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-2021/17

IDnomic ID CA (Version 1.3.7)

Paris, le 12 mai 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti CERTIFICATION

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-2021/17**
Nom du produit **IDnomic ID CA**
Référence/version du produit **Version 1.3.7**
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL 4 augmenté** ALC_FLR.3
Développeur **IDNOMIC** 175 rue Jean-Jacques Rousseau 92138 Issy-les-Moulineaux Cedex, France
Commanditaire **IDNOMIC** 175 rue Jean-Jacques Rousseau 92138 Issy-les-Moulineaux Cedex, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Accords de reconnaissance applicables **CCRA** Ce certificat est reconnu au niveau EAL2 augmenté de FLR.3. **SOG-IS** Ce certificat est reconnu au niveau EAL4 augmenté de FLR.3.

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 « IDnomic ID CA, Version 1.3.7 » développé par IDNOMIC, marque commerciale de KEYNECTIS SA.

Ce produit est une autorité de certification (AC) et intervient en tant que composant principal dans une infrastructure de gestion de clés (IGC). La TOE consiste en des programmes, formats de données, procédures, protocoles de communications, politiques de sécurité et mécanismes de cryptographie à clé publique fonctionnant ensemble pour permettre à des personnes d'établir des relations de confiance à travers l'usage de certificats électroniques.

1.2 Description du produit

1.2.1 *Introduction*

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

La cible de sécurité ne se réclame pas conforme à un profil de protection, mais s'inspire du profil de protection [PP].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la génération et le stockage de clés ;
- la génération et la distribution de certificats X509 et de listes de révocation de certificats (CRL) ;
- le séquestre et le recouvrement de clés ;
- les fonctions de gestion (par exemple : audit, configuration, archivage).

1.2.3 *Architecture*

Le produit est composé des éléments logiciels suivants :

- une bibliothèque *JavaScript* s'exécutant dans le navigateur de l'utilisateur final ;
- des composants applicatifs suivants s'exécutant sur le serveur d'application et réalisant les fonctions principales de la TOE :
    - *Administration Console* : l'application web qui fournit les fonctionnalités de configuration, d'audit et d'enrôlement simple,
    - *Connector Server* : l'application web qui fournit les services métiers relatifs au cycle de vie des certificats,
    - *Batch Server* : l'application web qui prend en charge les tâches asynchrones de l'AC, telles que la production des CRL et le traitement des enregistrements d'audit,
    - *Hardware Security Services* : le composant serveur relié au *Hardware Security Module* (HSM) qui traite les opérations cryptographiques demandées par les autres composants.

Ces éléments sont déployés dans une architecture *n-tiers*, composée d'un serveur web, de serveurs d'application et d'un serveur de base de données.

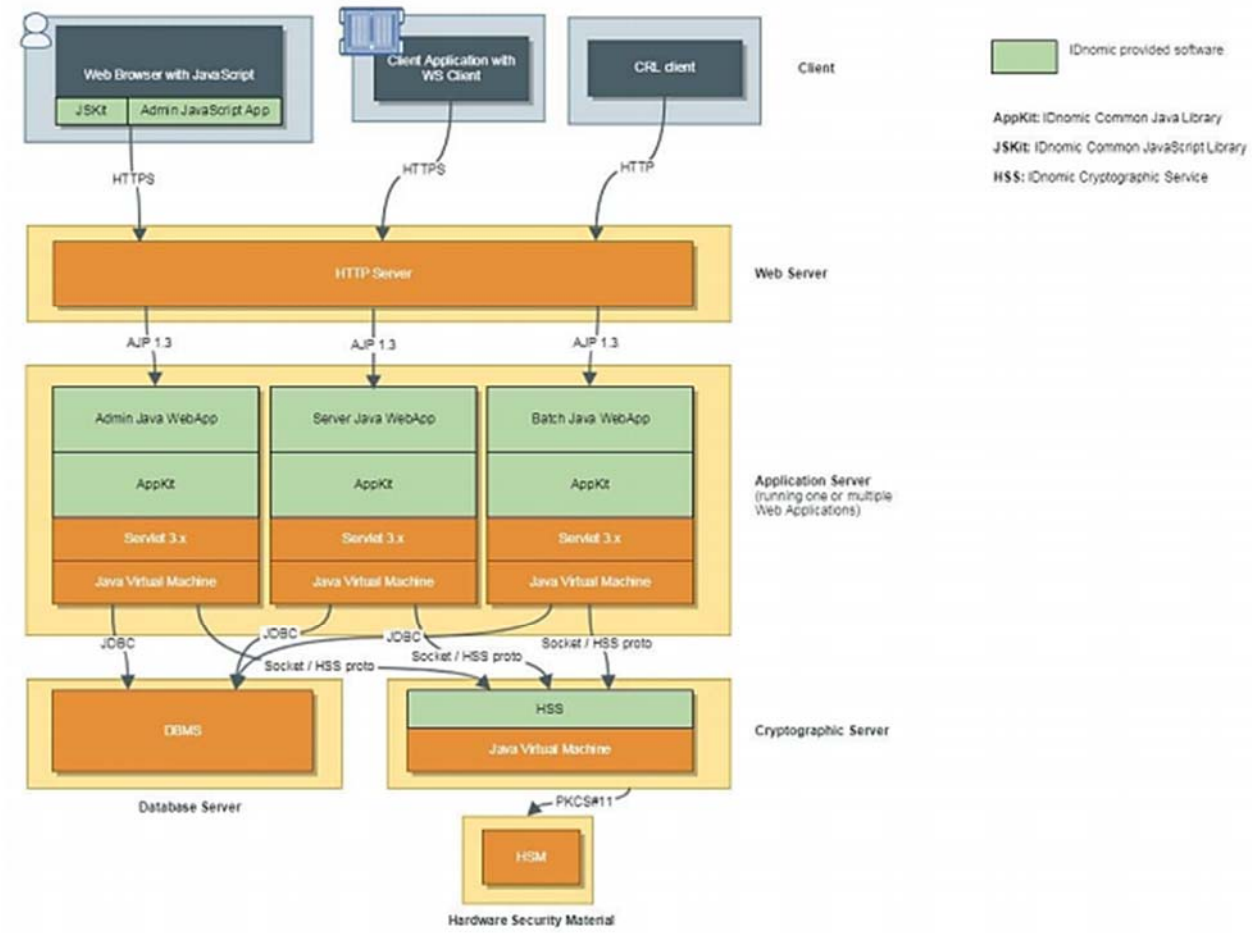

Figure 1: Architecture de la TOE

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 en accédant au menu « About » de l'IHM :

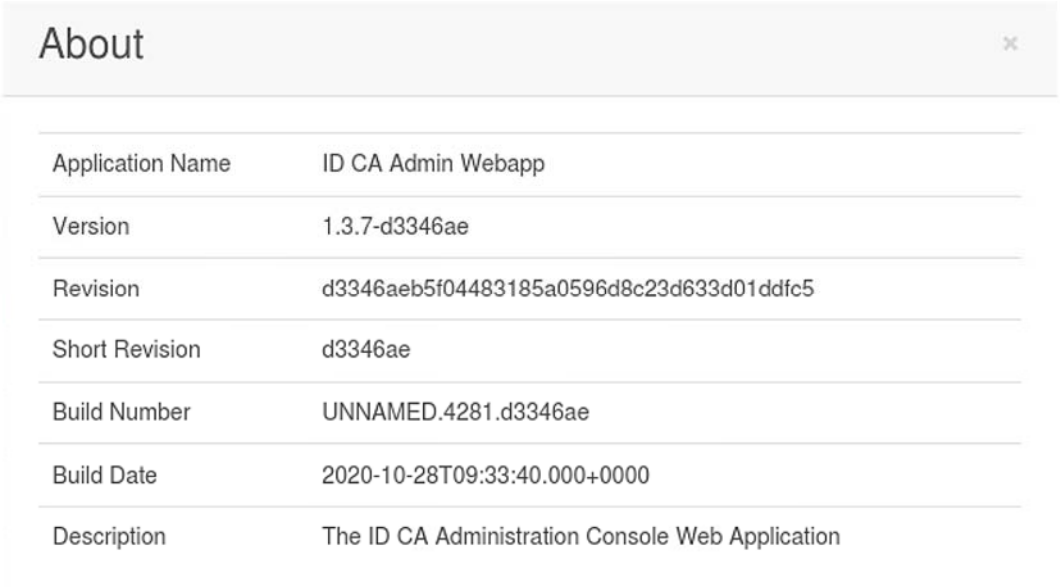

Figure 2: Identifiation de la version de la TOE

1.2.5 *Cycle de vie*

Les principales phases de développement sont décrites au chapitre 4 du document [CONF] :

- *Planning session* ;
- *Sprint* ;
- *Build* du produit ;
- Documentation.

Le produit a été développé sur le site suivant (voir [SITE]) :

IDNOMIC

175 rue Jean-Jacques Rousseau,
92130 Issy-les-Moulineaux
France

1.2.6 *Configuration évaluée*

Le certificat porte sur les configurations suivantes :

- le serveur web : *Apache* httpd version 2.4.6 ;
- le serveur d'application : *Apache Tomcat* 9 ;
- le serveur de base de données : *PostgreSQL* version 9.4 ;
- le module cryptographique : HSM *Bull Proteccio* version X147 V149 ;
- le système d'exploitation : RHEL version 7.4 ;
- l'environnement *Java* : JRE version 1.8.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1 révision 5 [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 29 avril 2021, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [EXP-CRY]. Ces résultats ont été pris 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 AVA_VAN.3 visé.

2.4 Analyse du générateur d'aléas

Ce générateur a fait l'objet d'une analyse.

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [RGS], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléas n'a pas révélé de faiblesse.

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 « IDnomic ID CA, Version 1.3.7 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté du composant ALC_FLR.3.

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] ainsi que réaliser une veille des vulnérabilités publiques afin s'assurer que les composants applicatifs déployés dans l'infrastructure (*Apache*, *Tomcat*, *PostgreSQL*) sont exempts de vulnérabilités.

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[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 :

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

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

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

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 :

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

ANNEXE A. 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
ADV 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 TSF*
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**3**	*Basic modular design*
AGD 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 Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	**4**	*Production support, acceptance procedures and automation*
	ALC_CMS	1	2	3	4	5	5	5	**4**	*Problem tracking 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 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 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 Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	**3**	*Focused vulnerability analysis*

ANNEXE B. Références documentaires du produits évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Common Criteria Security Target ID CA, version 7.3, 24 avril 2021, ID CA.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Évaluation Projet : ID-CA, référence OPPIDA/CESTI/ID-CA/RTE, version 1.1, 29 avril 2021, OPPIDA.
[EXP-CRY]	Cryptographic Analysis report, référence OPPIDA/CESTI/ ID-CA /CRYPTO/5.0, version 5.0, 12 novembre 2020, OPPIDA.
[CONF]	Liste de configuration du produit : *Configurations list of ID CA*,référence Configurations list of ID CA-V92, version 92.0 du 28 avril 2021.
[GUIDES]	Guide d'installation du produit : - ID_CA_Server_Installation_and_Upgrade_Guide, version 1.3, 30 juillet 2019. Guide d'administration du produit : - ID_CA_Configuration_and_Administration_Guide, version 1.3, 30 juillet 2019 ; - ID_CA_System_Maintenance_Guid, version 1.3, 30 juillet 2019.
[PP]	*Protection Profile Certification Authorities*, version 1.0, NIAP, 16 mai 2014.

ANNEXE C. 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.
[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*, avril 2017, 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.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.