Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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 2002/16

Micro-circuit ATMEL AT05SC1604R

(AT568C6 rev. I)

Août 2002

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

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

CERTIFICAT 2002/16

Micro-circuit ATMEL AT05SC1604R

(AT568C6 rev. I)

Développeur : ATMEL Smart Card ICs

Critères Communs
EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2, ALC_FLR.1, AVA_VLA.4)

Conforme au profil de protection PP/9806

Commanditaire(s) : ATMEL Smart Card ICs
Centre d'évaluation : CEA Leti

Le 12 août 2002,

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

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information publié au journal officiel de la République française le 19 avril 2002.

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.

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

Présentation

Executive Summary

1.1 Objet

Purpose

1 Ce document est le rapport de certification du micro-circuit ATMEL AT05SC1604R (AT568C6 rev. I).

This document is the certification report of the ATMEL AT05SC1604 integrated circuit (AT568C6 rev. I).

2 Ce produit est développé par ATMEL Smart Card ICs :

The developer of the product is ATMEL Smart Card ICs:

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

3 Le produit est fabriqué sur le site d'ATMEL de Rousset :

The product is manufactured in the ATMEL Rousset site:

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

4 La société DuPont Photomasks a également participé à la production du produit en tant que fabricant des réticules :

The DuPont Photomasks company also participates by the manufacturing of the photomasks:

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

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

This evaluation has been performed in conformance with Common Criteria [CC] and with the methodology defined in the CEM [CEM].

6 La cible d'évaluation atteint le niveau d'assurance EAL 4 augmenté des composants d'assurance suivants tirés de la partie 3 des Critères Communs :

The target of the evaluation reaches the EAL 4 assurance level augmented with the following Common Criteria Part 3 components:

- ADV_IMP.2 “Implementation of the TSF”,
- ALC_DVS.2 “Sufficiency of security measures”,
- ALC_FLR.1 "Basic flaw remediation",
- AVA_VLA.4 “Highly resistant”.

7 La cible d’évaluation est conforme au profil de protection PP/9806 [PP/9806].

The target of the evaluation is compliant with the protection profile PP/9806 [PP/9806].

1.2 Contexte de l’évaluation

Evaluation Context

8 La version précédente (révision H) du micro-circuit a été certifiée en mars 2002 (certificat 2002/03) [2002/03]. Ce certificat est couvert par un programme de maintenance PM 2002/02. Ce programme de maintenance permet de suivre les évolutions de la cible d’évaluation, de son environnement de développement et de son environnement d’utilisation. Grâce à la mise en place de ce programme de maintenance, la présente évaluation est réduite à une analyse d’impact sécuritaire des modifications apportées à la révision I.

The previous version of the integrated circuit (revision H) has been certified in march 2002 (certificate 2002/03). This certificate is included in the maintenance programme PM 2002/02. This maintenance programme allows the monitoring of all evolution of the product itself or the evolution of the development environment or of the operational environment. Due to the maintenance programme, this evaluation was limited to the evaluation of the security impact analysis of the new revision of the product.

9 L’évaluation s’est déroulée en juin 2002.

The evaluation has been carried out in june 2002.

10 Le commanditaire de l’évaluation est ATMEL Smart Card ICs :

The sponsor of the evaluation is ATMEL Smart Card ICs:

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

11 L’évaluation a été réalisée par le Centre d’Evaluation de la Sécurité des Technologies de l’Information du CEA Leti :

The evaluation has been performed by the Information Technology Security Evaluation Facility of CEA Leti:

- CESTI LETI
  CEA Grenoble
  17, rue des Martyrs

38054 Grenoble Cedex 9
France.

Chapitre 2

Description de la cible d'évaluation

Description of the Target of Evaluation

2.1 Périmètre de la cible d'évaluation

Scope of the Target of Evaluation

12 La cible d'évaluation est le micro-circuit ATMEL AT05SC1604R (AT568C6 rév. I).

The target of evaluation is the ATMEL AT05SC1604R (AT568C6 rev I) integrated circuit.

13 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 d'aléas.

The integrated circuit is build on the Motorola M68HC05SC microcontroler. It has 16Ko of ROM memory and 4Ko of EEPROM memory. A random number generator is also available in the target of evaluation.

14 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.

The integrated circuit will be used in a smartcard. This smartcard will be used for several applications (banking, pay-tv, ticketing, health,...) depending on the software which is present in the card. This software is outside the target of evaluation.

2.2 Mode d'utilisation de la cible d'évaluation

Target of Evaluation Mode of Operation

15 La cible d'évaluation est évaluée dans les modes suivants :

The target of evaluation is evaluated in the following mode:

- mode Test : mode de test uniquement actif en phase de production du micro-circuit et dans un environnement sécurisé ;
  Test mode: test mode only available in the production phase of the integrated circuit and in a secure environment;
- mode User : mode normal d'utilisation, le logiciel embarqué pilote complètement les fonctionnalités du micro-circuit.
  User mode: normal mode of operation, the embedded software completly controls the functionnality of the integrated circuit.

2.3 Fonctions de sécurité

Security Functions

16 Les fonctions de sécurité de la cible d'évaluation sont décrites dans la cible de sécurité [ST] :

The security functions of the target of evaluations are described in the security tagret [ST]:

- Contrôle du passage en mode TEST,
  test mode entry,
- Contrôle d'accès aux mémoires en mode TEST,
  access privileges in test mode,
- Blocage du mode TEST,
  test mode disable,
- Test du micro-circuit,
  TOE testing,
- Détection d'erreurs de données,
  data error detection,
- Contrôle d'accès aux mémoires en exploitation,
  illegal access and lockout,
- Détection d'évènements de sécurité,
  event audit,
- Réaction aux évènements de sécurité,
  event action,
- Non-observabilité des opérations réalisées par le micro-circuit,
  unobservability of operations,
- Génération d'aléas.
  random number generation.

2.4 Guides d'utilisation

Guidance Document

17 Les guides d'utilisation et d'administration de la cible d'évaluation disponibles sont :

The available guidance documents of the target of evaluation are:

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

b) 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

Evaluation Results

3.1 Exigences de sécurité d'assurance

Security Assurance Requirements

18 La cible d'évaluation a été évaluée au niveau EAL 4 augmenté des composants d'assurance suivants, tirés de la partie 3 des Critères Communs [CC] : ADV_IMP.2, ALC_DVS.2, ALC_FLR.1 et AVA_VLA.4.

The target of evaluation has been evaluated at the EAL4 assurance level augmented with the following Common Criteria Part 3 components: ADV_IMP.2, ALC_DVS.2, ALC_FLR.1 and AVA_VLA.4.

Assurance class	Assurance components
Security Target	ASE Security target evaluation
Configuration management	ACM_AUT.1 Partial CM automation ACM_CAP.4 Generation support and acceptance procedures ACM_SCP.2 Problem tracking CM coverage
Delivery and operation	ADO_DEL.2 Detection of modification ADO_IGS.1 Installation, generation , and start-up procedures
Development	ADV_FSP.2 Fully defined external interfaces ADV_HLD.2 Security enforcing high-level design **ADV_IMP.2 * Implementation of the TSF** ADV_LLD.1 Descriptive of low-level design ADV_RCR.1 Informal correspondance demonstration ADV_SPM.1 Informal TOE security policy model
Guidance documents	AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance
Life cycle support	**ALC_DVS.2 * Sufficiency of security measures** **ALC_FLR.1 * Basic flaw remediation** ALC_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools
Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: high-level design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
Vulnerability assessment	AVA_MSU.2 validation of analysis AVA_SOF.1 Strength of TOE security functions **AVA_VLA.4 * Highly resistant**

* EAL4 augmentations

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

For all the above assurance requirements, a «pass» verdict has been issued by the evaluator.

20 Les travaux d'évaluation qui ont été menés sont décrits dans le Rapport Technique d'Evaluation et le rapport d'analyse d'impact [RTE].

The evaluation tasks which have been done are described in the Evaluation Technical Report [RTE].

21 La plupart des verdicts d'évaluation ont pu être directement repris de l'évaluation de la version précédente de la cible d'évaluation certifiée en mars 2002 [2002/03] et maintenue dans le cadre du programme de maintenance PM 2002/02. Une analyse d'impact sécuritaire a été fournie par le développeur de la cible d'évaluation. La présente évaluation s'est focalisée sur cette analyse d'impact.

A major part of the verdicts are from the evaluation of the previous revision of the target of evaluation certified in march 2002 and maintained with the PM 2002/02 maintenance programme. A security impact analysis has been provided by the developer. The evaluation focused on this security impact analysis.

3.2 Tests fonctionnels et de pénétration

Functional and penetration testing

22 Dans le cadre de cette évaluation, l'évaluateur a vérifié sur le site d'ATMEL à Eastkilbride (Ecosse) que les tests fonctionnels ont bien été menés sur cette nouvelle version de la cible d'évaluation.

During the evaluation, the evaluator checked on site that ATMEL has tested the new revision of the target of evaluation.

23 L'évaluateur a également confirmé que les résultats de l'analyse de vulnérabilité et des tests de pénétration réalisés sur la version H restent exacts.

The evaluator also confirmed that the results of the vulnerability analysis done on the revision H remain valid.

3.3 Cotation des mécanismes cryptographiques

Evaluation of cryptographic mechanisms

24 Les mécanismes de nature cryptographique ont été évalués par la Direction centrale de la sécurité des systèmes d'information. Ils sont compatibles avec le niveau de résistance élevé visé.

The cryptographic mechanisms have been evaluated by the Direction Centrale de la Sécurité des Systèmes d'Information. Their strength is compatible with the level to be reached.

Chapitre 4

Certification

Certification

4.1 Verdict

Verdict

25 Ce présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL 4 augmenté des composants d'assurance suivants tirés de la partie 3 des Critères Communs [CC] :

The present report certifies that the target of evaluation satisfies to the requirements of the EAL 4 assurance level augmented with the following Common Criteria Part 3 components [CC]:

- ADV_IMP.2 "Implementation of the TSF",
- ALC_DVS.2 "Sufficiency of security measures",
- ALC_FLR.1 "Basic flaw remediation",
- AVA_VLA.4 "Highly resistant".

26 La cible d'évaluation est également conforme au profil de protection PP/9806 [PP/9806].

The target of the evaluation is also compliant with the protection profile PP/9806.

4.2 Restrictions

Restriction

27 La cible d'évaluation doit être utilisé dans sa configuration précisée au chapitre 2 et conformément aux procédures d'utilisation et d'administration prescrites dans la cible de sécurité [ST].

The target of evaluation shall be used in the configuration described in the chapter 2 and shall be used in the environnement described in the security target [ST].

28 Les recommandations du développeur exprimées dans les guides d'utilisation doivent impérativement être respectées.

The requirements present in the user and administrattor guidance shall be respected.

4.3 Certification

Certification

29 Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information, publié au journal officiel de la République française le 19 avril 2002.

This certificate is issued within the scope of the «décret 2002-535» of april 18th, 2002 dealing with the evaluation and the certification of the security provided by IT product and systems. The text of the «décret» was published april 19th, 2002 in the «journal officiel de la République française».

30 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.

Certification is not in itself a recommendation of the product. It does not guaranty that the certified product is totally exempt of exploitable vulnerabilities: it still subsist a residual probability that exploitable vulnerabilities have not been discovered: this probability is as low as the assurance level is high.

4.4 Reconnaissance internationale

International recognition

31 Afin de d'éviter les certifications multiples d'un même produit dans différents pays, il existe des accords de reconnaissance des certificats ITSEC et Critères Communs.

In order to avoid multiple certification of the same product in different countries, a mutual recognition of ITSEC and CC certificates was agreed.

32 Ce certificat répond aux exigences de l'accord suivant :

This certificate meets the requirements of the following agreement:

4.4.1 SOG-IS

33 L'accord SOG-IS [SOG-IS] sur la reconnaissance des certificats ITSEC est applicable depuis mars 1998. Cet accord a été signé par l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse. Cet accord a ensuite été étendu aux certificats Critères Communs pour tous les niveaux d'évaluation (EAL1 - EAL7).

The SOGIS-Agreement [SOG-IS] on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates based on the CC was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	Addition d'un ou de plusieurs composants d'assurance de la partie 3 des CC à une échelle prédéfinie d'assurance ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou par son environnement.
Cible d'évaluation	Produit ou système et documentation associée pour (administrateur et utilisateur) qui est l'objet d'une évaluation.
Cible de sécurité	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)	Paquet de composants d'assurance extraits de la partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Produit	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	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 :
- Part 1 : Introduction and general model, august 1999, version 2.1, réf : CCIMB-99-031 ;
- Part 2 : Security functional requirements, august 1999, version 2.1, réf : CCIMB-99-032 ;
- Part 3 : Security assurance requirements, august 1999, version 2.1, réf : CCIMB-99-033.

[CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information :
- Part 2 : Evaluation Methodology, august 1999, version 1.0, réf : CEM-99/045.

[PP/9806] Profil de protection PP/9806, "Smartcard Integrated Circuit, Version 2.0", septembre 1998.

[2002/03] Certificat 2002/03, Micro-circuit ATMEL AT05SC1604R (référence AT568C6 rev. H), Direction Centrale de la Sécurité des Systèmes d'Information, 25 mars 2002.

[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.
- IO internal report, réf. LETI.CESTI.IO.RI.001, CEA Leti, 18 juin 2002.

[SOG-IS] «Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.

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