



*Liberté • Égalité • Fraternité*  
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

## **Rapport de certification 2003/20**

### **Micro-circuit ATMEL AT90SC3232CS**

*Paris, le 13 novembre 2003*

*Le Directeur central de la sécurité des  
systèmes d'information*

*Henri Serres*  
[ORIGINAL SIGNE]



## Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en terme d'objectifs de sécurité.

Toutefois, la certification ne constitue pas en soi une recommandation du produit par l'organisme de certification, et ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables.

## Table des matières

<b>1. LE PRODUIT EVALUE.....</b>	<b>7</b>
1.1. CONTEXTE.....	7
1.2. IDENTIFICATION DU PRODUIT.....	7
1.3. LE DEVELOPPEUR.....	7
1.4. DESCRIPTION DU PRODUIT EVALUE .....	8
1.4.1. <i>Architecture</i> .....	8
1.4.2. <i>Cycle de vie</i> .....	10
1.4.3. <i>Périmètre et limites du produit évalué</i> .....	10
1.5. UTILISATION ET ADMINISTRATION.....	11
1.5.1. <i>Utilisation</i> .....	11
1.5.2. <i>Administration</i> .....	11
<b>2. L'EVALUATION .....</b>	<b>12</b>
2.1. CENTRE D'EVALUATION .....	12
2.2. COMMANDITAIRE.....	12
2.3. REFERENTIELS D'EVALUATION.....	12
2.4. EVALUATION DE LA CIBLE DE SECURITE.....	12
2.5. EVALUATION DU PRODUIT .....	12
2.5.1. <i>Développement du produit</i> .....	12
2.5.2. <i>Documentation</i> .....	13
2.5.3. <i>Livraison et installation</i> .....	13
2.5.4. <i>L'environnement de développement</i> .....	14
2.5.5. <i>Tests fonctionnels</i> .....	14
2.5.6. <i>Estimation des vulnérabilités</i> .....	14
<b>3. CONCLUSIONS DE L'EVALUATION.....</b>	<b>16</b>
3.1. RAPPORT TECHNIQUE D'EVALUATION .....	16
3.2. NIVEAU D'EVALUATION .....	16
3.3. EXIGENCES FONCTIONNELLES .....	17
3.4. RESISTANCE DES FONCTIONS .....	18
3.5. ANALYSE DES MECANISMES CRYPTOGRAPHIQUES .....	18
3.6. CONFORMITE A UN PROFIL DE PROTECTION.....	18
3.7. RECONNAISSANCE EUROPEENNE (SOG-IS).....	18
3.8. RECONNAISSANCE INTERNATIONALE (CC RA).....	18
3.9. RESTRICTIONS D'USAGE .....	19
3.10. OBJECTIFS DE SECURITE SUR L'ENVIRONNEMENT .....	19
3.11. SYNTHESE DES RESULTATS .....	19
<b>ANNEXE 1. RAPPORT DE VISITE DU SITE ATMEL ROUSSET .....</b>	<b>20</b>
<b>ANNEXE 2. RAPPORT DE VISITE DU SITE DE DUPONT PHOTOMASKS.....</b>	<b>21</b>
<b>ANNEXE 3. ANALYSE DES MECANISMES CRYPTOGRAPHIQUES.....</b>	<b>22</b>
<b>ANNEXE 4. EXIGENCES FONCTIONNELLES DE SECURITE DU PRODUIT EVALUE ..</b>	<b>23</b>
<b>ANNEXE 5. NIVEAUX D'ASSURANCE PREDEFINIS IS 15408 OU CC .....</b>	<b>26</b>
<b>ANNEXE 6. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>27</b>
<b>ANNEXE 7. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>31</b>



# Préface

## La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendu public (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification selon les ITSEC et les Critères Communs sont publiques et disponibles en français sur le site Internet :

[www.ssi.gouv.fr](http://www.ssi.gouv.fr)

Le site international concernant la certification selon les Critères Communs est accessible à l'adresse Internet :

[www.commoncriteria.org](http://www.commoncriteria.org)

## Accords de reconnaissance des certificats

L'**accord de reconnaissance** européen du SOG-IS de 1999 permet la reconnaissance entre les états signataires de l'accord<sup>1</sup>, des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :



La direction centrale de la sécurité des systèmes d'information passe aussi des **accords de reconnaissance** avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats

---

<sup>1</sup> En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties.

L'accord du Common Criteria Recognition Arrangement, permet la reconnaissance, par les pays signataires de l'accord<sup>1</sup>, des certificats délivrés dans le cadre du schéma Critères Communs. La reconnaissance mutuelle s'applique au niveau EAL4 ainsi qu'à la famille ALC\_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :



Les sites des organismes nationaux de certification des pays signataires de l'accord Common Criteria Recognition Arrangement sont :

Pays	Organisme certificateur	Site web
France	DCSSI	<a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>
Royaume-Uni	CESG	<a href="http://www.cesg.gov.uk">www.cesg.gov.uk</a>
Allemagne	BSI	<a href="http://www.bsi.bund.de">www.bsi.bund.de</a>
Canada	CSE	<a href="http://www.cse-cst.gc.ca">www.cse-cst.gc.ca</a>
Australie-Nouvelle Zélande	AISEP	<a href="http://www.dsd.gov.au/infosec">www.dsd.gov.au/infosec</a>
Etats-Unis	NIAP	<a href="http://www.niap.nist.gov">www.niap.nist.gov</a>

---

<sup>1</sup> En janvier 2003, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada et l'Australie-Nouvelle Zélande ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Espagne, la Finlande, la Grèce, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède et l'Autriche.

# 1. Le produit évalué

## 1.1. Contexte

Le produit évalué est le micro-circuit AT90SC3232CS dérivé des micro-circuits AT90SC19264RC et AT90SC9608RC déjà certifiés sous les références [2002/24] et [2003/11]. Ces composants appartiennent à la famille AVR ASL4 de composants ATMEL, fondée sur le standard industriel « AVR RISC low-power HCMOS core ».

Sur la base des informations fournies par le développeur [MOD\_SIA], l'évaluateur a estimé l'impact sur la sécurité des évolutions entre les deux micro-circuits AT90SC3232CS et AT90SC19264RC. Les résultats de cette analyse sont disponibles dans le rapport technique d'évaluation [RTE]. Cette analyse a permis de réutiliser au mieux les résultats de l'évaluation du AT90SC1926RC (et également du AT90SC9608RC). L'évaluateur a également réutilisé les résultats des travaux réalisés dans le cadre du programme de maintenance PM 2002/02 relatif aux produits ATMEL.

## 1.2. Identification du produit

Le produit évalué est le micro-circuit AT90SC3232CS, référence AT568D9 révision K. Ce micro-circuit inclut une librairie logicielle cryptographique en version 2.1 stockée dans une ROM dédiée.

## 1.3. Le développeur

Plusieurs acteurs interviennent dans la conception et fabrication du micro-circuit (cf. description du cycle de vie § 1.4.2 :

Le micro-circuit AT90SC3232CS est développé et testé par :

**Atmel East Kilbride**

Maxwell Building  
Scottish Enterprise technology Park  
East Kilbride  
SCOTLAND G75 0QR.

La préparation de la base de données de fabrication du masque du micro-circuit AT90SC3232CS ainsi que la fabrication du micro-circuit lui-même sont réalisées par :

**Atmel Rousset**

Z.I. Rousset Peynier  
13106 Rousset Cedex  
France.

Le masque du micro-circuit AT90SC3232CS est fabriqué par :

**DUPONT PHOTOMASKS**

74, Avenue Perroy  
13790 Rousset  
France.

## 1.4. Description du produit évalué

### 1.4.1. Architecture

L'architecture du micro-circuit AT90SC3232CS (en technologie 0.35µm) est la suivante :

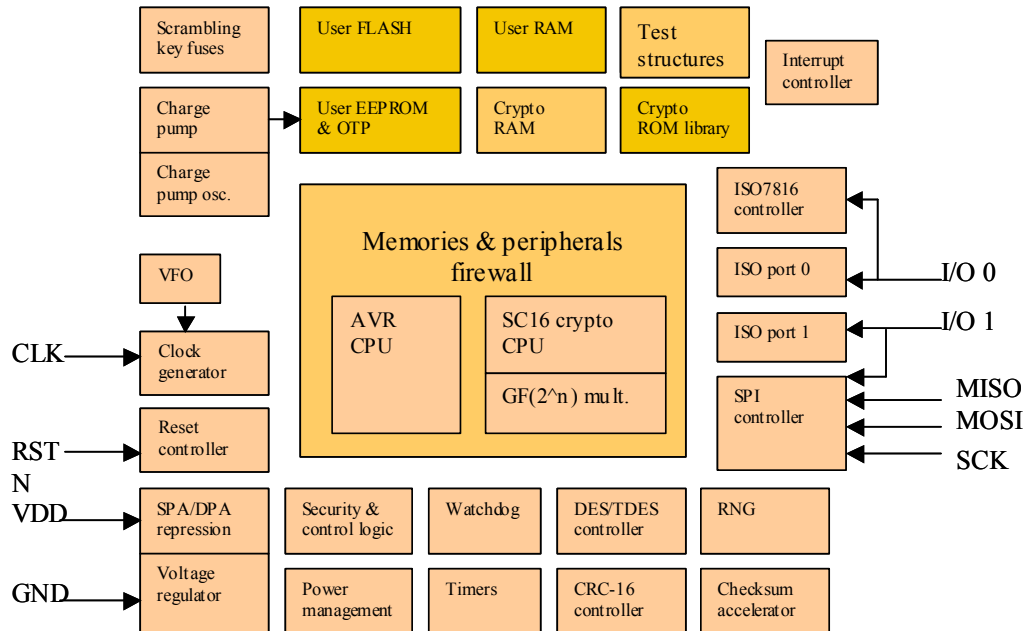


Figure 1 - micro-circuit ATMEL AT90SC3232CS

Chaque bloc du schéma constitue un sous-système du produit. L'architecture et le détail de chaque sous-système sont précisés dans la documentation de développement [ADV].

Les caractéristiques techniques du produit sont les suivantes :

- Processeur AVR RISC HCMOS Low Power core
- 32KB de mémoire FLASH pour le stockage des programmes,
- 32KB de mémoire EEPROM pour le stockage des programmes et des données avec 128 Bytes d'OTP (mémoire inscriptible non effaçable en mode « utilisateurs », pour stocker les données sensibles par exemple, ou servir de verrous sur les phases du cycle de vie notamment) et 384 bytes de bit d'adresse, une pompe de charge et ses oscillateurs,
- 3KB de mémoire RAM statique,
- 8KB de mémoire ROM dédiée au stockage de la librairie cryptographique,
- des clés de brouillage pour les mémoires,
- un accélérateur de calcul de checksum 32 bits (support à la détection d'erreur sur les données ou programmes en mémoire),
- un périphérique CRC-16 (support à la détection d'erreur sur les données ou programmes en mémoire),
- un générateur de nombres aléatoires,
- un accélérateur de calcul cryptographique DES/3DES et un multiplicateur GF2N (pour les courbes elliptiques),
- un coprocesseur cryptographique (SC16) incluant une librairie logicielle de 8KB en ROM (boîte à outils cryptographiques) permettant d'accélérer les calculs RSA



(avec et sans CRT) et SHA-1. La librairie fournit également des primitives permettant au logiciel embarqué de construire ses propres algorithmes mais ces primitives ne font pas partie du périmètre d'évaluation,

- des détecteurs tension, fréquence, température et lumière ultraviolette,
- un firewall protégeant l'accès à toutes les mémoires et périphériques, comportant trois modes d'utilisation,
- un régulateur de tension (le micro-circuit fonctionne dans une gamme de tension de 3.0V à 5.0V),
- 2 Timers,
- 2 ports série avec une interface et un contrôleur conforme au standard ISO7816,
- un périphérique d'interface série SPI,
- une structure de test dédiée, sciée lors de la mise en micro-module et accessible uniquement en mode test pour les tests de production.

Le micro-circuit comporte deux modes d'utilisation :

- un mode « Test » dans lequel le micro-circuit fonctionne sous le contrôle d'un logiciel de test, et utilisé sous le contrôle d'un système de test externe. Ce mode n'est utilisable 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 fusible. De plus, après découpage du « wafer », l'interface de test n'est plus accessible.
- un mode « utilisateur » dans lequel le micro-circuit fonctionne sous le contrôle du logiciel embarqué de la carte à puce. Les utilisateurs finaux ne peuvent utiliser le micro-circuit que dans ce mode.

Le micro-circuit seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou des applications et à être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont 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.

### 1.4.2. Cycle de vie

Le cycle de vie du produit inspiré du cycle de vie décrit dans le PP/9806 [PP9806] est le suivant :

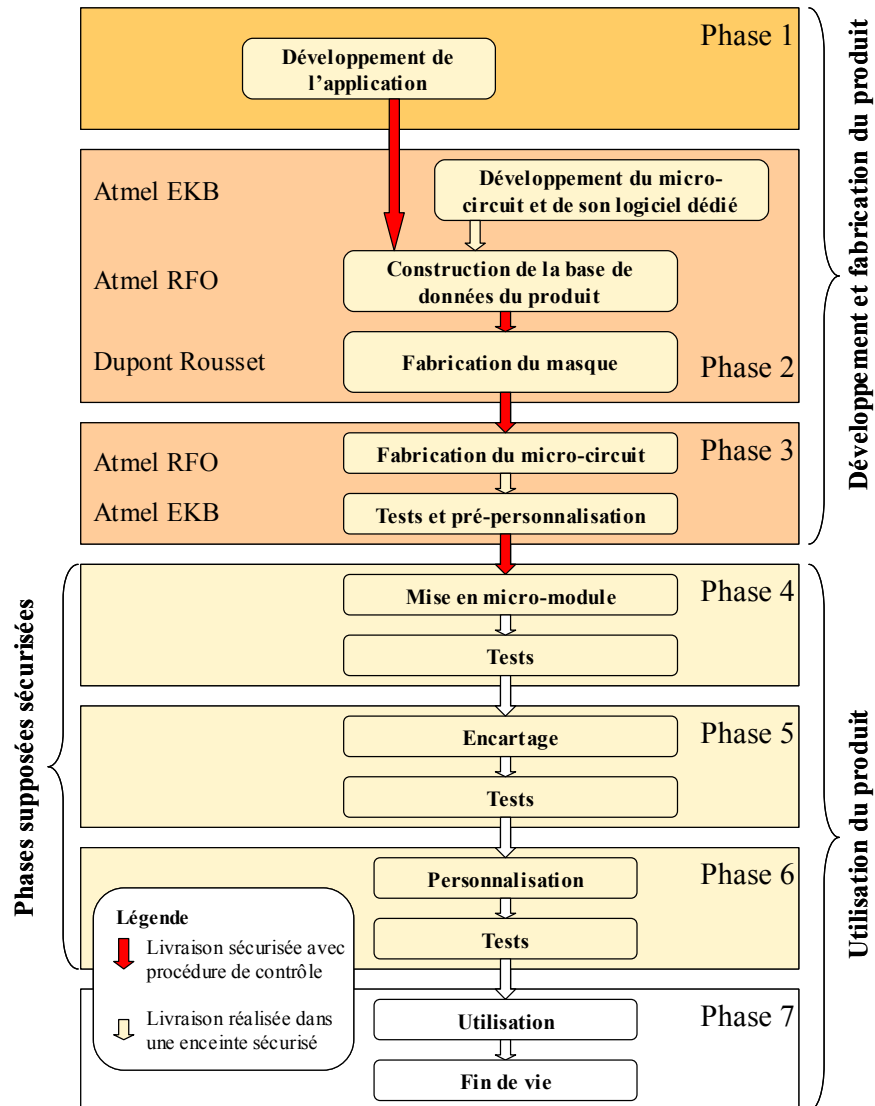


Figure 2 - Cycle de vie standard d'une carte à puce

### 1.4.3. Périmètre et limites du produit évalué

Ce rapport de certification présente les travaux d'évaluation relatifs au micro-circuit et à la librairie logicielle cryptographique identifiés au §1.2. Concernant la librairie logicielle cryptographique, seules les commandes relatives aux calculs RSA sont incluses dans le périmètre d'évaluation (commande 08, 09 et 0B).

Le logiciel de tests accessible en mode « test » décrit au paragraphe 1.4.1, ainsi que toute autre application éventuellement embarquée pour les besoins de l'évaluation ne font donc pas partie du périmètre d'évaluation.

En regard du cycle de vie, le produit évalué est le produit qui sort de la phase de fabrication, tests et pré-personnalisation (phase 3).

Ce micro-circuit comporte une spécificité : le logiciel applicatif n'est pas embarqué en mémoire ROM (logiciel figé lors de la phase de fabrication) mais en mémoire Flash. De fait,

il peut être chargé ultérieurement à la phase de fabrication du micro-circuit. En sortie de fabrication, le micro-circuit comporte en mémoire flash un petit programme permettant de charger le futur logiciel applicatif. Lors de cette opération, le programme de chargement est remplacé par le logiciel applicatif lui-même ce qui fait qu'il n'existe plus après cette étape. Pour la présente évaluation, il est considéré que le logiciel applicatif est embarqué dans le micro-circuit dans les locaux d'Atmel et sous sa responsabilité.

## **1.5. Utilisation et administration**

### ***1.5.1. Utilisation***

Le produit évalué n'est pas un produit mettant en œuvre une application particulière. Il s'agit d'une plate-forme matérielle offrant différents services pour les logiciels embarqués. De fait, il n'y a pas réellement d'utilisation à proprement parler. Les utilisateurs du micro-circuit peuvent être vus (cf. document [JIL\_IC]) comme étant les développeurs des applications ainsi que tous les acteurs intervenant dans les phases dites d'administration de la carte (phase 4 à 6) qui interviendront notamment dans la configuration et la personnalisation des applications embarquées.

### ***1.5.2. Administration***

Conformément au guide « The application of CC to Integrated Circuits » [JIL\_IC], les administrateurs du produit sont les différents intervenants des phases 4 à 7 du cycle de vie qui configurent (personnalisation) le produit final. Ces opérations sont en grande partie liées au type d'applications embarquées. Dans le cadre d'un micro-circuit, seules les interfaces d'administration propres au micro-circuit sont évaluées. Par ailleurs, les phases 4 à 6 dites d'administration sont couvertes par une hypothèse dans la cible de sécurité, qui suppose que les opérations associées à ces phases sont réalisées dans des conditions ne remettant pas en cause la sécurité du produit. Ces conditions n'ont pas été évaluées.

Les objectifs de sécurité sur l'environnement d'exploitation sont listés dans la cible de sécurité [ST] et repris dans le présent rapport au paragraphe 3.10.

---

## 2. L'évaluation

### 2.1. Centre d'évaluation

#### **CEACI (Thalès Microelectronics – CNES)**

18 avenue Edouard Belin  
31401 Toulouse Cedex 4

Téléphone : +33 (0)5 61 27 40 29

Adresse électronique : [ceaci@cnes.fr](mailto:ceaci@cnes.fr)

L'évaluation s'est déroulée de novembre 2002 à octobre 2003.

### 2.2. Commanditaire

#### **Atmel Smart Card ICs**

Maxwell Building  
Scottish Enterprise technology Park  
East Kilbride  
SCOTLAND G75 0QR.

### 2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'ensemble des interprétations finales listées dans les rapports d'évaluation.

### 2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation. Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 des Critères Communs [CC]. La cible de sécurité répond aux exigences de la classe ASE.

### 2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation respectent les exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].

#### ***2.5.1. Développement du produit***

La classe d'assurance ADV – développement – définit les exigences de raffinement pas à pas des fonctions de sécurité du produit depuis ses spécifications globales dans la cible de sécurité [ST] jusqu'à l'implémentation. Chacune des représentations des fonctions de sécurité du produit qui résulte de ce processus fournit des informations qui aident l'évaluateur à déterminer si les exigences fonctionnelles du produit ont été satisfaites.

L'analyse des documents associés à la classe ADV montre que les exigences fonctionnelles sont correctement et complètement raffinées dans les différents niveaux de représentation du produit (spécifications fonctionnelles (FSP), sous-systèmes (HLD), modules (LLD) et implémentation (IMP)), jusqu'à l'implémentation de ses fonctions de sécurité.

Les documents fournis pour la classe ADV – développement – répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

### **2.5.2. Documentation**

Du point de vue de l'évaluation, il n'y a pas à proprement parler d'administrateur du micro-circuit dans les phases d'utilisation du produit (phase 4 à 7 du cycle de vie). En effet, l'administration dans ces phases d'utilisation est liée à une application particulière qui est en dehors du périmètre de l'évaluation.

Le produit ne comportant pas d'application embarquée, pour l'évaluation, seuls les développeurs d'application et éventuellement les responsables intervenant dans les phases 4 à 6 pour des tâches spécifiques au micro-circuit sont considérés comme utilisateurs du produit.

Les guides utilisateur [USR] répondent aux exigences de la partie 3 des critères communs (cf. [CC]) en terme de contenu et de présentation des éléments de preuve.

### **2.5.3. Livraison et installation**

Conformément au guide pour l'évaluation « The application of CC to IC » (cf. [JIL\_IC]), les livraisons considérées sont :

- la livraison du code des applications embarquées au fabricant du micro-circuit,
- la livraison des informations nécessaires au fabricant du masque,
- la livraison du masque au fabricant du micro-circuit,
- la livraison des micro-circuits au responsable de l'étape suivante (mise en micro-module, encartage).

Les différents sites impliqués sont identifiés au §1.3 du présent rapport.

Tous les flux relatifs au site d'Atmel East Kilbride (EKB) sont évalués et audités régulièrement dans le cadre du programme de maintenance PM 2002/02. Les conclusions des travaux associés sont satisfaisantes. Ces flux n'ont donc pas fait l'objet d'évaluation pour ce projet. La spécificité du produit liée à la mémoire de type « flash » du composant a également été analysée dans le cadre de cette évaluation. Il est notamment requis que le logiciel applicatif soit chargé dans le micro-circuit dans l'environnement de développement d'ATMEL et sous sa responsabilité. La procédure associée de livraison du code du logiciel applicatif [DEL] a été évalué par le CEACI ainsi que son application à l'aide d'éléments de preuve fournis par le développeur.

Pour les sites d'Atmel et de Dupont Photomask à Rousset (RFO), les flux impliqués avaient été évalués et audités dans le cadre des projets précédent (cf. contexte §1.1). Seuls certains aspects liés aux changements de procédure depuis les projets précédents ont fait l'objet de vérification sur site.

Les procédures [DEL] et éléments de preuve associés pour les livraisons sont donc suffisants pour répondre aux exigences demandées : elles permettent de connaître l'origine de la livraison et de détecter une modification du produit pendant la livraison d'un site à un autre.

Concernant les exigences en terme d'installation, génération et démarrage, le produit final, après fabrication et personnalisation ne comprend pas de phase spécifique d'installation. Il est directement opérationnel, en attente des commandes conformes au protocole IS07816 de son interface. Le document [IGS] explique comment le produit après mise sous tension se met

dans un état stable en attente des commandes. Ce point avait été évalué et vérifié lors du projet précédent (cf. contexte §1.1). La tâche n'a pas été ré-ouverte pour le présent projet car l'analyse d'impact des changements ne le justifiait pas.

Les documents fournis pour la classe ADO – livraison et opération – répondent donc aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

#### ***2.5.4. L'environnement de développement***

Le développement du micro-circuit implique l'ensemble des sites identifiés au §1.3. L'environnement de développement du site d'Atmel East Kilbride (EKB) est évalué et audité dans le cadre du programme de maintenance PM 2002/02. Les conclusions des travaux associés sont satisfaisantes. L'environnement de développement lié à ce site n'a donc pas fait l'objet d'évaluation au sein de ce projet.

Pour les sites d'Atmel et de Dupont Photomask à Rousset (RFO), les aspects environnementaux avaient été évalués et audités dans le cadre du projet précédent (cf. contexte §1.1). Seuls certains aspects liés aux changements environnementaux depuis le projet précédent ont fait l'objet de vérification sur site, ainsi que l'évaluation de la mise à jour de certaines procédures Atmel (cf. Annexe 1). Les rapports d'audits se trouvent sous la référence [Audit].

Pour le développement et la fabrication du micro-circuit, le système de gestion de configuration est donc utilisé conformément au plan de gestion de configuration [ACM].

La liste de configuration [LGC] identifie les éléments tracés par le système de gestion de configuration. Les éléments de configuration identifiés dans la liste de configuration sont maintenus par le système de gestion de configuration. Les procédures de génération du produit sont efficaces pour s'assurer que les bons éléments de configuration sont utilisés pour générer le micro-circuit.

Les mesures de sécurité décrites dans les procédures fournissent le niveau nécessaire de protection pour maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation.

Les documents fournis pour la classe ACM – gestion de la configuration – et ALC – support au cycle de vie – répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

#### ***2.5.5. Tests fonctionnels***

L'évaluateur a vérifié que toutes les fonctions de sécurité et les interfaces de la spécification fonctionnelle du produit sont reliées à au moins un test fonctionnel dans la documentation de test. Il a vérifié aussi que toutes les caractéristiques fonctionnelles de chaque fonction de sécurité, telles qu'elles sont décrites dans la conception de haut niveau [ADV, chapitre 3], sont couvertes par les tests du développeur.

Les tests ont été réalisés sur des micro-circuits de référence : AT90SC3232CS (AT568D9 révision K). L'évaluateur a vérifié que ces micro-circuits correspondaient effectivement au produit identifié au §1.2 du présent rapport.

#### ***2.5.6. Estimation des vulnérabilités***

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement couvertes.

L'évaluateur a réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités supplémentaires.  
Le produit dans son environnement d'exploitation est résistant à des attaquants disposant d'un potentiel d'attaque **élevé**.

### 3. Conclusions de l'évaluation

#### 3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation du micro-circuit AT90SC3232CS, de référence AT568D9 révision K et sa librairie logicielle en version 2.1.

#### 3.2. Niveau d'évaluation

Le produit micro-circuit AT90SC3232CS, de référence AT568D9 révision K et sa librairie logicielle en version 2.1 a été évalué selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **EAL4<sup>1</sup> augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_IMP.2	Implementation of the TSF
ALC_DVS.2	Sufficiency of security measures
AVA_VLA.4	Highly resistant

Tableau 1 - Augmentations

Pour tous les composants du niveau d'évaluation du produit, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite
Class ACM	Configuration management	
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Class ADO	Delivery and operation	
ADO_DEL.2	Detection of modification	Réussite

<sup>1</sup> Annexe 5 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].



ADO_IGS.1	Installation, generation, and start-up procedures	Réussite
<b>Class ADV</b>	<b>Development</b>	
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite
ADV_SPM.1	Informal TOE security policy model	Réussite
<b>Class AGD</b>	<b>Guidance</b>	
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite
<b>Class ALC</b>	<b>Life cycle support</b>	
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite
<b>Class ATE</b>	<b>Tests</b>	
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite
<b>Class AVA</b>	<b>Vulnerability assessment</b>	
AVA_MSU.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

Tableau 2 - Composants et verdicts associés

### 3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** [ST chapitre 5] suivantes<sup>1</sup> :

- Potential violation analysis (FAU\_SAA.1)
- Cryptographic Key Generation (FCS\_CKM.1)
- Cryptographic operation (FCS\_COP.1)
- Complete access control (FDP\_ACC.2)
- Security attributes based access control (FDP\_ACF.1)
- Subset information flow control (FDP\_IFC.1)
- Simple security attributes (FDP\_IFF.1)
- Stored data integrity monitoring and action (FDP\_SDI.1)
- User attribute definition (FIA\_ATD.1)

<sup>1</sup> Annexe 4 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- User authentication before any action (FIA\_UAU.2)
- User Identification before any action (FIA\_UID.2)
- Management of security functions behaviour (FMT\_MOF.1)
- Management of security attributes (FMT\_MSA.1)
- Static attribute initialisation (FMT\_MSA.3)
- Specification of management functions (FMT\_SMF.1)
- Security management roles (FMT\_SMR.1)
- Unobservability (FPR\_UNO.1)
- Notification of physical attack (FPT\_PHP.2)
- Resistance to physical attack (FPT\_PHP.3)
- TOE Security Functions testing (FPT\_TST.1)

### **3.4. Résistance des fonctions**

Les fonctions suivantes ont fait l'objet d'une estimation du niveau de résistance :

- authentification de l'administrateur en mode test,
- protection de l'accès à la mémoire de test,
- audit des événements,
- non-observabilité.

Le niveau de résistance des fonctions de sécurité est jugé **élevé (SOF-High)**. Cette cotation est faite conformément au guide « Application of attack potential to smart-card » (cf. [JIL\_AP]).

### **3.5. Analyse des mécanismes cryptographiques**

Le produit a fait l'objet d'une analyse des mécanismes cryptographiques dans le cadre de l'évaluation. Les résultats sont en annexe (cf Annexe 3).

### **3.6. Conformité à un profil de protection**

Le produit évalué est conforme au profil de protection PP/9806 [PP/9806].

### **3.7. Reconnaissance européenne (SOG-IS)**

Ce certificat a été émis dans les conditions de l'accord du SOG-IS. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].

### **3.8. Reconnaissance internationale (CC RA)**

Ce certificat a été émis dans les conditions de l'accord du CC RA. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].

Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA [CC RA] : ADV\_IMP.2, ALC\_DVS.2 et AVA\_VLA.4 (Tableau 1).

### 3.9. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement (§ 3.10) ainsi que les recommandations se trouvant dans les guides utilisateur [USR] et administrateur [ADM].

Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification, et notamment que dans le cas où le code de l'application est chargé sur le micro-circuit dans l'environnement de développement du fondeur identifié au paragraphe 1.3 (ATMEL EKB).

### 3.10. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité suivants sont extraits de la cible de sécurité du produit [ST § 4.2].

#### **Objectifs de sécurité sur l'environnement concernant le système en phase d'utilisation**

Ces objectifs de sécurité concernent le système dans lequel sera utilisé le micro-circuit avec son application embarquée (extraits de la cible de sécurité [ST § 4.2.6]) :

- la communication entre la carte et le terminal doit être sécurisée (en terme de protocole et de procédure),
- le système (terminal, communication,...) doit garantir la confidentialité et l'intégrité des données sensibles qu'il stocke ou qu'il traite.

### 3.11. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le micro-circuit AT90SC3232CS identifié au paragraphe 1.2 et décrit au paragraphe 1.4.1 du présent rapport **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

## Annexe 1. rapport de visite du site **ATMEL Rousset**

Le développement du micro-circuit implique l'ensemble des sites identifiés au §1.3. L'environnement de développement du site d'Atmel East Kilbride (EKB) est évalué et audité régulièrement dans le cadre du programme de maintenance PM 2002/02. Les conclusions des travaux associés sont satisfaisantes. Ils n'ont donc pas fait l'objet d'évaluation pour ce projet. Pour le site d'Atmel à Rousset (RFO), les aspects environnementaux avaient été évalués et audités dans le cadre du projet précédent (cf. contexte §1.1). Seules certaines non-conformités résiduelles identifiées lors du projet précédent ont fait l'objet de vérification sur site, ainsi que l'évaluation de la mise à jour de certaines procédures Atmel :

Pour la phase correspondant à la préparation de la base de données, le site de développement d'Atmel situé au **Z.I. Rousset Peynier 13106 Rousset Cedex France**, a fait l'objet, dans le cadre de l'évaluation du micro-circuit AT90SC3232CS, de référence AT568D9 révision K et sa librairie logicielle en version 2.1, d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM\_AUT.1, ACM\_CAP.4)
- la livraison : **ADO** (ADO\_DEL.2)
- le support au cycle de vie : **ALC** (ALC\_DVS.2)

La visite par un membre du centre d'évaluation accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site.

## **Annexe 2. rapport de visite du site de Dupont Photomasks**

Le site de Dupont Photomasks à Rousset avait été évalué et audité dans le cadre du projet précédent (cf. contexte §1.1). Seules certaines non-conformités résiduelles identifiées lors du projet précédent ont fait l'objet de vérification sur site, ainsi que l'évaluation de la mise à jour de certaines procédures :

Pour la phase correspondant à la préparation de la base de données, le site de développement de **Dupont Photomasks** située au **74, Avenue Perroy 13790 Rousset France**, a fait l'objet, dans le cadre de l'évaluation du micro-circuit AT90SC3232CS, de référence AT568D9 révision K et sa librairie logicielle en version 2.1, d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM\_AUT.1, ACM\_CAP.4)
- la livraison : **ADO** (ADO\_DEL.2)
- le support au cycle de vie : **ALC** (ALC\_DVS.2)

La visite par un membre du centre d'évaluation accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site.

## **Annexe 3. Analyse des mécanismes cryptographiques**

Le micro-circuit AT90SC3232CS, de référence AT568D9 révision K et sa librairie logicielle en version 2.1 offrent les services cryptographiques suivants :

- un générateur de nombres aléatoires,
- un accélérateur de calcul cryptographique DES/3DES et un multiplicateur GF2N (pour les courbes elliptiques),
- un coprocesseur cryptographique (SC16) incluant sa librairie logicielle de 8KB en ROM (boîte à outils cryptographiques) permettant d'accélérer les calculs RSA (avec et sans CRT) et SHA-1. La librairie fournit également des primitives permettant au logiciel embarqué de construire ses propres algorithmes mais ces primitives ne font pas partie du périmètre d'évaluation.

Ces services ne concourent pas à la sécurité propre du micro-circuit. Il s'agit de services pour le logiciel embarqué. Pour cette raison, ces services ne sont pas analysés d'un point de vue cryptographique. Cependant le générateur aléatoire est traité comme un cas particulier et a fait l'objet d'une analyse.

Cette analyse n'a permis de mettre en évidence aucun biais statistique élémentaire. Ceci ne permet pas de dire que les données générées sont réellement aléatoires mais assure que le générateur ne souffre pas de défaut majeur de conception.

## Annexe 4. Exigences fonctionnelles de sécurité du produit évalué

Attention : les descriptions des composants fonctionnels suivants sont données à titre indicatif. Seule une lecture attentive de la cible de sécurité ([ST]) peut apporter la description exacte des exigences fonctionnelles du produit.

Class FAU	Security audit
Security audit analysis	
<b>FAU_SAA.1</b>	<i>Potential violation analysis</i> Le produit doit implémenter un seuil de détection élémentaire, défini selon une règle fixée (spécifiée dans la cible de sécurité [ST]).
Class FCS	Cryptographic support
Cryptographic key management	
<b>FCS_CKM.1</b>	<i>Cryptographic key generation</i> Le produit doit générer des clés cryptographiques conformément à un algorithme et des tailles de clés spécifiées qui peuvent être basés sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
Cryptographic operation	
<b>FCS_COP.1</b>	<i>Cryptographic operation</i> Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée (spécifiés dans la cible de sécurité [ST]).
Class FDP	User data protection
Access control policy	
<b>FDP_ACC.2</b>	<i>Complete access control</i> Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
<b>FDP_ACF.1</b>	<i>Security attribute based access control</i> Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Information flow control policy	
<b>FDP_IFC.1</b>	<i>Subset information flow control</i> Le produit doit appliquer les politiques de sécurité de contrôle de flux d'information, lesquelles sont spécifiées dans la cible de sécurité [ST] pour un sous-ensemble des opérations possibles sur un sous-ensemble des flux d'information.

Information flow control functions	
<b>FDP_IFF.1</b>	<i>Simple security attributes</i> Ce composant impose des attributs de sécurité aux informations, aux sujets qui déclenchent le transfert de ces informations ainsi qu'aux sujets qui reçoivent ces informations. Ce composant spécifie les règles qui doivent être appliquées par la fonction et décrit comment les attributs de sécurité sont choisis par la fonction.
Stored data integrity	
<b>FDP_SDI.1</b>	<i>Stored data integrity monitoring</i> Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées.
<b>Class FIA</b>	<b>Identification and authentication</b>
User attribute definition	
<b>FIA_ATD.1</b>	<i>User attribute definition</i> Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.
User authentication	
<b>FIA_UAU.2</b>	<i>User authentication before any action</i> Les utilisateurs doivent s'authentifier avant que toute action ne soit autorisée.
User identification	
<b>FIA_UID.2</b>	<i>User identification before any action</i> Les utilisateurs doivent s'identifier avant que toute action ne soit autorisée.
<b>Class FMT</b>	<b>Security management</b>
Management of functions in TSF	
<b>FMT_MOF.1</b>	<i>Management of security functions behaviour</i> Le produit doit limiter la capacité à gérer le comportement des fonctions de sécurité du produit à des utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]).
Management of security attributes	
<b>FMT_MSA.1</b>	<i>Management of security attributes</i> Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
<b>FMT_MSA.3</b>	<i>Static attribute initialisation</i> Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Specification of Management Functions	
<b>FMT_SMF.1</b>	<i>Specification of Management Functions</i> Le produit doit fournir les fonctions de gestion de la sécurité spécifiées dans la cible de sécurité [ST].
Security management roles	
<b>FMT_SMR.1</b>	<i>Security roles</i> Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiés dans la cible de sécurité [ST]).



Class FPR	Privacy
Unobservability	
<b>FPR_UNO.1</b>	<p><i>Unobservability</i></p> <p>Le produit n'autorise pas certains utilisateurs (spécifiés dans la cible de sécurité [ST]) à déterminer si certaines opérations (spécifiées dans la cible de sécurité [ST]) sont en cours d'exécution.</p>
Class FPT	Protection of the TSF
TSF physical protection	
<b>FPT_PHP.2</b>	<p><i>Notification of physical attack</i></p> <p>Le produit doit notifier automatiquement l'intrusion physique sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).</p>
<b>FPT_PHP.3</b>	<p><i>Resistance to physical attack</i></p> <p>Le produit doit empêcher ou résister à certaines intrusions physiques (spécifiées dans la cible de sécurité [ST]) sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).</p>
TSF self test	
<b>FPT_TST.1</b>	<p><i>TSF testing</i></p> <p>Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.</p>

## Annexe 5. Niveaux d'assurance prédéfinis IS 15408 ou CC

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
<b>Classe ACM</b> <b>Gestion de configuration</b>	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
<b>Classe ADO</b> <b>Livraison et opération</b>	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
<b>Classe ADV</b> <b>Développement</b>	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
<b>Classe AGD</b> <b>Guides d'utilisation</b>	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
<b>Classe ALC</b> <b>Support au cycle de vie</b>	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
<b>Classe ATE</b> <b>Tests</b>	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
<b>Classe AVA</b> <b>Estimation des vulnérabilités</b>	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

## Annexe 6. Références documentaires du produit évalué

[2002/24]	<p>Rapport de certification 2002/24          ATMEL AT90SC19264RC microcontroller (AT568D5 rev F)          SGDN/DCSSI  <i>Document publié sur le site : <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a></i></p>
[2003/11]	<p>Rapport de certification 2003/11          ATMEL AT90SC9608RC microcontroller (AT578A7 rév D)          SGDN/DCSSI  <i>Document publié sur le site : <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a></i></p>
[ACM]	<p>Document d'interface de la gestion de configuration :</p> <ul style="list-style-type: none"> <li>▪ FELIX CC configuration management (ACM interface document)          Référence : Felix_CM_v1.0, 25/08/03          ATMEL</li> </ul> <p>Plan de configuration :</p> <ul style="list-style-type: none"> <li>▪ FELIX CC configuration management Plan          Référence : Felix_CMP_v1.0, 01/09/03          ATMEL</li> </ul>
[ADV]	<p>FELIX CC Development activity (ADV interface document)          Référence : Felix_DVPT_V1.1 – 18/09/03          ATMEL</p> <p>Ce document présente une vue d'ensemble de la description des différents niveaux de conception et pointe sur les différents documents de description associés ayant servi pour l'évaluation.</p>
[Audit]	<ul style="list-style-type: none"> <li>▪ Visit Report - FELIX Project (Fab 7),          Référence : FLX_RDV_FAB7 version 1.0          CEACI</li> <li>▪ Visit Report - FELIX Project (Dupont),          Référence : FLX_RDV_DUP version 1.0          CEACI</li> </ul>
[DEL]	<p>Document d'interface des livraisons et opérations :</p> <ul style="list-style-type: none"> <li>▪ Felix CC delivery and operation (ADO interface document),          section 2 : « Evaluation of delivery (ADO_DEL.2) »,          Référence : Felix_del_v1.0 – 14/11/02,          ATMEL</li> </ul> <p>Procédure spécifique liée à la livraison du code</p> <ul style="list-style-type: none"> <li>▪ Top level customer code submission process»,          Référence : SITE/REF/002, Rev. 0,          ATMEL</li> </ul>

[IGS]	Felix CC delivery and operation (ADO interface document), section 3 : « Installation, generation and start-up (ADO_IGS.1) », Référence : Felix_del_v1.0 – 14/11/02, ATMEL
[LGC]	<p>Liste de configuration du design :</p> <ul style="list-style-type: none"> <li>▪ FELIX Design Configuration List, Référence : Felix_DCL_v1.1, 08/09/03 ATMEL</li> </ul> <p>Liste de configuration de la fabrication :</p> <ul style="list-style-type: none"> <li>▪ FELIX Manufacturing Configuration List, Référence : Felix_MCL_V1.0, 16/09/03 ATMEL</li> </ul> <p>Liste des patterns et des masques :</p> <ul style="list-style-type: none"> <li>▪ AT90SC3232CS (568D9) Rev 'K' PML, Référence : Felix_568D9_REVK_PML_v1.2, 28/07/03 ATMEL</li> </ul> <p>Liste des fournitures ATMEL :</p> <ul style="list-style-type: none"> <li>▪ FELIX deliverables list 9 October 2003, Référence : Felix_EDL_09Oct03 ATMEL</li> </ul>
[MOD_ SIA]	<p>Un document décrit les évolutions entre :</p> <ul style="list-style-type: none"> <li>▪ Felix Modules Update From VEGA2, Référence : Felix_MOD version 1.0 du 20/08/02 ATMEL</li> </ul> <p>Un document développeurs décrit l'impact de ces évolutions sur la sécurité du produit :</p> <ul style="list-style-type: none"> <li>▪ Felix Security Impact Analysis (Vega2 Derivative), Référence : Felix_SIA version 1.0 du 14/08/02 ATMEL</li> </ul>
[PP9806]	<p>Common Criteria for Information Technology Security Evaluation - Protection Profile : Smart Card Integrated Circuit Version 2.0, Issue September 1998. Certifié par le centre de certification français sous la référence 9806. <i>Document publié sur le site : <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a></i></p>
[RTE]	<ul style="list-style-type: none"> <li>▪ EVALUATION TECHNICAL REPORT OF FELIX Project, Référence : FLX_RTE, version 1.0L CEACI</li> <li>▪ ADDENDUM TO THE EVALUATION TECHNICAL REPORT OF FELIX Project Référence : FLX_RTE_ADD, version 1.0 CEACI</li> </ul>

[ST]	<p>FELIX Security target Référence : Felix_ST_V1.4 (15/10/03) Atmel</p>
[USR]	<p>Un document générique sert d'interface pour toute la documentation d'utilisation :</p> <ul style="list-style-type: none"> <li>▪ Felix Guidance AGD interface document Référence : Felix_guid_v1.0, 08/08/03 Atmel</li> </ul> <p>Les documents associés sont :</p> <ul style="list-style-type: none"> <li>▪ Technical Data AT90SC3232CS Data sheet, Référence : 1572BX, rev. B, 22/09/03, Atmel</li> <li>▪ AT90SC technical data (preliminary) Addressing Modes &amp; Instruction Set, Référence : 1323, Rev. B, 26 Feb 2001 Atmel</li> <li>▪ Toolbox v2.1 SC16 crypto-coprocessor library, Référence : TPR0096AX-14Aug02/ARCP, rev A, 12/03/03 Atmel</li> <li>▪ FELIX Wafer Sawing Recommendation, Référence : Felix_WSR_V1.0, 08/08/03 Atmel</li> <li>▪ Securing the RSA operations on the AT 90SC ASL 4, Référence : TPR0062C, rev. C, 13 May 2003 Atmel</li> <li>▪ Securing the DES/TDES on the AT90SC ASL 4, Référence : TPR0063C, rev. C, 21/03/03, Atmel</li> <li>▪ Checksum Accelerator use on the AT90SC ASL4 products, Référence : TPR0065-02July02/ARCP, rev. A, Atmel</li> <li>▪ Security recommendation for AT90SC ASL4, Référence : TPR0066C rev. C, 30/04/03 Atmel</li> <li>▪ Generating unpredictable random numbers on AT90SC Family devices, Référence : 1573CX rev. C, 21/03/03 Atmel</li> <li>▪ App note : Using the supervisor and user modes on the AT90SC ASL4 products, Référence : TPR0095A, rev. A, 11/03/03 Atmel</li> </ul>

	<ul style="list-style-type: none"><li data-bbox="502 224 1129 331">▪ Errata sheet AT90SC3232CS 568D9 Rev K, Référence : TPR0109AX, rev. A, 29/09/03 Atmel</li></ul>
--	---

## Annexe 7. Références liées à la certification

	Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
	Décret 2001-272 du 30 mars 2001- Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.
[CC]	<p>Critères Communs pour l'évaluation de la sécurité des technologies de l'information:</p> <ul style="list-style-type: none"> <li>▪ Part 1: Introduction and general model, august 1999, version 2.1, ref CCIMB-99-031 ;</li> <li>▪ Part 2: Security functional requirements, august 1999, version 2.1, ref CCIMB-99-032 ;</li> <li>▪ Part 3: Security assurance requirements, august 1999, version 2.1, réf: CCIMB-99-033.</li> </ul>
[CEM]	<p>Méthodologie d'évaluation de la sécurité des technologies de l'information:</p> <ul style="list-style-type: none"> <li>▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.</li> </ul>
[IS 15408]	<p>Norme IS/IEC 15408 :1999, comportant 3 documents :</p> <ul style="list-style-type: none"> <li>▪ IS 15408-1: (Part 1) Introduction and general model ;</li> <li>▪ IS 15408-2: (Part 2) Security functional requirements ;</li> <li>▪ IS 15408-3: (Part 3) Security assurance requirements ;</li> </ul>
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, may 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[JIL_IC]	Joint Interpretation Library - The Application of CC to Integrated Circuits, Version 1.0, January 2000
[JIL_AP]	Joint Interpretation Library - Application of attack potential to smart-cards, version 1.0, March 2002

Toute correspondance relative à ce rapport 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 cedex 07 SP

[certification.dcssi@sgdn.pm.gouv.fr](mailto:certification.dcssi@sgdn.pm.gouv.fr)

La reproduction de ce document sans altérations ni coupures est autorisée.