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-2022/33-R01

## ID-One Cosmo v9.1 embedding VITALE application (version 2.1.4)

Paris, le 14/10/2025 | 12:17 CEST

Vincent Strubel

# 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

# 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 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.cyber.gouv.fr.

# TABLE DES MATIERES

# 1 Résumé

| |
|---|
| Référence du rapport de certification<br>**ANSSI-CC-2022/33-R01** |
| Nom du produit<br>**ID-One Cosmo v9.1 embedding VITALE application** |
| Référence/version du produit<br>**version 2.1.4** |
| Type de produit<br>**Cartes à puce et dispositifs similaires** |
| Conformité à un profil de protection<br>***Protection profiles for secure signature creation device:***<br>*Part 2 : Device with key generation, v2.01, BSI-CC-PP-0059-2009-MA-02 ;*<br>*Part 3 : Device with key import, v1.0.2, BSI-CC-PP-0075-2012-MA-01 ;*<br>*Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012-MA-01 ;*<br>*Part 5 : Extension for device with key generation and trusted communication with signature creation application, v1.0.1, BSI-CC-PP-0072-2012-MA-01 ;*<br>*Part 6 : Extension for device with key import and trusted communication with signature creation application, v1.0.4, BSI-CC-PP-0076-2013-MA-01.* |
| Critère d'évaluation et version<br>**Critères Communs version 3.1 révision 5** |
| Niveau d'évaluation<br>**EAL4 augmenté**<br>ALC_DVS.2, AVA_VAN.5 |
| Référence du rapport d'évaluation<br>*Evaluation Technical Report (full ETR) - THERIA-R01*<br>référence LETI.CESTI.THER01.FULL.001<br>version 1.1<br>22 septembre 2025. |
| Fonctionnalité de sécurité du produit<br>voir 2.2.2 Services de sécurité |
| Exigences de configuration du produit<br>voir 4.2 Restrictions d'usage |
| Hypothèses liées à l'environnement d'exploitation<br>voir 4.2 Restrictions d'usage |
| Développeur<br>**IN SMART IDENTITY FRANCE**<br>2 place Samuel de Champlain<br>92400 Courbevoie, France |

Commanditaire

**IN SMART IDENTITY FRANCE**

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

SOG-IS

Ce certificat est reconnu au niveau EAL2.

# 2 Le produit

## 2.1 Présentation du produit

Le produit évalué est « ID-One Cosmo v9.1 embedding VITALE application, version 2.1.4 » développé par IDEMIA devenue aujourd'hui IN SMART IDENTITY FRANCE.
Ce produit offre des services de signature électronique (SSCD[1]) au travers des applications ADELE, VITALE1 et VITALE2, conformes aux profils de protections listés dans le paragraphe 1.2.1 ci-dessous.

Ce produit est destiné à être utilisé dans le cadre de l'application SESAM Vitale ainsi que pour des applications de signature électronique ; il est livré en configuration fermée et ne permet pas le chargement d'application en après émission.

## 2.2 Description du produit

### 2.2.1 *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].

### 2.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont détaillés dans la cible de sécurité [ST] au chapitre 3.4. « *TOE Functions* ». Ils sont résumés ci-après :

- la création de signature ou de sceau 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'export de clé publique (c'est-à-dire la SVD) ;
- l'établissement d'un canal de confiance pouvant permettre la création de signature électronique, l'import de la SCD ou l'export de la SVD dans un environnement non protégé ;
- l'authentification du porteur de carte basée sur la vérification d'un code PIN appelée également données d'authentification de référence (RAD[4]) ;
- le déblocage de la RAD.

[1] *Secure Signature Creation Device.*

[2] *Signature Creation Data.*

[3] *Signature Verification Data.*

[4] *Reference Authentication Data.*

De plus, le produit fournis aussi les mécanismes de sécurité décrits au chapitre 3.6 de la cible de sécurité [ST], à savoir :

- les mécanismes d'authentification (authentification du porteur de la carte, du mécanisme communiquant avec la carte afin d'établir un canal sécurisé, de l'administrateur de la TOE, authentification mutuelle avec l'entité communicante et authentification client/serveur) ;
- la cryptographie (génération de clés SCD/SVD ou de session, destruction de clés, authentification symétrique et asymétrique, création de signature, génération de nombres aléatoires, chiffrage/déchiffrage de message émis, génération et vérification de MAC, échange de clé Diffie-Hellman, calcul de hash, calcul et vérification de certificat, chiffrement/déchiffrement de données) ;
- la gestion de clés (importation de SCD, génération de SCD, désactivation de SCD, création, extension ou modification de certificat, création de SVD, gestion des clés d'authentification)
- la gestion de PIN ;
- la gestion de canaux sécurisés ;
- le contrôle d'accès aux différentes données de l'*applet* ;
- le stockage des données ;
- l'intégrité et la confidentialité des données sensibles.

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

### 2.2.3 *Architecture*

Le produit, dont l'architecture est détaillée aux chapitres 1 « *Introduction* » et 3 « *TOE Overview* » de la cible de sécurité [ST], est constitué :

- du microcontrôleur SLC32 certifié sous la référence [CER-IC] ;
- de la plateforme *Java Card* ouverte « ID-One Cosmo v9.1 » certifiée sous la référence [CER-PTF] ;
- de l'*applet* de signature VITALE composée des applications ADELE, VITALE1 et VITALE2 contenant entre autres les fonctionnalités SSCD ;
- d'une application AIP (Application d'Initialisation et de Personnalisation), une application d'administration utilisée en phase de pré-personnalisation et de personnalisation et inactive en phase « utilisation » ;
- d'un gestionnaire d'applications.

Parmi ces éléments, l'application AIP et le gestionnaire d'applications ne font pas partie de la cible d'évaluation (TOE[5]).

[5] *Target of Evaluation.*

### 2.2.4 *Identification du produit*

La version certifiée du produit est identifiable par les éléments détaillés dans la cible de sécurité [ST] au chapitre au chapitre 1.2 « *TOE Reference* » et dans le guide [AGD_OPE] au chapitre 2 « Identification du produit ».

Ces éléments peuvent être vérifiés par lecture des données CPLC de l'applet VITALE et de la plateforme, suivant la procédure d'identification décrite dans le guide [AGD_OPE] (voir [GUIDES]).

### 2.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 4 *« Life Cycle »* de la cible de sécurité [ST]. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

Pour l'évaluation, l'évaluateur a considéré comme :

- administrateur du produit : les agents qui agissent au nom de l'Etat ou de l'organisation émettrice et qui personnalisent la carte avec des données de l'utilisateur final ;
- utilisateur du produit : le titulaire légitime de la carte Vitale2.

### 2.2.6 *Configuration évaluée*

Le certificat porte sur la configuration identifiée au chapitre 2.2.4 du présent rapport.

# 3 L'évaluation

## 3.1 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).

## 3.2 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 de l'application VITALE dans la plateforme déjà certifiée dans le cadre d'un schéma national reconnu au titre de l'accord du SOG-IS.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « ID-One Cosmo v9.1 » (voir [CER-PLF]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

## 3.3 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 [ANA_CRY].

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 niveau d'attaquant 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.

# 4 La certification

## 4.1 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 (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2022/33-R01 a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

## 4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 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 le chapitre 8 du guide [AGD_PRE].

## 4.3 Reconnaissance du certificat

### 4.3.1 *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[6], 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 :

### 4.3.2 *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[7] , des certificats Critères Communs.

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 :

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

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

# ANNEXE A. Références documentaires du produit évalué

| | |
|---|---|
| [ST] | Cible de sécurité de référence pour l'évaluation :<br>- *Security Target ID-One Cosmo v9.1 embedding VITALE application*, référence FQR 110 9933, version 4, 12 mars 2025.<br>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :<br>- *ID-One Cosmo v9.1 embedding VITALE application Public Security Target*, référence FQR 110 9934, version 2, 7 août 2025. |
| [RTE] | Rapport technique d'évaluation :<br>- *Evaluation Technical Report (full ETR) - THERIA-R01*, référence LETI.CESTI.THER01.FULL.001, version 1.1, 22 septembre 2025. |
| [ANA_CRY] | Cotation des mécanismes cryptographiques THERIA, référence LETI.CESTI.THE.RT.007, version v1.1, 21 juin 2022. |
| [GUIDES] | Guide d'installation et d'administration du produit :<br>- [AGD_PRE] *Manuel de Pré-Personnalisation - Personnalisation*, référence FQR 110 9913, version 3.0, 24 mars 2025.<br><br>Guide d'utilisation du produit :<br>- [AGD_OPE] *Manuel utilisateur VITALE2 applet COSMO V9.1*, référence FQR 110 9914, version 2, 14 avril 2022. |
| [SITES] | Rapports d'analyse documentaire et d'audit de site pour la réutilisation :<br>- IDEMIA_2024_ALC_GEN_v1.0 ;<br>- IDEMIA2024_CRB_STAR_v1.0 ;<br>- IDEMIA2023_NOI-P_STAR_v1.0 ;<br>- IDEMIA_2023_VTR_STAR_v1.1. |
| [CER_IC] | *Certification Report BSI-DSZ-CC-1110-V7-2024 for Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 from Infineon Technologies AG*.<br>Certifié par le BSI *(Bundesamt für Sicherheit in der Informationstechnik)* le 30 septembre 2024, sous la référence BSI-DSZ-CC-1110-V7-2024. |
| [CER-PLF] | Plateforme ID-One Cosmo V9.1 masquée sur le composant IFX SLC 32 (Identification du matériel 092915).<br>Certifié par l'ANSSI le 9 mai 2025 sous la référence ANSSI-CC-2020/07-R01. |
| [PP-SSCD-Part2] | *Protection profiles for secure signature creation device – Part 2: Device with key generation*, référence : prEN 419211-2:2013, version 2.0.1 datée du 18 mai 2013. |

| | |
|---|---|
| | Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0059-2009-MA-02. |
| [PP-SSCD-Part3] | *Protection profiles for secure signature creation device – Part 3: Device with key import*, référence : prEN 419211-3:2013, version 1.0.2 datée du 14 septembre 2013.<br>Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0075-2012-MA-01. |
| [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 419211-4:2013, version 1.0.1 datée du 12 octobre 2013.<br>Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0071-2012-MA-01. |
| [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 419211-5:2013, version 1.0.1 datée du 12 octobre 2013.<br>Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0072-2012-MA-01. |
| [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 419211-6:2014, version 1.0.4 datée du 25 juillet 2014.<br>Maintenu par le BSI le 30 juin 2016 sous la référence BSI-CC-PP-0076-2013-MA-01. |

# 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] | Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.4. |
| [CRY-P-01] | Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1. |
| [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,* 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 3.2.1, février 2024. |
| [COMP] * | *Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018. |
| [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.