



PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

**Rapport de certification ANSSI-CC-PP-2012/01  
du profil de protection  
« Lecteur sécurisé de carte  
avec interface homme machine »  
(PP LSCIHM)  
version 1.6**

*Paris, le 5 avril 2012*

*Le directeur général de l'agence nationale  
de la sécurité des systèmes d'information*

Patrick Pailloux





---

## Avertissement

Ce rapport atteste la conformité de la version évaluée du profil de protection aux critères d'évaluation.

Un profil de protection est un document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale  
Agence nationale de la sécurité des systèmes d'information  
Centre de certification national  
51, boulevard de la Tour Maubourg  
75700 Paris cedex 07 SP

[certification.anssi@ssi.gouv.fr](mailto:certification.anssi@ssi.gouv.fr)

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

|                                                                                                        |                                                                                                        |
|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Référence du rapport de certification                                                                  |                                                                                                        |
| <b>ANSSI-CC-PP-2012/01</b>                                                                             |                                                                                                        |
| Nom du profil de protection                                                                            |                                                                                                        |
| <b>Lecteur sécurisé de carte avec interface homme machine<br/>(PP LSCIHM)</b>                          |                                                                                                        |
| Référence/version du profil de protection                                                              |                                                                                                        |
| <b>version 1.6</b>                                                                                     |                                                                                                        |
| Conformité à un profil de protection                                                                   |                                                                                                        |
| <b>Néant</b>                                                                                           |                                                                                                        |
| Critères d'évaluation et version                                                                       |                                                                                                        |
| <b>Critères Communs version 3.1 révision 3</b>                                                         |                                                                                                        |
| Niveau d'évaluation imposé par le PP                                                                   |                                                                                                        |
| <b>EAL 3 augmenté de<br/>ADV_FSP.4, ADV_IMP.1, ADV_TDS.3,<br/>ALC_FLR.3, ALC_TAT.1 et AVA.VAN.3</b>    |                                                                                                        |
| Rédacteur(s)                                                                                           |                                                                                                        |
| <b>Xiring</b><br>25 quai Gallieni<br>92158 Suresnes Cedex, France                                      | <b>Gemalto</b><br>6 rue de la Verrerie,<br>92197 Meudon Cedex, France                                  |
| Commanditaire                                                                                          |                                                                                                        |
| <b>ANSSI</b><br>51 boulevard de La Tour-Maubourg, 75700 Paris 07 SP, France                            |                                                                                                        |
| Centre d'évaluation                                                                                    |                                                                                                        |
| <b>THALES - CEACI (T3S – CNES)</b><br>18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France |                                                                                                        |
| Accords de reconnaissance applicables                                                                  |                                                                                                        |
| <b>CCRA</b><br>     | <b>SOG-IS</b><br> |

---

## 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 modifié. Ce décret indique que :

- L'agence nationale 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 publiques et disponibles en français sur le site Internet :

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

## Table des matières

|                                                      |           |
|------------------------------------------------------|-----------|
| <b>1. PRÉSENTATION DU PROFIL DE PROTECTION.....</b>  | <b>6</b>  |
| 1.1. IDENTIFICATION DU PROFIL DE PROTECTION.....     | 6         |
| 1.2. RÉDACTEUR.....                                  | 6         |
| 1.3. DESCRIPTION DU PROFIL DE PROTECTION .....       | 6         |
| 1.3.1. Généralités .....                             | 6         |
| 1.3.2. Parapheur électronique.....                   | 6         |
| 1.3.3. Canal sécurisé .....                          | 6         |
| 1.4. EXIGENCES FONCTIONNELLES.....                   | 7         |
| 1.5. EXIGENCES D'ASSURANCE .....                     | 7         |
| <b>2. L'ÉVALUATION .....</b>                         | <b>8</b>  |
| 2.1. RÉFÉRENTIELS D'ÉVALUATION .....                 | 8         |
| 2.2. COMMANDITAIRE .....                             | 8         |
| 2.3. CENTRE D'ÉVALUATION.....                        | 8         |
| 2.4. TRAVAUX D'ÉVALUATION.....                       | 8         |
| <b>3. LA CERTIFICATION .....</b>                     | <b>9</b>  |
| 3.1. CONCLUSION .....                                | 9         |
| 3.2. RECONNAISSANCE EUROPÉENNE (SOG-IS) .....        | 9         |
| 3.3. RECONNAISSANCE INTERNATIONALE (CC RA).....      | 9         |
| <b>ANNEXE 1. NIVEAU D'ÉVALUATION DU PRODUIT.....</b> | <b>10</b> |
| <b>ANNEXE 2. RÉFÉRENCES .....</b>                    | <b>11</b> |

---

## 1. Présentation du profil de protection

### 1.1. Identification du profil de protection

Titre : Lecteur de carte sécurisé avec interface homme machine [PP]

Nom : PP LSCIHM

Version : v1.6

Date : 20 décembre 2011

### 1.2. Rédacteur

Ce profil de protection a été rédigé par :

Xiring  
25 quai Gallieni  
92158 Suresnes Cedex, France

Gemalto  
6 rue de la Verrerie,  
92197 Meudon Cedex, France

### 1.3. Description du profil de protection

#### 1.3.1. Généralités

Ce profil de protection décrit les exigences de sécurité d'un lecteur de carte avec clavier et affichage permettant la saisie du code confidentiel. Le principal avantage de cette méthode est de s'affranchir des menaces pesant sur la gestion du code confidentiel dans le poste de travail.

En plus du mode de saisie simple du code confidentiel, le lecteur décrit par dans ce profil de protection est capable de gérer deux autres modes particuliers présentés ci-dessous.

#### 1.3.2. Parapheur électronique

Pour des applications de signature électronique, les cartes à puce utilisées (*Secure Signature Creation Device*) imposent une présentation du code confidentiel à chaque signature. Toutefois certaines applications fonctionnent dans un mode dit de « parapheur électronique » et permettent de signer électroniquement un ensemble de documents préalablement validés dans un environnement de confiance en ne présentant le code confidentiel à la carte qu'une seule fois.

#### 1.3.3. Canal sécurisé

Dans certaines situations, un code confidentiel peut être transmis directement à la carte dans un canal sécurisé depuis un environnement de confiance. Dans ce cas, le lecteur laisse passer, sans la traiter, la commande contenant le code confidentiel chiffré. Cette situation se retrouve par exemple pour transmettre un code confidentiel de déverrouillage à la carte à puce depuis un poste d'administration.

## 1.4. Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** (SFR) définies par le profil de protection sont les suivantes :

| Exigences fonctionnelles | Définitions                                                                                                                          |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| FDP_IFC.1                | Subset information flow control                                                                                                      |
| FDP_IFF.1                | Simple security attributes                                                                                                           |
| FDP_RIP.2                | Full residual information protection                                                                                                 |
| FDP_UIT.1                | Data exchange integrity addresses detection of modifications, deletions, insertions, and replay errors of the user data transmitted. |
| FPT_PHP.1                | Passive detection of physical attack                                                                                                 |
| FPT_TOE                  | Material protection                                                                                                                  |

Tableau 1 : Liste des SFR selon les packages définis dans le PP

Les exigences fonctionnelles du profil de protection sont liées à la partie 2 des Critères Communs [CC].

## 1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau 3. Ce niveau d'assurance est augmenté par les composants d'assurances suivants :

| Exigences d'assurance | Définitions                              |
|-----------------------|------------------------------------------|
| ADV_FSP.4             | Complete functional specification        |
| ADV_IMP.1             | Implementation representation of the TSF |
| ADV_TDS.3             | Basic modular design                     |
| ALC_FLR.3             | Systematic flaw remediation              |
| ALC_TAT.1             | Well-defined development tools           |
| AVA_VAN.3             | Focused vulnerability analysis           |

Tableau 2 – Augmentations

Les exigences d'assurance du profil de protection sont liées à la partie 3 des Critères Communs [CC].

---

## 2. L'évaluation

### 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC] à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

### 2.2. Commanditaire

#### **ANSSI**

51 boulevard de La Tour-Maubourg,  
75700 Paris 07 SP,  
France

### 2.3. Centre d'évaluation

#### **THALES – CEACI (T3S – CNES)**

18 avenue Edouard Belin  
BPI 1414  
31401 Toulouse Cedex 9  
France

### 2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 3 janvier 2012, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation relatives à la classe d'exigences d'assurance APE sont à « **réussite** ».

## 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.

### 3.2. Reconnaissance européenne (SOG-IS)

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

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord<sup>1</sup>, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Élémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



### 3.3. Reconnaissance internationale (CC RA)

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires<sup>2</sup>, 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 :



---

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

<sup>2</sup> 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, le Pakistan, les Pays-Bas, la République de Corée, 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<br>1                          | EAL<br>2 | EAL<br>3 | EAL<br>4 | EAL<br>5 | EAL<br>6 | EAL<br>7 | EAL<br>3+                                 | Intitulé du composant                     |
| ADV<br>Développement                      | ADV_ARC |                                   | 1        | 1        | 1        | 1        | 1        | 1        | 1                                         | Security architecture description         |
|                                           | ADV_FSP | 1                                 | 2        | 3        | 4        | 5        | 5        | 6        | 4                                         | Complete functional specification         |
|                                           | ADV_IMP |                                   |          |          | 1        | 1        | 2        | 2        | 1                                         | Implementation representation of the TSF  |
|                                           | ADV_INT |                                   |          |          |          | 2        | 3        | 3        |                                           |                                           |
|                                           | ADV_SPM |                                   |          |          |          |          | 1        | 1        |                                           |                                           |
|                                           | ADV_TDS |                                   | 1        | 2        | 3        | 4        | 5        | 6        | 3                                         | Basic modular design                      |
| AGD<br>Guides d'utilisation               | AGD_OPE | 1                                 | 1        | 1        | 1        | 1        | 1        | 1        | 1                                         | Operational user guidance                 |
|                                           | AGD_PRE | 1                                 | 1        | 1        | 1        | 1        | 1        | 1        | 1                                         | Preparative procedures                    |
| ALC<br>Support au cycle de vie            | ALC_CMC | 1                                 | 2        | 3        | 4        | 4        | 5        | 5        | 3                                         | Authorisation controls                    |
|                                           | ALC_CMS | 1                                 | 2        | 3        | 4        | 5        | 5        | 5        | 3                                         | Implementation representation CM coverage |
|                                           | ALC_DEL |                                   | 1        | 1        | 1        | 1        | 1        | 1        | 1                                         | Delivery procedures                       |
|                                           | ALC_DVS |                                   |          | 1        | 1        | 1        | 2        | 2        | 1                                         | Identification of security measures       |
|                                           | ALC_FLR |                                   |          |          |          |          |          |          | 3                                         | Systematic flaw remediation               |
|                                           | ALC_LCD |                                   |          | 1        | 1        | 1        | 1        | 2        | 1                                         | Developer defined life-cycle model        |
|                                           | ALC_TAT |                                   |          |          | 1        | 2        | 3        | 3        | 1                                         | Well-defined development tools            |
| ASE<br>Evaluation de la cible de sécurité | ASE_CCL | 1                                 | 1        | 1        | 1        | 1        | 1        | 1        | 1                                         | Conformance claims                        |
|                                           | ASE_ECD | 1                                 | 1        | 1        | 1        | 1        | 1        | 1        | 1                                         | Extended components definition            |
|                                           | ASE_INT | 1                                 | 1        | 1        | 1        | 1        | 1        | 1        | 1                                         | ST introduction                           |
|                                           | ASE_OBJ | 1                                 | 2        | 2        | 2        | 2        | 2        | 2        | 2                                         | Security objectives                       |
|                                           | ASE_REQ | 1                                 | 2        | 2        | 2        | 2        | 2        | 2        | 2                                         | Derived security requirements             |
|                                           | ASE_SPD |                                   | 1        | 1        | 1        | 1        | 1        | 1        | 1                                         | Security problem definition               |
|                                           | ASE_TSS | 1                                 | 1        | 1        | 1        | 1        | 1        | 1        | 1                                         | TOE summary specification                 |
| ATE<br>Tests                              | ATE_COV |                                   | 1        | 2        | 2        | 2        | 3        | 3        | 2                                         | Analysis of coverage                      |
|                                           | ATE_DPT |                                   |          | 1        | 1        | 3        | 3        | 4        | 1                                         | Testing: basic 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<br>Estimation des vulnérabilités      | AVA_VAN | 1                                 | 2        | 2        | 3        | 4        | 5        | 5        | 3                                         | Focused vulnerability analysis            |

## Annexe 2. Références

|                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. |                                                                                                                                                                                                                                                                                                                                                                                                           |
| [CPP/P/01]                                                                                                                                                                       | Procédure CPP/P/01 Certification de profils de protection, DCSSI.                                                                                                                                                                                                                                                                                                                                         |
| [CC]                                                                                                                                                                             | Common Criteria for Information Technology Security Evaluation :<br>Part 1: Introduction and general model,<br>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001;<br>Part 2: Security functional components,<br>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002;<br>Part 3: Security assurance components,<br>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003. |
| [CEM]                                                                                                                                                                            | Common Methodology for Information Technology Security Evaluation :<br>Evaluation Methodology,<br>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.                                                                                                                                                                                                                                         |
| [CC RA]                                                                                                                                                                          | Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, mai 2000.                                                                                                                                                                                                                                                                                 |
| [SOG-IS]                                                                                                                                                                         | Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.                                                                                                                                                                                                                                                               |
| [RTE]                                                                                                                                                                            | Protection Profile evaluation detailed technical report.<br>Project: PP LSC IHM, référence LSC_APE, version 3.0 du 3 janvier 2012.                                                                                                                                                                                                                                                                        |
| [PP]                                                                                                                                                                             | Profil de Protection Lecteur Sécurisé de Carte avec Interface Homme-Machine, version v1.6 du 20 décembre 2011.                                                                                                                                                                                                                                                                                            |