PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

SERVICE CENTRAL 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 2001/02

Micro-circuit ATMEL AT05SC3208R

(référence AT55898 rév. Q)

Janvier 2001

Ce document constitue le rapport de certification du produit “Micro-circuit ATMEL AT05SC3208R (référence AT55898 rév. Q)”.

Ce rapport de certification est disponible sur le site internet du Service Central de la Sécurité des Systèmes d'Information à l'adresse suivante :

www.scssi.gouv.fr

Toute correspondance relative à ce rapport de certification doit être adressée au :

Secrétariat général de la défense nationale
SCSSI
Centre de Certification de la Sécurité des Technologies de l’Information
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

Mél: ssi20@calva.net

Ce document est folioté de 1 à 28 et certificat.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

CERTIFICAT 2001/02

Micro-circuit ATMEL AT05SC3208R

(référence AT55898 rév. Q)

Développeur : ATMEL Smart Card ICs

EAL4 Augmenté

Conforme au profil de protection PP/9806

Commanditaire : ATMEL Smart Card ICs

Le 9 février 2001,

Le Commanditaire :
Le Directeur de la division
ATMEL Smart Card ICs
M. Lucien BRAU

L'Organisme de certification :
Le Directeur chargé de la sécurité des systèmes d'information
M. 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
SCSSI
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

IT Security Certified

Common Criteria

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du micro-circuit ATMEL AT05SC3208R (référence AT55898 rév. Q) dévelopé par ATMEL Smart Card ICs.

2 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 [3] :

- ADV_IMP.2 "Implémentation de la TSF",
- ALC_DVS.2 "Caractère suffisant des mesures de sécurité",
- ALC_FLR.1 "Correction d'anomalies élémentaire",
- AVA_VLA.4 "Résistance élevée",
- AMA_AMP.1 "Plan de maintenance de l'assurance",
- AMA_CAT.1 "Rapport de classification des composants de la TOE".

3 Ce produit est conforme au profil de protection "Smartcard Integrated Circuit" enregistré auprès du SCSSI sous la référence PP/9806, version 2.0 de septembre 1998 [7].

Chapitre 2

Résumé

2.1 Contexte de l'évaluation

4 L'évaluation a été menée conformément aux Critères Communs ([1] à [3]) et à la méthodologie définie dans le manuel CEM [4].

5 Elle s'est déroulée simultanément au développement du produit de février 2000 à janvier 2001.

6 Le commanditaire de l'évaluation, ATMEL Smart Card ICs (ci-après "le commanditaire"), est également le développeur de la cible d'évaluation (ci-après "le développeur") :

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

7 La cible d'évaluation est produite sur le site suivant :

- ATMEL Corporation
  1150 E. Cheyenne Mtn, Blvd.
  Colorado Springs, CO 80906
  Etats-Unis

8 La société DuPont Photomasks a également participé au développement de la cible d'évaluation en tant que fabricant des réticules utilisés dans la production du AT05SC3208R :

- DuPont Photomasks
  Avenue Victoire, ZI
  13106 Rousset Cedex
  France

- DuPont Photomasks
  1901 E. Morgan St.
  P. O. Box 4088
  Kokomo, Indiana 46904-4088
  Etats-Unis

9 L'évaluation a été conduite par le centre d'évaluation de la sécurité des technologies de l'information du CEA/LETI (ci-après "CESTI") suivant :

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

2.2 Description de la cible d'évaluation

10 La cible d'évaluation est le micro-circuit ATMEL AT05SC3208R (référence AT55898 rév. Q).

11 Ce produit répond aux exigences du profil de protection "Smartcard Integrated Circuit" enregistré auprès du SCSSI dans le catalogue des profils de protection certifiés sous la référence PP/9806 [7].

12 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, de télévision à péage, de transport, de santé,...).

13 Les logiciels applicatifs (système d'exploitation, applications spécifiques,…) qui seront embarqués sur le micro-circuit ne font pas l'objet de la présente évaluation et certification.

14 Le détail des fonctions de sécurité évaluées résumées ci-après est disponible dans la cible de sécurité [5] :

- Contrôle du passage en "Test Mode",
- Contrôle d'accès en "Test Mode",
- Blocage du "Test Mode",
- Tests de la TOE,
- Détection d'erreurs,
- Contrôle d'accès en "User Mode",
- Détection d'évènements de sécurité,
- Réaction aux évènements de sécurité,
- Non-observabilité,
- Opérations cryptographiques (DES matériel, Générateur de nombres aléatoires).

2.3 Conclusions de l'évaluation

15 Le produit soumis à évaluation dont la cible de sécurité [5] est partiellement reprise dans l'annexe A du présent rapport, satisfait aux exigences du niveau d'évaluation EAL 4 augmenté des composants d'assurance suivants :

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

- ALC_FLR.1 “Correction d’anomalies élémentaire”,
- AVA_VLA.4 “Résistance élevée”,
- AMA_AMP.1 “Plan de maintenance de l’assurance”,
- AMA_CAT.1 “Rapport de classification des composants de la TOE”.

16 Il est conforme aux exigences du profil de protection PP/9806 [7]. Par ailleurs, la résistance des fonctions de sécurité est cotée au niveau élevée (SOF-high).

17 La recherche de vulnérabilités exploitables au cours de l’évaluation a été définie par la quantité d’informations disponibles pour le niveau EAL4 et par la compétence, l’opportunité et les ressources correspondant à un potentiel d’attaque élevé tel qu’il est spécifié par le composant d’assurance AVA_VLA.4.

18 L'utilisation de la cible d'évaluation de manière sûre est soumise aux recommandations figurant au chapitre 6 du présent rapport.

Chapitre 3

Identification de la cible d'évaluation

3.1 Objet

19 La cible d'évaluation est le micro-circuit ATMEL AT05SC3208R (référence AT55898 rév. Q). L'identification du micro-circuit est possible par inspection optique.

20 Ce micro-circuit est destiné à recevoir les logiciels fournis par des développeurs d'applications. Ces logiciels applicatifs (le système d'exploitation de la carte ainsi que les applications éventuelles) ne font pas partie de l'évaluation. Le micro-circuit est ensuite inséré dans une carte porteur de format carte de crédit ou tout autre support. Par ailleurs, les phases d'encartage et de personnalisation de la cible d'évaluation sont hors du champ de l'évaluation.

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

- User Mode : mode normal d'utilisation,
- Test Mode : mode de test uniquement actif en phase de développement du micro-circuit et dans un environnement sécurisé,
- Failure Mode : mode en cas de fonctionnement anormal.

3.2 Historique du développement

22 Le micro-circuit AT05SC3208R a été développé par ATMEL Smard Card ICs sur le site de East Kilbride (Ecosse).

23 La fabrication des réticules utilisés dans la production du micro-circuit est réalisée par DuPont Photomasks sur leurs sites de Rousset (France) et Kokomo (Etats-Unis).

24 La production des micro-circuits est réalisée sur le site d'ATMEL Corporation à Colorado Springs (Etats-Unis).

3.3 Cycle de vie de la cible d'évaluation

25 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.

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

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

3.4 Description des matériels

28 Le micro-circuit AT05SC3208R est bâti autour du micro-contrôleur Motorola M68HC05SC. Il fait partie de la famille de micro-circuits EUROPA dévelopés par ATMEL Smart Card ICs.

29 Le micro-circuit AT05SC3208R contient également un module DES matériel et un générateur de nombres aléatoires matériel.

30 Il dispose de différents mécanismes de sécurité participant à la réalisation des fonctions dédiées à la sécurité pour lesquelles l'évaluation a été demandée.

3.5 Description des logiciels

31 Les seuls logiciels présents sur le micro-circuit sont les applications embarquées.

32 Ces applications sont hors du champ de la présente évaluation.

3.6 Description de la documentation

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

- Technical Data AT05SC3208R, réf. 1505CX, 18 décembre 2000 [8],
- Application Notes [9] :
  - Europa Application Note for Lockout, réf. 1527AX,
  - Europa Application Note for DES, réf. Euro_APP_015 v1.1,
  - Europa Application Note for CRC, réf. Euro_APP_016 v1.1,
  - Europa Application Note for RNG, réf. Euro_APP_017 v1.1,
  - Europa Supp. Security Application Note, réf. AT05_APP_006 v1.2.

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

34 Les caractéristiques de sécurité évaluées sont consignées dans la cible de sécurité [5] qui est la référence pour l'évaluation. Les paragraphes ci-après reformulent les éléments essentiels de ces caractéristiques.

4.2 Hypothèses

35 La cible d'évaluation [5] reprend les hypothèses identifiées dans le profil de protection PP/9806 auquel elle se conforme.

36 Ces hypothèses couvrent les aspects suivants :

- protection du logiciel embarqué pendant son développement,
- livraison de la cible d'évaluation entre les différentes étapes de son cycle de vie (phases 4 à 7),
- utilisation de la cible d'évaluation pendant les phases d'encartage et de personnalisation (phases 4 à 6*)*,
- protection des données sensibles de la cible d'évaluation échangées avec les équipements avec lesquels elle dialogue (terminaux, …).

37 Le détail de ces hypothèses est disponible dans la cible de sécurité [5].

4.3 Menaces

38 Les biens à protéger par la cible d'évaluation sont ceux identifiés dans le profil de protection PP/9806 :

- les données des applications,
- les logiciels embarqués,
- les informations de développement du micro-circuit,
- le micro-circuit lui-même.

39 La cible d'évaluation [5] reprend les menaces identifiées dans le profil de protection PP/9806 auquel elle se conforme. Elles peuvent être résumées comme suit :

- modification non autorisée de la conception du circuit et des données applicatives du micro-circuit,

- divulgation non autorisée de la conception du circuit, des données applicatives du micro-circuit, des informations de tests et des outils de développement.

40 Le détail de ces menaces est disponible dans la cible de sécurité [5].

4.4 Politiques de sécurité organisationnelles

41 Aucune politique de sécurité organisationnelle n'est identifiée dans la cible de sécurité.

4.5 Fonctions de sécurité évaluées

42 La liste des fonctions de sécurité évaluées est disponible dans la cible de sécurité [5]. Ces fonctions de sécurité peuvent être résumées comme suit :

- Contrôle du passage en "Test Mode",
- Contrôle d'accès en "Test Mode",
- Blocage du "Test Mode",
- Tests de la TOE,
- Détection d'erreurs,
- Contrôle d'accès en "User Mode",
- Détection d'évènements de sécurité,
- Réaction aux évènements de sécurité,
- Non-observabilité,
- Opérations cryptographiques (DES matériel, Générateur de nombres aléatoires).

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

43 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [6].

5.2 Principaux résultats de l'évaluation

44 Le produit répond aux exigences des Critères Communs pour le niveau EAL4 augmenté des composants d'assurance suivants tels que décrits dans la partie 3 des Critères Communs [3] :

- ADV_IMP.2 "Implémentation de la TSF",
- ALC_DVS.2 "Caractère suffisant des mesures de sécurité",
- ALC_FLR.1 "Correction d'anomalies élémentaire",
- AVA_VLA.4 "Résistance élevée",
- AMA_AMP.1 "Plan de maintenance de l'assurance",
- AMA_CAT.1 "Rapport de classification des composants de la TOE".

5.2.1 ASE : Evaluation de la cible de sécurité

45 Les critères d'évaluation sont définis par les sections ASE_DES.1.iE, ASE_ENV.1.iE, ASE_INT.1.iE, ASE_OBJ.1.iE, ASE_PPC.1.iE, ASE_REQ.1.iE, ASE_SRE.1.iE et ASE_TSS.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des Critères Communs [3].

46 La cible de sécurité [5] rassemble l'ensemble des caractéristiques de sécurité de la cible d'évaluation. Ces caractéristiques sont résumées au chapitre 4 du présent rapport de certification.

47 La cible de sécurité se réclamant conforme au profil de protection PP/9806 [7], l'évaluateur s'est assuré que le document est effectivement une instanciation correcte du profil de protection.

48 La cible de sécurité [5] contient également un résumé des spécifications des fonctions de sécurité du produit ainsi que les mesures d'assurance prises pour satisfaire les exigences d'assurance. L'évaluateur s'est assuré que ces fonctions de sécurité sont une représentation correcte des exigences fonctionnelles de sécurité et que les mesures d'assurance prises couvrent les exigences du niveau EAL4 augmenté proclamé dans le profil de protection PP/9806 [7].

5.2.2 ADV_FSP.2 : Définition exhaustive des interfaces externes

49 Les critères d'évaluation sont définis par les sections ADV_FSP.2.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

50 Le développeur a fourni la documentation spécifiant les fonctions de sécurité du produit. Les interfaces externes sont également décrites.

51 L'évaluateur a examiné ces spécifications et montré pour le niveau considéré qu'elles représentent une description complète et homogène des fonctionnalités de sécurité du produit.

5.2.3 ADV_SPM.1 : Modèle informel de politique de sécurité de la TOE

52 Les critères d'évaluation sont définis par les sections ADV_SPM.1.1E de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

53 L'évaluateur a examiné le modèle de politique de sécurité fourni par le développeur et a vérifié que les fonctions de sécurité identifiées dans la cible de sécurité respectent ce modèle.

5.2.4 ADV_HLD.2 : Conception de haut niveau - Identification des sous-systèmes dédiés à la sécurité

54 Les critères d'évaluation sont définis par les sections ADV_HLD.2.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

55 La conception de haut niveau du micro-circuit fournie par le développeur présente la structure générale du produit en termes de sous-systèmes. Les fonctionnalités et les interfaces de chacun de ces sous-systèmes sont expliquées permettant à l'évaluateur de vérifier que les exigences fonctionnelles identifiées dans la cible de sécurité sont bien réalisées dans la TOE.

56 La séparation entre les sous-systèmes dédiés à la sécurité et les autres a également été fournie.

5.2.5 ADV_LLD.1 : Conception de bas niveau descriptive

57 Les critères d'évaluation sont définis par les sections ADV_LLD.1.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

58 La conception de bas niveau du micro-circuit fournie par le développeur présente la décomposition des sous-systèmes dédiés en modules. Les fonctionnalités et les interfaces de chacun de ces modules sont expliquées permettant à l'évaluateur de vérifier que les exigences fonctionnelles identifiées dans la cible de sécurité sont bien réalisées dans la TOE.

59 Les relations et dépendances entre les modules ainsi que la séparation entre les modules dédiés à la sécurité et les autres ont également été fournis.

5.2.6 ADV_IMP.2 : Implémentation de la TSF

60 Les critères d'évaluation sont définis par les sections ADV_IMP.2.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

61 Le développeur a fourni l'ensemble des schémas descriptifs ou fichiers VHDL implémentant les fonctions de sécurité de la TOE.

62 Une analyse détaillée de ces éléments a été effectuée par l'évaluateur afin de vérifier, d'une part, que les exigences fonctionnelles identifiées dans la cible de sécurité sont bien réalisées dans la TOE, et d'autre part, de rechercher des vulnérabilités potentielles.

5.2.7 ADV_RCR.1 : Démonstration de correspondance informelle

63 Les critères d'évaluation sont définis par la section ADV_RCR.1.1E de la classe ADV, telle que spécifiée dans la partie 3 des Critères Communs [3].

64 Le développeur a fourni une documentation de correspondance pour chaque représentation des fonctions de sécurité. Cette documentation indique la correspondance entre les fonctions de sécurité telles qu'elles sont définies dans deux niveaux adjacents de spécifications.

65 L'évaluateur a donc pu s'assurer de la conformité des spécifications fonctionnelles de sécurité à travers la conception de haut niveau et de bas niveau du micro-circuit ainsi que son implémentation.

5.2.8 ACM_AUT.1 : Automatisation partielle de la gestion de configuration

66 Les critères d'évaluation sont définis par la section ACM_AUT.1.1E de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [3].

67 Le développeur a fourni la documentation des systèmes de gestion de configuration utilisés pour le développement du micro-circuit et des réticules.

68 Ces systèmes sont fondés sur une gestion automatique de la configuration à travers un outil de gestion de configuration permettant de s'assurer que seuls les changements autorisés sur le produit sont possibles. L'évaluateur a analysé la documentation et vérifié au cours des audits des différents sites de développement l'utilisation effective de ces outils de gestion de configuration, en accord avec les procédures du développeur.

5.2.9 ACM_CAP.4 : Aide à la génération et procédures de réception

69 Les critères d'évaluation sont définis par la section ACM_CAP.4.iE de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [3].

70 Le développeur a fourni la documentation du système de gestion de configuration.

71 Ce système impose un contrôle des objets produits au cours du développement chez le développeur du micro-circuit. Des procédures permettent de prendre en compte dans le système de gestion de configuration les objets composant la cible d'évaluation (procédure de réception). Des procédures gèrent également les révisions majeures et mineures de la cible d'évaluation. Le système de gestion de configuration énumère tous les composants élémentaires à partir desquels la cible d'évaluation a été construite.

72 Un système de gestion de configuration s'applique également chez le fabricant de réticules DuPont Photomasks. Les procédures utilisées sont en accord avec les principes du système de gestion de configuration du fondeur.

73 L'évaluateur s'est également assuré de l'absence d'incohérence dans la documentation fournie.

74 Enfin, des audits ont été menés sur les sites suivants pour s'assurer de l'utilisation effective des systèmes de gestion de configuration :

- ATMEL East Kilbride (Ecosse) pour la conception du micro-circuit,
- DuPont Photomasks Kokomo (Etats-Unis) et Rousset (France) pour la fabrication des réticules,
- ATMEL Colorado Springs (Etats-Unis) pour la production des micro-circuits.

5.2.10 ACM_SCP.2 : Couverture du suivi des problèmes par le système de gestion de configuration

75 Les critères d'évaluation sont définis par la section ACM_SCP.2.1E de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [3].

76 Le système de gestion de configuration appliquée par le développeur couvre le produit ainsi que l'ensemble de sa documentation ; il couvre également toute erreur de sécurité qui pourrait être découverte : il contrôle donc la documentation de conception du produit, la documentation de test du produit, les éléments de réalisation du produit, la documentation d'utilisation ainsi que la documentation d'administration.

5.2.11 ADO_DEL.2 : Détection de modification

77 Les critères d'évaluation sont définis par la section ADO_DEL.2.iE de la classe ADO, telle que spécifiée dans la partie 3 des Critères Communs [3].

78 L'évaluateur s'est assuré que les procédures de livraison mises en place entre les différents sites de fabrication et pour la distribution des produits évalués aux utilisateurs garantissent la sécurité de la TOE.

79 Les audits menés dans les différents sites de fabrication de la TOE ont permis de s'assurer de l'application effective de ces procédures.

5.2.12 ADO_IGS.1 : Procédures d'installation, de génération et de démarrage

80 Les critères d'évaluation sont définis par les sections ADO_IGS.1.iE de la classe ADO, telle que spécifiée dans la partie 3 des Critères Communs [3].

81 Aucune procédure d'installation n'est nécessaire pour un micro-circuit.

82 Les procédures de génération sont à interpréter comme la génération du micro-circuit à partir de sa conception mais également de l'intégration du code des applications embarquées et des options de configuration du développeur de masque.

83 La procédure de démarrage correspond au "reset" du micro-circuit.

84 L'évaluateur s'est assuré que ces procédures permettent un fonctionnement sûr de la TOE.

5.2.13 AGD_ADM.1 : Guide de l'administrateur

85 Les critères d'évaluation sont définis par la section AGD_ADM.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des Critères Communs [3].

86 L'administration de la TOE concerne les opérations réalisées lors de la phase de tests avant l'envoi des micro-circuits aux clients.

87 L'évaluateur s'est assuré de l'absence d'incohérence dans la documentation fournie aux administrateurs et a vérifié que ces procédures permettent une administration sûre du produit.

5.2.14 AGD_USR.1 : Guide de l'utilisateur

88 Les critères d'évaluation sont définis par la section AGD_USR.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des Critères Communs [3].

89 Le développeur a fourni la documentation d'utilisation des fonctions de sécurité du micro-circuit [8 et 9] à destination des développeurs des logiciels installés sur le micro-circuit. Ces guides contiennent un ensemble de recommandations pour le développement des logiciels applicatifs.

90 L'évaluateur s'est assuré que cette documentation permettait une utilisation sûre des fonctions de sécurité offertes par le micro-circuit.

5.2.15 ALC_DVS.2 : Caractère suffisant des mesures de sécurité

91 Les critères d'évaluation sont définis par la section ALC_DVS.2.iE de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [3].

92 L'évaluateur s'est assuré que des mesures de sécurité suffisantes sont mise en place pour protéger la TOE, ses informations de conception, les outils utilisés lors du

développement et de la fabrication des réticules et du micro-circuit et également pour protéger les applications fournies au fondeur pour être masquées.

93 Les sites suivants ont été audités pour s'assurer de l'application effective des mesures de sécurité :

- ATMEL East Kilbride (Ecosse) pour la conception du micro-circuit,
- DuPont Photomasks Kokomo (Etats-Unis) et Rousset (France) pour la fabrication des réticules,
- ATMEL Colorado Springs (Etats-Unis) pour la production des micro-circuits.

5.2.16 ALC_LCD.1 : Modèle de cycle de vie défini par le développeur

94 Les critères d'évaluation sont définis par la section ALC_LCD.1.1E de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [3].

95 L'évaluateur s'est assuré que le modèle de cycle de vie du micro-circuit mis en place par le développeur apporte une certaine qualité pour le processus de développement et de maintenance de la TOE.

5.2.17 ALC_TAT.1 : Outils de développement bien définis

96 Les critères d'évaluation sont définis par la section ALC_TAT.1.iE de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [3].

97 Le développeur a fourni la documentation relative aux outils de développement du micro-circuit (chaîne de développement du matériel). L'évaluateur s'est assuré que ces outils de développement utilisés sont bien définis.

5.2.18 ALC_FLR.1 : Correction d'anomalies élémentaires

98 Les critères d'évaluation sont définis par la section ALC_FLR.1.iE de la classe ALC, telle que spécifiée dans la partie 3 des Critères Communs [3].

99 L'évaluateur a vérifié que des procédures ont été mises en place par le développeur pour tracer et corriger les anomalies qui pourraient être découvertes lors de l'exploitation de la TOE.

5.2.19 ATE_FUN.1 : Tests fonctionnels

100 Les critères d'évaluation sont définis par la section ATE_FUN.1.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

101 Le développeur a fourni la documentation de test des fonctions de sécurité du micro-circuit.

102 Les tests sont menés en 4 phases :

- tests sur simulateurs lors de la phase de conception du micro-circuit,

- tests d'évaluation du silicone pour s'assurer du bon comportement des premiers échantillons,
- tests de caractérisation avant la mise en production,
- tests de production effectués sur les micro-circuits à l'issue de leur fabrication.

103 Une documentation détaillée a été fournie pour chacun des tests ; ces documentations décrivent le plan des tests, l'objectif des tests, les procédures de tests à réaliser ainsi que les résultats obtenus.

104 L'évaluateur s'est assuré de la complétude de cette documentation.

5.2.20 ATE_COV.2 : Analyse de la couverture

105 Les critères d'évaluation sont définis par la section ATE_COV.2.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

106 Le développeur a fourni une analyse de la documentation de test justifiant la couverture de l'ensemble des fonctions de sécurité par les tests menés lors des 4 phases présentées précédemment.

107 L'évaluateur a confirmé cette analyse de couverture.

5.2.21 ATE_DPT.1 : Tests : conception de haut niveau

108 Les critères d'évaluation sont définis par la section ATE_DPT.1.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

109 Le développeur a fourni une analyse de la documentation de test justifiant la complétude des tests vis-à-vis des sous-systèmes identifiés dans la conception de haut niveau.

110 L'évaluateur a examiné cette documentation et s'est assuré de sa cohérence.

5.2.22 ATE_IND.2 : Tests indépendants - échantillonnage

111 Les critères d'évaluation sont définis par les sections ATE_IND.2.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

112 L'évaluateur a effectué un ensemble de tests sur le micro-circuit. Il a procédé à un échantillonnage des programmes de tests du développeur et a mené des tests complémentaires. Pour des raisons matérielles, certains de ces tests ont été repassés chez le développeur.

5.2.23 AVA_MSU.2 : Validation de l'analyse

113 Les critères d'évaluation sont définis par la section AVA_MSU.2.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [3].

114 Le développeur a fourni une analyse de la documentation d'exploitation du produit permettant de vérifier l'absence d'information qui pourrait mener un utilisateur ou un administrateur à utiliser le micro-circuit de façon non sûre sans le savoir. Cette documentation identifie les modes d'exploitation de la cible d'évaluation ainsi que les conséquences et les implications de ces modes sur le maintien d'une exploitation sûre de la cible d'évaluation.

115 Les évaluateurs ont réalisé des tests complémentaires afin de confirmer les résultats de cette analyse.

5.2.24 AVA_SOF.1 : Évaluation de la résistance des fonctions de sécurité de la TOE

116 Les critères d'évaluation sont définis par la section AVA_SOF.1.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [3].

117 La seule fonction identifiée dans la cible de sécurité réalisée au moyen d'un mécanisme faisant appel au calcul des probabilités ou des permutations est la fonction d'entrée en Mode test.

118 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 réclamée dans la cible de sécurité.

5.2.25 AVA_VLA.4 : Résistance élevée

119 Les critères d'évaluation sont définis par les sections AVA_VLA.3.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [3].

120 Le développeur a fourni une documentation d'analyse des vulnérabilités potentielles du produit. L'évaluateur a examiné cette fourniture et réalisé sa propre analyse de vulnérabilités de manière indépendante.

121 L'évaluateur a réalisé des tests de pénétration, basés sur son analyse de vulnérabilités afin de pouvoir vérifier que le produit résiste aux attaques correspondant à un potentiel de l'attaquant élevé tel que défini par le composant AVA_VLA.4 "Résistance élevée".

5.2.26 AMA_AMP.1 : Plan de maintenance de l'assurance

122 Les critères d'évaluation sont définis par les sections AMA_AMP.1.iE de la classe AMA, telle que spécifiée dans la partie 3 des Critères Communs [3].

123 Pour mettre en place un processus de maintenance, le développeur a fourni un plan de maintenance identifiant les mesures et autres procédures mises en place par le développeur pour s'assurer que la confiance établie dans le micro-circuit certifié est maintenue en cas de modifications de la TOE ou de son environnement.

124 L'évaluateur s'est assuré que les mesures mises en place sont suffisantes et que le calendrier proposé pour les audits de maintenance et les éventuelles ré-évaluations est satisfaisant.

5.2.27 AMA_CAT.1 : Rapport de classification des composants de la TOE

125 Les critères d'évaluation sont définis par les sections AMA_CAT.1.iE de la classe AMA, telle que spécifiée dans la partie 3 des Critères Communs [3].

126 Le développeur a fourni une classification des éléments du micro-circuit identifiés dans les différentes représentations des fonctions de sécurité (conception de haut niveau, de bas niveau) et des outils utilisés lors du développement qui peuvent avoir un impact sur la sécurité du produit.

127 L'évaluateur s'est assuré que ce rapport de classification est complet et cohérent.

5.3 Verdicts

128 Pour tous les aspects des Critères Communs identifiés ci-dessus, un avis "réussite" a été émis.

Chapitre 6

Certification

Recommandations d'utilisation

129 La cible d'évaluation "Micro-circuit ATMEL AT05SC3208R (référence AT55898 rév. Q)" est soumise aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

a) Le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [5].

b) Les applications destinées à être installées sur le micro-circuit doivent impérativement respecter les guides d'utilisation [8 et 9] émis par ATMEL Smart Card ICs et notamment les recommandations de programmation qui y figurent.

Chapitre 7

Certification

7.1 Objet

130 Le micro-circuit ATMEL AT05SC3208R soumis à évaluation satisfait aux exigences du niveau d'évaluation EAL 4 augmenté des composants d'assurance suivants tels que décrits dans la partie 3 des Critères Communs [3] :

- ADV_IMP.2 "Implémentation de la TSF",
- ALC_DVS.2 "Caractère suffisant des mesures de sécurité",
- ALC_FLR.1 "Correction d'anomalies élémentaire",
- AVA_VLA.4 "Résistance élevée",
- AMA_AMP.1 "Plan de maintenance de l'assurance",
- AMA_CAT.1 "Rapport de classification des composants de la TOE".

131 La résistance des fonctions de sécurité est cotée au niveau élevée (SOF-high).

132 Il est également conforme aux exigences du profil de protection PP/9806 [7].

133 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL4 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élevé tel qu'il est spécifié par le composant d'assurance AVA_VLA.4.

7.2 Portée de la certification

134 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.

135 Le certificat ne s'applique qu'à la version évaluée du produit identifiée au chapitre 3.

136 Les travaux liés à la certification des versions ultérieures de la cible d'évaluation pourront être limités si un programme de maintenance est mis en place. Dans le cas contraire, une ré-évaluation du produit en fonction des modifications apportées sera nécessaire.

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.
Encartage	Insertion du composant masqué dans un support plastique en forme de carte.
Evaluation	Validation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Logiciel embarqué	Logiciel présent sur une puce.
Masque	Ensemble d'instructions organisées, reconnaissables et exécutables par le processeur d'un microcircuit électronique.
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.
Personnalisation	Inscription dans la mémoire de données du composant masqué des données spécifiques à une application.

Politique de sécurité organisationnelle	Une ou plusieurs règles, procédures, codes de conduite ou lignes directrices de sécurité qu'une organisation impose pour son fonctionnement.
Porteur	Utilisateur final de la carte.
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

[1] [CC-1] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 1 : Introduction et modèle général CCIB-99-031, version 2.1 Août 1999.

[2] [CC-2] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 2 : Exigences fonctionnelles de sécurité CCIB-99-032, version 2.1 Août 1999.

[3] [CC-3] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 3 : Exigences d'assurance de sécurité CCIB-99-033, version 2.1 Août 1999.

[4] [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.

[5] Cible de sécurité Europa Security Target, réf. Europa_ST v2.3, 22 décembre 2000.

[6] Rapport technique d'évaluation, réf. LETI.CESTI.BRU.RE.001 (diffusion contrôlée).

[7] Profil de Protection PP/9806 "Smartcard Integrated Circuit", version 2.0, septembre 1998.

[8] Technical Data AT05SC3208R, réf. 1505CX, 18 décembre 2000.

[9] Application Notes :
- Europa Application Note for Lockout, réf. 1527AX,
- Europa Application Note for DES, réf. Euro_APP_015 v1.1,
- Europa Application Note for CRC, réf. Euro_APP_016 v1.1,
- Europa Application Note for RNG, réf. Euro_APP_017 v1.1,
- Europa Supp. Security Application Note, réf. AT05_APP_006 v1.2.