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-2025/29

IDEMIA CA (Version 1.3.1)

Paris, le 14/10/2025 | 12:16 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	**ANSSI-CC-2025/29**
Nom du produit	**IDEMIA CA**
Référence/version du produit	**Version 1.3.1**
Type de produit	**Produits réseaux ou logiciels génériques**
Conformité à un profil de protection	***Néant***
Critère d'évaluation et version	**Critères Communs version 3.1 révision 5**
Niveau d'évaluation	**EAL4 augmenté** ALC_FLR.1
Référence du rapport d'évaluation	*Evaluation Technical Report of the project PEREGRINE-2* référence CC-ETR-PEREGRINE-2-1.05 version 1.05 21 juillet 2025.
Fonctionnalité de sécurité du produit	voir 2.2.2 Services de sécurité
Exigences de configuration du produit	voir 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation	voir 4.2 Restrictions d'usage
Développeur	**IN Smart Identity** 2 place Samuel Champlain 92400 Courbevoie, France
Commanditaire	**IN Smart Identity** 2 place Samuel Champlain 92400 Courbevoie, France
Centre d'évaluation	**AMOSSYS** 11 rue Maurice Fabre, 35000 Rennes, France

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.1.

SOG-IS

Ce certificat est reconnu au niveau EAL4 augmenté de ALC_FLR.1.

2 Le produit

2.1 Présentation du produit

Le produit évalué est « IDEMIA CA, Version 1.3.1 » développé par IN Smart Identity.

Ce produit est une application serveur de gestion de PKI (*Public Key Infrastructure*) constituant le cœur de la solution globale *Citizen PKI* développée par IN Smart Identity.

IDEMIA CA est développé en Java et offre, à travers une interface web, des services de gestion de certificats à clef publique pour les autorités de certification (*Certification Authorities - CA*) permettant la mise en place d'une PKI.

Le produit supporte les certificats à clef publique X509 ainsi que les certificats compacts de type CVC (*Card Verifiable Certificates*) pour le contrôle d'accès étendu (*Extended Access Control - EAC*).

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.

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

2.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit, décrits au chapitre 2.2.3 « *Usage and major security features* » de la cible de sécurité [ST], sont : :

- administration des ACs, des certificats, des requêtes de certificat et des statuts de certificats (pour les certificats X509 et EAC) ;
- journalisation et audit des évènements de sécurité ;
- authentification des utilisateurs ;
- séparation des privilèges et contrôle d'accès ;
- protection des communications ;
- support de différents modes cadrant les actions possibles des utilisateurs sur la cible d'évaluation (ROOT_CA, SUB_CA, END_ENTITY ou ALL).

2.2.3 *Architecture*

L'architecture du produit est décrite au chapitre 2.3 « *TOE Description* » de la cible de sécurité [ST].

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 2.1.3 « *TOE Identification* » :

Le produit offre un *REST API Endpoint* (URL /pki-ca/actuator/info), accessible à tout utilisateur autorisé, permettant via une requête d'afficher les éléments d'identification de la cible d'évaluation comme sur la figure ci-dessous.


```
{
  "app": {
    "name": "IDEMIA CA",
    "version": "1.3.1",
    "code": "203673",
    "build_number": "1.3.1_ea12b24",
    "java_version": "17.0.14",
    "certificate_type": "X509",
    "mode": "ROOT_CA"
  },
  "git": {
    "commit": {
      "id": "ea12b24"
    }
  }
```


Figure 1 – Identification de la cible d'évaluation.

2.2.5 *Cycle de vie*

Le produit a été développé sur les sites suivants :

Manille	**Courbevoie**
31F Robinsons Summit Center Condominium corporation 6783 Ayala Avenue Makati City 1209 Philippines	2 Place Samuel de Champlain 92400, Courbevoie France

Le cycle de vie du produit est le suivant :

- Développement (site Manille) ;
- Tests (site Manille) ;
- Rédaction documentation de tests (site Manille) ;
- Rédaction et revue de la documentation Critères Communs (site Manille) ;
- Livraison à IDEMIA Courbevoie (site Manille) ;
- Revue de la documentation Critères Communs (site Courbevoie) ;
- Livraison au client (site Courbevoie) ;
- Maintenance et support (site Courbevoie) ;
- Gestion de projet (site Courbevoie).

Les activités de développement, tests et maintenance suivent elles-mêmes un cycle de vie de type *DevSecOps*.

Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

2.2.6 *Configuration évaluée*

Le certificat porte sur le produit identifié dans la cible de sécurité [ST] au chapitre 2.3 « *TOE Description* », dans ses configurations permises par les [GUIDES].

Au regard du cycle de vie, le certificat porte sur le produit livré à l'issue de la phase de livraison au client.

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].

3.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en Annexe A), 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.

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-2025/29 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 les guides fournis [GUIDES].

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[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 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[2] , 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 :

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

[2] 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 : - *IDEMIA CA v1.3.1 – Security Target*, référence FQR 550 0219, version 11, 23 avril 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *IDEMIA CS v1.3.1 – Public Security Target*, référence FQR 151 007-403, version 1.0, 4 septembre 2025.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report of the project PEREGRINE-2*, référence CC-ETR-PEREGRINE-2-1.03, version 1.05, 21 juillet 2025.
[ANA_CRY]	*Analysis of cryptographic mechanisms - PEREGRINE-2*, référence CC-CRY-PEREGRINE-2-1.03, version 1.03, 15 mai 2025.
[GUIDES]	Guides d'installation et d'administration du produit : - *Preparative procedures*, référence FQR2201622, version 7, 17 avril 2025. Guide d'utilisation du produit : - *Operational user guidance*, référence FQR2201654, version 6, 17 avril 2025.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - IDEMIA-2025_ALC_GEN_v1.0 ; - IDEMIA_2024_MNL_STAR_v1.1 ; - IDEMIA2024_CRB_STAR_v1.1.
[PP]	*Certificate Issuing and Management Components Protection Profile*", NIST, version 1.5, 11 août 2011

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 5.0.
[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:* - *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - *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.
[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.