TANKER 1.7.2

Cible de sécurité CSPN

Kontrol SAS

6 rue des Ternes - 75 017 Paris – France - +33 (0) 1 85 09 21 64

TABLE DES MATIERES

1 Introduction

1.1 Objet du Document

Ce document est réalisé dans le cadre de l'évaluation CSPN du produit Tanker.

1.2 Identification du produit

Organisation éditrice	KONTROL SAS
Lien vers l'organisation	https://www.tanker.io/
Nom commercial du produit	Tanker
Numéro de la version évaluée	Tanker 1.7.2 associé à Submarine 1.1.1 et Botan 1.11.31
Catégories du produit	Identification, authentification et contrôle d'accès. Communication sécurisée. Stockage sécurisé.

2 Description du produit

2.1 Description générale

Tanker est un logiciel de chiffrement conçu et développé par KONTROL SAS permettant à un utilisateur de chiffrer le contenu d'un fournisseur de stockage en ligne de type Dropbox.

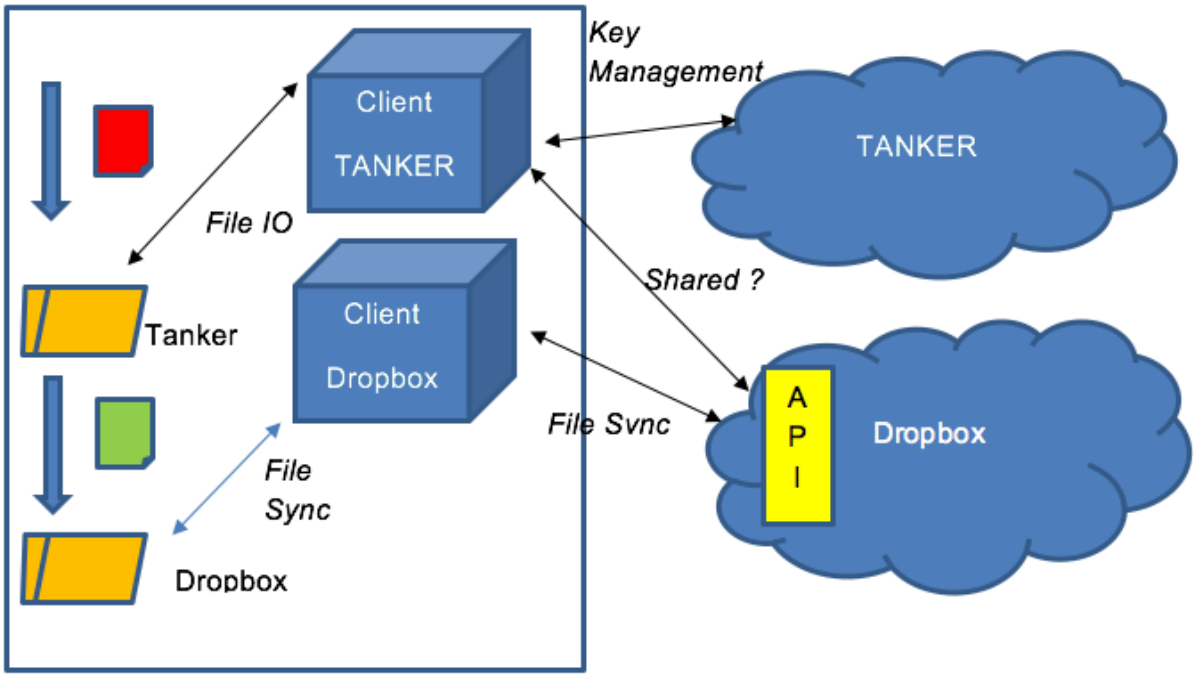
Le chiffrement se fait directement depuis la machine utilisateur (« end-to-end encryption ») et préserve les fonctionnalités de partage de la solution sous-jacente (Dropbox, One Drive, Google Drive…).

L'utilisateur installe sur son poste de travail Tanker et est invité à créer un compte Tanker lors de sa première utilisation et y raccorder son fournisseur de « Cloud » (ex. « Dropbox connect »). Lors de cette opération le compte Tanker est enregistré auprès de nos serveurs et l'association avec la clef publique effectuée.

Tanker travaille en combinaison avec le logiciel sous-jacent et monte un lecteur virtuel permettant de consulter et éditer les données chiffrées de façon transparente.

Les documents édités dans le « lecteur Tanker » sont chiffrés à la volée puis déposés dans le répertoire de la solution sous-jacente qui se charge de la synchronisation vers le Cloud distant.

Les fonctionnalités de partage sont maintenues grâce à l'utilisation de l'API de la solution sous-jacente en combinaison avec la base de profils Tanker associés aux comptes Cloud connectés.



2.2 Principe de fonctionnement

2.2.1 Aspects cryptographiques

Le client Tanker se comporte comme un logiciel de chiffrement de fichiers, de type PGP.

L'utilisateur possède deux bi-clefs, l'une servant à chiffrer (confidentialité) et la seconde à signer (intégrité, authenticité). Ces clefs sont générées localement, lors de la création du compte utilisateur.

L'infrastructure de Tanker se charge de stocker et distribuer les deux clefs publiques de chaque utilisateur, permettant ainsi :

- De chiffrer un document à destination d'un autre utilisateur (clef publique de chiffrement)
- De s'assurer que le document reçu est intègre et authentique (clef publique de signature)

Le schéma de chiffrement utilisé est classique et proche de celui utilisé par PGP :

- Chiffrement des données via un algorithme symétrique performant (AES)
- Chiffrement de la clef symétrique par les clefs publiques des personnes ayant accès (ECIES)
- Signature du message chiffré (ECDSA)

2.2.2 Installation

Le client Tanker est une application à télécharger depuis notre site internet et à installer directement sur le poste de travail de l'utilisateur. L'installation de Tanker peut se faire sans droits administrateurs sous macOS, Linux et optionnellement sous Windows[1].

2.2.3 Création de compte

Lors de la création d'un compte Tanker, l'utilisateur est muni d'un code d'enregistrement reçu par email permettant de valider l'accès à la boîte mail en question.

Deux bi-clefs publique/privée de chiffrement et signature sont alors générées localement par le client Tanker puis l'utilisateur est invité à se connecter à son fournisseur de Cloud.

Le compte Tanker est ensuite enregistré auprès de notre infrastructure, pour cela le client Tanker fourni au serveur :

- Le profil Tanker (UserId, nom, prénom, société, email)
- La clef publique de chiffrement générée
- La clef publique de signature générée
- L'identifiant du compte de Cloud connecté

L'infrastructure de Tanker maintient à jour un annuaire des comptes Tanker, des clefs publiques (signature et chiffrement) et des identifiants de Cloud associés.

2.2.4 Session

L'utilisateur se connecte sur le client Tanker via un mot de passe défini lors de la création du compte permettant de débloquer la clef privée stockée localement.

[1] Les droits administrateurs permettent l'affichage d'icônes et sont optionnels.

Le client Tanker démarre un serveur WebDAV local (127.0.0.1) et y connecte un lecteur réseau.

Lors de l'accès (via l'Explorateur Windows, Finder, ...) à ce lecteur le contenu du répertoire Cloud sous-jacent est affiché.

Lors de l'ouverture d'un document, le client Tanker récupère le fichier correspondant chiffré dans le dossier Cloud, le déchiffre localement et le renvoie via l'API WebDAV.

De la même manière, lors de l'écriture d'un fichier, l'API WebDAV permet de récupérer le contenu du fichier. Celui-ci est chiffré localement, signé puis déposé dans le répertoire Cloud.

L'émulation d'un serveur WebDAV permet au client Tanker d'intercepter les IO disque effectuées sur le lecteur réseau afin de chiffrer/déchiffrer les documents stockés sur la solution de Cloud directement depuis la machine utilisateur.

Note : Le client Tanker travaille en combinaison avec le client Cloud d'origine (client Dropbox, One Drive…) et n'effectue donc pas d'opérations de synchronisation.

2.2.5 Partage

Lors du chiffrement d'un fichier, le client Tanker interroge l'API de la solution de Cloud afin de déterminer si le document se situe dans un dossier partagé.

Le cas échéant, la liste des identifiants Cloud ayant accès à la ressource sont récupérés et les profils correspondants récupérés dans l'annuaire du serveur Tanker distant.

Les clefs publiques de chiffrement des personnes autorisées sont utilisées afin de permettre l'accès au document chiffré. L'infrastructure Tanker permet l'échange des clefs de chiffrement et leur révocation[2].

Les clefs publiques de signature récupérées sont elles utilisées pour vérifier l'authenticité des documents dans un scénario de partage.

2.3 Description des dépendances

Le client Tanker s'appuie uniquement sur un client de Cloud tierce installé et configuré au préalable par l'utilisateur.

Dans le cadre de cette CSPN le client Dropbox pour Windows sera utilisé.

[2] Clef de document symétrique surchiffrée par les clefs publiques des utilisateurs ayant accès

2.4 Description de l'environnement technique de fonctionnement

2.4.1 Poste client

Le client Tanker fonctionne sous les systèmes d'exploitation suivants :

- Windows 7 et versions ultérieures
- Linux (64 bits) et versions ultérieures
- Mac OS X 10.10 et versions ultérieures

Dans le cadre de cette CSPN, la cible de l'évaluation se restreint à « Windows 10 64 bits ».

Le poste client doit respecter les contraintes suivantes :

- Le système d'exploitation principal est sain et correctement mis à jour, en particulier au niveau des correctifs liés à la sécurité.
- Un antivirus est installé et régulièrement mis à jour.
- Le mot de passe du compte Tanker est soigneusement choisi.
- Le système ne contient aucun système de journalisation de frappe au clavier.
- L'utilisateur n'utilise pas un compte administrateur.
- L'utilisateur verrouille sa session lorsqu'il quitte son poste de travail

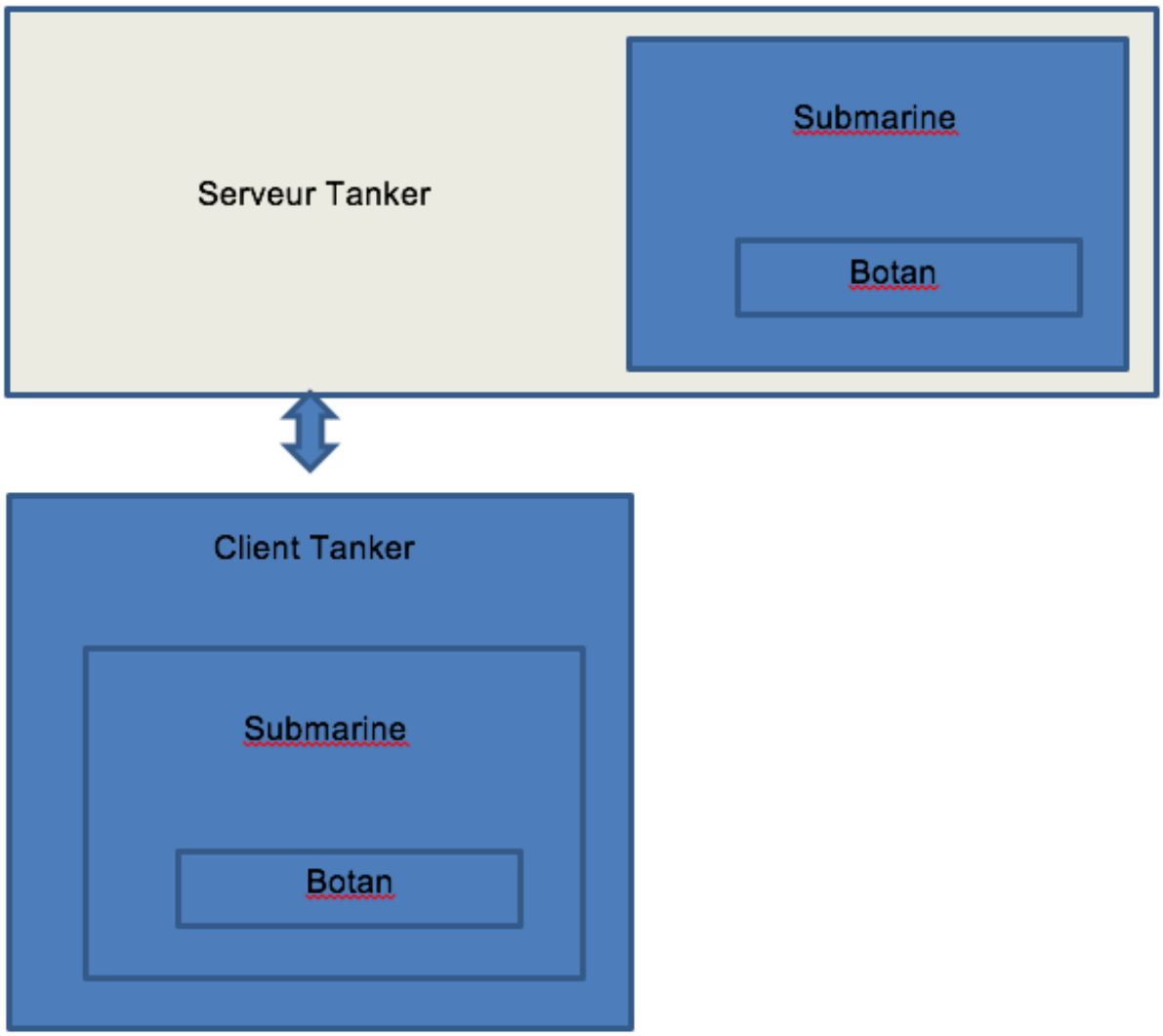
2.4.2 Infrastructure

Le client Tanker s'appuie sur une infrastructure serveur chargée de la gestion des comptes utilisateurs et des clefs (serveurs Tanker).

Dans le cadre de cette CSPN, l'infrastructure de pré-production sera utilisée.

2.5 Périmètre de l'évaluation

La solution Tanker est divisé en plusieurs briques principales : le client, le serveur et la brique cryptographique (gestion des clefs, signature, chiffrement, etc.)



La périmètre d'évaluation comporte :

- l'infrastructure serveur en boite noire, accessible depuis les API serveur Tanker.

- la librairie de chiffrement Submarine basée sur la librairie open source Botan en boite blanche, conformément aux exigences de la CSPN

- le client Tanker dans le cadre d'une utilisation standard (voir ci-dessous)

Le périmètre d'évaluation du client Tanker comporte :

- Les fonctionnalités d'authentification
- Le chiffrement/déchiffrement des données déposées sur le service de stockage
- La protection des données locales lorsque le client Tanker est fermé

Le périmètre d'évaluation ne comporte pas :

- Les API du service de stockage
- Les fonctionnalités et infrastructures propres au service de stockage (client du service/Serveurs du service)
- Le système d'exploitation hôte

3 Problématique de sécurité

3.1 Description des utilisateurs typiques

La solution Tanker s'adresse à des utilisateurs dans un cadre professionnel, sans compétences technique particulière.

Les utilisateurs ont un usage de leur poste de travail principalement centré sur les outils bureautiques et ne sont pas administrateur de leur machine.

3.2 Description des biens sensibles

(I : Intégrité, C : Confidentialité)

Les biens sensibles correspondent aux documents chiffrés déposés dans le dossier local du service de stockage (B1) et par extension sur les infrastructures du service de stockage (B2).

Les clefs de chiffrement utilisées pour chiffrer ces documents sont également considérées comme sensibles :

- B3 : La clef privée de l'utilisateur (I + C)

  Cette clef permet de déchiffrer les clefs surchiffrées des documents de l'utilisateur et ouvrir les conteneurs sécurisés locaux.

- B4 : Le cache de clefs publiques sur la machine (I)

  La falsification d'une clef publique permettrait de chiffrer un document avec la clef de l'attaquant.

- B5 : Les clefs utilisées pour chiffrer les documents (I + C)

  La connaissance d'une clef de chiffrement d'un document permet d'accéder à son contenu.

- B6 : Le mot de passe utilisateur (C)

  La connaissance du mot de passe utilisateur permet d'ouvrir une session Tanker (sous réserve d'avoir accès à la machine utilisateur).

3.3 Description des hypothèses sur l'environnement

On pose comme hypothèse le fait que le poste de travail sur lequel est installé Tanker respecte un minimum de bonnes pratiques en termes de sécurité.

Le mot de passe Tanker ne doit pas être accessible en clair sur la machine (stocké dans un fichier) ni être identique à un mot de passe utilisé pour la session et/ou sur un site internet tierce.

La machine doit disposer d'un antivirus à jour et être exempte de trojan/virus ou keylogger.

Le compte courant d'utilisation ne doit pas être un compte administrateur.

L'utilisateur verrouille sa session lorsqu'il quitte son poste de travail. En cas d'absence prolongée, il ferme Tanker.

3.4 Description des menaces

Dans un contexte professionnel, une entreprise utilisatrice d'un service de stockage distant fait face aux menaces suivantes :

- M1 : Vol d'identifiants du service et accès non-autorisé

  Un attaquant ayant volé les identifiants (login+mot de passe, token oauth) peut se connecter au compte de la victime et accéder aux données (lire, modifier, effacer).

- M2 : Vol de machine utilisateur et accès aux données locales

  Un attaquant ayant volé une machine peut accéder au cache du service de stockage stocké en clair sur la machine.

- M3 : Accès non-légitime a un document chiffré

  Un attaquant accès d'une manière ou d'un autre à un document chiffré déposé sur le service de stockage (intrusion, vol, etc.).

- M4 : Mauvaise gestion des accès par l'entreprise (ex-employé)

  Un utilisateur de l'entreprise peut commettre des erreurs de gestion dans la liste de personnes ayant accès à des dossiers partagés : ajout d'une mauvaise personne, non mise à jour suite au départ d'un employé, etc.

- M5 : Fuite d'un document interne via un lien partagé

Le mécanisme de « lien partagé » permet de donner l'accès à un document situé sur le service de stockage distant avec une traçabilité minime et aucune gestion d'accès (la connaissance du lien web donne l'accès au document).

3.5 Description des fonctions de sécurité du produit

Tanker met en place les fonctions de sécurité suivantes :

- S1 : Stockage local sécurisé

Les données internes du client Tanker (caches de clefs, configuration, etc.) sont stockées chiffrées sur le disque.

- S2 : Par extension, chiffrement sur les serveurs distants du service de stockage

Le client du service de stockage distant synchronise le dossier local contenant les documents chiffrés vers les serveurs distants.

- S3 : Verrouillage local (lors de la fermeture de Tanker)

Lorsque le client Tanker est stoppé, les documents chiffrés sont inaccessibles (à l'inverse du client d).

- S4 : Dashboard de visualisation des « collaborateurs » (partages en dehors de l'entreprise)

L'utilisateur peut facilement visualiser la liste des personnes avec qui il partage des dossiers dans une vue synthétique.

- S5 : Sécurisation de l'infrastructure serveur Tanker

Les serveurs Tanker hébergent la liste des comptes Tanker et les clefs de chiffrement publiques associées. Ces serveurs sont hébergés sut une infrastructure sécurisée.

3.6 Matrices de couvertures

3.6.1 Menaces et biens sensibles

(I : Intégrité, C : Confidentialité)

	B1 Documents locaux	B2 Documents sur serveurs service de stockage	B3 Clef privée de l'utilisateur	B4 Cache de clefs publique	B5 Clef des documents	B6 Mot de passe utilisateur
M1 Vol d'identifiants service de stockage et accès non-autorisé		IC				
M2 Vol de machine utilisateur et accès aux données locales	IC		IC	IC	IC	IC
M3 Accès non-légitime a un document chiffré		IC				
M4 Mauvaise gestion des accès par l'entreprise		IC				
M5 Fuite d'un document interne via un lien partagé		C				

3.6.2 Menaces et fonctions de sécurité

(I : Intégrité, C : Confidentialité)

	S1 Stockage local sécurisé	S2 Chiffrement sur serveurs du service de stockage	S3 Verrouillage local	S4 Dashboard collaborateurs	S5 Sécurisation de l'infrastructure serveur Tanker
M1 Vol d'identifiants service de stockage et accès non-autorisé		IC		I	
M2 Vol de machine utilisateur et accès aux données locales	IC		IC		
M3 Accès non-légitime a un document chiffré	IC	IC			IC
M4 Mauvaise gestion des accès par l'entreprise		IC		I	
M5 Fuite d'un document interne via un lien partagé	C	C	C		C