible d'évaluation doit assurer la continuité de ses fonctions de sécurité,
- la cible d'évaluation ne doit pas contenir d'erreurs de conception, d'implémentation ou dans son exécution,
- la cible d'évaluation doit se prémunir contre toute divulgation non autorisée de ces mécanismes de sécurité,
- la cible d'évaluation doit se prémunir contre toute divulgation non autorisée des informations sensibles contenues dans les mémoires,
- la cible d'évaluation doit se prémunir contre toute modification non autorisée des informations sensibles contenues dans les mémoires.

Chapitre 4

Certification

4.1 Verdict

31 Le présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL4 augmenté des composants d'assurances suivants extraits de la partie 3 des Critères Communs [CC] :

- ADV_IMP.2 "Implémentation de la TSF",
- ALC_DVS.2 "Caractère suffisant des mesures de sécurité",
- ALC_FLR.1 "Correction élémentaire d'anomalies",
- AVA_VLA.4 "Résistance élevée".

32 De plus, la cible d'évaluation répond aux exigences du profil de protection "Smartcard Integrated Circuit" enregistré auprès de la DCSSI [PP/9806].

4.2 Recommandations

33 La cible d'évaluation "Micro-circuit ATMEL AT05SC1604R (référence AT568C6 rév. H)" est soumise aux recommandations d'utilisation exprimées ci-dessous.

a) Le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [ST].

b) Les applications destinées à être installées sur le micro-circuit doivent impérativement respecter les guides d'utilisation émis par ATMEL Smart Card ICs et notamment les recommandations de programmation qui y figurent [GUIDE].

4.3 Certification

34 La certification ne constitue pas en soi une recommandation du produit. Elle ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle que des vulnérabilités exploitables n'aient pas été découvertes ; probabilité d'autant plus faible que le niveau d'assurance est élevé.

35 Le certificat ne s'applique qu'à la version évaluée du produit identifiée au chapitre 2. La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	L'addition d'un ou de plusieurs composants d'assurance de la Partie 3 à un EAL ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou son environnement.
Cible d'évaluation	Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Niveau d'assurance de l'évaluation (EAL)	Un paquet composé de composants d'assurance tirées de la Partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Une expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Produit	Un ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.
Profil de protection	Un ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

Annexe B

Références

[CC] Critères Communs pour l'évaluation de la sécurité des technologies de l'information :
- Partie 1 : Introduction et modèle général CCIMB-99-031, version 2.1 Août 1999.
- Partie 2 : Exigences fonctionnelles de sécurité CCIMB-99-032, version 2.1 Août 1999.
- Partie 3 : Exigences d'assurance de sécurité CCIMB-99-033, version 2.1 Août 1999.

[CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information :
- Partie 2 : Méthodologie d'évaluation CEM-99/045, version 1.0 Août 1999.

[PP/9806] Profil de protection «Smartcard Integrated Circuit Protection Profile» version 2.0, septembre 1998.

[2001/02] Certificat 2001/02 «Micro-circuit ATMEL AT05SC3208R (référence AT55898 rév. Q)», janvier 2001.

[ST] - EUROPA AT05SC1604R Security Target, revision 1.1, 29 novembre 2001.
- EUROPA AT05SC1604R Security Target - Lite, Revision 1.2, 22 février 2002.

[RTE] Rapport Technique d'Evaluation, réf. LETI.CESTI.OLY.RTE.001, CEA Leti, 21 janvier 2002.

[GUIDE] - AT05SC1604R technical data, réf. 1522BX, 12/10/00.
- Europa Application Note for CRC, réf. Euro_APP_016 v1.1,
- Europa Application Note for RNG, réf. Euro_APP_017 v1.1,
- AT05SC1604R Supp. Security Application Note, AT05_APP_016, V1.5.

Ce rapport de certification est disponible sur le site internet de la Direction centrale de la sécurité des systèmes d'information à l'adresse suivante :

www.ssi.gouv.fr

Toute correspondance relative à ce rapport de certification 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 07 SP

certification.dcssi@sgdn.pm.gouv.fr