PREMIÈRE 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-2022/10

CrossinG

Version 2.1.2

Paris, le 8 septembre 2022

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

Guillaume POUPARD

[ORIGINAL SIGNE]

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-2022/10**
Nom du produit **CrossinG**
Référence/version du produit **Version 2.1.2**
Catégorie de produit **Communication sécurisée**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **CHAPSVISION** 4 rue du Port Aux Vins 92150 Suresnes, France
Développeur **CHAPSVISION** 4 rue du Port Aux Vins 92150 Suresnes, France
Centre d'évaluation **AMOSSYS** 11 rue Maurice Fabre 35000 Rennes, France
Fonctions de sécurité évaluées Filtrage réseau Contrôle des données à transférer Cloisonnement interne des processus Communications sécurisées Mise à jour sécurisée Authentification des utilisateurs et administrateurs Contrôle d'accès aux fichiers de configuration et aux journaux Journalisation locale Export sécurisé de la configuration et des journaux Protection contre la perte de disponibilité Autoprotection contre accès non autorisés et exécution de code malveillant
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage 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.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « CrossinG, Version 2.1.2 » développé par CHAPSVISION.

Ce produit est une passerelle d'interconnexion permettant le transfert sécurisé de fichiers entre des réseaux dont les domaines opérationnels sont différents, par exemple entre un réseau public (Internet) et un réseau isolé (Intranet, réseau sensible), entre un Système d'information de gestion et un Système de contrôle industriel, etc.

Le produit se présente sous la forme d'une *appliance* matérielle, fonctionnant comme un sas et disposant de quatre interfaces réseau physiques, connectées aux deux domaines opérationnels, au réseau d'administration et au réseau de supervision, comme le montre la figure suivante :

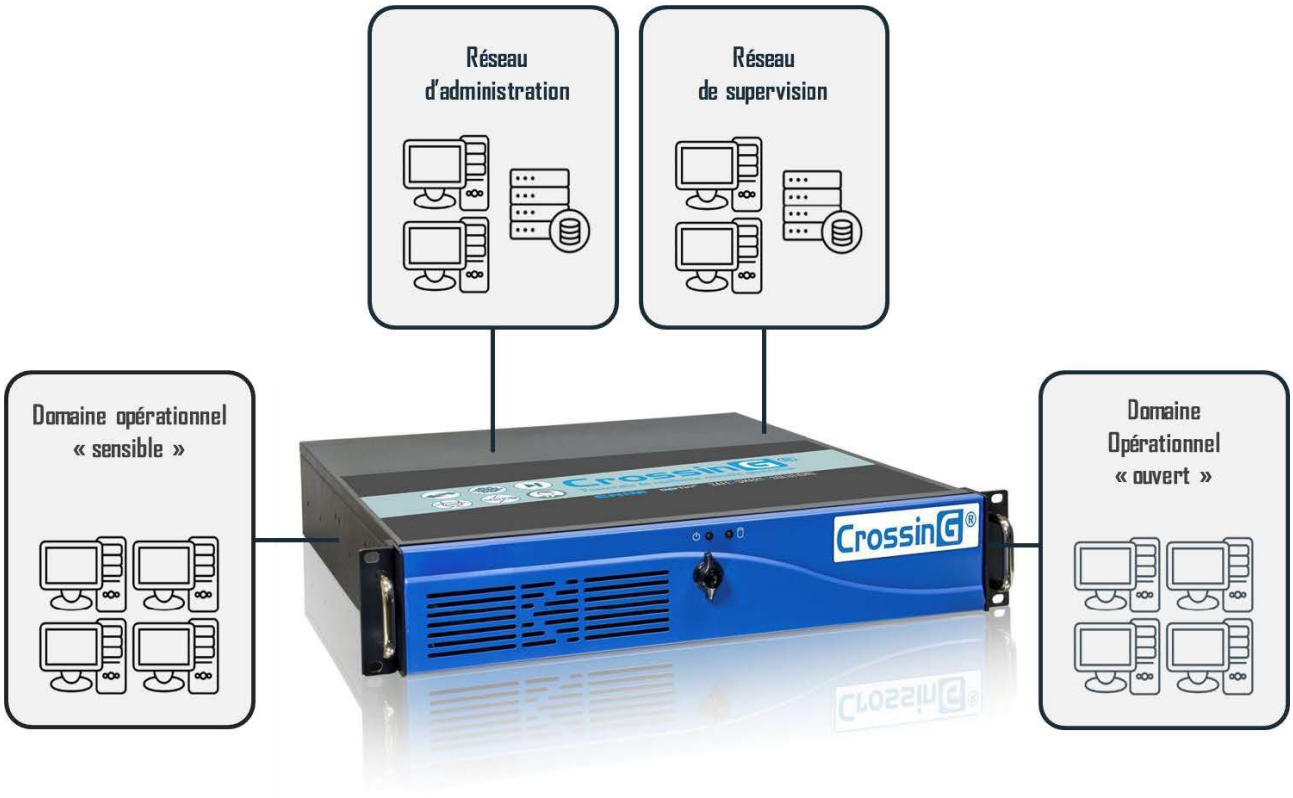


Figure 1 – Présentation du produit

La passerelle combine plusieurs mécanismes de sécurité durant les transferts de fichiers pour assurer la défense en profondeur des systèmes d'information sensibles et des infrastructures critiques, en accord avec la politique de sécurité de l'organisation.

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	CrossinG
Numéro de la version évaluée	Version 2.1.2

La version certifiée du produit peut être identifiée :

- au bas des interfaces *web* d'administration, d'initialisation et de supervision :
- depuis l'interface d'administration, dans le menu Documentation puis dans la fiche de version.

1.2.3 *Fonctions de sécurité*

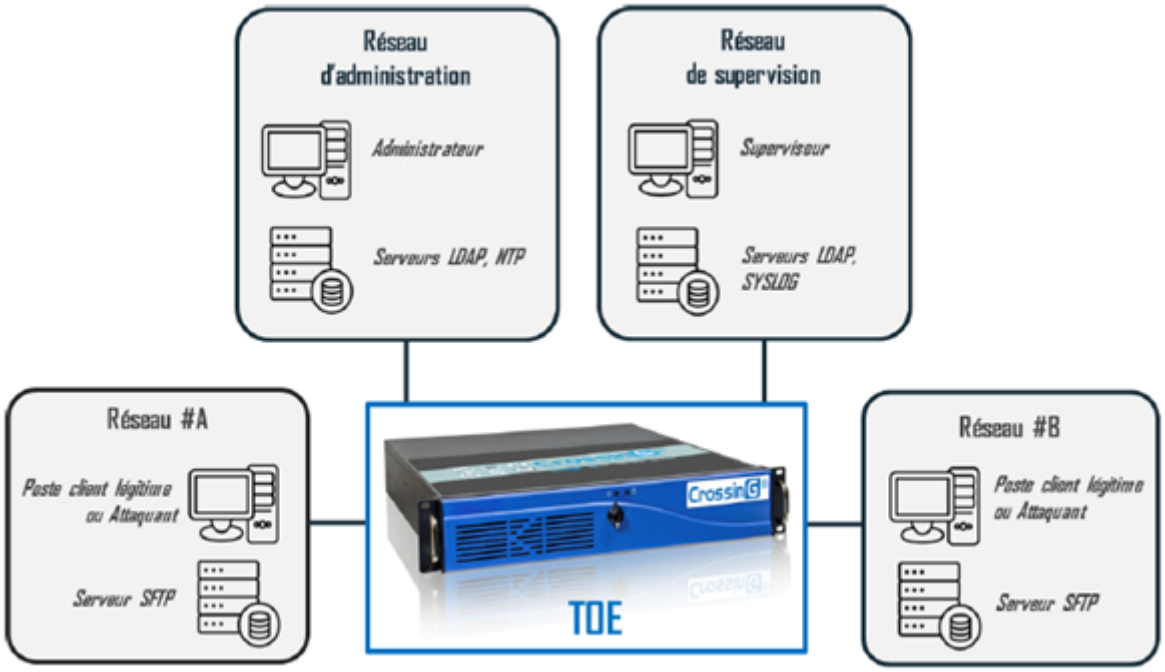
Les fonctions de sécurité évaluées du produit sont :

- le filtrage réseau ;
- le contrôle des données à transférer ;
- le cloisonnement interne des processus ;
- les communications sécurisées ;
- la mise à jour sécurisée ;
- l'authentification des utilisateurs et administrateurs ;
- le contrôle d'accès aux fichiers de configuration et aux journaux ;
- la journalisation locale ;
- l'export sécurisé de la configuration et des journaux ;
- la protection contre la perte de disponibilité ;
- l'autoprotection contre les accès non autorisés et contre l'exécution de code malveillant.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond à une *appliance* physique fournie par le développeur et initialisée par l'évaluateur en suivant les procédures et directives décrites dans [GUIDES].

La plateforme de tests est présentée ci-dessous :



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

Une *appliance* physique et des certificats ont été livrés à l'évaluateur, qui a utilisé la documentation d'installation fournie par le développeur pour initialiser la plateforme avec les certificats fournis.

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 et fourni les résultats de l'analyse dans le rapport d'expertise des mécanismes cryptographiques [ANA_CRY].

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

Les interfaces permettant de réaliser la configuration du produit sont intuitives et faciles à utiliser. Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur familier.

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 [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.

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 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.

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 « CrossinG, Version 2.1.2 » 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 [CDS], notamment :

- les réseaux d'administration et de supervision doivent correspondre à des réseaux dédiés, cloisonnés entre eux, isolés et non accessibles pour les agents de menace ;
- les réseaux d'administration et de supervision doivent être déconnectés d'Internet ;
- les recommandations de sécurité doivent être respectées (chapitre 9.8 du guide d'administration [GUIDES]) ;
- la configuration de vérifications d'empreintes (intégrité) de fichiers sans vérifications des signatures associées ne doit pas être utilisée (chapitre 13.10.4 du guide d'administration [GUIDES]) ;
- les algorithmes MD5 ou SHA1 pour les signatures et vérification d'empreintes ne doivent pas être utilisés (chapitre 13.10.4 du guide d'administration [GUIDES]);
- l'accès au serveur *web* d'initialisation doit être protégé.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - CrossinG Cible de sécurité, référence BTSSI-CG-2-1_CSPN_Cible, révision U, 4 août 2022.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN – Produit CrossinG version 2.1.2, référence CSPN-RTE-BTSSI-CG-DR-2.03, version 2.03, 4 août 2022.
[ANA_CRY]	Rapport d'expertise des mécanismes cryptographiques : - Expertise des mécanismes cryptographiques – Produit CrossinG version 2.1.2, référence CSPN-CRY-BTSSI-CG-DR-2.03, version 2.03, 4 août 2022.
[GUIDES]	Guides d'installation et configuration du produit : - Guide de démarrage, référence BTSSI-CG-2-1_GuideDemarrage ; - Guide d'administration, référence BTSSI-CG-2-1_GuideAdmin, révision N, 27 juillet 2022 ; - Guide de supervision, référence BTSSI-CG-2-1_GuideSupervision, révision D, 8 octobre 2020 ; - Guide cryptographique, référence BTSSI-CG-2-1_GuideCrypto, révision H, 27 juillet 2022.

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.