PREMIER MINISTRE

*Liberté*
*Égalité*
*Fraternité*

**Secrétariat général de la défense et de la sécurité nationale**

Agence nationale de la sécurité des systèmes d'information

# Rapport de certification ANSSI-CC-2021/36

## ID-A v1.0 on ID-ONE COSMO X (Codes SAAAAR : 417692 et 417641)

Paris, le 27 juillet 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

# 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 présupposées 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 l'Agence nationale de la sécurité des systèmes d'information (ANSSI) 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 et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

**ANSSI-CC-2021/36**

Nom du produit

**ID-A v1.0 on ID-ONE COSMO X**

Référence/version du produit

**Code SAAAR de l'applet : 417692**
**Code SAAAR du Common package : 417641**

Conformité à un profil de protection

***Protection profiles for secure signature creation device:***
*Part 2 : Device with key generation, v2.0.1, BSI-CC-PP-0059-2009-MA-01;*
*Part 3 : Device with key import, v1.0.2, BSI-CC-PP-0075-2012;*
*Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012;*
*Part 5 : Extension for device with key generation and trusted communication with signature creation application, v1.0.1, BSI-CC-PP-0072-2012;*
*Part 6 : Extension for device with key import and trusted communication with signature creation application, v1.0.4, BSI-CC-PP-0076-2013.*

Critère d'évaluation et version

**Critères Communs version 3.1 révision 5**

Niveau d'évaluation

**EAL 5 augmenté**
ALC_DVS.2, AVA_VAN.5

Développeurs

**IDEMIA**
2 place Samuel de Champlain
92400 Courbevoie, France

**INFINEON TECHNOLOGIES AG**
AIM CC SM PS – Am Campeon 1-12
85579 Neubiberf, Allemagne

Commanditaire

**IDEMIA**
2 place Samuel de Champlain
92400 Courbevoie, France

Centre d'évaluation

**CEA - LETI**
17 avenue des martyrs,
38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

**CCRA**

Ce certificat est reconnu au niveau EAL2.

**SOG-IS**

# PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est « ID-A v1.0 on ID-ONE COSMO X, Code SAAAR de l'*applet* : 417692, Code SAAAR du *Common package* : 417641 » développé par IDEMIA.

Ce produit est une carte à puce constituée d'un logiciel conforme au standard IAS ECC v2 et d'un microcontrôleur sécurisé disposant d'interface avec et sans contact. Il est destiné à être utilisée comme dispositif sécurisé de création de signature (SSCD[1]). Il peut être utilisé dans différents types de documents (carte d'identité, carte de santé, carte d'entreprise, etc.).

## 1.2 Produit

### 1.2.1 *Introduction*

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

Cette cible de sécurité est conforme aux profils de protection [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

### 1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont décrits au chapitre « 3.3 TOE Usage and Major Security Features » de la cible de sécurité [ST]. Ils comprennent notamment :

- la création de signature électronique ;
-
- la génération des clés de signature (c'est-à-dire la génération de la donnée de création de signature (SCD[2]) et de la donnée de vérification de signature (SVD[3]) associée) ;
- l'import des clés de signature (c'est-à-dire de la SCD et, optionnellement, de la SVD associée) ;
- l'établissement d'un canal de confiance pouvant permettre la création de signatures électroniques, l'import de la SCD ou l'export de la SVD dans un environnement non protégé ;
- le support de eServices permettant au porteur de carte de réaliser notamment des authentifications client/serveur, du déchiffrement de clé ;
- le support de protocoles d'authentification (symétrique et asymétrique) ;

l'authentification du porteur de carte basée sur la vérification d'un code PIN ou par biométrie ou les deux.

Les principaux services de sécurité de la plateforme sont décrits dans [CER-PTF].

[1] *Secure Signature Creation Device.*

[2] *Signature Création Data.*

[3] *Signature Verification Data.*

### 1.2.3 *Architecture*

Le périmètre d'évaluation (TOE[4]) est constitué :

- du microcontrôleur SLC37, développé par INFINEON TECHNOLOGIES AG et certifié sous la référence [CER-IC] ;
- de la plateforme ouverte ID-One COSMO X, développée par IDEMIA et certifiée sous la référence [CER-PTF] ;
- de l'application ID-A v1.0 composée de l'*applet* ID-A v1.0 et du *Common package*, développés par IDEMIA et en composition sur la plateforme. Ces briques logicielles sont disponibles sous les quatre configurations suivantes :
    - configuration 1 : l'*applet* ID-A sans le support des mécanismes « *asymmetric role authentication* » et « *asymmetric device authentication* » et le *Common package* sans le support de l'authentification par biométrie ;
    - configuration 2 : l'*applet* ID-A avec le support des mécanismes « *asymmetric role authentication* » et « *asymmetric device authentication* » et le *Common package* sans le support de l'authentification par biométrie ;
    - configuration 3 : l'*applet* ID-A sans le support des mécanismes « *asymmetric role authentication* » et « *asymmetric device authentication* » et le *Common package* avec le support de l'authentification par biométrie ;
    - configuration 4 : l'*applet* ID-A avec le support des mécanismes « *asymmetric role authentication* » et « *asymmetric device authentication* » et le *Common package* avec le support de l'authentification par biométrie.

Ces éléments sont décrits dans la cible de sécurité [ST].

D'éventuels patchs logiciels, correspondants à de futures mises à jour du produit, ainsi que d'éventuelles applications peuvent être chargés sur la plateforme Java Card ouverte, à côté de l'application « ID-A v1.0 », comme décrit dans le certificat de la plateforme [CER-PTF]. Ces éléments ne font pas partis du périmètre de cette évaluation.

### 1.2.4 *Identification du produit*

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

La version certifiée du produit est identifiable par les éléments ci-après. Ces éléments sont détaillés dans la cible de sécurité [ST] au chapitre « 1.3 TOE Reference » et dans le guide [AGD_OPE] au chapitre « 4.2 Identification of the product ».

[4] *Target Of Evaluation.*

| Configuration | Détails | Version commerciale (Code SAAAR + version + configuration) | Version interne |
|---|---|---|---|
| 1 | ID-A : ***No*** *Asymmetric Role and Device authentication* | **41 76 92** FF 01 01 00 00 **01 01** | 01 01 01 07 01 01 00 08 |
| | Common package : ***No*** *biometric authentication* | **41 76 41** FF 01 00 00 00 **02 01** | |
| 2 | Applet : ***With*** *Asymmetric Role and Device authentication* | **41 76 92** FF 01 01 00 00 **02 01** | 01 02 01 07 01 01 00 08 |
| | Common package : ***No*** *biometric authentication* | **41 76 41** FF 01 00 00 00 **02 01** | |
| 3 | ID-A : ***No*** *Asymmetric Role and Device authentication* | **41 76 92** FF 01 01 00 00 **01 01** | 01 01 01 07 01 04 00 07 |
| | Common package : ***With*** *biometric authentication* | **41 76 41** FF 01 00 00 00 **03 01** | |
| 4 | Applet : ***With*** *Asymmetric Role and Device authentication* | **41 76 92** FF 01 01 00 00 **02 01** | 01 02 01 07 01 04 00 07 |
| | Common package : ***With*** *biometric authentication* | **41 76 41** FF 01 00 00 00 **03 01** | |

La procédure d'identification est décrite au paragraphe 3.2.2 du guide [AGD_PRE] et au §4 du guide [AGD_OPE] (voir [GUIDES]).

Les éléments d'identification du microcontrôleur et de la plateforme sont décrits dans le rapport de certification de la plateforme [CER-PTF].

La principale différence entre le produit et la TOE (composition de l'application ID-A v1.0 sur la plateforme ID-One COSMO X) correspond aux applications qui seront chargées pré-émission et post-émission sur ce produit et aux *patchs* optionnels pouvant être installés sur la plateforme (voir [CER-PTF]).

### 1.2.5 *Cycle de vie*

Quatre cycles de vie du produit sont décrits au chapitre 4 de la cible de sécurité [ST]. Ils sont décomposés en sept phases conformes au [PP0084] :

| **Phase** | |
|---|---|
| Phase 1 | Développement de la plateforme |
| Phase 2 | Développement du microcontrôleur |
| Phase 3 | Fabrication du microcontrôleur |
| Phase 4 | Conditionnement (*packaging*) du produit |
| Phase 5 | Pré-Personnalisation |
| Phase 6 | Personnalisation |
| Phase 7 | Utilisation opérationnelle |

Les quatre cycles de vie diffèrent notamment, par les méthodes de chargement des briques logicielles sur le produit, à savoir :

- Option 1 : la plateforme et l'application ID-A v1.0 sont chargées ensemble par le fabricant du microcontrôleur ;
- Option 2 : la plateforme et l'application ID-A v1.0 sont chargées ensemble avec le *IC loader*, soit dans un site de productions IDEMIA audité, soit sur des sites de productions non audités ou externes ;
- Option 3 : la plateforme est chargée sur un des sites du fabricant du microcontrôleur et l'application ID-A v1.0 est :
    - soit chargée de façon sécurisée sur n'importe quel site (site externe ou un des sites IDEMIA audités) (les mécanismes de protection possible sont décrits au chapitre 4.1.2 de la cible [ST]),
    - soit chargée en clair dans un des sites IDEMIA audités ;
- Option 4 : la plateforme est chargée avec l'IC loader sur n'importe quel site (site externe ou un des sites IDEMIA audités) et l'application ID-A v1.0 est :
    - soit chargée de façon sécurisée sur n'importe quel site (site externe ou un des sites IDEMIA audités) (les mécanismes de protection possible sont décrits au chapitre 4.1.2 de la cible [ST]),
    - soit chargée en clair dans un des sites IDEMIA audités.

Le tableau suivant situe le point de livraison de la TOE en fonction de l'option suivie :

| Option | Sites | Point de livraison |
|---|---|---|
| Option 1 | Sites du fabricant du microcontrôleur | Après la phase 3 |
| Option 2 | Sites IDEMIA audités | Après la phase 4 |
| | Sites externes | Après la phase 3 |
| Option 3 | Sites IDEMIA audités | Après la phase 4 |
| | Sites externes | Après la phase 3 |
| Option 4 | Sites IDEMIA audités | Après la phase 4 |
| | Sites externes | Après la phase 3 |

Le produit a été développé sur les sites suivants (voir [SITES]) :

| | |
|---|---|
| **IDEMIA – Courbevoie [CRB]**<br>2, place Samuel de Champlain<br>92400 Courbevoie, France | **IDEMIA – Pessac [PSC]**<br>Bâtiment Elnath,<br>11 avenue de Canteranne,<br>33600 Pessac, France |
| **IDEMIA – Vitré [VTR]**<br>Avenue d'Helmstedt<br>BP 90308<br>35503 Vitré Cedex, France | **IDEMIA – Shenzhen [SZN]**<br>4F, Great wall technology building<br>No 2, Kefa Rd<br>Science and technology park,<br>Nanshan district, Shenzhen, 518057, PR of China |

| | |
|---|---|
| **IDEMIA – Haarlem [HAA]**<br>Oudeweg 32,<br>2031 CC Haarlem, The Netherlands | **IDEMIA – Noida [NOI-D]**<br>Syscom India Private Limited<br>PLOT-1A, sector 73,<br>Noida Uttar Pradesh 201307, India |
| **IDEMIA – Ostrava [OST]**<br>Jelinkova 1174/3A, 721 00 Ostrava-Svinov,<br>Czech Republic | **IDEMIA – Noida [NOI-P]**<br>Syscom India Private Limited<br>Plot No 60-61, NSEZ,<br>Phase II, Dadri Road,<br>Noida-201305 Uttar Pradesh India |
| **IDEMIA – Jakarta [JKT]**<br>AIA Central 38th Floor,<br>Jl. Jenderal Sudirman Kav. 48A,<br>Jakarta 12930, Indonesia | **IDEMIA – Manilla [MNL]**<br>19F BPI – PhilamLife Makati Building,<br>6811 Ayala Ave.,<br>1209 Makati City, Philippines |

Les sites de développement et de fabrication du microcontrôleur sont couverts par le certificat [CER-IC], ceux du développement de la plateforme par le certificat [CER-PTF].

### 1.2.6 *Configuration évaluée*

Le certificat porte sur toutes les configurations du produit décrites au chapitre 1.2.4 de ce présent document. L'évaluation a été effectuée sur la configuration du produit la plus complète, c'est-à-dire la configuration 4 avec les mécanismes « *asymmetric role authentication* » et « *asymmetric device authentication* » et l'authentification par biométrie.

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante (comme indiqué dans le certificat [CER-PTF]). Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

# 2 L'évaluation

## 2.1 Référentiels d'évaluation

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

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

## 2.2 Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel sur la plateforme déjà certifiée par ailleurs (voir [CER-PTF]).

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme ID-One COSMO X, certifiée sous la référence ANSSI-CC-2021/29, voir [CER-PTF].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 21 juillet 2021, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

## 2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le potentiel d'attaque visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

## 2.4 Analyse du générateur d'aléa

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER-IC]).

Par ailleurs, comme requis dans le référentiel [ANSSI Crypto], la sortie du générateur physique d'aléa subit un retraitement de nature cryptographique. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le potentiel d'attaque visé (voir [CER-PTF]).

# 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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

## 3.2 Restrictions d'usage

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

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment en ce qui concerne la vérification et le chargement d'applications, qui doivent être effectués conformément aux résultats de l'évaluation de la plateforme (voir [CER-PTF]).

## 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 2010 permet la reconnaissance, par les pays signataires de l'accord[5], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :


### 3.3.2 *Reconnaissance internationale critères communs (CCRA)*

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[6] , des certificats Critères Communs.

[5] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

[6] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

# ANNEXE A. Références documentaires du produit évalué

| | |
|---|---|
| [ST] | Cible de sécurité de référence pour l'évaluation :<br>- *Security Target ID-A v1.0 on I-One Cosmo X,* référence FQR 550 0156, version 5, 16/07/2021.<br>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :<br>- *ID-A v1.0 on Cosmo X – Public Security Target, FQR 550 0200, version 3*, 16/07/2021. |
| [RTE] | Rapport technique d'évaluation :<br>- *Evaluation Technical Report – HEMERA-X,* référence LETI.CESTI.HEMX.FULL.001, version 1.2, 21 juillet 2021. |
| [ANA-CRY] | Cotation des mécanismes cryptographiques – HEMERA-X, référence LETI.CESTI.HEMX.RT.007, version 1.0, 17 mai 2021. |
| [CONF] | Liste de configuration du produit :<br>- *ID-A on ID-One Cosmo X – Configuration List*, référence FQR 401 8721, version 16, 09/07/2021. |
| [GUIDES] | Guide d'installation du produit :<br>- [AGD_PRE] ID-A on ID-One Cosmo X - AGD_PRE, référence FQR 401 8717, version 7, 09/07/ 2021.<br><br>Guide d'administration du produit :<br>- [AGD_OPE] ID-A on ID-One Cosmo X - AGD_OPE, référence FQR 401 8718, version 6, 08/07/ 2021.<br><br>Guide cryptographique :<br>- *[AGD_CRY] ID-A on Cosmo X – Recommendations for Compatibility with QR and QSCD*, référence 401 8925, version 2, 12 mai 2021. |

| | |
|---|---|
| [SITES] | Rapports d'analyse documentaire :<br>- *IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities),* référence IDEMIA R&D site 2018_GEN_v1.1, 19/06/2019 ;<br>- *IDEMIA Development Environment - ALC Class Evaluation Report (Generic Documentary activities),* référence IDEMIA-2019_GEN_v1.1, 01/07/2019 ;<br>- *IDEMIA Development Environment - ALC Class Evaluation Report (Generic Documentary activities*), référence IDEMIA2020_GEN_v1.0, 20/07/2020.<br><br>Rapports d'audit de site pour la réutilisation :<br>- [CRB] *Site Technical Audit Report CRB*, référence IDEMIA2020_CRB_STAR_v1.0, 19/01/2020 ;<br>- [HAA] *Site Technical Audit Report IDEMIA Haarlem,* référence IDEMIA2020_Haarlem_STAR_v1.0, 04/11/2020 ;<br>- [PSC] *Site Technical Audit Report PSC*, référence IDEMIA2020_PSC_STAR_v1.0, 14/01/2021 ;<br>- [VTR] *Site Technical Audit Report IDEMIA Vitré*, référence IDEMIA-2019_VTR_STAR_v1.1, 08/01/2020 ;<br>- [SZN] *Site Technical Audit Report IDEMIA Shenzhen,* référence IDEMIA-2019_SZN_STAR_v1.0, 08/11/2019 ;<br>- [OST] *Site Technical Audit Report OST*, référence IDEMIA-2019_OST_STAR_v1.0, 24/06/2019 ;<br>- [NOI-P] *Site Technical Audit Report NOI-P*, référence IDEMIA-2019_NOIP_STAR_v1.1, 19/07/2019 ;<br>- [NOI-D] *Site Technical Audit Report NOI-D*, référence IDEMIA-R&D site 2018_NOI-D_STAR_v1.0, 17/04/2019 ;<br>- [MNL] *Site Technical Audit Report IDEMIA Manila,* référence IDMIA2020_MNL_STAR_v1.1, 8/02/2021 ;<br>- [JKT] *Site Technical Audit Report IDEMIA Jakarta*, IDEMIA2020_JKT_STAR_v1.0, 18/12/2020. |
| [PP-SSCD-Part2] | *Protection profiles for secure signature creation device – Part 2: Device with key generation*, référence : prEN 14169-2:2012, version 2.0.1 datée du 23 janvier 2012.<br>Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01. |
| [PP-SSCD-Part3] | *Protection profiles for secure signature creation device – Part 3: Device with key import*, référence : prEN 14169-3:2012, version 1.0.2 datée du 24 juillet 2012.<br>Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012. |
| [PP-SSCD-Part4] | *Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application*, référence : prEN 14169-4:2012, version 1.0.1 datée du 14 novembre 2012.<br>Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012. |

| | |
|---|---|
| [PP-SSCD-Part5] | *Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application*, référence : prEN 14169-5:2012, version 1.0.1 datée du 14 novembre 2012.<br>Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012. |
| [PP-SSCD-Part6] | *Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application*, référence : prEN 14169-6:2013, version 1.0.4 datée du 3 avril 2013.<br>Certifié par le BSI le 16 avril 2013 sous la référence BSI-CC-PP-0076-2013. |
| [PP0084] | *Protection Profile, Security IC Platform Protection Profile with Augmentation Packages*, version 1.0, 13 janvier 2014.<br>Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-PP-0084-2014. |
| [CER-IC] | *BSI-DSZ-CC-1107-2020 for IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design step T11 with firmware 80.306.16.0, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.11.003, optional ACL v3.02.000 and user guidance*.<br>Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 17 novembre 2020 sous *la référence BSI-DSZ-CC-1107-2020.* |
| [CER-PTF] | Rapport de certification ANSSI-CC-2021/29, ID-One Cosmo X (Code SAAAAR : 093363).<br>Certifiée par l'ANSSI le 5 juillet 2021 sous la référence ANSSI-CC-2021/29. |

# ANNEXE B. Références liées à la certification

| | |
|---|---|
| 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. | |
| [CER-P-01] | Procédure ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI. |
| [CRY-P-01] | Procédure ANSSI-CC-CRY-P01 Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, ANSSI. |
| [CC] | *Common Criteria for Information Technology Security Evaluation:*<br>- *Part 1: Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001;<br>- *Part 2: Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002;<br>- *Part 3: Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003. |
| [CEM] | *Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004. |
| [JIWG IC] * | *Mandatory Technical Document - The Application of CC to Integrated Circuits*, version 3.0, février 2009. |
| [JIWG AP] * | *Mandatory Technical Document – Application of attack potential to smartcards and similar devices*, version 3.1, juin 2020. |
| [COMP] * | *Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018. |
| [OPEN] | *Certification of « Open » smart card products*, version 1.1 (*for trial use*), 4 février 2013. |
| [CCRA] | *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014. |
| [SOG-IS] | *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee. |
| [ANSSI Crypto] | Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020. |

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.