



PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2008/17

Microcontrôleur RISC S3FS9CI 32-bit pour applications S-SIM

Paris, le 23 juin 2008

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

Patrick Pailloux
[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 termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par la Direction centrale de la sécurité des systèmes d'information (DCSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.



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
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.



| | |
|---------------------------------------|--|
| Référence du rapport de certification | DCSSI-2008/17 |
| Nom du produit | Microcontrôleur RISC S3FS9CI 32-bit pour applications S-SIM |
| Référence/version du produit | Microcontrôleur référence : S3FS9CI version 2 Librairies logicielles : Test Rom code version 1, Secure Cryptographic library version 3.8S, RNG1 library version 3.0 |
| Conformité à un profil de protection | BSI-PP-0002-2001 Smart card IC Platform Protection Profile Version 1.0 July 2001 |
| Critères d'évaluation et version | Critères Communs version 2.3 conforme à la norme ISO 15408:2005 |
| Niveau d'évaluation | EAL 4 augmenté ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4 |
| Développeur | Samsung Electronics Co. Ltd San#24 Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, 449-711, République de Corée |
| Commanditaire | Samsung Electronics Co. Ltd San#24 Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, 449-711, République de Corée |
| Centre d'évaluation | CEA - LETI 17 rue des martyrs, 38054 Grenoble Cedex 9, France Tél : +33 (0)4 38 78 40 87, mél : cesti.leti@cea.fr |
| Accords de reconnaissance applicables | <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p>CCRA</p>  </div> <div style="text-align: center;"> <p>SOG-IS</p>  </div> </div> <p>Le produit est reconnu au niveau EAL4.</p> |

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 rendus publics (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 sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

| | |
|---|-----------|
| 1. LE PRODUIT | 6 |
| 1.1. PRESENTATION DU PRODUIT | 6 |
| 1.2. DESCRIPTION DU PRODUIT EVALUE | 6 |
| 1.2.1. <i>Identification du produit</i> | 6 |
| 1.2.2. <i>Services de sécurité</i> | 6 |
| 1.2.3. <i>Architecture</i> | 6 |
| 1.2.4. <i>Cycle de vie</i> | 8 |
| 1.2.5. <i>Configuration évaluée</i> | 9 |
| 2. L’EVALUATION | 10 |
| 2.1. REFERENTIELS D’EVALUATION..... | 10 |
| 2.2. TRAVAUX D’EVALUATION | 10 |
| 2.3. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES | 10 |
| 2.4. ANALYSE DU GENERATEUR D’ALEAS..... | 10 |
| 3. LA CERTIFICATION | 11 |
| 3.1. CONCLUSION | 11 |
| 3.2. RESTRICTIONS D’USAGE..... | 11 |
| 3.3. RECONNAISSANCE DU CERTIFICAT | 11 |
| 3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> | 11 |
| 3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> | 12 |
| ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT..... | 13 |
| ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE | 14 |
| ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION | 16 |

1. Le produit

1.1. Présentation du produit

Le produit évalué est le microcontrôleur RISC S3FS9CI 32-bit, développé par Samsung Electronics Co. Ltd.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications S-SIM. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, 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.

1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité s'inspire du profil de protection [PP0002].

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF §2].

La version certifiée du produit est identifiable par les éléments suivants :

- microcontrôleur référence : S3FS9CI version 2 ;
- bibliothèques logicielles : « Test ROM Code » version 1.0, « Secure Crypto. Library » version 3.8S et « RNG1 Library » version 3.0.

Le produit est physiquement identifié par son code d'identification dessiné sur la couche de métal supérieure. La mémoire flash est également écrite avec l'ensemble des données d'identification. Ces données sont détaillées dans le document de gestion de configuration (cf. [CONF §2.2.2.2]).

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- détection, enregistrement et réaction aux attaques environnementales ;
- contrôle d'accès ;
- non-réversibilité des phases « test » et « user » ;
- contre-mesures matérielles pour la non-observabilité.

1.2.3. Architecture

Le produit S3FS9CI est constitué des éléments suivants :

- une partie matérielle composée :
 - d'un processeur RISC SC100 16/32-bits ;
 - de mémoires : 768Ko de mémoire flash NOR, 32KB de mémoire ROM pour les programmes, 8KB de mémoire ROM pour le programme de test, 50KB de



- mémoire RAM et 2KB de mémoire RAM dédiée pour les calculs cryptographiques;
- de modules de sécurité : module de protection mémoires (MPU), module pour le chiffrement / déchiffrement des mémoires, contrôle d'intégrité à la volée (CRC), détecteurs de sécurité (température, voltage, fréquence, probing) ;
 - de modules fonctionnels : gestion des entrées/sorties en mode contact, port série avec une interface et un contrôleur conforme au standard ISO7816, coprocesseur sécurisé DES/T-DES et AES, coprocesseur sécurisé Tornado™ pour le chiffrement asymétrique RSA.
- une partie « logiciels dédiés » en ROM intégrant :
- une bibliothèque pour les calculs arithmétiques modulaires pour le support à la cryptographie asymétrique RSA (optionnelle) ;
 - une bibliothèque pour la génération déterministe de nombres aléatoires (DRNG) ;
 - des logiciels dédiés de tests du microcontrôleur.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

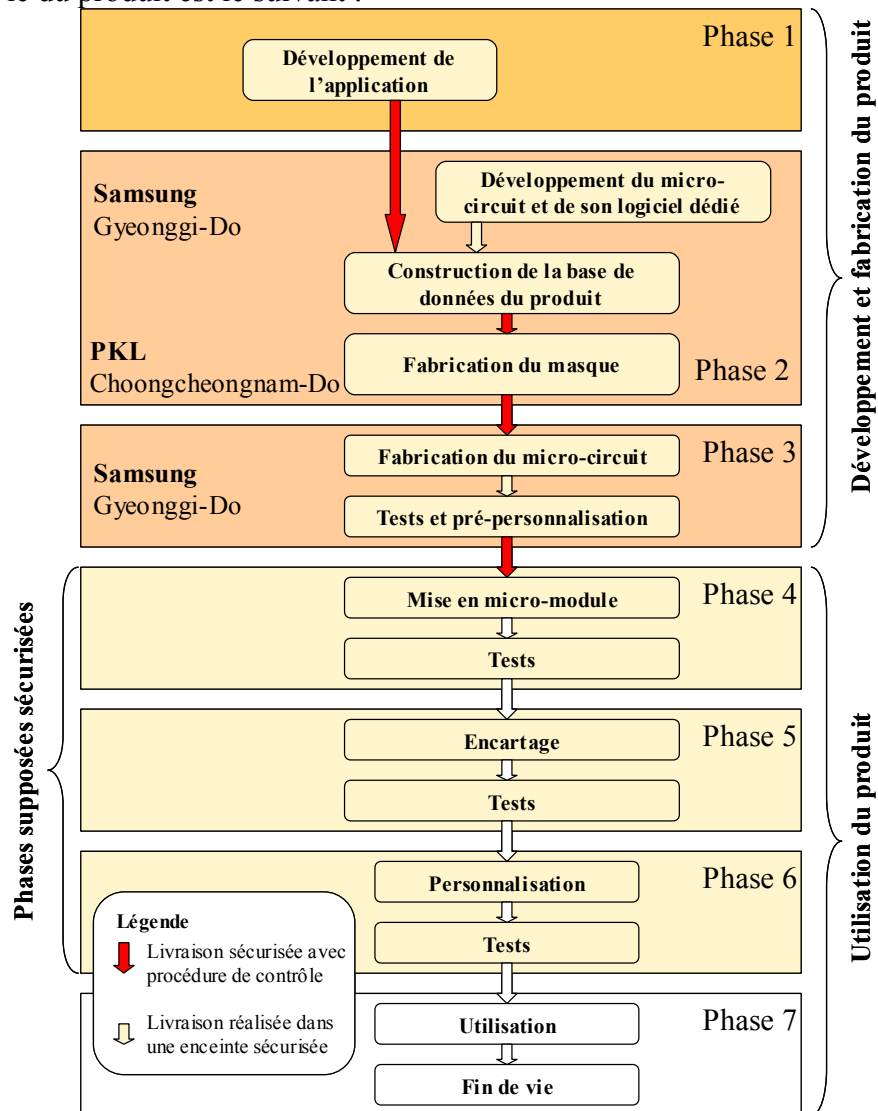


Figure 1 - Cycle de vie du produit

Le design du produit est réalisé par :

Samsung Electronics Co. Ltd - C&M Development team

San#24 Nongseo-Ri, Giheung-Eup,
Yongin-City, Gyeonggi-Do, 449-711,
République de Corée

Les réticules du microcontrôleur sont fabriqués par :

PKL

493-3 Sungsung-dong, Cheonan-City,
Choongcheongnam-Do, 330-300,
République de Corée



Le produit est fabriqué par :

Samsung Electronics Co. Ltd – Line 5

San#24 Nongseo-Ri, Giheung-Eup,
Yongin-City, Gyeonggi-Do, 449-711,
République de Corée

Le produit est fabriqué et testé par :

Samsung Electronics Co. Ltd – Line 2

San#24 Nongseo-Ri, Giheung-Eup,
Yongin-City, Gyeonggi-Do, 449-711,
République de Corée

Le microcontrôleur comporte deux modes d'utilisation :

- un mode « Test », dans lequel le fonctionnement du microcontrôleur est testé à l'aide d'un système de test externe. Cette étape est réalisée dans l'enceinte sécurisée du site du développeur. Après la phase de test, le mode « test » est inhibé de façon irréversible. L'interface de test n'est alors plus accessible ;
- un mode « utilisateur », dans lequel le microcontrôleur fonctionne sous le contrôle du logiciel embarqué de la carte à puce. Les utilisateurs finaux ne peuvent utiliser le microcontrôleur que dans ce mode.

1.2.5. Configuration évaluée

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur seul. Toute application, éventuellement embarquée pour les besoins de l'évaluation, ne fait pas partie du périmètre d'évaluation.

Les interfaces d'extension mémoire ne font pas partie du périmètre d'évaluation, de même que les interfaces MMC et USB.

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

Pour les besoins de l'évaluation, le microcontrôleur S3FS9CI a été fourni au centre d'évaluation avec un système d'exploitation logiciel dédié, dans un mode dit « ouvert¹ ».

¹ Mode permettant de charger et d'exécuter du code natif en Flash et de déconnecter les mécanismes sécuritaires paramétrables.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par la DCSSI et compatibles avec le document [AIS 34], ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation¹ du produit S3CC9GW certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 21 février 2007 sous la référence BSI-DSZ-CC-0400-2007.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 18 juin 2008, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « réussite ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

2.4. Analyse du générateur d'aléas

Le produit évalué offre un générateur d'aléas déterministe qui peut être utilisé par le logiciel embarqué.

La conformité du générateur de nombres aléatoires au référentiel cryptographique de la DCSSI (cf. [REF-CRY]) a été évaluée.

Le générateur atteint le niveau « standard ».

¹ Réutilisation des résultats relatifs à l'environnement de développement

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « Microcontrôleur RISC S3FS9CI 32-bit pour applications S-SIM » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Ce certificat donne une appréciation de la résistance du produit S3FS9CI à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST] au chapitre 4.2 et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance 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 suivante :



¹ Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires¹, des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, la République de Corée, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

| Classe | Famille | Composants par niveau d'assurance | | | | | | | Niveau d'assurance retenu pour le produit | |
|--------------------------------------|---------|-----------------------------------|-------|-------|-------|-------|-------|-------|---|--|
| | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 | EAL 4+ | Intitulé du composant |
| ACM Gestion de configuration | ACM_AUT | | | | 1 | 1 | 2 | 2 | 1 | Partial CM automation |
| | ACM_CAP | 1 | 2 | 3 | 4 | 4 | 5 | 5 | 4 | Configuration support and acceptance procedures |
| | ACM_SCP | | | 1 | 2 | 3 | 3 | 3 | 2 | Problem tracking CM coverage |
| ADO Livraison et opération | ADO_DEL | | 1 | 1 | 2 | 2 | 2 | 3 | 2 | Detection of modification |
| | ADO_IGS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Installation, generation and start-up procedures |
| ADV Développement | ADV_FSP | 1 | 1 | 1 | 2 | 3 | 3 | 4 | 2 | Fully defined external interfaces |
| | ADV_HLD | | 1 | 2 | 2 | 3 | 4 | 5 | 2 | Security enforcing high-level design |
| | ADV_IMP | | | | 1 | 2 | 3 | 3 | 2 | Implementation of the TSF |
| | ADV_INT | | | | | 1 | 2 | 3 | | |
| | ADV_LLD | | | | 1 | 1 | 2 | 2 | 1 | Descriptive low-level design |
| | ADV_RCR | 1 | 1 | 1 | 1 | 2 | 2 | 3 | 1 | Informal correspondence demonstration |
| | ADV_SPM | | | | 1 | 3 | 3 | 3 | 1 | Informal TOE security policy model |
| AGD Guides d'utilisation | AGD_ADM | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Administrator guidance |
| | AGD_USR | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | User guidance |
| ALC Support au cycle de vie | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 | 2 | Sufficiency of security measures |
| | ALC_FLR | | | | | | | | | |
| | ALC_LCD | | | | 1 | 2 | 2 | 3 | 1 | Developer defined life-cycle model |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 | 1 | Well-defined development tools |
| ATE Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 | 2 | Analysis of coverage |
| | ATE_DPT | | | 1 | 1 | 2 | 2 | 3 | 1 | Testing: high-level design |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 | 1 | Functional testing |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | Independent testing – sample |
| AVA Estimation des vulnérabilités | AVA_CCA | | | | | 1 | 2 | 2 | | |
| | AVA_MSU | | | 1 | 2 | 2 | 3 | 3 | 3 | Analysis and testing of insecure states |
| | AVA_SOF | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Strength of TOE security function evaluation |
| | AVA_VLA | | 1 | 1 | 2 | 3 | 4 | 4 | 4 | Highly resistant |

Annexe 2. Références documentaires du produit évalué

| | |
|----------|--|
| [ST] | <p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - Project Chinook - Security Target of S3FS9CI 32-bit RISC Microcontroller For S-SIM, Version 1.7, 28th May 2008 Samsung Electronics Co. Ltd <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - Security Target Lite of S3FS9CI 32-bit RISC Microcontroller For S-SIM, Version 1.0, 4th June 2008 Samsung Electronics Co. Ltd |
| [RTE] | <p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Chinook – Rapport technique d'évaluation, Référence : LETI.CESTI.CHI.RTE.001 - v1.0 - 29/05/2008, CESTI LETI <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :</p> <ul style="list-style-type: none"> - Chinook project - Evaluation Technical Report – lite, Référence : CESTI.LETI.CHI.ETR.002, Version 1.1 CESTI LETI |
| [CONF] | <p>Project < CHINOOK >, Configuration Management Documentation (Class ACM_AUT/CAP/SCP), Version 1.5, Issued on 27th May, 2008, Samsung Electronics Co. Ltd</p> |
| [GUIDES] | <p>Les guides du produit sont constitués des documents suivants :</p> <ul style="list-style-type: none"> - Project <CHINOOK> Guidance Documents (Class AGD), Version 1.4, Issued on 26th May 2008, Samsung Electronics Co. Ltd - User's manual – S3FS9CI – 32-bit CMOS Microcontroller for S-SIM, Revision 1.12, May 2008, Samsung Electronics Co. Ltd - Security Application Note - S3FS9CI, version 1.11, Samsung Electronics Co. Ltd - Application Note - RSA Crypto Library with TORNADO™ V3.8S, Version 1.10, Samsung Electronics Co. Ltd - Application Note - DRNG Software Library, Version 3.0, Samsung Electronics Co. Ltd |



| | |
|----------|---|
| | <ul style="list-style-type: none">- Project Chinook - Test-Administrator's Guidance, Version 1.1, Issued on 12th March 2008, Samsung Electronics Co. Ltd |
| [PP0002] | Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.</i> |

Annexe 3. 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. |
| [CER/P/01] | Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005. |
| [CEM] | Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005. |
| [CC IC] | Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006. |
| [CC AP] | Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2007-04-001 version 2.3, revision 1, April 2007. |
| [COMP] | Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007. |
| [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. |
| [REF-CRY] | Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto. |



| | |
|----------|---|
| [AIS 34] | Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, BSI (Bundesamt für Sicherheit in der Informationstechnik) |
|----------|---|