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 2002/24

ATMEL AT90SC19264RC microcontroller
(AT568D5 rev F)

Novembre 2002

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma français
d'évaluation et de certification
de la sécurité des technologies de l'information

CERTIFICAT 2002/24

ATMEL AT90SC19264RC microcontroller

(AT568D5 rev F)

Développeur : ATMEL Smart Card ICs

Critères Communs

EAL4 Augmenté

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

Conforme au profil de protection PP/9806

Commanditaire : ATMEL Smart Card ICs

Centre d'évaluation : CEACI

Le 4 novembre 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 AT90SC19264RC (AT568D5 rev F).

This document is the certification report of the AT90SC19264RC (AT568D5 rev F) microcontroller.

2 Le produit est développé par ATMEL Smart Card ICs :

The developer of the product is ATMEL Smart Card ICs:

- ATMEL Smart Card ICs
  Z.I. Rousset Peynier
  13106 Rousset Cedex
  France

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 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].

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

The target of 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",
- AVA_VLA.4 "Highly resistant".

6 La cible d'évaluation est conforme au profil de protection PP/9806.

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

1.2 Contexte de l'évaluation

Evaluation Context

7 L'évaluation s'est déroulée d'octobre 2001 à octobre 2002.

The evaluation has been carried out from october 2001 to october 2002.

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

The sponsor of the evaluation is ATMEL Smart Card ICs:

- ATMEL Smart Card ICs
  Z.I. Rousset Peynier
  13106 Rousset Cedex
  France

9 L'évaluation a été réalisée par le Centre d'Evaluation du CEACI :

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

- CEACI (Thalès Microelectronics - CNES)
  18, avenue Edouard Belin
  31401 Toulouse Cedex 4
  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

10 La cible d'évaluation est le micro-circuit AT90SC19264RC (AT568D5 rev F).

The target of evaluation is the AT90SC19264RC (AT568D5 rev F) microcontroller.

11 La cible d'évaluation est le micro-circuit destiné à être utilisé dans une carte à puce, indépendamment de son interface physique et de la façon dont il est encarté. Une carte à puce peut être composée d'autres éléments (tels que des batteries ou une antenne) mais ces éléments ne sont pas inclus dans la cible d'évaluation.

The target of evaluation is the single chip microcontroller unit to be used in a smart card product, independent of the physical interface and the way it is packaged. Generally, a smart card product may include other elements (such as batteries or antenna,...), but these are not in the scope of the target of evaluation.

12 Le AT90SC19264RC fait partie de la famille AVR ASL4. Les composants de la famille AVR ASL4 sont conçus autour du micro-contrôleur ATMEL AVR RISC. Ce dernier, incluant des fonctionnalités de sécurité, est basé sur le standard "AVR RISC low-power HCMOS core" et fourni un jeu d'instruction couvrant les fonctionnalités les plus courantes. Les composants de la famille AVR ASL4 sont conçus en conformité au standard ISO 7816 pour les circuits intégrés.

The target of evaluation is the AT90SC19264RC device from the AVR ASL4 family of smart card devices. The devices in the AVR ASL4 family are centred around the ATMEL's AVR RISC family of single-chip microcontroller devices. The AVR RISC family, with designed-in security features, is based on the industry-standard AVR RISC lowpower HCMOS core and gives access to the powerful instruction set of this widely used device. The AVR ASL4 family of devices is designed in accordance with the ISO standard for integrated circuit cards (ISO 7816), where appropriate.

13 Bien que la cible d'évaluation soit uniquement matérielle, elle nécessite un logiciel embarqué pour tester certaines caractéristiques de sécurité lors de sa phase de développement. En phase d'utilisation finale, ce logiciel de test n'existe plus. Le logiciel de tests est chargé en mémoire EEPROM puis est effacé avant que les circuits ne quittent l'environnement de test.

Although the target of evaluation is only hardware, it requires embedded software to test the device and demonstrate certain security characteristics during the development phase. In the end-usage phase there is no embedded test software in the target of the evaluation. Test software is downloaded into the device EEPROM and is fully erased before devices leave the test environment.

14 La cible d'évaluation est constituée des mémoires non volatiles ATMEL: 192Ko de mémoire programme AVR ROM, 64Ko de mémoire programmable EEPROM et 6Ko de mémoire statique RAM.

The TOE widely uses ATMEL high density non volatile memories: it features 192Kbytes of AVR ROM program memory, 64Kbytes of EEPROM program/data memory, 6Kbytes of static RAM memory.

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 modes:

- 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 completely controls the functionality 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 evaluation 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'évènements de sécurité,
  event audit,
- réaction aux évènements de sécurité,
  event action,
- non-observabilité des opérations réalisées par le micro-circuit,
  unobservability of operations,
- réalisation d'opérations cryptographiques (DES, TDES, SHA-1, RSA avec et sans CRT, génération d'aléas, génération de clés RSA).
  cryptographic operations (DES, TDES, SHA-1, RSA with/without CRT, RNG, RSA key generation).

2.4 Guides d'utilisation

Guidance documentation

17 La cible d'évaluation est livrée avec les guides d'utilisation et d'administration suivants :

The available guidance documentation for the target of evaluation is:

a) Technical Data AT90SC19264RC Data sheet, ref 1563AX, 06/06/02.

b) Application Notes :

- SC16 Toolbox ver.2.0 Application Note, ref TPR0045A rev A, 30/04/02,
- Securing the RSA operations on the AT90SC ASL4, ref TPR0062A rev A, 15/03/02,
- Securing the DES/TDES on the AT90SC ASL4, ref TPR0063A rev A, 02/07/02,
- Checksum Accelerator use on the AT90SC ASL4 products, ref TPR0065 rev A, 02/07/02,
- Security recommendation for AT90SC ASL4, ref TPR0066A rev A, 09/07/02,
- Generation unpredictable random numbers on AT90SC Family devices, ref 1573BX rev A, 17/07/02,
- Using the supervisor and user mode in the AT90SC19264RC, ref TPR0067A rev A, 19/08/02,
- Errata sheet AT90SC19264RC 568D5 revF, ref TPR0071A rev A, 12/09/02.

Chapitre 3

Résultats de l'évaluation

Evaluation results

3.1 Exigences d'assurance de sécurité

Security assurance requirements

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

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

21 Dans le cadre des travaux d'évaluation, un audit organisationnel du site de développement et de fabrication d'ATMEL à Rousset (France) a été réalisé. Cet audit a permis de s'assurer de l'application de mesures de sécurité suffisantes pour protéger la cible d'évaluation et sa documentation associée lors de son développement et de sa fabrication.

During the evaluation, an organisational audit has been performed on the development and production site of ATMEL in Rousset (France). This audit gives confidence in the application of sufficient security measures to protect the target of evaluation and its associated documentation.

3.2 Tests fonctionnels et de pénétration

Functional and penetration testing

22 Le développeur a fourni sa documentation de test fonctionnel du produit. Ces tests sont réalisés par ATMEL sur leurs sites de Rousset (France) et Eastkilbride (Royaume-uni).

The developer of the target of evaluation has provided its test documentation. Functional testing is performed in the site of Rousset (France) and Eastkilbride (United Kingdom).

23 L'évaluateur a réalisé de son côté des tests fonctionnels pour s'assurer par échantillonnage que les fonctions de sécurité fonctionnent effectivement.

The evaluator has performed independent tests to check by sampling that the TOE security functions perform as specified.

24 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 décrits dans la cible de sécurité [ST] :

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 defeat the security objectives described in the security target [ST]:

- la cible d'évaluation doit se prémunir contre les attaques physiques,
  the TOE must prevent physical tampering with its security critical parts,
- la cible d'évaluation doit se prémunir contre le 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 se prémunir contre 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 se prémunir contre toute divulgation non autorisée 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 se prémunir contre toute modification non autorisée 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,
- les services cryptographiques doivent être disponibles pour les utilisateurs pour assurer l'intégrité et la confidentialité de leurs informations sensibles.
  cryptographic capability shall be available for users to maintain integrity and confidentiality of sensitive data.

3.3 Cotation des mécanismes cryptographiques

Assessment of the strength of the cryptographic mechanisms

25 La cible d'évaluation ne dispose pas de fonctions utilisant des mécanismes de nature cryptographique pour assurer sa 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

26 Ce présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL 4 augmenté des composants d'assurance suivants 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",
- AVA_VLA.4 "Highly resistant".

27 La cible d'évaluation est conforme au profil de protection PP/9806.

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

4.2 Restrictions

Restrictions

28 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].

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

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

4.3 Certification

Certification

30 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».

31 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.

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 remains a residual probability that exploitable vulnerabilities have not been discovered.

4.4 Reconnaissance internationale

International recognition

32 Afin 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.

33 Ce certificat répond aux exigences de l'accord SOG-IS :

This certificate meets the requirements of the SOG-IS agreement:

34 L'accord SOG-IS [SOG-IS] relatif à 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 SOG-IS Agreement [SOG-IS] in the field of mutual recognition of ITSEC certificates became effective on March 3rd, 1998. This agreement was signed by 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.
- CCIMB final interpretations.

[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, "Smart card Integrated Circuit, Version 2.0", septembre 1998.

[ST] - VEGA2 Security Target revision 1.5, ref VEGA2_ST, 10/10/02,
- VEGA2 Security Target Lite revision 1.0, ref VEGA2_Stlite, 25/10/02

[RTE] Evaluation Technical Report version 2.0, ref VG2_RTE, 25/10/02.

[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