Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2018/23

CRYPTOBOX
(version 2.1.48)

Paris, le 24 mai 2018

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

Guillaume POUPARD
[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

ANSSI-CC-2018/23

Nom du produit

CRYPTOBOX

Référence/version du produit

2.1.48

Conformité à un profil de protection

Aucune

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 3 augmenté

ALC_FLR.3, AVA_VAN.3

Développeur :

Ercom

6, rue Dewoitine, 78140 Vélizy, France

Commanditaire

Ercom

6, rue Dewoitine, 78140 Vélizy, France

Centre d'évaluation

Amossys

4 bis allée du bâtiment, 35000 Rennes, France

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2 augmenté d'ALC_FLR.3.

SOG-IS

Ce certificat est reconnu au niveau EAL3 augmenté d'ALC_FLR.3.

Préface

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 Premier ministre 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 sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le logiciel « CRYPTOBOX, version 2.1.48 » développé par la société *ERCOM*.

Ce produit embarqué dans une plateforme, permet le stockage sécuritaire de données sensibles dans un *cloud* administré par un tiers. Ainsi, les entreprises gardent le contrôle de leurs données et les rendent accessibles uniquement aux collaborateurs autorisés afin qu'ils puissent effectuer des travaux coopératifs.

1.2. Description du produit

1.2.1. Introduction

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

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'authentification des utilisateurs ;
- le contrôle d'accès aux fichiers protégés ;
- le stockage sécurisé de données dans un *cloud* qui n'est pas considéré de confiance ;
- la modification de fichiers ;
- le partage sécurisé de fichiers ;
- la sauvegarde et la récupération de comptes utilisateurs.

1.2.3. Architecture

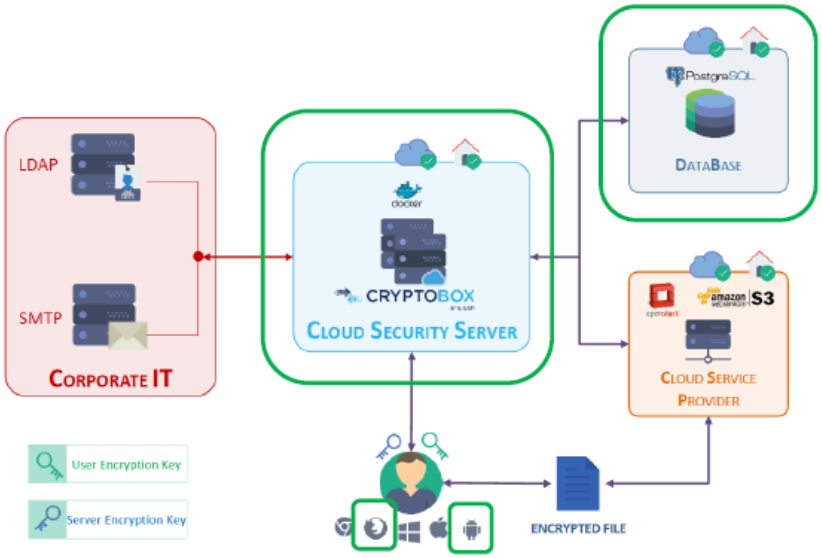

Figure 1 – Schéma d'architecture de haut niveau

Les composants inclus dans la TOE (encadrés en vert sur la figure ci-dessus) sont les suivants :

- le *Cloud Security Server* (CSS) qui communique avec la base de données et centralise les évènements d'audits notamment les journaux d'accès aux fichiers protégés. Son cœur cryptographique est le *Security Module* (SM) qui est responsable de l'authentification des utilisateurs, du contrôle d'accès et du stockage d'une partie des clés de chiffrement ;
- la *DataBase* qui contient les différentes clés de chiffrement des documents du *Cloud Service Provider*, les données utilisateurs (notamment les clés publiques), les métadonnées des documents partagés et d'autres données nécessaires au fonctionnement de la TOE ;
- des *User Agents* qui permettent aux utilisateurs d'accéder, modifier et partager des documents de manière sécurisée, à partir des applications *CRYPTOBOX WEB* et *CRYPTOBOX ANDROID*.

Le *Cloud Service Provider* assure le stockage des données chiffrées (fichiers et métadonnées) et leur disponibilité aux utilisateurs. Ce composant est hors du périmètre de l'évaluation de la TOE.

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

Comme mentionné dans [GUIDES], la version du produit est identifiable en sélectionnant « A propos de Cryptobox ».

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement, la livraison et le support aux clients du produit sont réalisés sur les sites de *ERCOM* ;
- l'installation, l'administration et l'utilisation du produit correspondent au déploiement du produit par le client.

Le produit est développé sur les sites suivants :

ERCOM VELIZY	**ERCOM PARIS**
6, rue Dewoitine bâtiment Rubis 78140 Vélizy-Villacoublay France	6, rue du Général Larminat 75015 Paris France

La livraison du produit et le support aux clients sont effectués sur le site suivant :

ERCOM VELIZY

6, rue Dewoitine
bâtiment Rubis
78140 Vélizy-Villacoublay
France

Pour l'évaluation, l'évaluateur a considéré les rôles suivants :

- administrateur : personne chargée de définir les droits des comptes utilisateurs, de consulter les journaux d'audit relatifs aux évènements et de valider le *process* de récupération de compte ;
- utilisateurs :
  - propriétaire : propriétaire de l'espace de travail (*workspace*) qui gère les droits des utilisateurs du *workspace* et qui dispose des mêmes droits qu'un rédacteur ;
  - rédacteur : utilisateur qui est autorisé à lire et écrire dans les documents du *workspace* ;
  - lecteur : utilisateur qui ne peut que lire les documents du workspace ;
  - trustee : utilisateur désigné pour la récupération d'un compte lorsque son propriétaire a oublié son mot de passe.

1.2.6. Configuration évaluée

La configuration évaluée inclut :

- le serveur Cryptobox (logiciels CSS et SM) installé sur un système *UBUNTU* version 16.04.3 ;
- la base de données installée sur un système *UBUNTU* version 16.04.3 avec la solution PostgreSQL v9.5.12 ;
- un agent *ANDROID* installé sur *ANDROID* version 7.1.1 ;
- un agent web *FIREFOX* embarqué sur *FIREFOX* version 58.0.2 sur Windows 10 64 bits.

Pour effectuer l'évaluation, les différents éléments de la TOE ont été installés sur des machines virtuelles, appartenant à quatre réseaux privés :

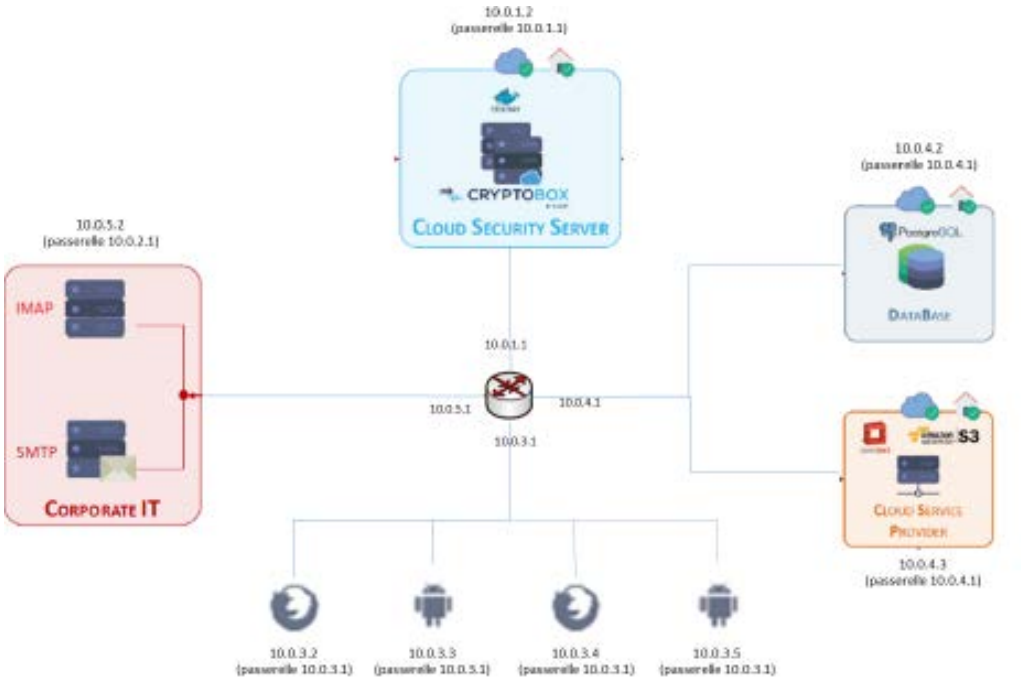

Figure 2 : Plateforme d'évaluation

Les machines 10.0.3.4 et 10.0.3.5 servent de point d'entrée de la TOE lors de tests pour jouer le rôle d'utilisateurs légitimes ou illégitimes.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 15 mai 2018, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI.

Les résultats ont été pris 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 AVA_VAN.3 visé.

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [EXP-CRY]. Ces résultats ont été pris 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 AVA_VAN.3 visé.

2.4. Analyse du générateur d'aléas

Les données aléatoires se basent sur les librairies utilisées :

- le serveur CSS utilise le générateur de *OpenSSL* v1.0.2g pour les communications HTTPS et HMAC-SHA256 DRBG de la librairie *mbed TLS* ;
- le client *ANDROID* utilise le générateur /dev/urandom[1] retraité par l'algorithme SHA-1.
- le client Web utilise le générateur de *FIREFOX* avec la fonction *getRandomValues*.

Ces générateurs de nombres aléatoires ont été évalués. Les tests statistiques réalisés sur les sorties des divers générateurs utilisés par la TOE n'ont pas révélé de biais sur les données aléatoires générées.
Les résultats ont été pris en compte dans l'analyse de vulnérabilité réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

[1] Générateur de nombre aléatoires du noyau *LINUX*.

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. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit logiciel « CRYPTOBOX, version 2.1.48 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

3.2. 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 d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre strictement les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs.
La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	**3**	Functional specification with complete summary
	ADV_IMP				1	1	2	2		
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**2**	Architectural design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	**3**	Authorisation controls
	ALC_CMS	1	2	3	4	5	5	5	**3**	Implementation representation CM coverage
	ALC_DEL		1	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			1	1	1	2	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			1	1	1	1	2	**1**	Developer defined life-cycle model
	ALC_TAT				1	2	3	3		
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	**2**	Analysis of coverage
	ATE_DPT			1	1	3	3	4	**1**	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	**1**	Functional testing
	ATE_IND	1	2	2	2	2	2	3	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Cryptobox 2.1, version 2aa090b, 25/4/2018, *ERCOM*.
[RTE]	Rapport technique d'évaluation : - Projet « Cryptobox », référence RTE-CRYPTOBOX-1.02, version 1.02, 15/5/2018, *AMOSSYS*.
[ANA-CRY]	Expertise des mécanismes cryptographiques : - Projet « Cryptobox », référence CRY-CRYPTOBOX-1.01, version 1.01, 26/4/2018, *AMOSSYS*.
[EXP-CRY]	Expertise des mécanismes cryptographiques : Projet « Cryptobox », référence CRY-CRYPTOBOX-1.01, version 1.01, 26/4/2018, *AMOSSYS*.
[CONF]	Liste de configuration du produit : - Evaluation configuration list for Cryptobox-v2.1.48, référence ALC_CMS_1, version b625610, *ERCOM*. - Cryptobox source configuration list, référence ALC_CMS_2, version 2.1.48, *ERCOM*.
[GUIDES]	Guide d'installation du produit : - Installation Guide - Cloud Security Server - Cryptobox v2.1, version 2.1.5-8-gf070ff5, mars 2018, *ERCOM*. Guide d'administration du produit : - Administration - Interface Web - Cryptobox v2.1, version 2.1.5-10-gaff3bb4, avril 2018, *ERCOM*. Guide d'utilisation du produit : - Guide utilisateur - Interface Web - Cryptobox v2.1, version 2.1.5-12-gfc32f67, avril 2018, *ERCOM*.

Annexe 3. 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.	
[CER/P/01]	Procédure ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; - Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; - Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[REF]	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.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.