PREMIÈRE 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-2023/04

Logiciel Single-tenant MIP NPM en tant que service (SaaS), en hébergement Cloud non privé, sur socle IaaS

Version 7.28.0

Paris, le 21 Juin 2023

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

Emmanuel NAEGELEN

[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-CSPN-2023/04**
Nom du produit **Logiciel Single-tenant MIP NPM en tant que service (SaaS), en hébergement Cloud non privé, sur socle IaaS**
Référence/version du produit **Version 7.28.0**
Catégorie de produit **Administration et supervision de la sécurité**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **MALTEM INSIGHT PERFORMANCE** Technopôle Izarbel 64210 Bidart, France
Développeur **MALTEM INSIGHT PERFORMANCE** Technopôle Izarbel 64210 Bidart, France
Centre d'évaluation **AMOSSYS** 11 rue Maurice Fabre 35000 Rennes, France
Fonctions de sécurité évaluées Identification et authentification de chaque utilisateur du bénéficiaire ; Contrôle d'accès et gestion des droits entre utilisateurs du bénéficiaire ; Stockage sécurisé ; Communications sécurisées.
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage 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 « Logiciel Single-tenant MIP NPM en tant que service (SaaS), en hébergement Cloud non privé, sur socle IaaS, Version 7.28.0 » développé par MALTEM INSIGHT PERFORMANCE.

La solution MIP NPM fournit un *monitoring* avancé des réseaux, des applications et de l'expérience utilisateurs sur les systèmes d'information, grâce à des agents dans le *Cloud*, dans les *data centers* privés, ou sur sites. Cette solution permet aux décideurs IT d'accéder à une vue globale de la capacité et des usages des infrastructures, d'assurer le SLA et de diminuer la durée des pannes informatiques.

Le portail MIP NPM se connecte préalablement au réseau de l'entreprise bénéficiaire par un lien VPN, et envoie ensuite des requêtes SNMPv3 vers les routeurs et les agents de mesure réseau mis en place pour mesurer la performance.

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

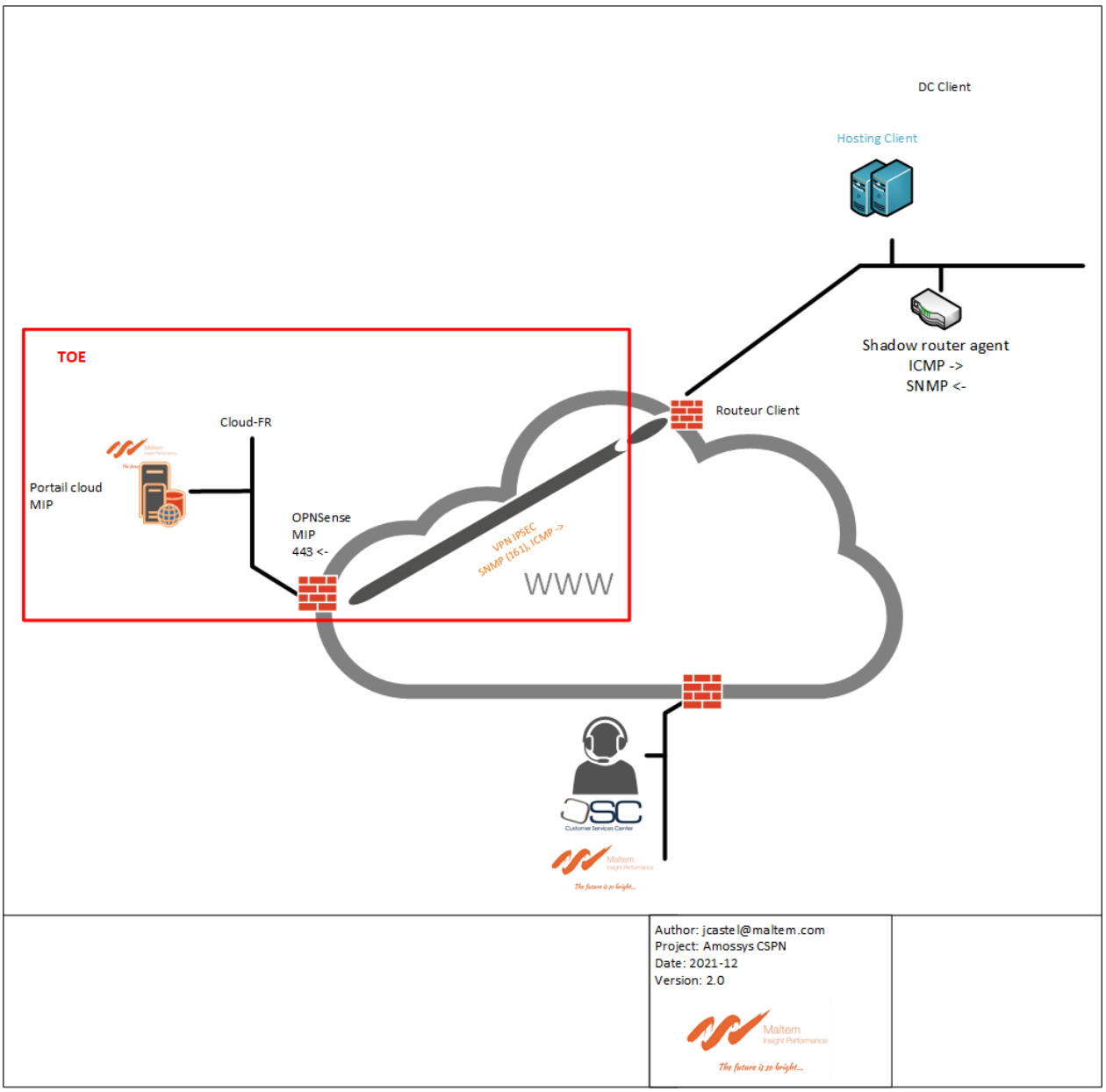

Figure 1 - Schéma de déploiement cloud du produit commercialisé.

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	Logiciel Single-tenant MIP NPM en tant que service (SaaS), en hébergement Cloud non privé, sur socle IaaS
Numéro de la version évaluée	Version 7.28.0

La version certifiée du produit peut être identifiée via l'interface web (accessible à l'utilisateur final comme à l'administrateur métier) : le numéro de version est visible dans le coin inférieur gauche de l'interface (voir figure ci-dessous) :

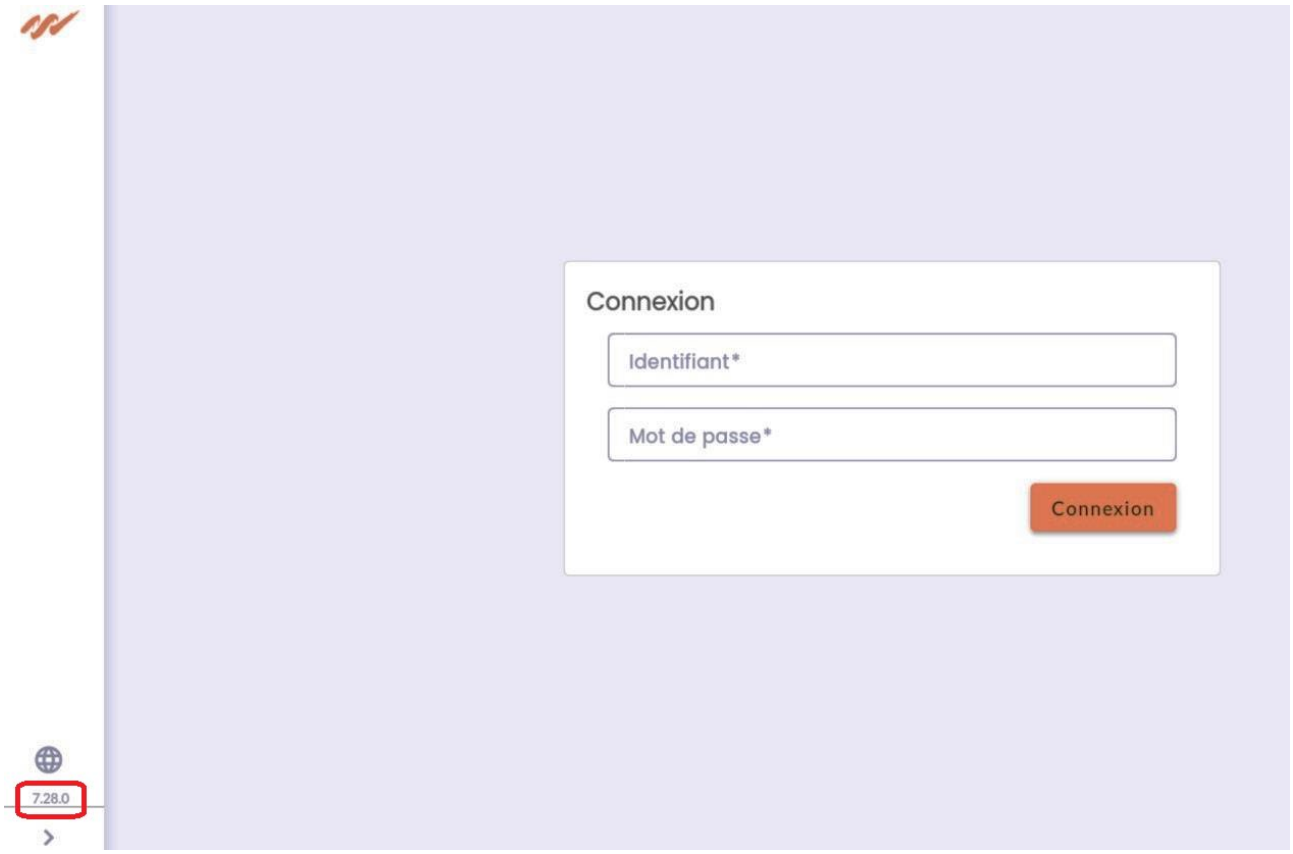

Figure 2 – Identification de la version du produit

L'administrateur système peut également s'assurer de la version du produit en vérifiant la dénomination des conteneurs *Docker*.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- Identification et authentification de chaque utilisateur du bénéficiaire ;
- Contrôle d'accès et gestion des droits entre utilisateurs du bénéficiaire ;
- Stockage sécurisé ;
- Communications sécurisées.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond à l'ensemble des éléments suivants :

- le portail MIP NPM en version 7.28.0 ;
- l'environnement fonctionnant sur *Docker Swarm* pour le mettre en œuvre ;
- les communications utilisateur ;
- les communications métier (flux permettant la collecte des agents de mesure réseau).

La plateforme de test est constituée des éléments suivants :

- le portail MIP, installé sur une version Debian 11, version 5.10.162-1 du kernel, sans interface graphique ;
- deux pare-feux OPNsense version 22.7.11, installés chacun sur FreeBSD 13.1-RELEASE-p5 ;
- un agent/*shadow router*, qui est une *appliance* Cisco 1900 K9 ;
- un tunnel IPsec reliant les deux pare-feux ;
- un poste client sur le réseau client.

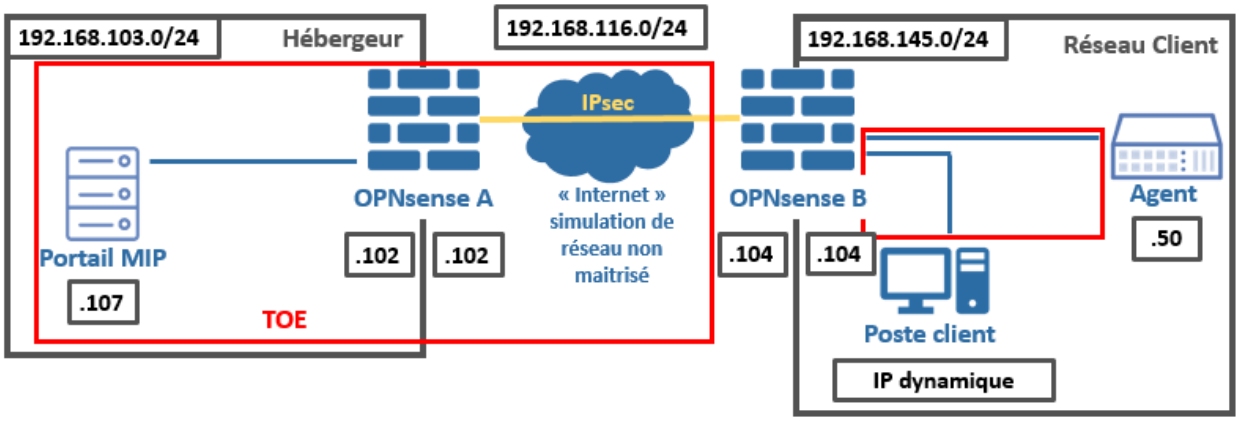

Figure 2 – Plateforme de test

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et aux dispositions de [NOTE-06].

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

Le processus d'installation consiste en plusieurs étapes :
- récupération des conteneurs depuis un dépôt *Docker* privé du développeur ;
- exécution d'un script *bash* de configuration de l'instance locale ;
- configuration du produit depuis l'interface web.

Les deux premières étapes sont entièrement automatisées en environnement de production.

La troisième étape de configuration du produit est décrite dans la documentation fournie.

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

Aucune non-conformité n'a été constatée.

2.2.1.3 Notes et remarques diverses

Dans le cadre commercial général, le développeur installe le produit à distance chez le client de manière automatisée.

Dans le cadre de l'évaluation, l'installation a été réalisée par l'évaluateur, assisté en présentiel par le développeur, au sein des locaux du CESTI. La procédure d'installation reste cependant identique.

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, ainsi que certains éléments de code non compilés présents sur la TOE (fichiers de script et langages interprétés).

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

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

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 est modérément simple d'utilisation.

Le bénéficiaire, l'entreprise cliente de la prestation, ne dispose que de droits limités sur le produit, la totalité des activités d'administration étant à la charge du développeur.

Toutefois, le cas d'usage classique du produit est simple, et aucun défaut de configuration n'est possible pour un utilisateur standard.

2.2.7.3 Notes et remarques diverses

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

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 [ANA_CRY].

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.

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 « Logiciel Single-tenant MIP NPM en tant que service (SaaS), en hébergement Cloud non privé, sur socle IaaS, Version 7.28.0 » 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].

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité CSPN - Logiciel *Single-tenant* MIP NPM en tant que service (SaaS) - version 7.28.0, en hébergement *Cloud* non privé, sur socle IaaS - référence CSPN-ST-MIP-2.09, version 2.09, 25 avril 2023.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN - Logiciel *Single-tenant* MIP NPM en tant que service (SaaS) - version 7.28.0, en hébergement *Cloud* non privé, sur socle IaaS - référence CSPN-RTE-MIP2-2.02, version 2.02, 10 mai 2023.
[ANA_CRY]	Rapport technique d'évaluation des mécanismes cryptographiques : - Expertise des mécanismes cryptographiques - Logiciel *Single-tenant* MIP NPM en tant que service (SaaS) - version 7.28.0, en hébergement Cloud non privé, sur socle IaaS - référence CSPN-CRY-MIP2-2.02, version 2.02, 10 mai 2023.
[GUIDES]	Guides d'utilisation, d'administration ou d'installation du produit : - Documentation utilisateur : accessible via https://[adresse IP du portail MIP NPM]/docs ; - Documentation de la gestion des API : accessible via l'adresse https://[adresse IP du portail MIP NPM]/dev.

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. 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. 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.
[NOTE-06]	Note d'application - Méthodologie d'évaluation CSPN pour les logiciels déployés sur des infrastructures de *cloud computing*, référence ANSSI-CSPN-NOTE-06, version 1.0, 2 mars 2021.