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-CSPN-2021/16

# Digital Secure Storage Server (D3S)

## Version 5.5.0.65

Paris, le 7 juillet 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<br>**ANSSI-CSPN-2021/16** |
| Nom du produit<br>**Digital Secure Storage Server (D3S)** |
| Référence/version du produit<br>**Version 5.5.0.65** |
| Catégorie de produit<br>**Stockage sécurisé** |
| Critère d'évaluation et version<br>**CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)** |
| Commanditaire<br>**IDEMIA**<br>2 Place Samuel de Champlain<br>92400 Courbevoie, France |
| Développeur <cas un développeur><br>**IDEMIA**<br>2 Place Samuel de Champlain<br>92400 Courbevoie, France |
| Centre d'évaluation<br>**OPPIDA**<br>4-6 avenue du vieil étang, Bâtiment B<br>78180 Montigny le Bretonneux, France |
| Fonctions de sécurité évaluées<br>Authentification des utilisateurs<br>Chainage des lots de traces<br>Chiffrement et déchiffrement des lots de traces<br>Validation des lots de traces<br>Scellement des lots de traces<br>Protection des données de configuration |
| Fonctions de sécurité non évaluées<br>Néant |
| Restriction(s) d'usage<br>Non |

# PREFACE

## 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 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 CSPN 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 « Digital Secure Storage Server (D3S), Version 5.5.0.65 » développé par IDEMIA.

Il offre un service de coffre-fort électronique à destination de l'Autorité nationale des jeux (ANJ), afin de recueillir et d'archiver les données échangées entre les joueurs et la plateforme de l'opérateur de jeux à l'occasion des opérations de jeux.

La figure ci-dessous explicite l'architecture du produit.

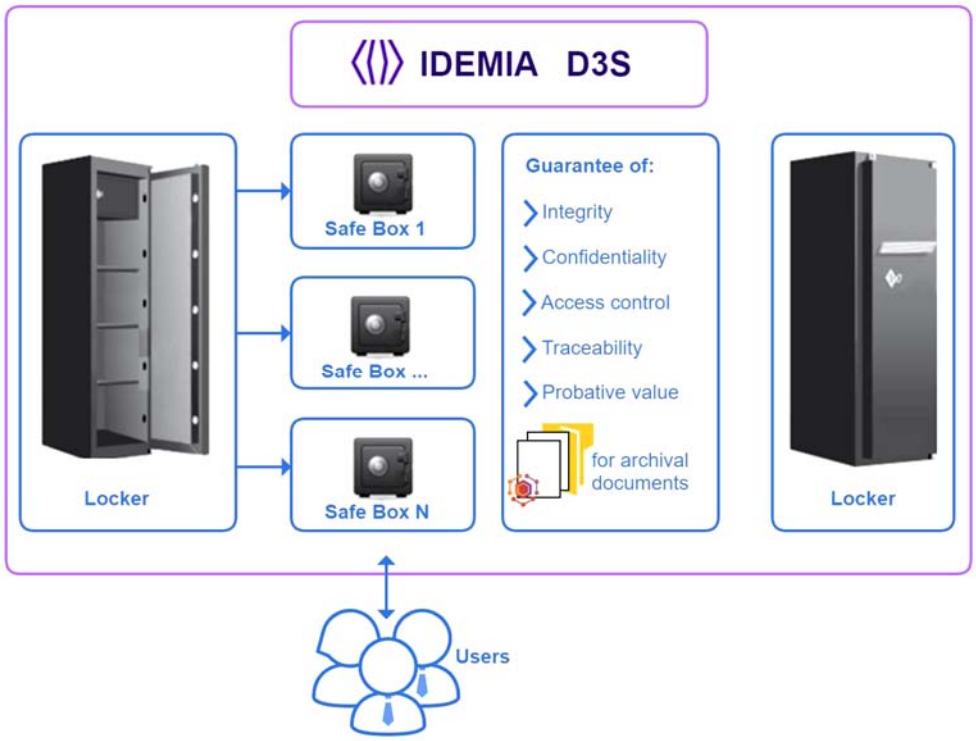


**Figure 1 - Architecture Produit.**

## 1.2 Description du produit évalué

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

### 1.2.1 *Catégorie du produit*

| | | |
|---|---|---|
| ☐ | 1 | détection d'intrusions |
| ☐ | 2 | anti-virus, protection contre les codes malicieux |
| ☐ | 3 | pare-feu |
| ☐ | 4 | effacement de données |
| ☐ | 5 | administration et supervision de la sécurité |
| ☐ | 6 | identification, authentification et contrôle d'accès |
| ☐ | 7 | communication sécurisée |
| ☐ | 8 | messagerie sécurisée |
| ☒ | **9** | **stockage sécurisé** |
| ☐ | 10 | environnement d'exécution sécurisé |
| ☐ | 11 | terminal de réception numérique (*Set top box*, STB) |
| ☐ | 12 | matériel et logiciel embarqué |
| ☐ | 13 | automate programmable industriel |
| ☐ | 99 | autre |

### 1.2.2 *Identification du produit*

| Produit | |
|---|---|
| Nom du produit | Digital Secure Storage Server (D3S) |
| Numéro de la version évaluée | Version 5.5.0.65 |

La version certifiée du produit peut être identifiée directement depuis la page de gestion.

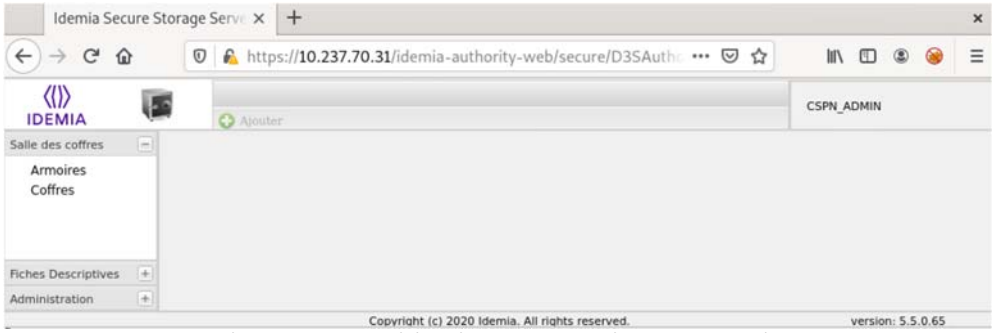


**Figure 2 – Identification de la version du produit**

| Outil | |
|---|---|
| Nom de l'outil | D3S ARJEL Client (d3sc) |
| Numéro de la version évaluée | Version 5.5.0.65 |

La version utilisée pendant l'évaluation peut être retrouvée en parcourant le fichier BUILD.txt

```
$ cat release/idemia-d3s-arjel-client-5.5.0.65/BUILD.txt
Product-Title: D3S Client ARJEL Edition
Project-Group: io.idemia.trust.custom.arjel
Project-Artifact: idemia-d3s-arjel-setup-client
Project-Version: 5.5.0.65
Build-Jdk: Oracle Corporation 1.8.0 151
Build-Time: 2020-11-19 18:01:38
```

**Figure 3 – Identification de la version de l'outil d3sc**

### 1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'authentification des utilisateurs ;
- le chaînage des lots de traces ;
- le chiffrement et le déchiffrement des lots de traces ;
- la validation des lots de traces ;
- le scellement des lots de traces ;
- la protection des données de configuration.

### 1.2.4 *Configuration évaluée*

La configuration évaluée correspond à la version déployée dans le cadre de l'utilisation faite par l'ANJ.

# 2 L'évaluation

## 2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en ANNEXE B.

## 2.2 Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

## 2.3 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

### 2.3.1 *Installation du produit*

#### *2.3.1.1 Particularités de paramétrage de l'environnement et options d'installation*

L'installation du produit étant réalisée par IDEMIA, l'évaluateur n'a pas eu à installer le coffre-fort D3S.

#### *2.3.1.2 Description de l'installation et des non-conformités éventuelles*

Sans objet.

#### *2.3.1.3 Durée de l'installation*

Sans objet.

#### *2.3.1.4 Notes et remarques diverses*

Néant.

### 2.3.2 *Analyse de la documentation*

La documentation est suffisamment complète et permet de prendre en main le produit.

### 2.3.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit. Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

### 2.3.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

### 2.3.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

### 2.3.6 *Analyse des vulnérabilités (conception, construction, etc.)*

#### *2.3.6.1 Liste des vulnérabilités connues*

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

#### *2.3.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert*

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

### 2.3.7 *Analyse de la facilité d'emploi*

#### *2.3.7.1 Cas où la sécurité est remise en cause*

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

#### *2.3.7.2 Avis d'expert sur la facilité d'emploi*

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur familier.

#### *2.3.7.3 Notes et remarques diverses*

Aucune note, ni remarque n'a été formulée dans le [RTE].

## 2.4 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

## 2.5 Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

# 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.

Ce certificat atteste que le produit «  Digital Secure Storage Server (D3S), Version 5.5.0.65 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

## 3.2 Recommandations et 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 spécifiés dans la cible de sécurité [CDS], et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations et restrictions suivantes.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

# ANNEXE A. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | *Security target C.S.P.N. Electronic SAFE D3S*<br>Référence : Idemia_d3s_cible_cspn ;<br>Version : 1.0 ;<br>Date : 23 juin 2021. |
| [RTE] | Rapport Technique d'Évaluation CSPN D3S 5.5 - Digital Secure Storage Server (D3S)<br>Référence : OPPIDA/CESTI/D3S 5.5/RTE/1.0 ;<br>Version : 1.1 ;<br>Date : 15 juin 2021. |
| [GUIDES] | Guides techniques du développeur :<br>Référence : Idemia_d3s_FR_manager_guide-1.3EN.pdf ;<br>Version : 1.3 ;<br>Date : 16 juin 2020.<br><br>Référence : Idemia_d3s_FR_auditor_guide-1.3EN.pdf<br>Version : 1.3 ;<br>Date : 19 juin 2020.<br><br>Référence : Idemia_d3s_JEL_DeveloperGuide_WSFR-1.8EN.pdf ;<br>Version : v1.8 ;<br>Date : 19 juin 2020.<br><br>Référence : Idemia_d3s_FR_shell_console_guide-1.4EN.pdf ;<br>Version : v1.4 ;<br>Date : 19 juin 2020.<br><br>Référence : Idemia_d3s_FR_operator_initialization-1.3EN.pdf ;<br>Version : v1.3 ;<br>Date : 03 novembre 2020.<br><br>Référence : Idemia_d3s_FR_access_rights_config_file-1.0EN.pdf ;<br>Version : v1.0 ;<br>Date : 06 novembre 2020.<br><br>Référence : Idemia_d3s_FR_KC_Scripts-1.1EN.pdf ;<br>Version : v1.1 ;<br>Date : 03 novembre 2020.<br><br>Référence : Idemia_D3S_Gaming_PrivilegesList_FRv1.0EN.pdf ;<br>Version : v2.5 ;<br>Date : 17 juin 2020.<br><br>Référence : Idemia_D3S_Gaming_FunctionalSpec_FR_CSPN-v2.7EN.pdf ;<br>Version : v1.2 ;<br>Date : 17 juin 2020. |

# ANNEXE B. Références 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. | |
| [CSPN] | Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01/2.1 du 13 janvier 2020.<br><br>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018.<br><br>Documents disponibles sur www.ssi.gouv.fr. |
| [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. |