Cible de Sécurité CSPN

Olvid

— PUBLIC -

Version 2.2

Identification du document

Caractéristiques

Objet	Cible de Sécurité CSPN – Olvid
Nombre de pages	18
Diffusion	PUBLIC

Historique

Version	Date	État
1.0	29/11/2019	Première version
2.0	24/12/2019	Ajout des groupes et corrections mineures
2.1	31/01/2020	Modifications mineures
2.2	05/04/2020	Reformulations suite aux remarques de l'ANSSI et inclusion des sauvegardes

Table des matières

1. Introduction

1.1. Objectif du document

Ce document constitue la cible de sécurité du produit Olvid dans le cadre d'une évaluation CSPN.

1.2. Identification du produit

Nom du produit	Olvid
Version évaluée	IOS 0.8.2
Organisation éditrice	Olvid
Lien vers l'organisation	https://olvid.io/
Nom commercial du produit	Olvid
Catégorie de produit	Communications sécurisées

1.3. Documents de référence

Référence	Description
ANSSI_RGS	RGS Annexe B2 – Gestion des clés cryptographiques

2. Argumentaire (description) du produit

2.1. Description générale du produit

Olvid est un logiciel de messagerie instantanée. *Olvid* permet l'échange sécurisé de messages entre deux contacts. La sécurité des messages est garantie par du chiffrement de bout en bout.

2.1.1. Applications Olvid

Les applications Olvid permettant l'échange de messages sont disponibles sur deux plateformes : iOS et Android. Seule la plateforme iOS est concernée par cette CSPN.

2.1.2. Serveur Olvid

Les applications Olvid communiquent leurs messages au travers d'un serveur. Ce serveur permet uniquement la mise en relation de messages entre les contacts.

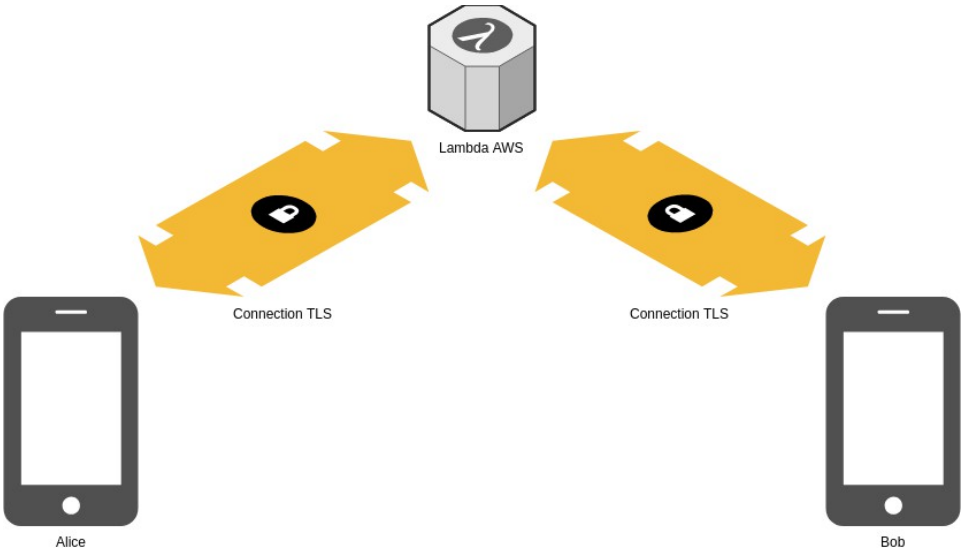

Figure 1: Interaction entre deux utilisateurs Olvid et le serveur

2.2. Description de la manière d'utiliser le produit

Lors de l'installation de l'application Olvid l'utilisateur est amené à se créer une identité. L'application génère ensuite un ensemble de clés asymétrique. Les informations personnelles saisies par l'utilisateur ne sont pas envoyées au serveur, seules les clés publiques le sont.

2.2.1. Ajout d'un contact

Afin de communiquer avec un contact il est nécessaire de l'ajouter dans l'application. Cette étape est réalisée en scannant un QR code (ou en envoyant une invitation par mail, SMS, etc.) permettant de récupérer les clés publiques et le nom du contact. Il est ensuite nécessaire d'échanger deux codes à 4 chiffres. Ces deux derniers codes ont pour vocation d'assurer l'authentification mutuelle. Il est donc nécessaire qu'ils soient échangés via un canal authentique.

On entend par canal authentique un moyen de communication avec lequel on a une garantie sur l'identité de son interlocuteur et la garantie que les messages échangés sont intégres. Ce canal authentique n'a par contre pas besoin d'être confidentiel. Un appel téléphonique, ou un échange de vive voix en face à face sont des exemples de canaux authentiques.

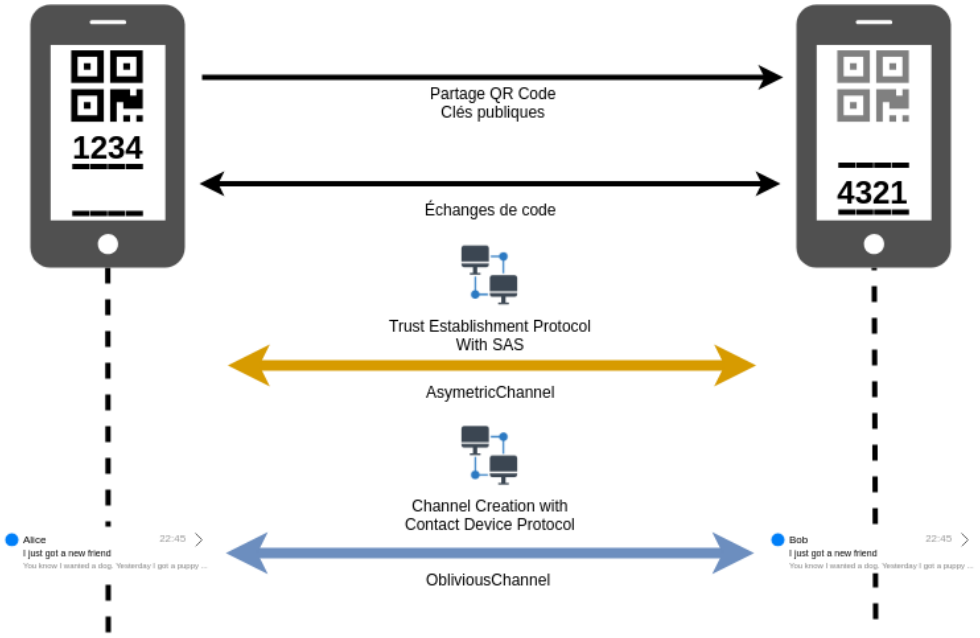

Figure 1: Établissement d'une connexion sécurisée

2.2.2. Envoi d'un message

Il est ensuite possible d'envoyer des messages à ses contacts. Ces messages sont simplement déposés sur le serveur puis récupérés par l'application du contact. Tous les messages échangés sont chiffrés de bout en bout et authentifiés.

2.2.3. Envoi de pièce jointe

Il est possible d'envoyer des pièces jointes en plus des messages textuels. Les pièces jointes sont découpées en morceaux de tailles fixe et déposées sur le serveur Olvid. Les pièces jointes échangées sont chiffrées de bout en bout et authentifiées. Un message envoyé au destinataire contient la liste des URLS des différentes parties des pièces jointe. Ce message, comme tous les messages textuels, est chiffré de bout en bout et authentifié.

2.2.4. Mise en relation par un tiers

Il est possible de mettre en relation deux utilisateurs par le biais d'un utilisateur jouant le rôle de tiers de confiance.

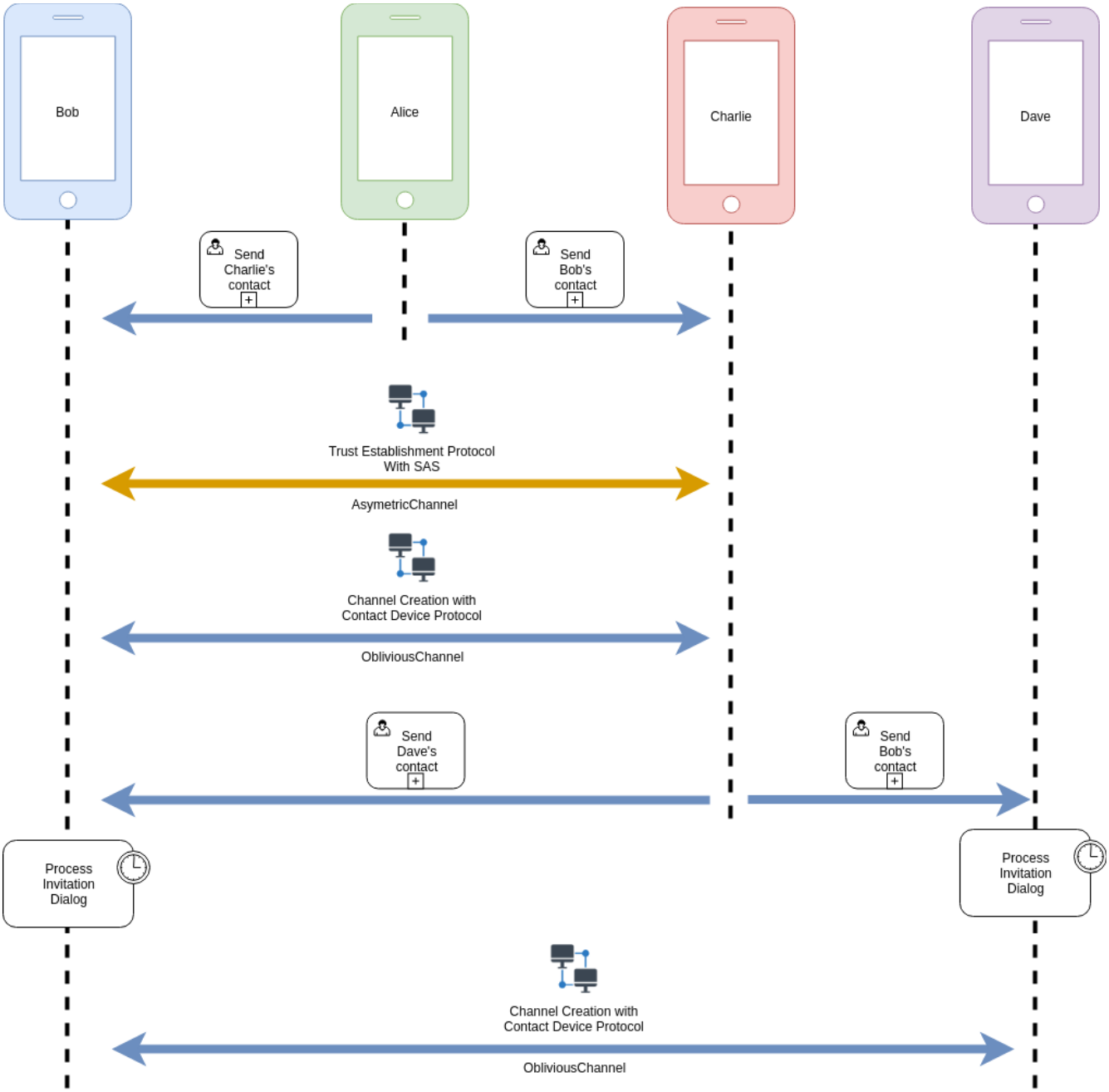

Figure 2: Mise en relation de contacts

Si Alice communique avec Bob, et qu'Alice communique également avec Charlie, alors Alice peut mettre en relation Bob et Charlie. Cette mise en contact s'effectue de manière automatique car Alice et Bob d'une part, Alice et Charlie d'autre part sont des contacts de premiers niveau.

Il est possible pour Charlie, en communication avec Dave, de le mettre en relation avec Bob. Il s'agit alors d'un contact de second niveau entre Dave et Bob, alors une demande de confirmation de l'invitation s'affiche sur les applications de Bob et Dave.

2.2.5. Groupes : création, administration et envoi de messages

Il est également possible de créer des groupes afin d'envoyer des messages à plusieurs destinataires à la fois. Chaque groupe possède un administrateur (celui qui crée le groupe) qui peut inviter de nouveaux membres dans le groupe.

Lors de la création d'un groupe, tous les membres sont automatiquement mis en relation : l'administrateur du groupe joue le rôle de tiers de confiance pour « pousser » à tous les membres la clé publique associée au nom de chacun.

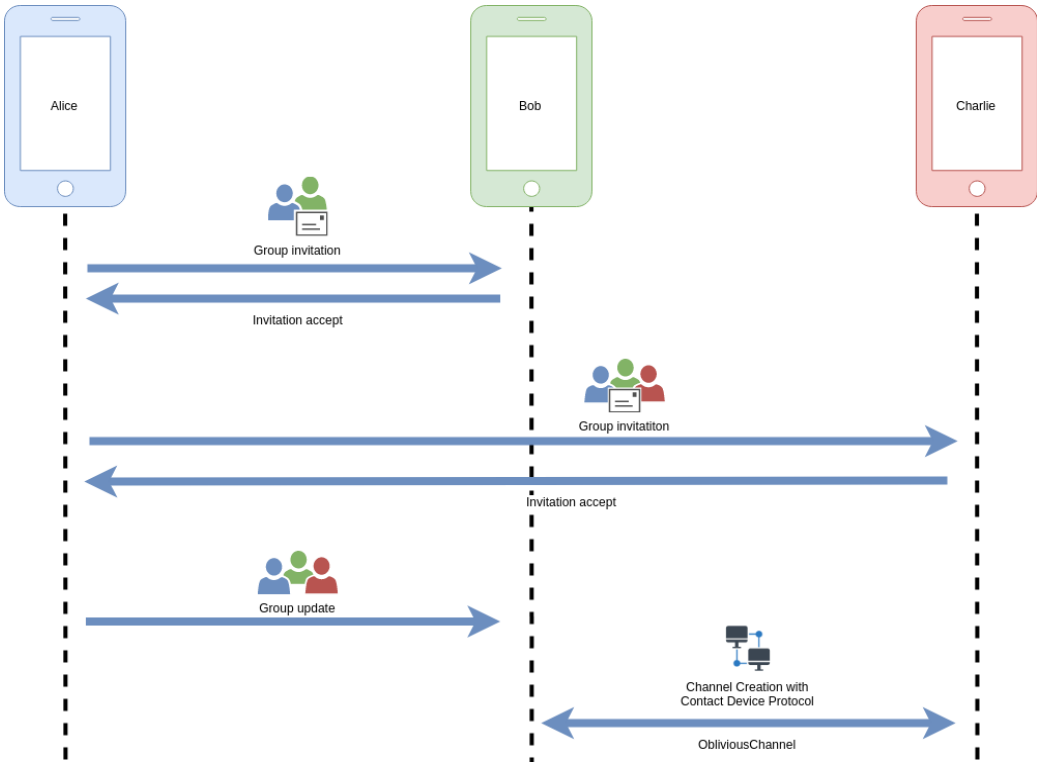

Figure 3: Administration d'un groupe par son administrateur

L'envoi de messages et pièces jointes au sein d'un groupe repose sur le même mécanisme que pour les messages directs. Chaque membre du groupe chiffre et envoie son message pour l'ensemble des membres du groupe.

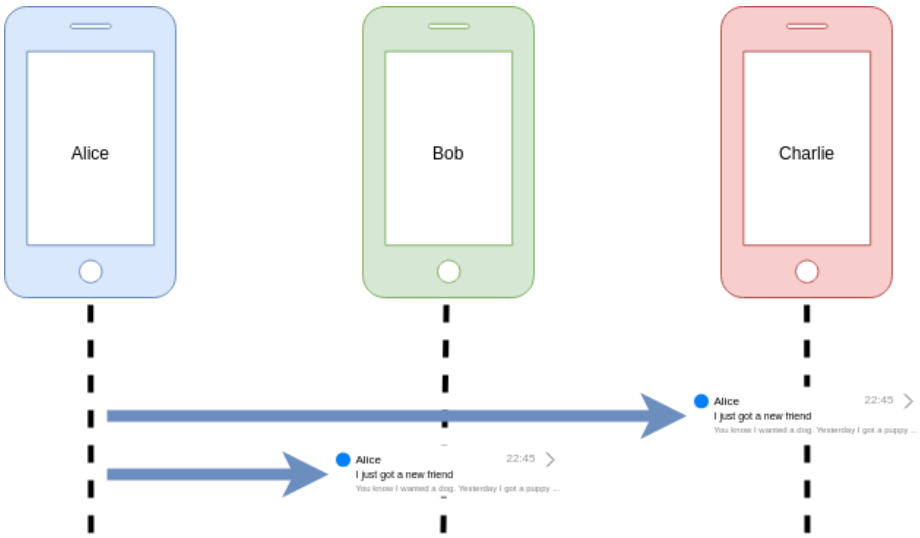

Figure 4: Alice envoi un message au groupe

Il n'est pas possible d'enlever un membre d'un groupe.

2.2.6. Sauvegarde du carnet de contacts Olvid

La construction de son carnet de contacts Olvid impliquant un travail de la part de l'utilisateur, il est proposé d'effectuer des sauvegardes chiffrées de l'ensemble des contacts Olvid. En pratique, cette fonctionnalité de sauvegarde permet d'exporter ses propres clés long terme Olvid (ainsi que les détails qui leurs sont associés, comme le nom choisi au moment de l'installation) ainsi que l'ensemble des clés publiques des contacts (avec les détails qui leurs sont associés, comme le nom du contact ou la source de confiance de ce contact) et l'ensemble des groupes auxquels l'utilisateur appartient.

Avant de pouvoir effectuer une sauvegarde, l'application génère une clé de sauvegarde pour l'utilisateur, qu'il doit copier (par exemple sur un papier). Cette clé de sauvegarde est indispensable à la restauration de la sauvegarde.

Une fois la clé générée, l'utilisateur peut exporter un fichier de sauvegarde chiffré qu'il sera lui même chargé de transférer sur un nouvel appareil pour procéder à la restauration.

2.3. Description de l'environnement prévu pour son utilisation

L'application Olvid s'installe sur des équipements mobiles iOS. Le serveur Olvid est opéré par la société éponyme et est hébergée par la société Amazon.

2.4. Description des hypothèses sur l'environnement

L'application Olvid doit être installée sur un système sain, correctement mis à jour. Les utilisateurs sont considérés comme non hostiles.

Le serveur ne rentre pas dans la cible de sécurité, il est considéré comme non sûr mais effectuant tout de même son rôle du point de vue de la disponibilité.

H1. Installation et Initialisation

- L'application Olvid est installée depuis le store

H2. Utilisateur

- L’application Olvid est utilisée par une personne non hostile.
- L'utilisateur connaît les contacts avec qui il souhaite échanger, et a le moyen de s'appuyer sur un canal authentique (typiquement, un échange de vive voix, en face à face ou par téléphone) pour l'échange des codes à 4 chiffres.
- Les membres actifs d’un groupe sont tous considérés de confiance.

H3. Serveur

- Le serveur est considéré comme non sûr.
- Le serveur assure tout de même la disponibilité des messages.
- La remise de tous les messages est garantie.

2.5. Description des dépendances

L’application est installée sur les systèmes suivants

- iOS :
  - iOS 13

2.6. Description des utilisateurs typiques concernés

Les utilisateurs disposent de privilèges identiques et échangent des messages entre eux. Ils disposent chacun de l’application installée sur un système iOS.

2.7. Définition du périmètre de l’évaluation

L’évaluation porte sur les différentes fonctionnalités de l’application Olvid décrites dans les chapitres 2.1 et 2.2 :

- L’ajout d’un contact ;
- L’envoi de messages et de pièces jointes à un contact ;
- La création de groupe et l'envoi de messages de groupes ;
- Les communications entre l’application et le serveur ;
- La création et la restauration d'une sauvegarde du carnet de contacts ;

La sécurité du serveur Olvid est considéré hors cible. En effet, l’application doit pouvoir fonctionner correctement avec un serveur compromis tant que ce dernier n’empêche pas la disponibilité des messages.

3. Description de l’environnement technique dans lequel le produit doit fonctionner

3.1. Matériel compatible ou dédié

L’application Olvid est installée sur un matériel Apple où est installé le système d’exploitation iOS.

3.2. Système d’exploitation retenu

Le système d’exploitation retenu pour l’évaluation est iOS 13.

4. Description des biens sensibles que le produit doit protéger

Les biens sensibles que Olvid doit protéger selon les critères de Confidentialité – C, Intégrité – I et Disponibilité – D sont les suivants :

Bien	C	I	D
Identité de l'utilisateur	X	X	
Messages échangés	X	X	
Pièces jointes échangées	X	X	

5. Description des menaces

5.1. Agents menaçants

Les agents menaçants sont les suivants :

- les attaquants extérieurs étant capable d'envoyer des messages à destination des utilisateurs de l'application ;
- les attaquants extérieurs, capable d'intercepter et de modifier les flux de communications entre l'application et le serveur ;
- les attaquants disposant d'un accès privilégié au serveur Olvid ;
- les attaquants ayant accès à une sauvegarde du carnet de contacts des utilisateurs ;

Sont considérées comme hors cible toutes les attaques nécessitant un accès physique à l'appareil de l'utilisateur ou s'appuyant sur un malware installé sur cet appareil. Olvid a en effet vocation à protéger les données à partir du moment où elles quittent l'appareil, mais s'appuie uniquement sur les mécanismes d'isolation proposés par iOS pour la protection des données « au repos ».

5.2. Menaces

Note : il est explicitement considéré qu'un attaquant peut prendre le contrôle du serveur. Cette menace est couverte par les cas M1. et M2. (modification et interception de messages).

Les menaces identifiées sont les suivantes :

M1. Modification d'informations sur le réseau

Un attaquant injecte des données dans les communications entre l'application et le serveur et modifie les données échangées (messages applicatifs et protocolaires).

M2. Interception d'informations sur le réseau

Un attaquant intercepte les communications entre l'application et le serveur et récupère des informations sensibles (messages applicatifs et protocolaires).

M3. Usurpation d'identité

Un attaquant se fait passer pour un correspondant légitime.

M4. Récupération d'un fichier de sauvegarde des contacts

Un attaquant récupère un fichier de sauvegarde du carnet de contact d'un utilisateur.

6. Description des fonctions de sécurité du produit

F1. Authentification des utilisateurs

Les utilisateurs Olvid sont identifiés par une clé publique, dénoté par la suite *Identity*.

L'authentification initiale des utilisateurs est réalisé par le protocole suivant :

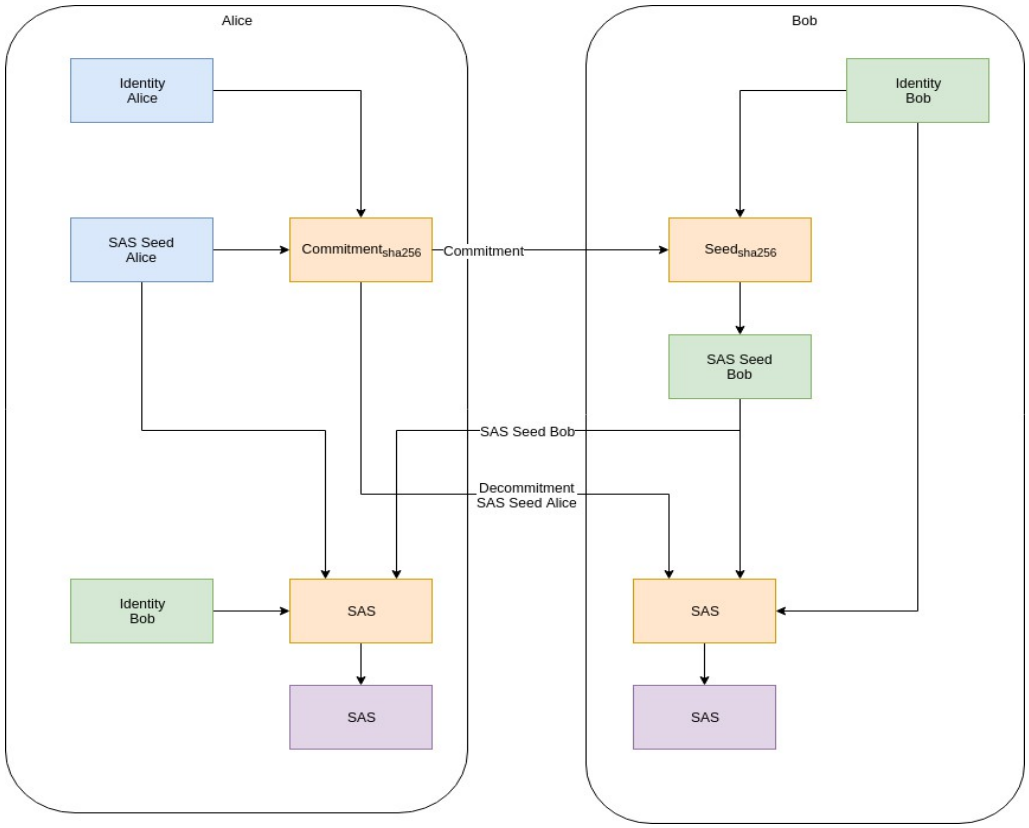

Figure 5: Protocole d'authentification initiale

Les étapes suivantes correspondent à l'authentification mutuelle entre les utilisateurs Alice et Bob.

1. Bob envoie une invitation Ovlid à Alice par un canal externe non sécurisé (SMS, email, WhatsApp, etc.). Cette invitation contient l'identité de Bob.

2. Alice crée une mise en gage basée sur son identité et un aléa appelé *SAS Seed Alice*. Elle envoie la mise en gage à Bob.

3. Bob calcule un HMAC-sha256 de sa propre identité et de la mise en gage reçue. Il envoie ce dernier, appelé *SAS Seed Bob,* à Alice.

4. Alice envoie la valeur de sa mise en gage (identité et aléa) à Bob.

5. Alice et Bob calculent le hash sha256 de l'identité de Bob concaténée au *SAS Seed Alice*. Puis ils XORent le résultat avec le *SAS Seed Bob*.

6. Le résultat du XOR est utilisé comme graine pour initialiser un PRNG qui génère un entier dans l'intervalle [0;100 000 000[permettant de calculer les 8 chiffres du SAS.

Ainsi Alice et Bob obtiennent la même valeur finale (le SAS). Il est alors demandé aux utilisateurs de confirmer que ces deux chaînes sont égales en s'en échangeant, par un canal sain, une moitié chacun sous forme de code à 4 chiffres. Cet échange est présenté dans la Figure 1.

F2. Authentification des échanges

Les messages protocolaires sont échangés via un chiffrement asymétrique. L'algorithme utilisé est ECIES avec les composantes suivantes :

- La courbe elliptique Curve25519 avec le générateur suivant :
  - x :97713840419632025638706794280599358161641879964441831068338940080239109523 47
  - y :46316835694926478169428394003475163141307993866256225615783033603165251855960
- L'algorithme MAC HMAC-SHA256
- L'algorithme de chiffrement AES256 avec le mode CTR
- L'algorithme de dérivation de clé basé sur FIPS 800-90A HMAC DRBG à base de SHA-256

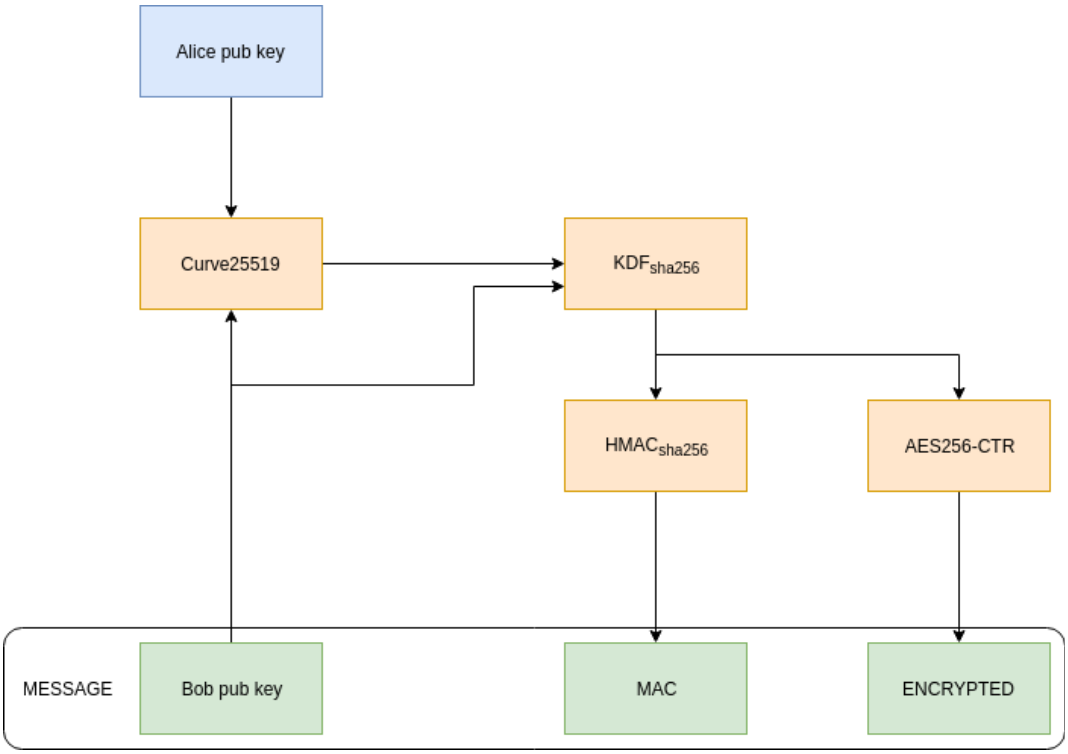

Figure 6: Chiffrement ECIES d'un message de Bob pour Alice

F3. Chiffrement des messages et des pièces jointes

Les messages applicatifs échangés entre deux contacts sont chiffrés de bout en bout. Les messages protocolaires sont, quant à eux, chiffrés en utilisant des algorithmes asymétriques lorsqu'ils transportent des données utilisées pour l'établissement du chiffrement de bout en bout.

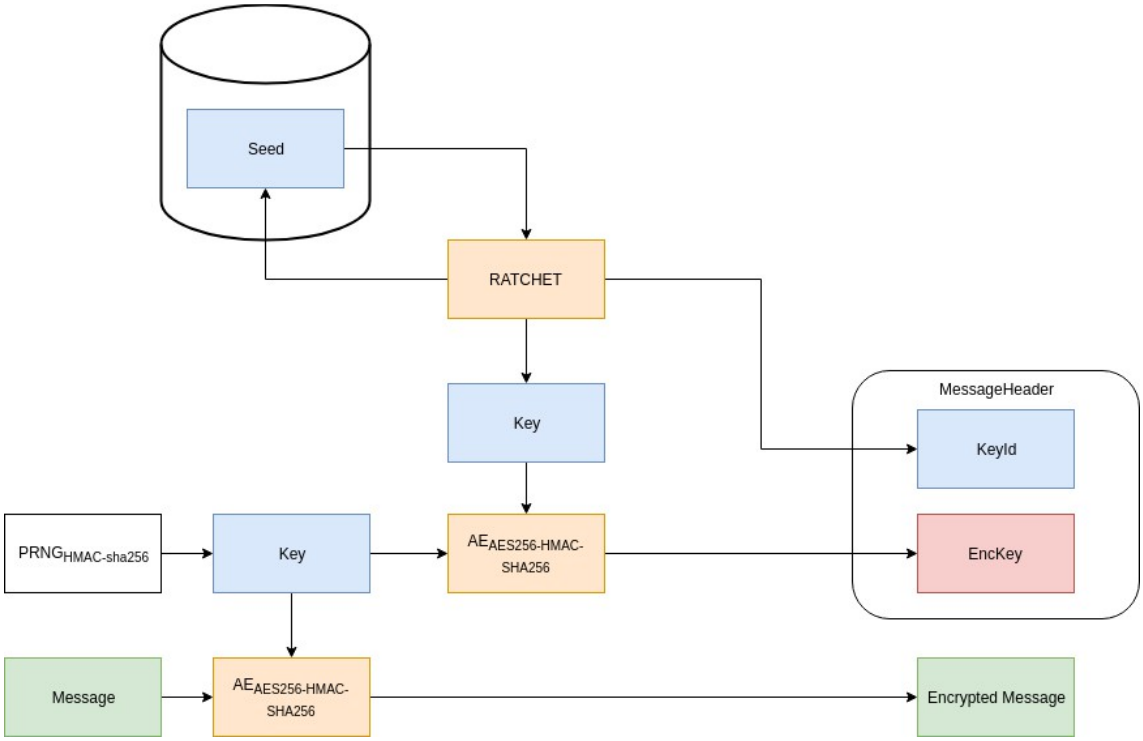

Figure 7: Chiffrement de bout en bout

Les messages applicatifs sont chiffrés en AES256-CTR avec un HMAC-SHA256. La clé utilisée pour chiffrer le message est éphémère. Elle est elle-même chiffré en AES256-CTR avec un HMAC-SHA256. La clé utilisée pour chiffrer la clé de message est quant-à elle générée par un mécanisme de cliquet simple basé sur la fonction de dérivation de clé HMAC-SHA256. Cette clé est à usage unique, une nouvelle étant dérivée pour chaque message.

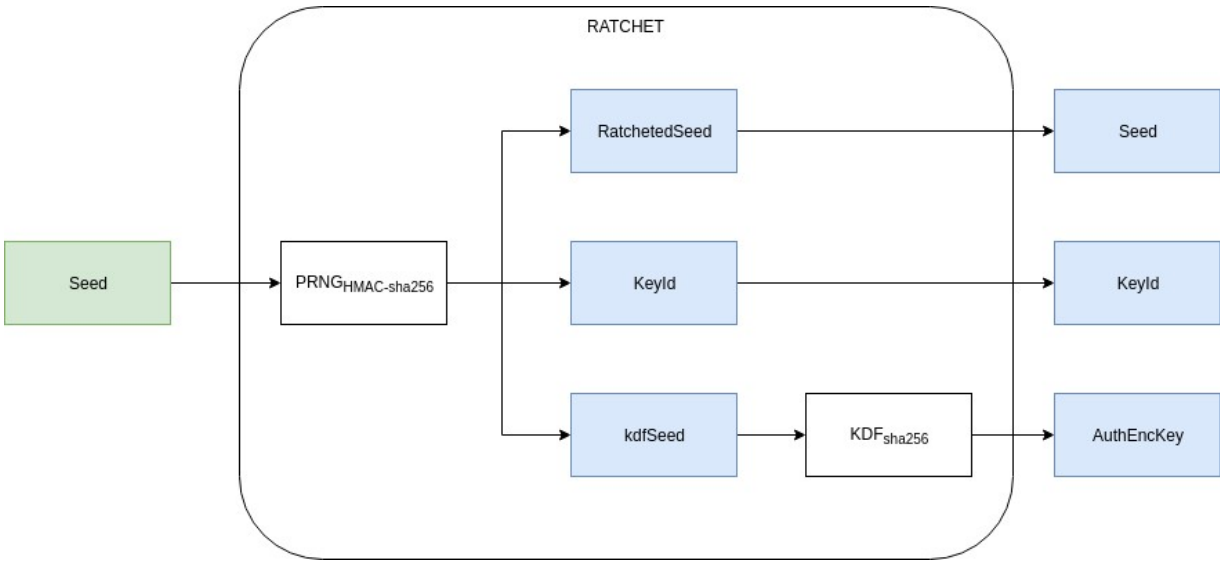

Figure 8: Mécanisme de cliquet

Chaque message applicatif peut être accompagné de pièces jointes. Ces pièces jointes sont chacune chiffrées avec une clé

éphémère AES256-CTR puis HMAC-SHA256. Les clés éphémères des pièces jointes sont ajoutées à la fin du contenu de message applicatif avant son chiffrement. Les pièces jointes sont chiffrées par bloc (typiquement de 2Mo) et les blocs sont déposés sur le serveur indépendamment du message.

F4. Chiffrement des sauvegardes du carnet de contact

Le chiffrement des sauvegardes s'appuie sur une « clé de sauvegarde » composé de 32 caractères (lettres majuscules et chiffres, en excluant les lettres O, I, S et Z) soit une entropie de 160 bits. Cette clé est en fait une graine utilisée pour initialiser un PRNG et lui faire générer :

- un identifiant unique de 32 bytes (pas utilisé à ce jour)
- une paire de clé de chiffrement (ECIES sur Curve 25519)
- une clé de MAC (HMAC SHA256)

Ces éléments, à l'exception de la clé privée de déchiffrement ECIES sont conservés sur le smartphone pour effectuer les sauvegardes. La clé privée ne pourra être reconstruire qu'avec la connaissance de la graine.

Une sauvegarde est un export JSON des éléments pertinents des bases de données d'identité auquel on adjoint un timestamp et un numéro de version du format du JSON utilisé. Ce JSON est ensuite compressé puis chiffré grace à la clé publique ECIES. Un MAC du chiffré est ajouté à la suite de ce dernier.

Il est ensutie proposé à l'utilisateur de sauver le fichier de sauvegarde chiffrée ainsi généré sur son appareil. Le but étant qu'il dépose ce fichier sur un espace de stockage garantissant une bonne disponibilité des données.

Il est important de noter que seuls des éléments à « durée de vie longue » sont sauvegardés. En particulier, aucune clé de canal sécurisé n'est sauvegardée. De nouveaux canaux doivent être reconstruits après une restauration.

7. Couverture des menaces

	M1. Modification d'informations sur le réseau	M2. Interception d'informations sur le réseau	M3. Usurpation d'identité	M4. Récupération d'un fichier de sauvegarde
F1. Authentification des utilisateurs			X	
F2. Authentification des échanges	X			
F3. Chiffrement des messages et des pièces jointes		X		
F4. Chiffrement des sauvegardes du carnet de contact				X