Document de Sécurité et Confidentialité iCanText

Introduction : Principes Fondateurs

iCanText est une plateforme de messagerie conçue avec la confidentialité et la sécurité comme piliers fondateurs. Son objectif est d'atteindre un niveau d'**hyper confidentialité**, défini par les principes suivants :

1. **Souveraineté de l'Utilisateur :** L'utilisateur, et lui seul, contrôle son identité et ses clés cryptographiques. Il n'existe aucune autorité centrale.
2. **Minimisation des Données :** Le système est conçu pour fonctionner en ne collectant et en ne stockant que le strict minimum d'informations nécessaires à son fonctionnement. Aucune donnée personnelle (email, pseudo, numéro de téléphone) n'est requise.
3. **Confidentialité des Contenus :** Les messages échangés sont systématiquement chiffrés de bout-en-bout, les rendant illisibles pour quiconque en dehors de la conversation, y compris les nœuds qui relaient l'information.
4. **Confidentialité des Métadonnées :** Au-delà du contenu, iCanText s'efforce de protéger les métadonnées (qui parle à qui, quand, et à quelle fréquence). C'est un différenciateur clé par rapport aux messageries traditionnelles.

Ce document détaille les mécanismes architecturaux et cryptographiques mis en œuvre pour atteindre ces objectifs.

Chapitre 1 : Identité Souveraine et Gestion des Clés

Le fondement de la sécurité d'iCanText repose sur le principe que chaque utilisateur est le seul gardien de son identité numérique.

1.1. Génération et Propriété des Clés

Toutes les clés cryptographiques sont générées et stockées exclusivement sur l'appareil de l'utilisateur. Elles ne sont jamais transmises à un serveur ou à un autre utilisateur. L'identité d'un utilisateur n'est pas un pseudonyme enregistré dans une base de données, mais est directement et mathématiquement dérivée de sa clé publique de signature. Cela supprime le besoin d'un système de comptes centralisé et ancre l'identité dans une preuve cryptographique non falsifiable.

1.2. Stockage Sécurisé de l'Identité

Pour les utilisateurs souhaitant conserver leur identité entre les sessions, le "keystore" (contenant les paires de clés) est chiffré sur l'appareil à l'aide d'algorithmes robustes. La clé de chiffrement est elle-même dérivée d'un mot de passe choisi par l'utilisateur via une fonction de dérivation de clé à forte complexité (PBKDF2). Ce mécanisme garantit que :

- Le mot de passe n'est jamais stocké ni transmis.
- L'accès physique à l'appareil ne suffit pas pour compromettre les clés sans connaître le mot de passe.
- Les attaques par force brute contre le mot de passe sont rendues extrêmement lentes et coûteuses.

1.3. Identités Éphémères

Pour une confidentialité maximale, iCanText permet la création d'identités "éphémères". Ces identités n'existent qu'en mémoire pour la durée de la session et ne laissent aucune trace sur le stockage de l'appareil. C'est le mode de fonctionnement par défaut, aligné avec le principe de minimisation des données.

1.4. Vérification d'Identité et Toile de Confiance

La confiance dans l'identité d'un correspondant est établie par un mécanisme de "toile de confiance" décentralisée. Chaque paire de clés possède une "empreinte" (fingerprint) unique et vérifiable. Les utilisateurs peuvent comparer ces empreintes via un canal externe sécurisé (par exemple, de vive voix) pour s'assurer qu'ils communiquent avec la bonne personne. Une fois vérifiée, l'application marque l'identité comme "de confiance", offrant une protection robuste contre les attaques d'usurpation d'identité (Man-in-the-Middle).

1.5. Gouvernance par Certificats Cryptographiques

Au-delà de l'identité individuelle, iCanText intègre un système de gouvernance et de contrôle d'accès décentralisé basé sur des certificats numériques. Ces certificats sont des documents signés cryptographiquement qui accordent des permissions spécifiques (comme l'administration d'un canal ou l'accès à l'espace de travail).

- **Chaîne de Confiance :** Toute permission découle d'une chaîne de confiance cryptographique qui remonte jusqu'au "Fondateur" de l'espace de travail. Chaque certificat est signé par une autorité (un administrateur) qui doit elle-même prouver son droit de le faire via son propre certificat.
- **Permissions Auditables :** L'ensemble des certificats forme un registre de permissions vérifiable par tous les membres. Cela rend la gouvernance transparente et empêche toute prise de contrôle illégitime.

Chapitre 2 : Sécurité des Communications

Chaque message et chaque interaction sur le réseau sont protégés par plusieurs couches de sécurité cryptographique.

2.1. Chiffrement de Bout-en-Bout (E2EE)

Les conversations privées entre deux utilisateurs sont protégées par un chiffrement de bout-en-bout. Un secret partagé est dérivé à l'aide des clés de chiffrement respectives

des participants (via l'algorithme ECDH). Ce secret n'est connu que d'eux deux et est utilisé pour chiffrer tous les messages de la conversation. Aucun nœud intermédiaire relayant le message ne peut en déchiffrer le contenu.

2.2. Chiffrement des Canaux de Groupe

Les conversations dans les canaux de groupe sont également chiffrées. Une clé symétrique unique est générée pour chaque canal. Cette clé est distribuée de manière sécurisée (chiffrée individuellement pour chaque membre) uniquement aux participants autorisés.
Pour renforcer la sécurité, le système utilise un mécanisme de ratchet (similaire à Megolm). Chaque message est chiffré avec une clé dérivée de la clé de session principale et d'un compteur qui avance à chaque message. Cela offre une **confidentialité future** : si la clé de session d'un canal est compromise à un instant T, elle ne peut pas être utilisée pour déchiffrer les messages *envoyés précédemment* dans ce canal.

2.3. Authenticité et Intégrité

Chaque message diffusé sur le réseau est numériquement signé par la clé privée de signature de son expéditeur. À la réception, chaque nœud vérifie cette signature. Ce mécanisme garantit deux choses :

- **Authenticité :** Le destinataire est certain de l'identité de l'expéditeur.
- **Intégrité :** Le message n'a pas été altéré ou modifié pendant son transit. Toute modification invaliderait la signature, et le message serait immédiatement rejeté.

Chapitre 3 : Contrôle d'Accès, Confidentialité des Métadonnées et Anonymat

Protéger le contenu ne suffit pas. iCanText intègre des mécanismes avancés pour dissimuler qui parle à qui.

3.1. Absence de Serveur Central

Contrairement aux architectures classiques, iCanText n'utilise pas de serveur central pour gérer les identités, les listes de contacts ou l'historique des messages. Cela élimine le point de défaillance unique et la cible de surveillance la plus évidente. Un serveur de signalisation minimaliste est utilisé uniquement pour la découverte initiale de pairs, mais il n'a aucune connaissance des identités cryptographiques ni du contenu des échanges.

3.2. Routage Scellé ("Onion Routing")

Pour les communications unicast (messages privés, messages système), iCanText utilise une technique de routage scellé. Avant d'envoyer un message, l'expéditeur détermine un chemin à travers le réseau P2P. Le message est ensuite encapsulé dans plusieurs couches de chiffrement, comme les pelures d'un oignon.

- Chaque nœud intermédiaire sur le chemin ne peut déchiffrer que sa propre couche.
- Cette couche lui révèle uniquement l'identité du nœud précédent et du nœud suivant.
- Aucun intermédiaire ne connaît simultanément l'expéditeur d'origine et le destinataire final.
  Ce mécanisme empêche l'analyse du trafic par les pairs qui relaient les messages, protégeant ainsi les métadonnées de la communication.

3.3. Diffusion par Inondation Contrôlée (Flooding)
Pour les messages publics ou les annonces réseau (comme les élections), le système utilise une diffusion par inondation. Pour éviter la saturation, chaque message possède une durée de vie (TTL) qui est décrémentée à chaque saut. De plus, chaque nœud maintient un cache des messages récents pour ne pas retraiter ou relayer un message qu'il a déjà vu, brisant ainsi les boucles de diffusion.

3.4. Réseau Dynamique et Résilient par Conception
La robustesse d'iCanText ne repose pas sur des serveurs infaillibles, mais sur la résilience collective de ses utilisateurs. Le réseau P2P est conçu pour être en constante évolution :

- **Auto-réparation :** Si un nœud se déconnecte, les autres participants recalculent dynamiquement les meilleures routes pour contourner la panne. Le réseau se "guérit" lui-même pour maintenir la connectivité sans aucune intervention, garantissant la continuité du service.
- **Persistance Distribuée :** L'historique des conversations n'est pas stocké centralement, mais est répliqué entre les appareils des participants. Tant qu'au moins un membre d'un canal reste en ligne, les données de ce canal persistent et restent accessibles, évitant toute perte de données due à une panne unique.

3.5. Contrôle d'Accès à l'Espace de Travail

Pour empêcher des participants non désirés de rejoindre un réseau privé, iCanText implémente plusieurs modes de contrôle d'accès stricts, définis par les administrateurs de l'espace de travail :

- **Accès par Mot de Passe :** L'accès peut être restreint par un mot de passe partagé. Lors d'une tentative de connexion, le réseau lance un défi cryptographique au nouvel arrivant, qui doit prouver sa connaissance du mot de passe sans jamais le transmettre en clair. Le mot de passe est combiné à un "sel" aléatoire et haché, rendant les attaques par écoute ou par rejeu inefficaces.
- **Accès sur Invitation Uniquement :** Pour une sécurité maximale, l'accès peut être limité aux seules personnes disposant d'un certificat d'invitation à usage unique. Ce certificat est un "jeton" cryptographique émis et signé par

un administrateur. Il ne peut être utilisé qu'une seule fois, garantissant que seuls les individus explicitement invités peuvent rejoindre le réseau.

Chapitre 4 : Analyse des Menaces et Stratégies de Mitigation

Voici une liste non exhaustive des risques et attaques possibles, ainsi que les stratégies de défense mises en œuvre par iCanText.

Menace / Attaque	Description	Mitigation dans iCanText
Usurpation d'Identité / Man-in-the-Middle (MitM)	Un attaquant se fait passer pour un autre utilisateur pour intercepter ou altérer les communications.	**Chiffrement E2EE et Signatures :** Le contenu est illisible. **Vérification d'empreintes :** La comparaison hors-bande des empreintes cryptographiques permet de garantir l'identité du correspondant, rendant le MitM détectable.
Attaque Sybil	Un attaquant crée un grand nombre de fausses identités pour obtenir une influence disproportionnée sur le réseau.	**Coût de l'Identité :** Bien que facile à créer, une identité Sybil n'a aucune confiance ni autorité. **Gouvernance Décentralisée :** Les élections de portiers sont basées sur un score (stabilité, connectivité), rendant coûteux pour un attaquant de faire élire ses nœuds. **Système de Permissions :** Les identités Sybil n'ont aucun droit sans un certificat émis par un administrateur de confiance.
Attaque par Éclipse	Un attaquant isole un nœud du reste du réseau en contrôlant tous ses voisins directs, lui fournissant une fausse vision de la topologie.	**Diversification des Voisins :** Les mécanismes de réparation de topologie et de recherche de raccourcis encouragent la connexion à des pairs variés, rendant l'isolement complet plus difficile. Le nombre de voisins est activement géré.
Écoute et Analyse de Trafic	Un observateur (externe ou un pair malveillant) analyse les flux de données pour déduire qui communique avec qui.	**Routage Scellé :** Dissimule l'origine et la destination finale des messages privés aux nœuds intermédiaires. **Chiffrement de Canal :** Tous les messages de groupe sont chiffrés, rendant leur contenu opaque.
Attaque par Rejeu (Replay Attack)	Un attaquant intercepte un message valide et le renvoie ultérieurement pour perturber le système.	**ID de Message Uniques :** Chaque message possède un ID unique contenant un timestamp. Les nœuds maintiennent un cache des ID récents et rejettent systématiquement tout message déjà vu.
Déni de Service (DDoS) / Inondation	Un attaquant sature le réseau ou un nœud spécifique avec un grand volume de messages	**Décentralisation :** L'absence de serveur central rend une attaque DDoS classique inefficace. **TTL (Time-To-Live) :** Limite la portée de la

	inutiles.	diffusion des messages. **Blocage par les Pairs :** Les utilisateurs peuvent bloquer les nœuds malveillants, les isolant du réseau.
Attaques sur le Routage	Un pair malveillant annonce de fausses routes (par exemple, un chemin très court vers tout le monde) pour attirer le trafic.	**Poison Reverse & Hystérésis :** Des techniques classiques de stabilisation des protocoles de routage sont utilisées pour prévenir les boucles et les oscillations rapides. La confiance dans les routes est pondérée par la latence mesurée, rendant les fausses annonces détectables.
Attaques sur la Gouvernance	Un attaquant tente de manipuler l'élection des "Portiers" (nœuds de confiance) pour prendre le contrôle des points d'entrée du réseau.	**Élection Déterministe Basée sur le Mérite :** Les élections ne sont pas basées sur un vote simple, mais sur un score de performance (stabilité, connectivité, ressources). L'algorithme est public et déterministe, rendant difficile pour un attaquant de truquer le résultat sans contribuer positivement et durablement au réseau.
Partitionnement du Réseau (Split-Brain)	Des sous-groupes de nœuds perdent la connexion entre eux et chacun croit être le seul réseau valide, créant des "univers parallèles" incohérents.	**Anti-Split-Brain au Démarrage :** Lors de la création d'un nouvel espace de travail, un mécanisme de départage déterministe (basé sur l'ID cryptographique) est utilisé. Si plusieurs utilisateurs tentent de créer le même espace simultanément, un seul "fondateur" est élu, empêchant la fragmentation dès l'origine.
Accès Non Autorisé au Réseau	Un individu malveillant tente de rejoindre un espace de travail privé pour espionner ou perturber les conversations.	**Contrôles d'Accès Stricts :** Les administrateurs peuvent configurer l'espace pour exiger soit un mot de passe (vérifié via un protocole de défi-réponse sécurisé), soit un certificat d'invitation cryptographique à usage unique, bloquant ainsi tout accès non sollicité.

Chapitre 5 : Périmètre et Limites de la Confidentialité

L'objectif d'hyper confidentialité est ambitieux. Il est important de définir clairement ce qui est protégé et ce qui constitue une limite ou un compromis inhérent à l'architecture.

Ce qui EST Protégé :

- **Le contenu de toutes les communications** (privées et de groupe).
- **L'identité de l'expéditeur et du destinataire** vis-à-vis des nœuds intermédiaires (grâce au routage scellé).
- **La liste de vos contacts et des canaux auxquels vous appartenez** vis-à-vis d'un observateur externe.
- **Votre identité à long terme**, qui n'est liée à aucune information personnelle.

- **Absence de Traces Locales (par défaut) :** L'application fonctionne sans installation. En mode éphémère (par défaut), l'identité et les messages n'existent qu'en mémoire. À la fermeture de la page, tout disparaît sans laisser de trace dans le cache du navigateur ou sur le disque dur.

Limites et Compromis :

- **Visibilité de l'Adresse IP :** Comme dans la plupart des réseaux P2P qui n'utilisent pas une couche d'anonymisation de type Tor, votre adresse IP est visible par les **voisins directs** auxquels vous êtes connecté. C'est un compromis nécessaire pour établir une connexion directe.
- **Analyse de Trafic par un Adversaire Global :** Un adversaire disposant de capacités de surveillance à l'échelle d'Internet (par exemple, un fournisseur d'accès à Internet ou une agence gouvernementale) pourrait potentiellement corréler les timings et les volumes de trafic pour tenter de déduire des schémas de communication, même si le contenu et les métadonnées intra-réseau sont protégés.
- **Sécurité de l'Appareil :** iCanText protège les données en transit et au repos, mais ne peut pas se protéger contre un appareil (ordinateur ou téléphone) déjà compromis par un logiciel malveillant.

En conclusion, iCanText offre un niveau de confidentialité et de sécurité bien supérieur à celui des applications de messagerie centralisées traditionnelles, en particulier concernant la protection des métadonnées et la souveraineté de l'identité. Les utilisateurs doivent cependant rester conscients des limites inhérentes aux systèmes P2P en matière d'anonymat au niveau de la couche réseau.iCanText optimise la confidentialité au sein du réseau, mais ne peut remplacer un outil d'anonymisation dédié comme Tor pour masquer l'activité réseau elle-même.

Comment iCanText se compare-t-il ?

Une analyse comparative face aux messageries centralisées et décentralisées populaires.

Caractéristique	iCanText	Signal	Tox / Jami	Briar	WhatsApp / Messenger	Telegram
Architecture	P2P (Maillage Partiel Dynamique)	Centralisée	P2P (DHT)	P2P (Réseau d'amis + Tor)	Centralisée	Centralisée

Chiffrement E2EE	✓ Oui (par défaut)	✓ Oui (par défaut)	✓ Oui (par défaut)	✓ Oui (par défaut)	✓ Oui (par défaut)	⚠ Optionnel
Protection des Métadonnées	✓ Élevée (Routage Scellé)	✗ Limitée	⚠ Partielle	✓ Très Élevée (via Tor)	✗ Nulle	✗ Nulle
Anonymat de l'Identité	✓ Total (basée sur clé crypto)	✗ Non (N° tél.)	✓ Élevé	✓ Élevé	✗ Non (N° tél. / Profil)	✗ Non (N° tél.)
Mise à l'échelle (Scalabilité)	✓ Élevée (Routage optimisé)	✓ Très Élevée	⚠ Limitée (DHT)	✗ Faible (petits groupes)	✓ Très Élevée	✓ Très Élevée
Stockage des Messages	✓ En mémoire (par défaut)	⚠ Sur appareil	⚠ Sur appareil	⚠ Sur appareil	⚠ Sur appareil + Cloud (backup)	✗ Sur serveur (par défaut)
Fonctionnement sans Internet	✗ Non	✗ Non	✗ Non	✓ Oui (offline)	✗ Non	✗ Non
Aucune Installation Requise	✓ Oui (Web App)	✗ Non (App)	✗ Non (App)	✗ Non (App)	✗ Non (App)	✗ Non (App)
Résilience aux Pannes Réseau	✓ Très Élevée (auto-réparation)	✗ Nulle (point central)	⚠ Moyenne	✓ Très Élevée	✗ Nulle (point central)	✗ Nulle (point central)
Contrôle d'Accès Avancé	✓ Oui (Mots de passe, Invitations)	⚠ Groupes privés simples	✗ Non	✗ Non (basé sur contact direct)	⚠ Groupes privés simples	⚠ Groupes privés/publics