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 2003/02

ATMEL AT05SC3208R microcontroller
(référence AT568D6 Rev E)

SÉCURITÉ TI CERTIFICATION

Janvier 2003

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma Français

d'Évaluation et de Certification

de la Sécurité des Technologies de l'Information

CERTIFICAT 2003/02

ATMEL AT05SC3208R microcontroller

(référence AT568D6 Rev E)

Développeur(s) : ATMEL Smart Card ICs

Critères Communs

EAL4 Augmenté

(ADV_IMP.2, ALC_DVS.2, AVA_VLA.4, ALC_FLR.1)

Conforme au profil de protection PP/9806

Commanditaire(s) : ATMEL Smart Card ICs

Centre d'évaluation : CEA/LETI

Le 27 janvier 2003,

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 AT05SC3208R (référence AT568D6 Rev E).

This document is the certification report of the ATMEL AT05SC3208R microcontroller (reference AT568D6 Rev E).

2 Ce produit est développé par ATMEL Smart Card ICs sur les sites de East Kilbride et Rousset :

The developer of the target of evaluation is ATMEL Smart Card ICs in the East Kilbride and Rousset site:

- **Atmel East Kilbride**
  Maxwell Building,
  Scottish Enterprise technology Park
  Birniehill Roundabout
  East Kilbride, G75 0QR
  Ecosse

- **Atmel Rousset**
  Z.I. Rousset Peynier
  13106 Rousset Cedex
  France.

3 Ce produit est fabriqué sur les sites d'ATMEL de North Tyneside et d'East Kilbride :

The product is manufactured in the ATMEL North Tyneside and East Kilbride site:

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

4 Les sociétés DuPont Photomasks et Compugraphics ont également participé à la production du produit en tant que fabricant des réticules :

The DuPont Photomasks et Compugraphics companies also participate by the manufacturing of the photomasks:

- **DuPont Photomasks**
  Avenue Victoire, Z.I.

13106 Rousset Cedex
France.

- **Compugraphics International Ltd**
  Newark Road North
  Eastfield industrial Estate
  Glenrothes
  Fife, KY7 4NT
  Ecosse

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 Le produit évalué est un dérivé des micro-circuits suivant déjà certifiés de la famille de composants ATMEL EUROPA : ATMEL AT05SC3208R (référence AT55898 rév. Q) et ATMEL AT05SC1604R (référence AT568C6 rev. I). Une analyse systématique des différences entre les produits déjà certifiés et le présent produit a été menée afin de capitaliser au maximum les travaux des évaluations précédentes qui ne sont pas impactés par les évolutions du produit. Cette réévaluation s'est également fondée sur le programme de maintenance PM 2002/02 des produits déjà cités. Certaines tâches n'ont donc pas été ré-ouvertes par le centre d'évaluation. L'évaluation s'est déroulée de octobre 2002 à décembre 2002.

The evaluated product is a derivative of previously certified microcontroller from he EUROPA family of smartcard devices: ATMEL AT05SC3208R (reference AT55898 rev. Q) and ATMEL AT05SC1604R (reference AT568C6 rev. I). An analysis of the differences between these two certified microcontroller and the current evaluated circuit has been done in order to allow a maximum reuse of previous result that are still valid regarding the evolution of the product. This re-evaluation was also done using the maintenance program of the two certified products mentioned. Therefore, some evaluation tasks were not redone. The evaluation has been carried out from October 2002 to december 2002.

9 Le commanditaire de l'évaluation est ATMEL Smart Card ICs :

The sponsor of the evaluation is ATMEL Smart Card ICs:

- Maxwell Building,
  Scottish Enterprise technology Park
  Birniehill Roundabout
  East Kilbride, G75 0QR
  Ecosse

10 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

11 La cible d'évaluation est le micro-circuit ATMEL AT05SC3208R (référence AT568D6 Rev E).

The target of evaluation is the ATMEL AT05SC3208R microcontroller (reference AT568D6 Rev E).

12 Le micro-circuit est bâti autour du micro-contrôleur 8 bit Motorola M68HC05SC. Il embarque 32Ko de mémoire ROM, 1Ko de mémoire RAM et 8Ko de mémoire EEPROM. Il dispose également d'un générateur d'aléas et d'un coprocesseur DES.

The integrated circuit is build on the 8 bit Motorola M68HC05SC microcontroller. It has 32Ko of ROM memory, 1Ko of RAM memory and 8Ko of EEPROM memory. A random number generator and a hardware DES module are also available in the target of evaluation.

13 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

14 La cible d'évaluation est évaluée dans le mode suivant :

The target of evaluation is evaluated in the mode:

- 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 uniquement 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 fusibles. Le micro-circuit est alors en mode "user".

  "test" mode, in which the microcontroller runs under the control of test software written to EEPROM via a test interface, and in conjunction with stimulus provided by an external test system. This mode is intended to be used solely by authorized development staff in a secure environment. After testing, "test" mode is permanently disabled by blowing fuses and the microcontroller is set to "user mode".

- mode "user" dans lequel le micro-circuit fonctionne sous le contrôle du logiciel embarqué de la carte à puce. Les clients et utilisateurs ne peuvent utiliser le micro-circuit que dans ce mode.
  "user" mode, in which the microcontroller runs under control of the smartcard embedded software. It is intended that customers and end-users will always use the microcontroller in user mode.

2.3 Fonctions de sécurité

Security Functions

15 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 target [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'événements de sécurité,
  Event audit,
- Réaction aux événements de sécurité,
  Event action,
- Non-observabilité des opérations réalisées par le micro-circuit,
  Unobservability of operations,
- Fonctions cryptographiques.
  cryptography.

2.4 Guides d'utilisation

Guidance Document

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

The available guidance documents of the target of evaluation are:

- Sinope CC Guidance, Ref. Sinope_GUID V1.0, 21/08/02,
- Technical Data AT05SC3208R, Ref. 1554BX, 15/05/02,
- CRC Module on the AT05SC Family, Ref. 1536BX, 01/10/02,
- RNG Module on the AT05SC Family, Ref. 1537BX, 28/08/02,
- Europa Test Specification, v0.4,
- Europa Test Mode Entry Specification and Signal Descriptions, Ref. EUROPATME_ARSP, V0.2,

- AT05SC Supplementary Security Application Note, Ref. 1580AX (8 Nov 02),
- Hardware DES on the AT05SC Family, Ref. 1535CX, 24/10/02.

Chapitre 3

Résultats de l'évaluation

Evaluation Results

3.1 Exigences de sécurité d'assurance

Security Assurance Requirements

17 La cible d'évaluation a été évaluée au niveau EAL 4 augmenté des composants d'assurance suivants, extraits 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_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools **ALC_FLR.1 * Flaw remediation**
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

18 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.

19 Les travaux d'évaluation qui ont été menés sont décrits dans le Rapport Technique d'Evaluation [RTE] accompagné de son addendum [RTE add].

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

20 Aucun audit organisationnel n'a été menée car les sites de développement et de fabrication concernés sont couverts par le programme de maintenance PM 2002/02.

No organisational audit has been performed because development and manufacturing site that are concerned are cover by the maintenance program PM 2002/02.

3.2 Tests fonctionnels et de pénétration

Functional and penetration testing

21 Le développeur a fourni sa documentation de test fonctionnel du produit. Ces tests sont réalisés par Atmel sur son site de East Kilbride (Ecosse).

The developer of the target of evaluation has provided its test documentation. Functional testing is performed in the site of Atmel East kilbride (Scotland).

22 L'évaluateur a réalisé de son côté des tests fonctionnels pour s'assurer par échantillonnage que les fonctions de sécurité fonctionnent effectivement. Cette tâche s'est également appuyé sur les résultats de l'évaluation du micro-circuit certifié ATMEL AT05SC3208R (référence AT55898 rév. Q).

The evaluator has performed independent tests to check by sampling that the TOE security functions perform as specified. This task was done using partially the result of the previous evaluation of the certified product ATMEL AT05SC3208R (reference AT55898 rev. Q).

23 L'évaluateur a 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. Ces objectifs sont décrits dans la cible de sécurité [ST], ils concernent principalement les aspects suivants :

The evaluator lead a vulnerability analysis, confirmed by penetration testing, to ensure that an attacker with a high attack potential (AVA_VLA.4 assurance requirements) cannot bypass the security objectives for the target of evaluation. These security objectives are described in the security target [ST], it can be summarised as follow:

- la cible d'évaluation doit se protéger des attaques physiques,
  the TOE must prevent physical tampering with its security critical parts,
- la cible d'évaluation doit empecher son clonage fonctionnel,
  the TOE functionality needs to be protected from cloning,
- la cible d'évaluation doit assurer la continuité de ses fonctions de sécurité,
  the TOE must ensure the continued correct operation of its security functions,
- la cible d'évaluation ne doit pas contenir d'erreur de conception, d'implémentation ou d'exécution,
  the TOE must not contain flaws in design, implementation or operation,
- la cible d'évaluation doit empecher toute divulgation non autorisée de ses mécanismes de sécurité physique,

the TOE shall ensure that the hardware security mechanisms are protected against unauthorized disclosure,

- la cible d'évaluation doit assurer la confidentialité des informations sensibles contenues dans ses mémoires,
  the TOE shall ensure that sensitive information stored in memories is protected against unauthorized access,
- la cible d'évaluation doit assurer l'intégrité des informations sensibles contenues dans ses mémoires,
  the TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification,
- la cible d'évaluation doit offrir des services de calculs cryptographiques afin d'assurer l'intégrité et la confidentialité des données sensibles,
  Cryptographics capability shall be available for users to maintain integrity and confidentiality of sensitive data.

3.3 Cotation des mécanismes cryptographiques

Evaluation of cryptographic mechanisms

24 La cible d'évaluation ne dispose pas de fonctions utilisant des mécanismes de nature cryptographique pour assurer sa propre sécurité.

The target of evaluation does not use for its own security any functions based on cryptographic mechanisms.

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 extraits 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 [PP/9806].

4.2 Restrictions

Restriction

27 La cible d'évaluation doit être utilisée dans la 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 environment 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 administrator 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 related to 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.

Certification is not in itself a recommendation of the product. It does not guaranty that the certified product is totally exempt of exploitable vulnerabilities.

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 des accords suivants :

This certificate meets the requirements of the following agreements:

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 CC certificates 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.

[ST] Sinope Security Target, reference Sinope_ST_v1.2 (10 Jan 03).

[ST-Lite] Sinope Security Target Lite, reference Sinope_ST_Lite V1.1 (29 Jan 03).

[RTE] Sinope Evaluation Technical Report, reference: LETI.CESTI.SIN.RTE.001.

[RTE add] Addendum to SINOPE ETR (SIN.RTE.001), reference LETI.CESTI.SIN.RTE.002.

[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