PREMIER MINISTRE

*Liberté*
*Égalité*
*Fraternité*

Agence nationale de la sécurité
des systèmes d'information

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

# Rapport de certification ANSSI-CSPN-2023/23

# UBIKA WAAP Gateway

## Version 6.11.1 sur appliances 1450 et 4450

Paris, le 1er Février 2024

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

Vincent STRUBEL

[ORIGINAL SIGNE]

SÉCURITÉ 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-2023/23** |
| Nom du produit<br>**UBIKA WAAP Gateway** |
| Référence/version du produit<br>**Version 6.11.1 sur appliances 1450 et 4450** |
| Catégorie de produit<br>**Pare-feu** |
| Critère d'évaluation et version<br>**CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)** |
| Commanditaire<br>**UBIKA**<br>501 rue Denis Papin, Le Millenium, Bâtiment B<br>34000 Montpellier, France |
| Développeur<br>**UBIKA**<br>501 rue Denis Papin, Le Millenium, Bâtiment B<br>34000 Montpellier, 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>Filtrage des données HTTP<br>Sécurité des cookies<br>Sécurité des données XML<br>Sécurité des données JSON<br>Terminaison TLS/SSH<br>Validation de certificats clients<br>Authentification des administrateurs<br>Durcissement du socle de l'appliance<br>Politique et sécurisation des mises à jour<br>Stockage sécurisé des clés de chiffrement |
| Fonctions de sécurité non évaluées<br>Sans objet |
| Restriction(s) d'usage<br>Oui (cf. §3.2) |

# 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.cyber.gouv.fr.

## TABLE DES MATIERES

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est « UBIKA WAAP Gateway, Version 6.11.1 sur appliances 1450 et 4450 » développé par UBIKA.

Ce produit est un pare-feu applicatif web, également appelé WAAP pour *Web Application and API Protection*, qui permet de protéger les services et applications web des menaces, dans un contexte interne comme externe.

Cette protection est assurée par des règles de filtrage appliquées aux requêtes HTTP reçues, les actions correspondantes et les éléments inspectés étant définis par les administrateurs.

Le produit UBIKA WAAP Gateway doit être placé en amont des serveurs et services web à protéger vis-à-vis des zones à risque, et s'utilise en coupure entre les utilisateurs et les serveurs web.

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

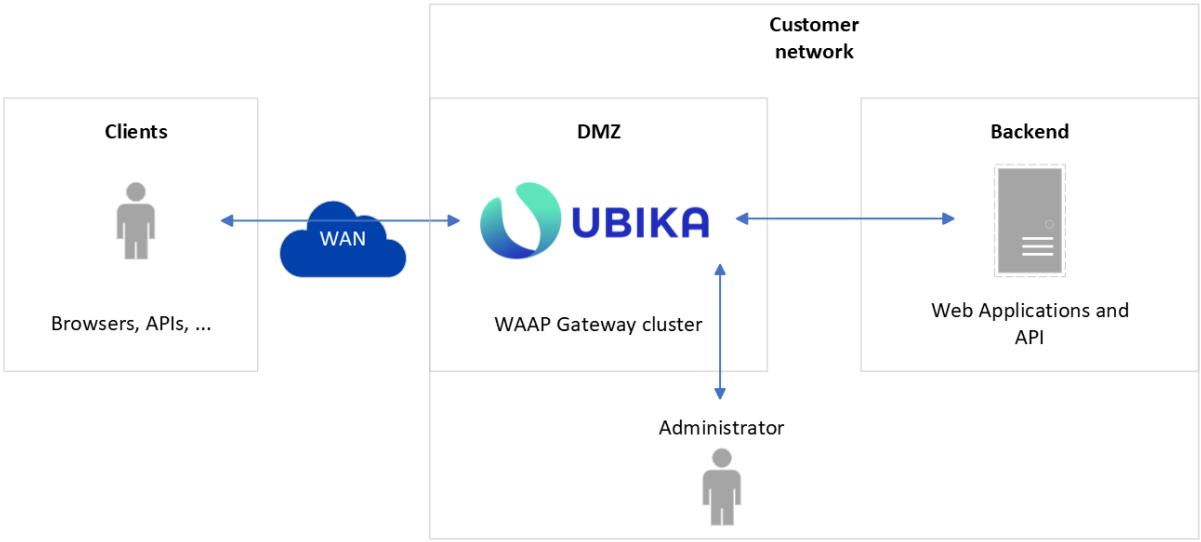


**Figure 1 - Architecture cible d'utilisation du produit.**

## 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 | UBIKA WAAP Gateway |
| Numéro de la version évaluée | *Version 6.11.1 sur appliances 1450 et 4450* |

La version certifiée du produit peut être identifiée en se connectant sur l'*appliance* (1450 ou 4450) avec le client lourd :

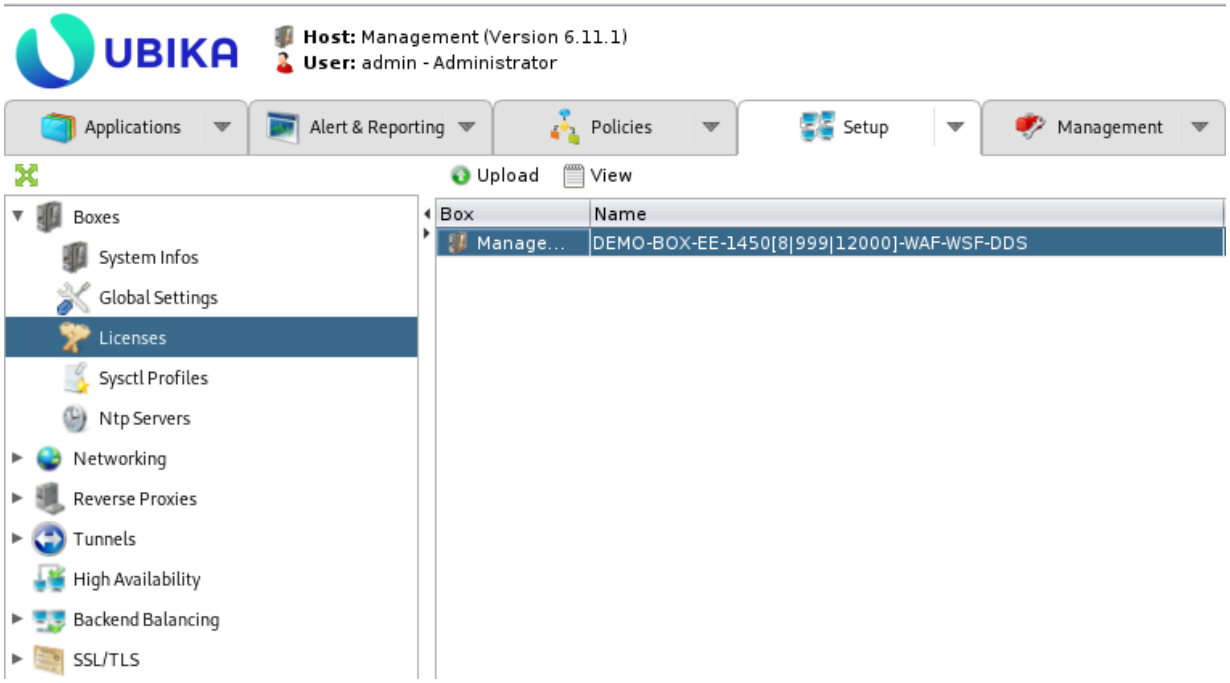


**Figure 2 – Identification de la version certifiée (*appliance* 1450).**

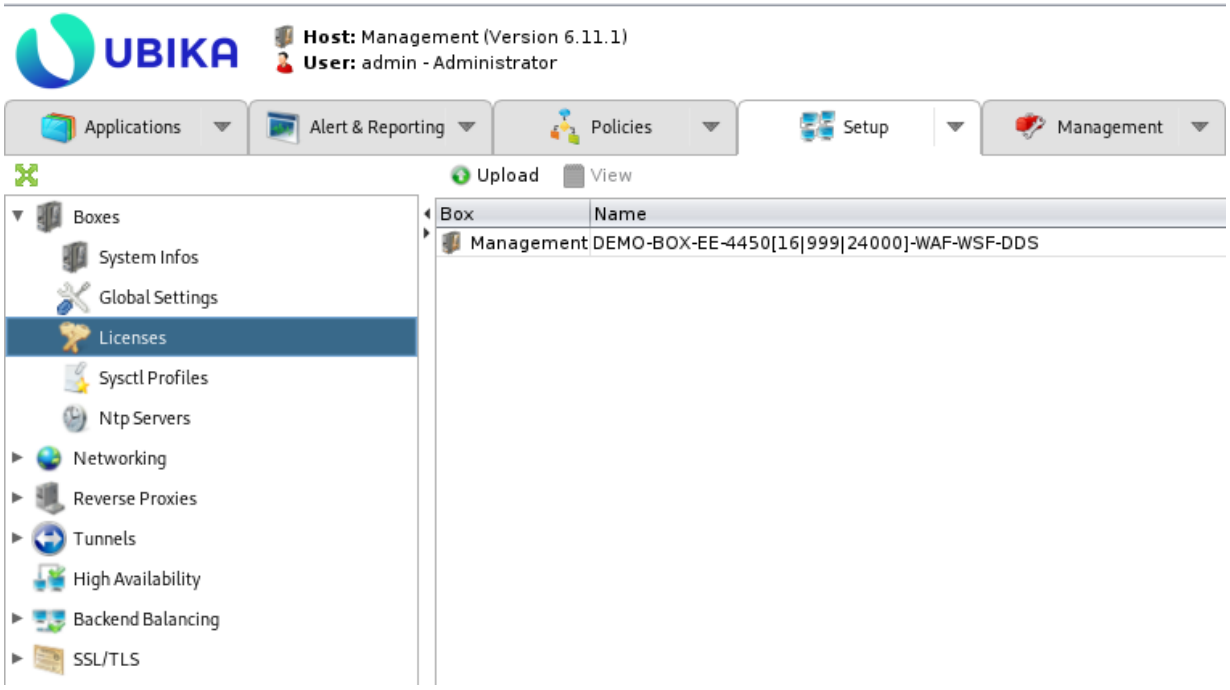


**Figure 3 – Identification de la version certifiée (*appliance* 4450).**

### 1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- le filtrage des données HTTP ;
- la sécurité des cookies ;
- la sécurité des données XML ;
- la sécurité des données JSON ;
- la terminaison TLS/SSH ;
- la validation de certificats clients ;
- l'authentification des administrateurs ;
- le durcissement du socle de l'*appliance* ;
- la politique et sécurisation des mises à jour ;
- le stockage sécurisé des clés de chiffrement.

### 1.2.4 *Configuration évaluée*

La configuration évaluée correspond à la plateforme de test ci-dessous :

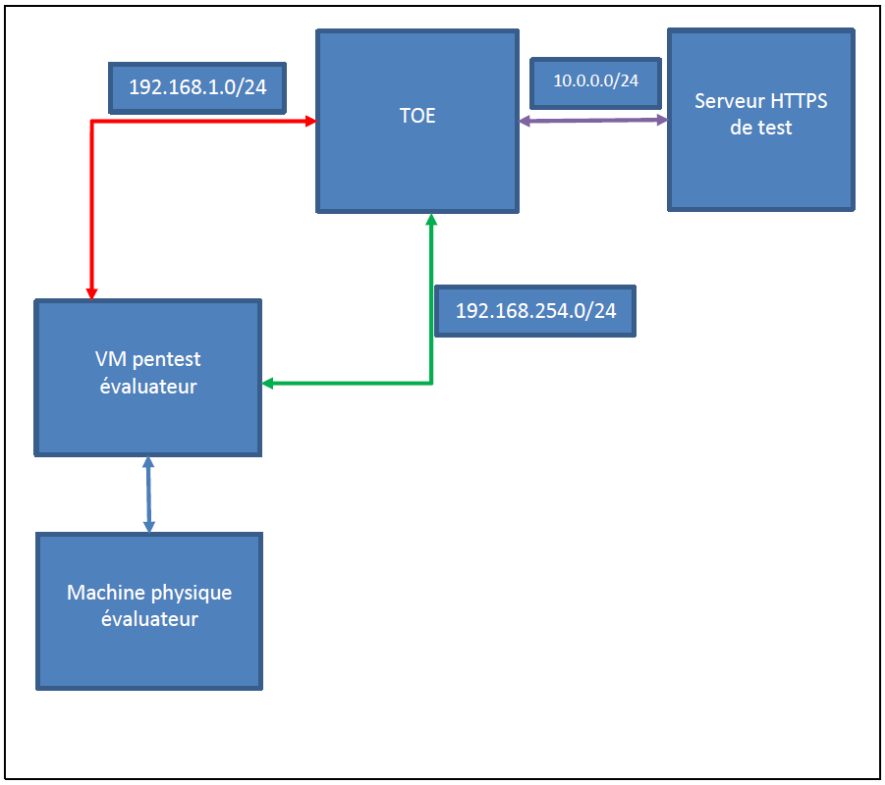


**Figure 4 – Plateforme de test.**

La plateforme de test est constituée des éléments suivants :

- le produit évalué (la TOE), au centre, agissant comme un pare-feu applicatif (WAF) en coupure entre la machine de test et la machine à protéger ;
- la machine à protéger, sous forme de serveur HTTPS de test simulant un service web protégé par la TOE ;
- une machine virtuelle de test, permettant :
  - de requêter indirectement le serveur HTTPS de test, dans un rôle de client légitime ou d'attaquant ;
  - de se connecter à l'interface d'administration de la TOE.
- une machine physique de test, reliée à la machine virtuelle de test par un tunnel SSH, permettant de réaliser certains tests selon le contexte.

# 2 L'évaluation

## 2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

## 2.2 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].

### 2.2.1 *Installation du produit*

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

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

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

Le produit est fourni par le développeur, sous la forme d'une *appliance* (modèle 1450 ou 4450) qui doit ensuite être configurée à l'aide d'une application de configuration dédiée à installer sur le poste de l'administrateur. La configuration comprend celle des interfaces réseaux (client, administrateur, serveur applicatif), de la date et de l'heure, d'un reverse proxy ainsi que d'un tunnel entre l'interface client et l'interface serveur applicatif.

#### *2.2.1.3 Notes et remarques diverses*

Sans objet.

### 2.2.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

### 2.2.3 *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.

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

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

### 2.2.5 *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.

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

#### *2.2.6.1 Liste des vulnérabilités connues*

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

#### *2.2.6.2 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]

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

#### *2.2.7.1 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.

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

Le produit nécessite un certain nombre de configurations avant d'être fonctionnel.

#### *2.2.7.3 Notes et remarques diverses*

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

## 2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) 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 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.

## 2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

# 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 « UBIKA WAAP Gateway, Version 6.11.1 sur appliances 1450 et 4450 » 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 suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- une modification de configuration du produit devra être réalisée, comme indiquée dans le guide suivant : https://documentation.ubikasec.com/waap-gateway-fr/v6.11/get-started/add-a-tunnel-to-secure-a-web-application.html#workflow-waap-default, afin de bloquer les attaques CSRF utilisant la méthode http GET ;
- le certificat x509 par défaut proposé par l'interface d'administration du produit devra être remplacé par un certificat respectant les recommandations de l'ANSSI en termes de durée de validité et d'utilisation du protocole OCSP, comme indiqué dans le guide suivant : https://documentation.ubikasec.com/waap-gateway-fr/v6.11/get-started/administration-interface-to-manage-the-cluster.html#accepter-le-certificat-de-la-pki-du-waap-de-management.

# ANNEXE A. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | Cible de sécurité de référence pour l'évaluation :<br>- Cible de sécurité UBIKA WAAP Gateway 6.11.1, version 5.2, 13 novembre 2023. |
| [RTE] | Rapport technique d'évaluation :<br>- Rapport Technique d'Evaluation CSPN, référence OPPIDA/CESTI/UBIKAWAAP610/RTE/1.4, version 1.4, 10 janvier 2024. |
| [GUIDES] | Guides d'administration et d'installation du produit :<br>- https://documentation.ubikasec.com/pages/viewpage.action?pageId=55261606[1] |

[1] Tous les guides du produit sont accessibles en ligne à cette adresse avec un compte client.

# 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. | |
| [CSPN] | Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 4.0, 3 mars 2022.<br><br>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0,6 septembre 2018. |
| [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, 26 janvier 2021. |
| [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. |