



**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-2025/16

KEEPASSXC
version 2.7.9

Paris, le 17/11/2025 | 15:15 CET

Vincent Strubel



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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CSPN-2025/16
Nom du produit	KEEPASSXC
Référence/version du produit	version 2.7.9
Catégorie de produit	Stockage sécurisé
Critère d'évaluation et version	CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)
Commanditaire	ANSSI 51 boulevard de la Tour Maubourg 75007 Paris, France
Développeur	KeePassXC Team Friesstr. 1 99423 Weimar, Germany
Centre d'évaluation	SYNACKTIV 5 boulevard Montmartre 75002 Paris, France
Accord de reconnaissance applicable	
Ce certificat est reconnu dans le cadre du [BSZ_CSPN]	
Fonctions de sécurité évaluées	<i>Anti-screenshot/recording Clipboard protection Database protection Memory protection Prompt of each password access from a browser extension KeeShare segregation ssh-agent interaction</i>
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 cyber.gouv.fr.

TABLE DES MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit évalué.....	6
1.2.1	Catégorie du produit	6
1.2.2	Identification du produit.....	6
1.2.3	Fonctions de sécurité.....	7
1.2.4	Configuration évaluée	7
2	L'évaluation.....	8
2.1	Référentiels d'évaluation	8
2.2	Travaux d'évaluation	8
2.2.1	Installation du produit.....	8
2.2.2	Analyse de la documentation.....	8
2.2.3	Revue du code source (facultative).....	8
2.2.4	Analyse de la conformité des fonctions de sécurité	8
2.2.5	Analyse de la résistance des mécanismes des fonctions de sécurité	8
2.2.6	Analyse des vulnérabilités (conception, construction, etc.)	9
2.2.7	Analyse de la facilité d'emploi	9
2.3	Analyse de la résistance des mécanismes cryptographiques	10
2.4	Analyse du générateur d'aléa.....	10
3	La certification	11
3.1	Conclusion.....	11
3.2	Recommandations et restrictions d'usage	11
3.3	Reconnaissance du certificat.....	11
ANNEXE A.	Références documentaires du produit évalué	12
ANNEXE B.	Références liées à la certification	13

1 Le produit

1.1 Présentation du produit

Le produit évalué est « KEEPASSXC, version 2.7.9 » développé par KeePassXC Team.

Ce produit est un coffre-fort de mot de passe.

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

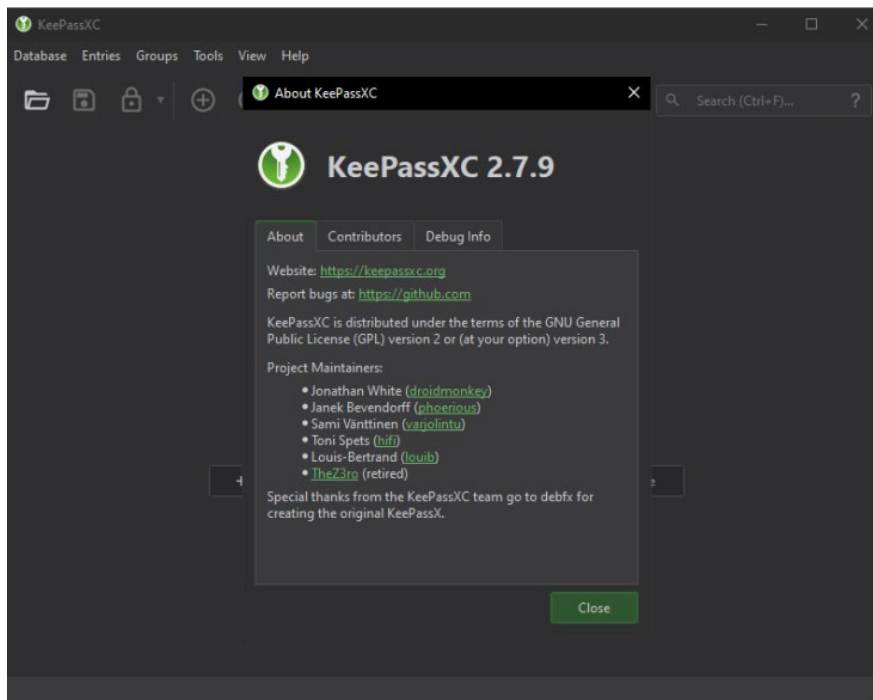
<input type="checkbox"/>	1	détection d'intrusions
<input type="checkbox"/>	2	anti-virus, protection contre les codes malicieux
<input type="checkbox"/>	3	pare-feu
<input type="checkbox"/>	4	effacement de données
<input type="checkbox"/>	5	administration et supervision de la sécurité
<input type="checkbox"/>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

1.2.2 Identification du produit

Produit	
Nom du produit	KEEPASSXC
Numéro de la version évaluée	version 2.7.9

La version certifiée du produit peut être identifiée de la manière suivante :

- La version peut être lue dans les parties « *about* » et « *help* » du menu :



1.2.3 Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- *Anti-screenshot/recording*
- *Clipboard protection*
- *Database protection*
- *Memory protection*
- *Prompt of each password access from a browser extension*
- *KeeShare segregation*
- *ssh-agent interaction*

1.2.4 Configuration évaluée

La configuration évaluée testé est la suivante :

Version de KEEPASSXC compilée AMD64 pour Windows 10

Microsoft Windows 10

SSH version is OpenSSH_for_Windows_9.5p1

LibreSSL 3.8.2

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 logiciel a été téléchargé depuis le site officiel de KEEPASSXC : <https://keepassxc.org>.

Le programme est téléchargé comme un paquet MSI. Le hachage du fichier MSI est disponible sur la même page ainsi que la signature PGP.

La clé PGP signée est stockée dans le dossier keys.opengpg.org.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 Analyse de la documentation

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'intégralité 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

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

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 inexploitable 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

Il est important de choisir un mot de passe pour la base de données robuste.

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 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

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 « KEEPASSXC, version 2.7.9 » 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 :

- Utiliser un mot de passe robuste pour la base de données.

3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ (*Beschleunigte Sicherheitszertifizierung* ou Certification de sécurité accélérée).



ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : <ul style="list-style-type: none">- CSPN Security Target KeePassXC CSPN, version 1.6, 11 septembre 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : <ul style="list-style-type: none">- CSPN Security Target KeePassXC CSPN, version 1.7, 28 octobre 2025
[RTE]	Rapport technique d'évaluation : <ul style="list-style-type: none">- CSPN-2024-KEEPASSXC, version 1.4, 29 octobre 2025
[GUIDES]	Guide d'utilisation du produit : <ul style="list-style-type: none">- KeePassXC: <i>Getting Started Guide</i>, version 2.7.10

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]	<p>Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 5.0, 12 janvier 2023.</p> <p>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 5.0, 12 juillet 2024.</p> <p>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 4.0, 12 juillet 2024.</p>
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.2, 18 mars 2025.
[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.
[BSZ_CSPN]	<i>Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI</i> , référence <i>bsz_cspn_mutual_recognition_agreement</i> , version 2.0, mai 2024.

