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-CSPN-2017/02

Tanker version 1.7.2 pour Windows 10 associé à Submarine 1.1.1 et Botan 1.11.31

Paris, le 17 février 2017

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-CSPN-2017/02

Nom du produit

Tanker

Référence/version du produit

Version 1.7.2

Catégorie de produit

Stockage sécurisé

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

Kontrol sas

96 bis boulevard Raspail,
75006 Paris,
France

Centre d'évaluation

Quarkslab

71 avenue des Ternes,
75017 Paris,
France

Fonctions de sécurité évaluées

Stockage sécurisé des données
Communications sécurisées avec l'infrastructure distantes
Protection locale des clés
Gestion des documents partagés

Fonction(s) de sécurité non évaluées

Néant

Restriction(s) d'usage

Non

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 CSPN 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 « Tanker, version 1.7.2 pour Windows 10, associé à Submarine 1.1.1 et Botan 1.11.31 » développé par *KONTROL SAS*.

Le but du produit est de chiffrer tout contenu, avant que ce dernier ne soit stocké en ligne par un fournisseur de stockage. Pour cela, le logiciel Tanker une fois exécuté sur un ordinateur, créé un lecteur virtuel sous la forme d'un répertoire et réplique les logiciels clients des fournisseurs de stockage tels que Dropbox. Tout contenu déposé dans ce dossier sera ainsi automatiquement chiffré à la volée par le produit avant d'être envoyé à l'infrastructure du fournisseur de stockage. Le produit offre également la possibilité de partager un document avec un autre utilisateur. Le document sera ainsi chiffré pour cet utilisateur de façon transparente.

Pour fonctionner, le produit s'appuie sur une infrastructure gérée par Tanker. Cette dernière est en charge de stocker et distribuer les clés publiques des utilisateurs lors d'un partage de document par exemple.

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

Nom du produit	Tanker
Numéro de la version évaluée	1.7.2

Le numéro de la version du produit est affiché au lancement du logiciel Tanker.

L'évaluation du produit s'appuie sur les librairies suivantes :
- Submarine en version 1.1.1 ;
- Botan en version 1.11.31.

1.2.3. Configuration évaluée

La version Windows de Tanker a été utilisée. Aucune configuration du produit n'est à faire.

Comme présenté en introduction, le produit s'appuie sur l'infrastructure Tanker pour le *Key Management*, à savoir le stockage et la distribution des clés publiques des utilisateurs.

En ce qui concerne le fournisseur de stockage, dans le cadre de l'évaluation CSPN, il est instancié par Dropbox. Il donc est à noter que l'utilisateur du produit doit pour utiliser Tanker disposer d'un compte Dropbox ainsi que du client Dropbox installé sur son ordinateur. En effet, l'application Tanker créée un lecteur virtuel pointant vers le dossier Dropbox local et réalise le chiffrement/déchiffrement des contenus, mais c'est le client Dropbox qui va ensuite faire la synchronisation des contenus vers le répertoire distant de l'infrastructure de stockage.

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

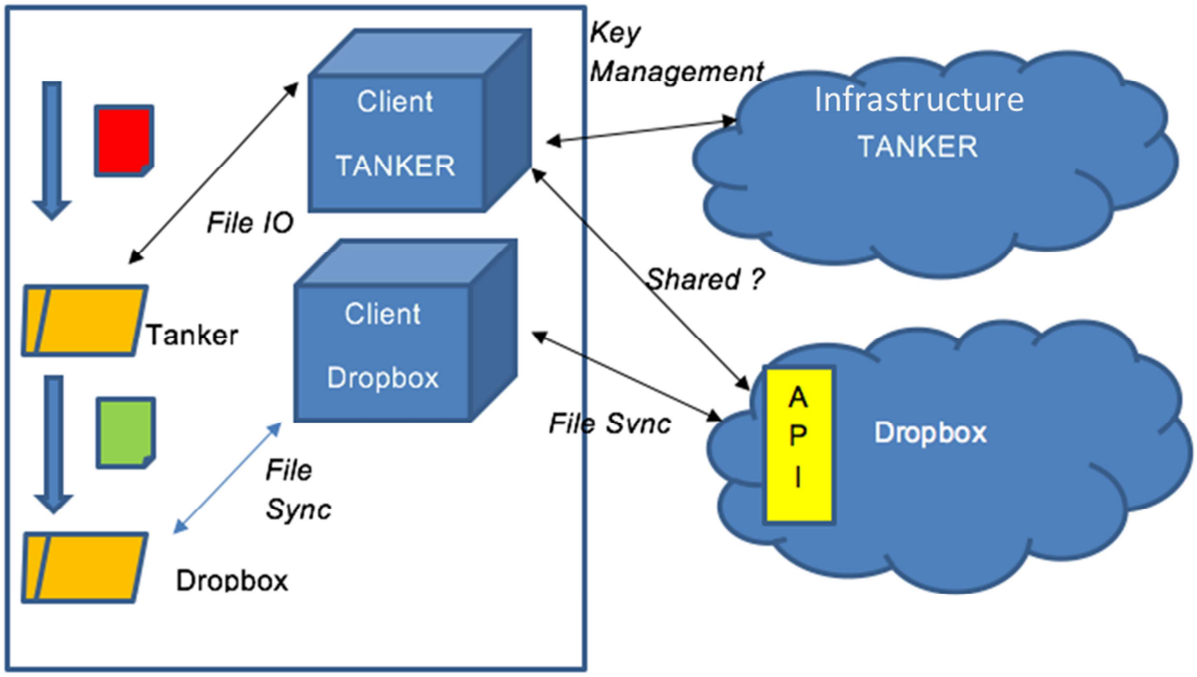

Figure 1 - Architecture du produit.

1.2.4. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- stockage sécurisé des données ;
- communications sécurisées avec l'infrastructure distantes (Tanker et Dropbox) ;
- protection locale des clés ;
- gestion des documents partagés.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. 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].

2.3.1. Installation du produit

2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.3.

2.3.1.2. Description de l'installation et des non-conformités éventuelles

L'installation consiste à copier le binaire « TankerApp.exe » vers un répertoire local.

L'application peut ensuite être lancée avec des droits d'utilisateur Windows ou les droits administrateur Windows. Ces derniers droits servent simplement à enregistrer les icônes Tanker dans le système Windows dans le but :

- de les mettre en surimpression sur les fichiers chiffrés par le produit dans l'explorateur de document ;
- de les afficher dans les menus contextuels[1] ajoutés par Tanker pour chiffrer, déchiffrer et partager un fichier.

En aucun cas il est nécessaire d'avoir les droits administrateur Windows pour utiliser Tanker.

2.3.1.3. Durée de l'installation

L'installation consistant à copier un binaire, la durée est négligeable.

2.3.1.4. Notes et remarques diverses

Comme décrit dans la documentation, après avoir installé le produit il faut suivre les étapes suivantes :

- entrer un coupon d'invitation fourni par Tanker ;

[1] Le menu « clic droit » de l'explorateur Windows.

- associer le compte Dropbox au compte Tanker ;
- si l'utilisateur a un rôle d'administrateur de l'équipe associée au compte Dropbox Business, associer ce compte administrateur au compte administrateur Tanker ;
- choisir un mot de passe ;
- générer ses clés de chiffrement.

Il y a donc deux types d'utilisateurs pour le produit Tanker : utilisateur standard (appelé utilisateur ensuite) et administrateur.

2.3.2. Analyse de la documentation

La documentation utilisateur est claire et s'adresse aux utilisateurs grand public. Elle contient également des recommandations générales de sécurité à destination des utilisateurs sans compétences particulières en informatique.

2.3.3. Revue du code source (facultative)

Le code source de l'application métier n'a pas été fourni. Par contre le code source des briques cryptographiques, à savoir *Submarine* et *Botan*, a été communiqué et donc revu par l'évaluateur. Ce dernier a estimé qu'il est clairement organisé et correctement documenté.

2.3.4. Analyse de la conformité des fonctions de sécurité

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

2.3.5. 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.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

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

2.3.6.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été découvert de vulnérabilité du produit qui puisse remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

L'évaluateur a pu poser des questions aux responsables de Tanker au cours de l'évaluation. Des réponses rapides et détaillées ont été fournies, montrant une très bonne connaissance de leur produit.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. 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.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Aucune recommandation particulière n'est formulée par l'évaluateur.

2.3.8.3. Avis d'expert sur la facilité d'emploi

Le logiciel Tanker a été conçu pour être simple d'utilisation, tout en apportant une sécurité totalement transparente pour l'utilisateur. De plus, aucune configuration n'étant réalisable par l'utilisateur, ce dernier ne peut pas abaisser la sécurité du produit, sauf à utiliser un mot de passe faible pour son compte Tanker.

2.3.8.4. Notes et remarques diverses

Deux remarques ont été faites par l'évaluateur :

- la gestion des documents partagés se faisant au travers du tableau de bord de visualisation des « collaborateurs », elle n'est pas accessible aux utilisateurs, mais uniquement aux administrateurs ;
- la sécurité de l'infrastructure gérée par Tanker n'a pas été évaluée car l'évaluateur n'a eu accès qu'à ses interfaces externes.

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité au [RGS] ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le générateur d'aléa est donc un générateur standard, utilisant une fonction de hachage atteignant le niveau standard. Il est conforme aux spécifications cryptographiques.

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 « Tanker, version 1.7.2 pour Windows 10, associé à Submarine 1.1.1 et Botan 1.11.31 » 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. 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].

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN TANKER 1.7.2* Date : *9 janvier 2017*
[SPEC-CRY]	*Cible de sécurité CSPN, Spécifications cryptographiques* Date : *10 janvier 2017*
[RTE]	*Évaluation CSPN - Tanker 1.7.2* Référence : *17-01-266-REP ;* Version : 1.1 ; Date : *24 janvier 2017*

Annexe 2. Références 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 (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr/
[RGS]	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_B_1), voir www.ssi.gouv.fr/.