

Aionda Mail Security Whitepaper

Zero-Knowledge · Post-Quantum · Made in Germany

Version 1.5 — July 2026

Aionda GmbH
Stuttgart, Germany

contact-46epp9ba@contact.aionda.com
<https://mail.aionda.com>

PUBLIC DOCUMENT

Contents

1. Resume executif	3
2. Modele de menace	3
3. Vue d'ensemble de l'architecture	5
4. Authentification Zero-Knowledge (OPAQUE)	6
5. Cle maitre du coffre-fort & Shamir Secret Sharing	7
6. KEM hybride post-quantique	8
7. Pipeline de chiffrement des e-mails	10
8. Couche de transport API chiffrée	12
9. Cryptographie du partage de dossiers	13
10. Vault Drive — Stockage de documents chiffré	15
11. Aionda Chat — Messagerie E2EE post-quantique	21
12. Appels video Aionda — visioconference E2EE post-quantique	27
13. Taches Aionda - Gestion de taches chiffrée de bout en bout	31
14. Protections contre les canaux auxiliaires	34
15. Gestion et cycle de vie des clés	35
16. Mecanisme de recuperation	36
17. Authentification sans mot de passe (Passkeys)	37
18. Guardian : protection MITM & signature des reponses	38
19. Archive e-mail d'entreprise (Blockchain)	41
20. Ce que le serveur voit — et ce qu'il ne voit pas	45
21. Reference des algorithmes	47
22. Comparaison avec d'autres fournisseurs	48
23. Limites & transparence	49
24. Feuille de route	51
Historique du document	51
Contact	52

1. Resume executif

Aionda Mail est un service de messagerie chiffre Zero-Knowledge et post-quantique, opere par Aionda GmbH a Stuttgart, en Allemagne. Le service combine des adresses e-mail jetables (DEAs) avec une boite aux lettres entierement chiffree — une combinaison qu'aucun autre fournisseur ne propose.

Proprietes de securite fondamentales :

- **Architecture Zero-Knowledge** : Tout le chiffrement et le dechiffrement s'effectue exclusivement dans le navigateur de l'utilisateur. Le serveur n'a jamais acces au contenu des e-mails dans la boite aux lettres securisee, aux mots de passe ou aux cle de chiffrement.
- **Securite post-quantique** : Le mecanisme hybride d'encapsulation de cle (X25519 + ML-KEM-1024) protege toutes les donnees contre les attaques des ordinateurs classiques et quantiques.
- **Authentification Zero-Knowledge** : Le protocole OPAQUE (RFC 9807) garantit que les mots de passe ne sont jamais transmis ni stockes sur le serveur — meme pas sous forme de hachages.
- **Shamir Secret Sharing (2-of-3)** : La cle maitre du coffre-fort est divisee en trois parts protegees par le mot de passe, la passkey et la cle de recuperation. Deux parts quelconques suffisent a reconstruire la cle maitre.
- **Perfect Forward Secrecy** : Chaque requete API utilise une paire de cle cryptographiques unique et a usage unique. La compromission d'une requete n'affecte aucune autre.
- **Protection MITM (Guardian)** : L'extension de navigateur verifie independamment toutes les reponses du serveur via des signatures Ed25519 et detecte les attaques de type « homme du milieu » grace a la verification des certificats TLS — meme face aux proxys d'entreprise et aux CDN compromis.
- **Archive e-mail conforme GoBD** : Les comptes d'entreprise beneficient d'une chaine de hachage inviolable (blockchain SHA3-256) avec contenu chiffre de bout en bout (Hybrid KEM), une piste d'audit complete, une mise en suspens juridique et une retention configurable — conforme aux reglementations allemandes GoBD.
- **Pas de recuperation de mot de passe** : En cas de perte du mot de passe et de toutes les methodes de recuperation, les donnees sont irrecoverables. C'est un choix de conception — cela prouve que le serveur ne peut pas acceder aux donnees.

Juridiction : Droit allemand (RGPD/DSGVO), aucun partage de donnees avec des services de renseignement etrangers.

2. Modele de menace

2.1 Contre quoi Aionda Mail protege

Menace	Protection
Compromission du serveur (fuite de base de donnees, acces interne)	Tout le contenu des e-mails est chiffre avec des cle que le serveur ne possede jamais
Ecoute reseau (FAI, Wi-Fi, CDN)	Transport API chiffre de bout en bout via Hybrid KEM

Menace	Protection
Inspection CloudFlare	Les requetes API sont chiffrees avant de quitter le navigateur ; CloudFlare ne voit que du texte chiffre. L'extension Guardian detecte les alterations de reponses via des signatures Ed25519
Proxys MITM d'entreprise (ZScaler, Fortinet, etc.)	L'extension Guardian detecte les certificats de proxy via une liste de blocage des emetteurs (Firefox)
Attaques par ordinateur quantique (« recolter maintenant, dechiffrer plus tard »)	ML-KEM-1024 (NIST FIPS 203) offre une resistance post-quantique
Vol de base de donnees de mots de passe	OPAQUE ne stocke que des enregistrements cryptographiques, pas de hachages de mots de passe
Attaques hors ligne par force brute sur les mots de passe	OPAQUE empeche les attaques hors ligne ; la limitation de debit cote serveur empeche les attaques en ligne
Analyse de la taille des e-mails	Le Bucket Padding masque les tailles reelles des e-mails
Canaux auxiliaires de compression (CRIME/BREACH)	Le Bucket Padding est applique apres la compression
Enumeration d'utilisateurs	Reponses factices deterministes pour les comptes inexistants

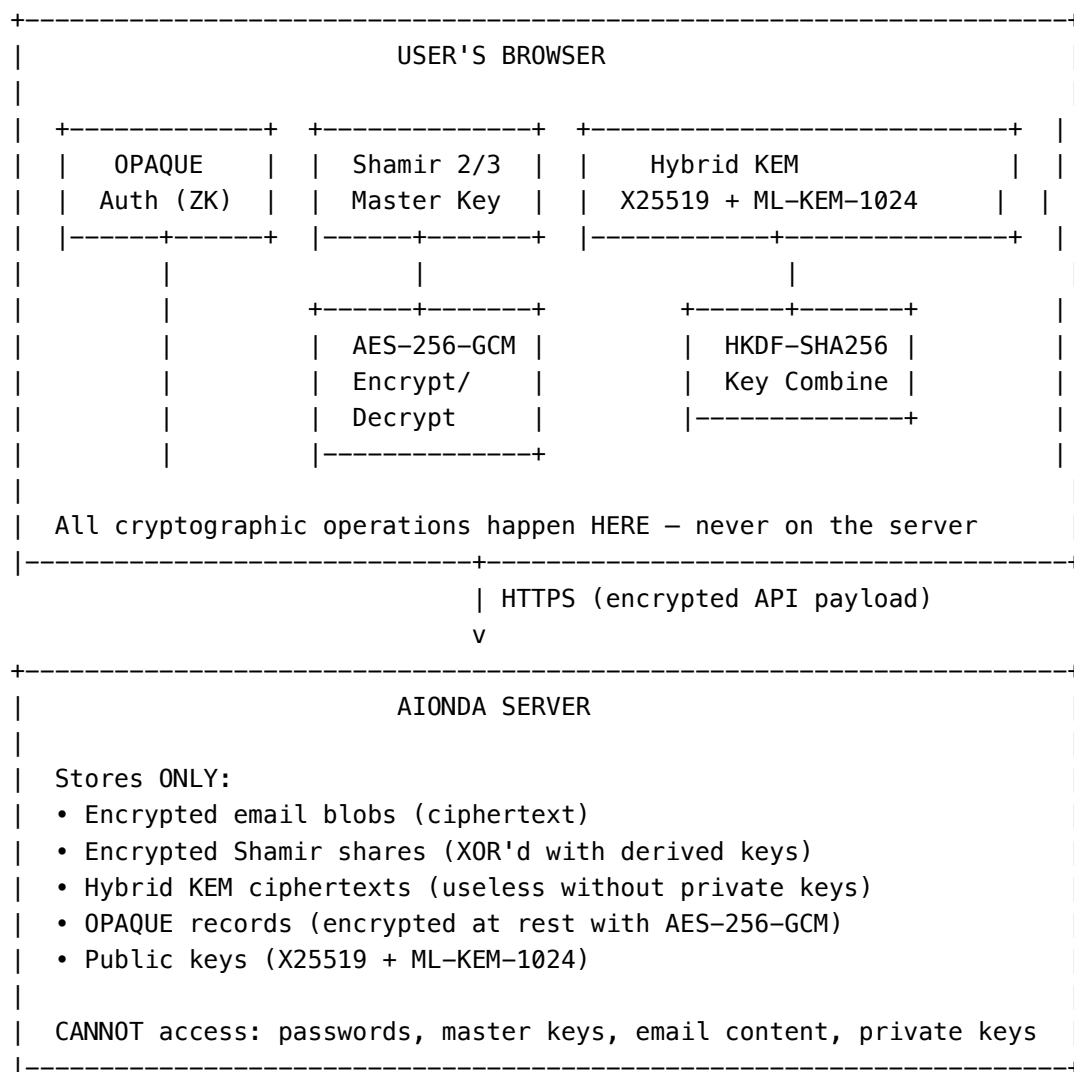
2.2 Contre quoi Aionda Mail ne protege PAS

Limitation	Explication
Appareil compromis	Si un logiciel malveillant controle le navigateur, il peut lire le contenu dechiffre
Metadonnees vers des destinataires externes	Les e-mails vers Gmail/Outlook circulent en clair apres avoir quitte les serveurs d'Aionda (sauf si PGP est utilise)
Metadonnees des e-mails sur les serveurs	Les horodatages, les adresses IP et les tailles des e-mails chiffres sont visibles par le serveur
Confiance dans la livraison web	Le navigateur telecharge du JavaScript depuis les serveurs d'Aionda a chaque visite (voir la section 18 pour les mesures d'attenuation)
Cryptanalyse sous contrainte physique	Aucun systeme cryptographique ne protege contre la coercion physique

2.3 Principe de conception

Aionda Mail suit le modele du « **serveur honnete** » : le systeme est concu de sorte que meme un serveur totalement compromis — ou un operateur malveillant — ne puisse dechiffrer les donnees des utilisateurs. La securite ne repose pas sur la confiance envers l'operateur. Elle repose sur les mathematiques.

3. Vue d'ensemble de l'architecture



3.1 Vue d'ensemble des composants

Composant	Objectif	Emplacement
OPAQUE (RFC 9807)	Authentification par mot de passe Zero-Knowledge	Client + Serveur
Shamir Secret Sharing	Protection de la cle maitre du coffre-fort (seuil 2-of-3)	Client uniquement
Hybrid KEM (X25519 + ML-KEM-1024)	Encapsulation de cles post-quantique pour les e-mails	Client + Serveur
AES-256-GCM	Chiffrement symetrique authentifie	Client + Serveur
HKDF-SHA256	Derivation de cles a partir de secrets partages hybrides	Client + Serveur

Composant	Objectif	Emplacement
BIP39	Encodage de la cle de recuperation (mnemonique de 24 mots)	Client uniquement
WebAuthn PRF	Deverrouillage du coffre-fort par passkey	Client uniquement
Bucket Padding	Protection contre les canaux auxiliaires	Client + Serveur

4. Authentification Zero-Knowledge (OPAQUE)

4.1 Pourquoi pas le hachage de mot de passe ?

Les services traditionnels stockent des hachages de mots de passe (bcrypt, Argon2). Bien que meilleure que le texte en clair, cette approche presente des faiblesses fondamentales :

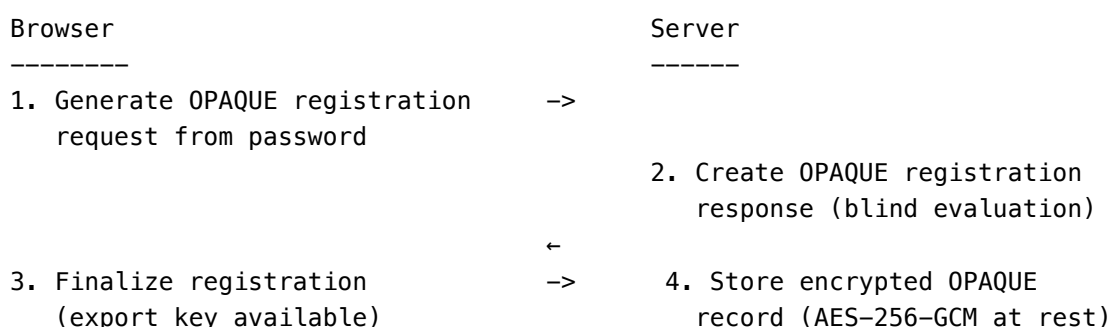
- Le serveur voit le mot de passe lors de la connexion (meme brievement en RAM)
- Les hachages de mots de passe peuvent etre attaques par force brute hors ligne si la base de donnees est volee
- Le serveur pourrait etre modifie pour enregistrer les mots de passe

OPAQUE elimine ces trois problemes. Le mot de passe ne quitte jamais le navigateur — ni en clair, ni sous forme de hachage, sous aucune forme.

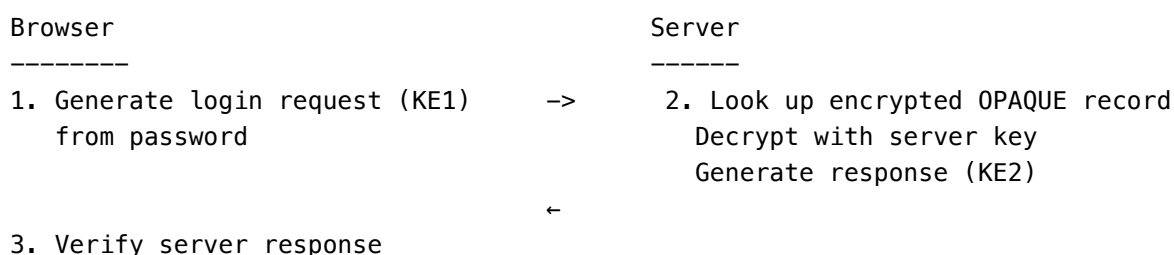
4.2 Fonctionnement d'OPAQUE

OPAQUE (RFC 9807) est un protocole d'echange de cles authentifie par mot de passe asymetrique (aPAKE). Il utilise un mecanisme de defi-reponse cryptographique ou le serveur peut verifier que l'utilisateur connait le bon mot de passe sans jamais apprendre ce qu'il est.

Inscription (une seule fois) :



Connexion (a chaque session) :



Compute session key + KE3	->	4. Verify KE3 (cryptographic proof)
Password verified locally!		If valid: session authenticated
		If invalid: reject (max 3 attempts)

Propriétés essentielles :

- Le mot de passe est vérifié **cote client** à l'étape 3 — le serveur ne le voit jamais
- Le serveur stocke un **enregistrement OPAQUE**, qui n'est pas un hachage de mot de passe et ne peut pas être attaqué par force brute hors ligne
- Les enregistrements OPAQUE sont en outre **chiffres au repos** avec AES-256-GCM à l'aide d'une clef cote serveur
- **Protection contre l'énumération d'utilisateurs** : les comptes inexistants reçoivent des réponses factices déterministes avec un timing identique
- **Limitation de débit** : maximum 3 tentatives d'authentification par session, délai d'expiration de session de 120 secondes

4.3 Implementation

- **Bibliothèque** : @serenity-kit/opaque (basée sur WASM, qualité production)
- **Composant serveur** : microservice dédié aux opérations cryptographiques OPAQUE
- **Format base64** : base64url (compatible URL, sans remplissage) pour la compatibilité du protocole
- **Journalisation d'audit** : tous les événements d'authentification sont journalisés avec horodatages et adresses IP

4.4 Migration SRP

Les comptes existants utilisant SRP-6a sont automatiquement migrés vers OPAQUE lors de la prochaine connexion. Après la migration, le vérificateur SRP est définitivement supprimé. La migration est unidirectionnelle — les comptes ne peuvent pas revenir à SRP.

5. Clef maître du coffre-fort & Shamir Secret Sharing

5.1 Génération de la clef maître

Lorsqu'un utilisateur active la boîte aux lettres chiffrée, une **clef maître de 256 bits (32 octets)** est générée à l'aide du générateur de nombres aléatoires cryptographiquement sûr du navigateur (`crypto.getRandomValues`).

Cette clef maître est la racine de tout le chiffrement. Elle ne quitte jamais le navigateur en clair. Elle n'est stockée nulle part — ni dans le navigateur, ni sur le serveur, sous aucune forme.

5.2 Shamir Secret Sharing (2-of-3)

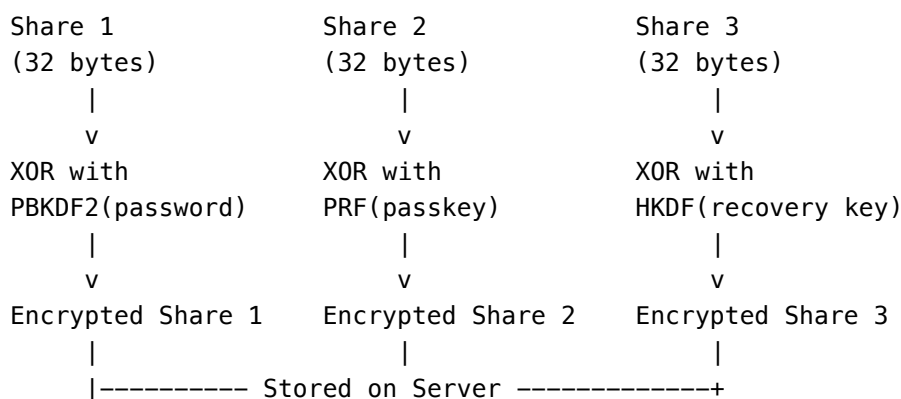
La clef maître est divisée en trois parts à l'aide du schéma **Shamir's Secret Sharing** sur le corps de Galois $GF(2^8)$ avec le polynôme irréductible AES ($x^8 + x^4 + x^3 + x + 1$).

Master Key (32 bytes, generated once)

```

|
|---- Shamir Split (k=2, n=3) ----+
|                                     |
v                                     v

```



Propriete de seuil : deux quelconques des 3 parts suffisent a reconstruire la cle maitre par interpolation de Lagrange. Le serveur ne stocke que les parts chifrees — et ne peut en dechiffrer aucune.

5.3 Protection des parts

Chaque part est combinee par XOR avec une cle derivee d'un facteur d'authentification different :

Part	Proteege par	Derivation de cle
Part 1	Mot de passe	PBKDF2-SHA256, 600 000 iterations, sel aleatoire de 32 octets
Part 2	Passkey (FIDO2)	Extension WebAuthn PRF, liee au materiel
Part 3	Cle de recuperation	HKDF-SHA3-256 avec sel lie au compte

Scenarios de reconstruction :

- **Connexion normale :** Mot de passe (Part 1) + Passkey (Part 2) -> Cle maitre
- **Passkey perdue :** Mot de passe (Part 1) + Cle de recuperation (Part 3) -> Cle maitre
- **Changement de mot de passe :** Passkey (Part 2) + Cle de recuperation (Part 3) -> Cle maitre

5.4 Protection du stockage de session

Meme au sein d'une session de navigateur, la cle maitre n'est jamais stockee en clair :

1. Une cle AES-256 ephemere est generee
2. La cle maitre est chiffee avec cette cle ephemere
3. Seul le blob chiffee est place dans le `sessionStorage`
4. La cle ephemere n'existe qu'en memoire JavaScript (liberee par le ramasse-miettes a la fermeture de l'onglet)

6. KEM hybride post-quantique

6.1 Pourquoi le post-quantique ?

Les ordinateurs quantiques executant l'algorithme de Shor pourraient casser la cryptographie a cle publique classique (RSA, ECDH, X25519) en temps polynomial. Bien que des ordina-

teurs quantiques a grande echelle n'existent pas encore, la menace des attaques « **recolter maintenant, déchiffrer plus tard** » est réelle : des adversaires pourraient stocker des données chiffrées aujourd'hui et les déchiffrer lorsque les ordinateurs quantiques seront disponibles.

6.2 Approche hybride

Aionda Mail utilise un **mecanisme hybride d'encapsulation de cles** combinant :

- **X25519** (Curve25519 ECDH) — securite classique eprouvee, niveau de securite de 128 bits
- **ML-KEM-1024** (NIST FIPS 203, anciennement Kyber-1024) — securite post-quantique, niveau de securite NIST 5

L'approche hybride offre une **defense en profondeur** : la cle combinee est sure tant qu'**au moins un** des deux algorithmes reste incasse.

6.3 Processus d'encapsulation

Sender (encrypting an email):

1. Generate ephemeral X25519 keypair
2. X25519 key agreement with recipient's public key
-> x25519SharedSecret (32 bytes)
3. ML-KEM-1024 encapsulation with recipient's public key
-> mlKemSharedSecret (32 bytes) + mlKemCiphertext (1568 bytes)
4. Combine secrets:
combinedSecret = x25519SharedSecret || mlKemSharedSecret (64 bytes)
5. Derive final key:
sharedSecret = HKDF-SHA256(
 ikm = combinedSecret,
 salt = nil,
 info = "trashmail-hybrid-kem-v1",
 length = 32
)
6. Use sharedSecret to wrap the email's ephemeral AES-256 key

6.4 Processus de decapsulation

Recipient (decrypting an email):

1. X25519 key agreement:
x25519Shared = X25519(recipientPrivateKey, ephemeralPublicKey)
2. ML-KEM-1024 decapsulation:
mlKemShared = ML-KEM-1024.Decapsulate(mlKemCiphertext, recipientPrivateKey)
3. Combine and derive (identical to sender):
sharedSecret = HKDF-SHA256(x25519Shared || mlKemShared, "trashmail-hybrid-kem-v1")

4. Unwrap email's ephemeral AES-256 key using sharedSecret
5. Decrypt email content with ephemeral key

6.5 Tailles des clés

Parametre	Taille	Standard
X25519 public key	32 octets	RFC 7748
X25519 private key	32 octets	RFC 7748
ML-KEM-1024 public key	1 568 octets	NIST FIPS 203
ML-KEM-1024 private key	3 168 octets	NIST FIPS 203
ML-KEM-1024 ciphertext	1 568 octets	NIST FIPS 203
Secret partage combine	32 octets	Sortie HKDF-SHA256

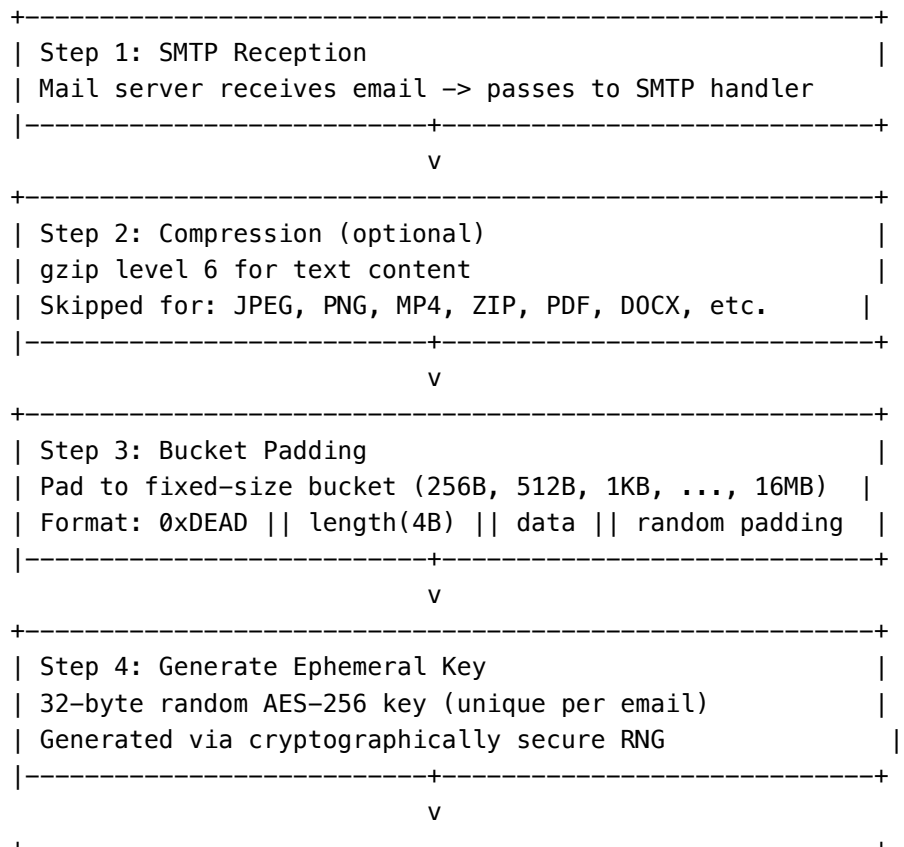
6.6 Bibliotheque

- **ML-KEM-1024** : @noble/post-quantum (auditee, implementation en JavaScript pur)
- **X25519** : API WebCrypto (crypto.subtle.deriveBits)
- **HKDF** : @noble/hashes (conforme RFC 5869)

7. Pipeline de chiffrement des e-mails

7.1 E-mail entrant (SMTP -> Stockage chiffré)

Lorsqu'un e-mail arrive sur le serveur SMTP d'Aionda Mail :



```

| Step 5: AES-256-GCM Encryption |
| Each field encrypted separately: |
|   • Subject   • From   • To |
|   • Body (HTML) • Body (plaintext) • Headers |
| Nonce: 12 bytes random per field |
| Tag: 16 bytes authentication |
| Format: nonce(12) || tag(16) || ciphertext |
|-----+-----+-----+
|                                     v
+-----+
| Step 6: Hybrid KEM Key Wrapping |
| Ephemeral key wrapped with recipient's public keys: |
|   X25519 + ML-KEM-1024 -> shared secret |
|   AES-256-GCM(ephemeral_key, shared_secret) |
| Format: version(1) || x25519_ct(32) || mlkem_ct(1568) |
|           || wrap_iv(12) || encrypted_key(48) |
|-----+-----+-----+
|                                     v
+-----+
| Step 7: Secure Erasure |
| sodium_memzero() clears ephemeral key from RAM |
| Only encrypted blobs remain |
|-----+-----+-----+
|                                     v
+-----+
| Step 8: Database Storage |
| Stored in vault_emails table: |
|   encrypted_subject, encrypted_from, encrypted_to, |
|   encrypted_body, encrypted_body_text, |
|   encrypted_headers, wrapped_ephemeral_key |
| Threading: SHA-256 hashes of Message-ID/In-Reply-To |
|           (not plaintext – zero-knowledge threading) |
|-----+-----+-----+

```

7.2 Lecture d'un e-mail (dechiffrement dans le navigateur)

Le processus inverse se deroule entierement dans le navigateur :

1. Recuperation de l'e-mail chiffre depuis le serveur via l'API chiffee
2. Analyse de la cle ephemere encapsulee (extraction du texte chiffre X25519 + texte chiffre ML-KEM)
3. **Decapsulation Hybrid KEM** a l'aide des cles privees du coffre-fort -> secret partage
4. Dechiffrement de la cle ephemere AES-256
5. **Dechiffrement AES-256-GCM** de chaque champ (objet, expéditeur, destinataire, corps, en-tetes)
6. Reordonnancement des octets : format serveur (nonce || tag || ct) -> format WebCrypto (nonce || ct || tag)
7. Suppression du Bucket Padding (detection des octets magiques 0xDEAD)
8. Decompression si gzip (detection des octets magiques 0x1F8B)

9. Decodage UTF-8 vers texte en clair

7.3 Envoi d'un e-mail

Lors de la composition et de l'envoi d'un e-mail :

1. Le client chiffre le contenu de l'e-mail avec un protocole de defi-reponse
2. Le serveur recoit le payload chiffre, le déchiffre de maniere ephemere (en memoire uniquement), et l'envoie via SMTP
3. Le serveur retourne les en-tetes MIME generes au client (chiffres)
4. Le client chiffre une copie avec la cle maitre du coffre-fort et la stocke dans le dossier Envoyes
5. Le texte en clair ephemere cote serveur est immediatement detruit — jamais ecrit sur disque

7.4 Pieces jointes

Chaque piece jointe est chiffree independamment :

- Cle ephemere AES-256 separee par piece jointe
- Encapsulation Hybrid KEM separee par piece jointe
- Nom de fichier et type MIME chiffres separement
- Pas de compression pour les formats deja compresses (JPEG, ZIP, PDF, etc.)

7.5 Regroupement des e-mails (Zero-Knowledge)

Le regroupement des e-mails (classement des e-mails lies) utilise uniquement des **hachages SHA-256** des en-tetes Message-ID et In-Reply-To. Le serveur ne voit jamais les chaines Message-ID reelles — il peut regrouper les e-mails par egalite de hachage sans en connaitre le contenu.

8. Couche de transport API chiffree

8.1 Problematique

Meme avec HTTPS, certains intermediaires peuvent inspecter le trafic :

- **CloudFlare** (CDN/protection DDoS) termine le TLS et peut voir les requetes en clair
- **Les proxys d'entreprise** peuvent effectuer une inspection TLS
- **Les parametres API** (comme ?cmd=read_email&id=123) exposent des metadonnees

8.2 Solution : API chiffree de bout en bout

Toutes les communications API sont en outre chiffrees de bout en bout entre le navigateur et le serveur applicatif, a l'interieur du tunnel HTTPS :

Browser

Server

Phase 1: Key Exchange (once per session)

GET /get_encryption_keys

->

Return 20 pre-generated
Hybrid KEM keypairs

← {uuid, x25519_pub, mlkem_pub}

Phase 2: Encrypted Request (every API call)

-
1. Pick random keypair from cache
 2. Hybrid KEM encapsulate → shared secret
 3. gzip compress request payload
 4. Bucket-pad compressed data
 5. AES-256-GCM encrypt with shared secret
 6. Generate ephemeral response keypair
 7. POST /e {

encrypted_payload,
 key_uuid,
 x25519_ciphertext,
 mlkem_ciphertext,
 response_x25519_pub,
 response_mlkem_pub

 →

8. Validate key ownership
 9. Hybrid KEM decapsulate
 10. AES-256-GCM decrypt
 11. Decompress
 12. Route to API controller
 13. Execute business logic
 14. Encrypt response with
 client's response keys
 15. Return encrypted response
 16. Hybrid KEM decapsulate response
 17. AES-256-GCM decrypt
 18. Decompress → plaintext response

8.3 Propriétés essentielles

- **Usage unique** : chaque paire de clés API est utilisée exactement une fois, puis définitivement invalidée
- **Perfect Forward Secrecy** : la compromission d'une clé de requête n'affecte aucune autre requête
- **Liées à la session** : les clés sont revendiquées par une session spécifique et ne peuvent pas être réutilisées par une autre
- **Pool de clés** : le serveur maintient environ 100 000 paires de clés pré-générées
- **Reapprovisionnement automatique** : le client demande automatiquement de nouvelles clés lorsque le cache tombe en dessous de 10
- **Durée de vie des clés** : les clés revendiquées expirent après 24 heures
- **Bidirectionnel** : la requête ET la réponse sont chiffrées — le serveur ne retourne jamais de texte en clair

8.4 Ce que voit CloudFlare

Avec cette architecture, CloudFlare (ou tout proxy terminant le TLS) ne voit que :

- POST /e — un point d'entrée unique et opaque
- Un blob binaire de données chiffrées
- Aucun nom de commande API, aucun paramètre, aucun identifiant d'e-mail, aucune donnée utilisateur

9. Cryptographie du partage de dossiers

9.1 Modele de partage

Les utilisateurs peuvent partager des dossiers chiffrés avec d'autres utilisateurs d'Aionda Mail. Le mécanisme de partage utilise le Hybrid KEM pour chiffrer une clé spécifique au dossier pour chaque destinataire.

9.2 Flux de partage

Folder Owner

Recipient

1. Derive folder key from master key:
`folderKey = HKDF-SHA256(masterKey, folderUuid)`
2. Fetch recipient's public keys:
`recipient.x25519_pub (32 bytes)`
`recipient.mlkem_pub (1568 bytes)`
3. Hybrid KEM encapsulate:
`hybridEncapsulate(recipient.x25519_pub, recipient.mlkem_pub)`
`-> {x25519Ciphertext, mlkemCiphertext, sharedSecret}`
4. Encrypt folder key:
`wrappedKey = AES-256-GCM(folderKey, sharedSecret, nonce)`
5. Store on server:
`{x25519_ct, mlkem_ct, nonce, wrappedKey, permissions}`
6. Fetch sharing record from server
7. Hybrid KEM decapsulate:
`hybridDecapsulate(x25519_ct, mlkem_ct,`
`own_x25519_priv, own_mlkem_priv)`
`-> sharedSecret`
8. Decrypt folder key:
`folderKey = AES-GCM-decrypt(`
`wrappedKey, sharedSecret, nonce)`
9. Decrypt emails in folder using folderKey

9.3 Modele de permissions

Permission	Capacite
readonly	Lire les e-mails du dossier (dechiffrement uniquement)
einliefern	Soumettre de nouveaux e-mails dans le dossier
bearbeiten	Modifier le contenu du dossier
antworten	Repondre aux e-mails du dossier
vollzugriff	Acces complet, y compris le transfert de propriete

9.4 Copie inter-coffres (Re-Wrapping)

Lorsqu'un destinataire copie un e-mail d'un dossier partage vers son propre coffre-fort, la cle de l'e-mail doit être **re-encapsulée** pour sa propre paire de clés Hybrid KEM. Cette opération est réalisée entièrement côté client :

1. Déchiffrement de la cle du dossier partage à l'aide des clés privées du destinataire
2. Déchiffrement de la cle éphémère de l'e-mail à l'aide de la cle du dossier
3. Re-encapsulation de la cle éphémère avec les propres clés publiques du destinataire
4. Stockage de la copie re-encapsulée dans le coffre-fort du destinataire

Le serveur facilite le transfert mais ne voit jamais aucune cle en clair.

10. Vault Drive — Stockage de documents chiffré

Vault Drive est le stockage de documents Zero-Knowledge d'Aionda Mail. Contrairement aux e-mails, qui utilisent des clés éphémères par message, Drive utilise une **architecture à cle par fichier** : chaque document reçoit sa propre cle AES-256-GCM de 32 octets, générée côté client et enveloppée avec la cle maître.

10.1 Pourquoi des clés par fichier ?

L'architecture à cle par fichier offre trois avantages clés :

1. **Partage granulaire** : Des documents individuels peuvent être partagés sans exposer la cle maître. Le serveur re-enveloppe simplement la cle du fichier pour le destinataire — le contenu reste inchangé.
2. **Isolation en cas de compromission** : Si une seule cle de fichier est compromise (p.ex. via un lien partagé), tous les autres documents restent protégés.
3. **Partage efficace sans re-chiffrement** : Lors du partage, le contenu n'a pas besoin d'être re-chiffré — tous les destinataires lisent le même texte chiffré avec une cle re-enveloppée.

10.2 Flux de téléchargement montant

Client

Serveur

1. Générer une cle de fichier aléatoire :

```
fileKey = randomBytes(32)
```
2. Chiffrer contenu, nom, type MIME :

```
encContent = AES-256-GCM(content, fileKey, nonce1)
encName     = AES-256-GCM(name,   fileKey, nonce2)
encMime     = AES-256-GCM(mime,   fileKey, nonce3)
```
3. Envelopper la cle de fichier avec la cle maître :

```
wrappedKey = AES-256-GCM(fileKey, masterKey, nonce4)
```
4. Envoyer le paquet chiffré :

```
POST /e {
```

```

    encContent, encName, encMime,
    wrappedKey, wrappedKeyNonce
}

```

5. Stocker dans vault_files + vault_file_c
(textes chiffrés purs, aucun matériel)

10.3 Flux de téléchargement descendant

1. Récupérer chunk + wrapped_key depuis le serveur
2. Déballer la cle de fichier :
fileKey = AES-256-GCM-decrypt(wrappedKey, masterKey, nonce)
3. Déchiffrer contenu, nom, MIME :
content = AES-256-GCM-decrypt(encContent, fileKey, nonce1)

Le déchiffrement s'effectue dans un **Web Worker** qui ne conserve la cle maitre que temporairement en memoire. Après l'operation, la memoire est ecrasee.

10.4 Partage — re-enveloppement de cle uniquement

L'avantage central des cles par fichier apparait lors du partage : le contenu n'est **pas** re-chiffre. Seule la cle de fichier de 32 octets est re-enveloppee avec le KEM hybride du destinataire.

Proprietaire

Destinataire

1. Déballer la cle de fichier :
fileKey = AES-GCM-decrypt(wrappedKey, masterKey)
2. Charger les cles publiques du destinataire :
recipient.x25519_pub, recipient.mlkem_pub
3. Encapsulation KEM hybride :
hybridEncapsulate(recipient.x25519_pub,
recipient.mlkem_pub)
-> {x25519_ct, mlkem_ct, sharedSecret}
4. Envelopper la cle de fichier avec sharedSecret :
shareWrappedKey = AES-256-GCM(fileKey,
sharedSecret, nonce)
5. Enregistrer le partage :
INSERT INTO vault_file_shares {
file_uuid, recipient_account_id,
x25519_ephemeral, mlkem_ciphertext,
share_wrapped_key, permissions
}
6. Charger l'enregistrement + chunk
7. Decapsulation KEM hybride :
hybridDecapsulate(x25519_ct, mlkem_ct,
own_x25519_priv, own_mlkem_priv)
-> sharedSecret
8. Déballer la cle de fichier :

```

fileKey = AES-GCM-decrypt(
    shareWrappedKey, sharedSecret)
9. Dechiffrer le MEME texte chiffre :
content = AES-GCM-decrypt(
    encContent, fileKey)

```

Le propriétaire n'a pas besoin de la cle maitre du destinataire — seulement des cle publiques KEM hybrides, que le serveur stocke en clair.

10.5 Partage de dossier (récursif)

Lorsqu'un dossier est partagé, le client traite récursivement tous les documents et sous-dossiers contenus. Chaque fichier recoit son propre enregistrement de partage contenant la cle de fichier du document respectif, re-enveloppée pour le destinataire. Le dossier lui-même n'a pas de cle de dossier — la structure est liée via des UUIDs parents.

Important : L'étape d'encapsulation KEM est effectuée **par opération**, pas par fichier. Tous les fichiers d'un partage par lot utilisent le même `sharedSecret` — ce qui rend l'opération efficace sans réduire la sécurité (chaque fichier a toujours sa propre cle).

10.6 Modèle d'autorisations

Autorisation	Peut effectuer
Lecture	Telecharger, previsualiser, lire les metadonnees
Acces complet	+ renommer, televerser une nouvelle version, deplacer dans le dossier partage, televerser de nouveaux documents
Impossible	Supprimer (proprietaire uniquement), sortir du dossier partage (proprietaire uniquement)

Les autorisations sont stockées dans l'enregistrement `vault_file_shares` et appliquées côté serveur. La cryptographie protège le contenu — le contrôle d'accès protège les opérations.

10.7 Renommage, écrasement et mises à jour de metadonnées

Pour les documents partagés, les opérations de renommage et d'écrasement sont effectuées directement sur l'enregistrement `vault_files` — pas sur les enregistrements de partage individuels. Tous les destinataires voient immédiatement le nouveau nom ou contenu, car ils référencent le même texte chiffré.

Lors d'un **écrasement** (nouvelle version), une **nouvelle cle de fichier** est générée, l'ancien texte chiffré est remplacé, et tous les enregistrements de partage existants sont re-enveloppés côté client avec la nouvelle cle. Le propriétaire doit charger les cle publiques de tous les destinataires pour cette opération.

10.8 Previsualisation et déchiffrement en mémoire

Les images, PDF et autres documents sont déchiffrés **exclusivement en mémoire** pour la prévisualisation. Il n'y a pas de cache disque avec des données en clair. Le client utilise le **VaultDataLayer**, un cache IndexedDB chiffré qui stocke les textes chiffrés de manière persistante et ne les déchiffre qu'à la demande.

Les miniatures ne sont **jamais** générées côté serveur — le serveur ne voit jamais le contenu.

Les miniatures sont generees cote client a partir de l'original dechiffre et egalement mises en cache chiffrees.

10.9 Ce que le serveur voit

Visible par le serveur	Non visible
Contenu chiffre (octets aleatoires)	Contenu en clair
Nom de fichier chiffre (octets aleatoires)	Nom de fichier en clair
Type MIME chiffre (octets aleatoires)	Type de fichier (image, PDF, texte...)
Taille du fichier (paddee aux limites de buckets)	Taille originale reelle
Horodatage du televersement	Cle de fichier, cle maitre
ID du compte proprietaire	Contenus des sous-dossiers
UUID du dossier parent (pour la structure)	Noms des dossiers (egalement chiffrees)
Enregistrements de partage avec textes chiffrees KEM	Cle maitre du destinataire, cle de fichier deballee

10.10 Application des quotas

L'application des quotas se fait cote serveur sur la base de la **taille chiffree du fichier** (y compris le padding de bucket). Le serveur ne connaît pas la taille reelle en clair — le surcote de padding est intentionnellement paye par l'utilisateur pour empecher la fuite de taille.

Limites : - **Gratuit** : 100 Mo de stockage total, max. 10 Mo par document - **Plus** : 1 Go de stockage total, max. 100 Mo par document

10.11 Partage externe — liens de partage publics

Les documents Vault Drive peuvent etre partages avec des destinataires qui **n'ont pas de compte Aionda Mail**, via des liens de partage publics servis depuis le domaine isole `mail.aionda.com`. La fonctionnalite preserve le principe zero-knowledge en traitant chaque partage comme une **enveloppe cryptographique independante**, decouplee de la cle maitre du coffre du proprietaire.

Modes de protection :

Mode	Facteur de confiance	Cas d'usage
link_only	Fragment d'URL (jamais envoye au serveur)	Confort — toute personne disposant du lien peut acceder
password	Cle derivee par Argon2id	Transfert hors bande du mot de passe (SMS, appel telephonique)
recipient_pubkey	KEM hybride (X25519 + ML-KEM-1024)	Securise post-quantique lorsque le destinataire a preenregistre des cles publiques

10.11.1 Creation du partage (client proprietaire)

1. fileKey := AES-GCM-decrypt(vault_files.wrapped_key, masterKey)
2. shareKey := randomBytes(32) // ephemere, par partage
3. wrappedFileKey := AES-GCM(fileKey, shareKey) // nouvelle enveloppe
4. unlockVerifier := HMAC-SHA256(shareKey, "unlock:" || shareUuid) // preuve de connaissance
5. Si protection par mot de passe :
 - salt := randomBytes(16)
 - pwKey := Argon2id(password, salt, t=3, m=64MB, p=1)
 - wrappedShareKey := AES-GCM(shareKey, pwKey)
 - > Lien : https://mail.aionda.com/s/<shareUuid>
 - Sinon (link_only) :
 - > Lien : https://mail.aionda.com/s/<shareUuid>#<base64(shareKey)>
 - (fragment d'URL – les navigateurs ne transmettent jamais les fragments au serveur)
6. Metadonnees chiffrees (par partage, avec shareKey) :
 - encFilename, encMime, encMessage // toutes AES-GCM
7. POST /e (transport API chiffre, voir §8)
 - > le serveur stocke l'enregistrement de partage – ne voit jamais le texte clair

La distribution du lien est choisie par le proprietaire — pas par Aionda Mail. Apres la creation, le proprietaire decide du canal : copier le lien, QR code, brouillon mailto: dans son propre client, Signal, SMS, AirDrop ou tout autre canal hors bande. Aionda Mail ne voit, n'envoie et ne journalise jamais la distribution sortante — le serveur sait uniquement quelles share-UUIDs existent. Cela importe pour deux raisons : (a) le proprietaire choisit le canal qu'il juge le plus sur (politique de conformite, messagerie preferee, scan QR en face a face), et (b) pour les partages proteges par mot de passe, cela permet la **separation des canaux** — lien via canal A, mot de passe via canal B — afin qu'un canal compromis seul ne donne jamais acces.

10.11.2 Acces au partage (destinataire, sans compte) Le destinataire visite https://mail.aionda.com/s/. La Share Page est un **bundle separe** du Manager, avec son propre build reproductible, un manifeste Subresource Integrity et un endpoint /.well-known/integrity.json pour la verification hors ligne.

1. Bootstrap de la Share Page (le client genere un keypair KEM hybride ephemere)
2. share_fetch_meta -> { wrapped_file_key, salt?, encrypted_message, ... }
3. Phase d'unlock – produit un unlock_token a usage unique :
 - mode password : le serveur verifie la derivation Argon2id -> unlock_token
 - mode link_only : le client calcule HMAC-SHA256(shareKey, "unlock:" || uuid)
 - le serveur verifie contre unlockVerifier stocke
 - > unlock_token
4. fileKey := AES-GCM-decrypt(wrappedFileKey, shareKey)
5. share_download_chunk (par chunk, unlock_token requis)
6. Le client hache le texte clair, appelle share_confirm_download

Le unlock_token unifie le flow pour les trois modes de protection et permet un rate-limiting et un audit logging centralises — l'accès link_only exige la preuve de connaissance du fragment, les bots et crawlers sans fragment ne peuvent donc pas declencher de telechargement.

10.11.3 Politiques imposees Chaque partage doit declarer les elements suivants a la creation (tous appliques cote serveur) :

- **expires_at** — obligatoire, 7 jours par default, maximum 90 jours
- **max_downloads** — compteur obligatoire, 10 par default
- **Rate-limiting** — les tentatives Argon2 sur les partages proteges par mot de passe sont limitees par hash d'IP et par partage
- **revoked_at** — le proprietaire peut revoquer tout partage en un clic ; les tentatives d'unlock et telechargements ulterieurs renvoient une reponse unifiee « partage indisponible » (meme erreur qu'expire/epuise — pas d'oracle d'enumeration)

10.11.4 Chaine d'audit infalsifiable Tous les evenements d'accès pertinents sont ajoutes a la hash chain existante `enterprise_audit_log` (SHA3-256, voir §18.2). Les types d'action suivants sont reserves au partage externe :

`EXT_SHARE_CREATED`, `EXT_SHARE_EMAIL_SENT`, `EXT_SHARE_VIEWED`, `EXT_SHARE_UNLOCKED`, `EXT_SHARE_PREVIEWED`, `EXT_SHARE_DOWNLOAD_STARTED`, `EXT_SHARE_DOWNLOAD_CONFIRMED`, `EXT_SHARE_INTEGRITY_BROKEN`, `EXT_SHARE_PASSWORD_FAIL`, `EXT_SHARE_REVOKED`, `EXT_SHARE_ROTATED`, `EXT_SHARE_EXPIRED`.

Les hashes d'IP et user-agent utilisent un **sel rotatif quotidien** (`vault_drive_external_share_daily_salts`, purge apres 30 jours) — les hashes historiques deviennent non reversibles apres rotation du sel (conformite RGPD), tout en conservant une correlation court terme pour le proprietaire.

10.11.5 Rotation de cle (rewrap du partage) Le proprietaire peut faire pivoter un partage a tout moment sans reuploader le contenu :

1. `new_shareKey := randomBytes(32)`
2. `new_wrappedFileKey := AES-GCM(fileKey, new_shareKey)`
3. INSERT nouvelle ligne de partage ; `old.linked_to_uuid := new.share_uuid`
4. `old.revoked_at := NOW()`

Les destinataires utilisant l'ancien lien recoivent « partage indisponible ». Le proprietaire distribue le nouveau lien. Les evenements d'accès des deux partages restent lies via `linked_to_uuid` dans la chaine d'audit.

10.11.6 Ce que fait la revocation — et ce qu'elle ne fait pas La revocation **stoppe la livraison future cote serveur** du partage. Elle **ne revoque pas** retroactivement les share keys, file keys ou chunks deja livres. Un destinataire qui a deja telecharge le texte clair — ou qui a capture le fragment du lien — peut continuer a utiliser ce materiel localement. Pour les cas exigeant une assurance plus forte, combiner : `expires_at` court, `max_downloads` bas, protection par mot de passe et l'extension navigateur Guardian chez le destinataire.

10.11.7 Ce que voit le serveur

Le serveur voit	Le serveur ne voit PAS
<code>share_uuid</code> , <code>file_uuid</code> , <code>account_id</code> (proprietaire)	Nom de fichier, type MIME, contenu, message en clair
<code>wrapped_file_key</code> , <code>wrapped_share_key</code> (chiffres)	<code>share_key</code> (<code>link_only</code> : vit uniquement dans le fragment d'URL, cote client)

Le serveur voit	Le serveur ne voit PAS
unlock_verifier (sortie HMAC, non reversible) protection_mode, expires_at, max_downloads, allow_preview encrypted_filename, encrypted_mime, encrypted_message (chiffres) sender_display_name en clair (le destinataire le voit avant l'unlock) Entrees de la chaine d'audit pour chaque evenement d'accès	Mot de passe, cle derivee Argon2 Identite du destinataire (uniquement hash sale IP/UA, purge apres 30 jours) Leurs contenus en clair

11. Aionda Chat — Messagerie E2EE post-quantique

Aionda Chat est la surface de messagerie temps réel intégrée à Aionda Mail. Contrairement aux e-mails — qui utilisent des clefs ephemeres a usage unique par message — les conversations de chat sont longues et necessitent **forward secrecy** et **post-compromise security** pour chaque message individuel. Pour cela, nous avons concu un protocole dedie : **AAR (Aionda Async Ratchet)** — une variante post-quantique du X3DH + Double Ratchet de Signal, dans laquelle chaque etape Diffie-Hellman est remplacee par un KEM hybride (X25519 + ML-KEM-1024).

11.1 Pourquoi un protocole dedie ?

E-mail et chat ont des profils de securite fondamentalement differents :

Propriete	E-mail	Chat
Cadence	Sporadique (minutes/heures)	Temps reel (secondes)
Duree de session	Message unique	Continue, jours a annees
Unite de forward secrecy	Par message	Par message au sein d'une longue session
Recuperation post-compromise	Non requise (cle one-shot)	Requise — chaque nouveau message restaure d'un compromis passe
Asynchronisme	Eleve (destinataire souvent hors ligne)	Eleve (destinataire souvent hors ligne)
Dynamique de groupe	Liste de destinataires statique	Ajout/retrait dynamique

Une conversation de chat qui reutiliserait simplement la pipeline e-mail devrait soit (a) bruler une nouvelle paire de clefs ephemeres a chaque frappe (inacceptablement lent), soit (b) partager une seule cle de conversation statique (pas de forward secrecy). Aucune n'est acceptable. AAR resout cela en maintenant un etat de cle a ratchet continu par pair — chaque message fait progresser l'etat de maniere irreversible.

11.2 Briques de construction

AAR utilise exactement quatre primitives :

KEM hybride	X25519 + ML-KEM-1024	(encapsulation de cles)
AEAD	AES-256-GCM	(chiffrement des messages)
KDF	HKDF-SHA256	(derivation de cles)
Signatures	Ed25519	(liaison d'identite, signature SPK)

Aucune nouvelle hypothese cryptographique n'est introduite – chaque primitive est aussi utilisee ailleurs dans le systeme et a ete auditee independamment.

11.3 KeyBundle — le materiel de handshake asynchrone

Chaque utilisateur publie un **KeyBundle** sur le serveur lors de l'activation initiale du chat. Le bundle permet aux pairs de commencer a envoyer des messages meme si l'utilisateur est hors ligne.

KeyBundle (par compte, hybride de bout en bout) :

Cle d'identite (IK)	– long terme
-- IK.x25519_pub	
-- IK.mlkem_pub	
-- IK.ed25519_pub	– utilisee pour signer la SPK
Signed Pre-Key (SPK)	– rotation hebdomadaire
-- SPK.x25519_pub	
-- SPK.mlkem_pub	
-- Signature Ed25519	– signe la concatenation, lie SPK a IK
One-Time Pre-Keys (OPK)	– pool d'environ 100, consommees atomiquement
-- OPK.x25519_pub	
-- OPK.mlkem_pub	

Stockage serveur : Seules les moities publiques de chaque cle sont stockees, plus signatures et metadonnees. Les moities privees ne quittent jamais le navigateur d'origine. Le serveur applique un UPDATE ... LIMIT 1 SET consumed_ts = NOW() atomique lorsqu'une OPK est recuperee, garantissant la semantique d'usage unique sous des requetes concurrentes.

Quand le pool d'OPK descend sous 20, le client le reapprovisionne avec un nouveau lot — cela empeche le handshake asynchrone de se degrader vers un mode degenere sans entropie one-time.

11.4 Handshake style PQXDH (X3DH-PQ)

Pour demarrer une nouvelle conversation avec Bob, Alice recupere le bundle de Bob (IK_B, SPK_B, une OPK_B) et la signature Ed25519 de Bob sur SPK_B. Alice verifie la signature, puis effectue quatre encapsulations KEM hybrides :

1. Verifier la signature Ed25519 sur SPK_B – lie SPK a l'identite long terme
2. Generer la cle ephemere d'Alice (EK_A) :
EK_A.x25519, EK_A.mlkem (one-time, jetee immediatement apres le handshake)

3. Quatre encapsulations KEM hybrides :

```

ss1 = HKEM(IK_A_priv ⊗ SPK_B_pub)    – Identite Alice -> SPK Bob
ss2 = HKEM(EK_A_priv ⊗ IK_B_pub)    – Ephemere Alice -> Identite Bob
ss3 = HKEM(EK_A_priv ⊗ SPK_B_pub)    – Ephemere Alice -> SPK Bob
ss4 = HKEM(EK_A_priv ⊗ OPK_B_pub)    – Ephemere Alice -> OPK Bob

```

(chaque ss_i est lui-meme la combinaison HKDF d'un secret X25519
ET d'un secret ML-KEM – voir Section 6.4)

4. Derivation de la cle racine :

```

SK = HKDF-SHA256(
    IKM  = ss1 || ss2 || ss3 || ss4,
    info = "AAR-X3DH-v1" || consumed_OPK_id
)

```

5. Oublier toute matiere ephemere privatee ; SK ensemence le ratchet.

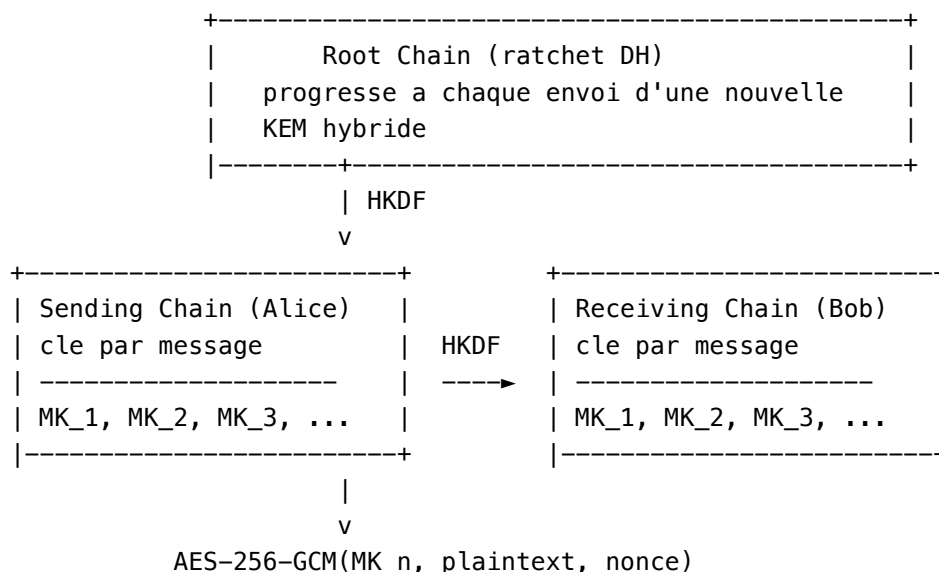
La construction garantit :

- **Authentification mutuelle** via la SPK_B signee Ed25519 et la liaison IK_A
- **Forward secrecy** meme si IK_B est compromis ulterieurement — $ss3$ et $ss4$ utilisent des cle ephemeres des deux cotes
- **Securite post-quantique** car chaque ss_i inclut un terme ML-KEM — un attaquant collectant le trafic d'aujourd'hui pour un futur ordinateur quantique ne peut pas reconstruire les quatre secrets
- **Resistance au rejeu** par consommation atomique des OPK — le declencheur cote serveur de Bob refuse de liberer la meme OPK deux fois

L'identifiant de l'OPK consommee par Alice est lie au parametre `info` de HKDF — Bob ne peut donc reproduire la meme cle racine qu'avec la meme OPK, et une seule fois.

11.5 Double Ratchet — cle par message

Apres le handshake, les deux cotes font progresser un etat **Double Ratchet** pour chaque message :



Chaque evenement de chat porte la **cle publique de ratchet** actuelle de l'expediteur (paire hybride, ~1,6 Ko). Quand le destinataire recoit un message dont la cle de ratchet differe de la derniere vue, les deux parties effectuent une nouvelle KEM hybride, derivent une nouvelle cle racine et reinitialisent leurs chaines. C'est le **ratchet DH** dans la terminologie Signal — sauf que chaque etape est un KEM hybride complet, pas un seul Diffie-Hellman.

Garanties par message :

- **Forward secrecy** : la suppression de MK_n rend le message n indechiffable, meme avec l'etat long terme complet au moment de la capture
- **Post-compromise security** : une fois qu'une etape DH-ratchet fraiche a eu lieu apres un compromis, tous les messages suivants sont proteges de l'attaquant
- **Livraison hors ordre** : les cles de message sont mises en cache pour les messages tardifs (plafonnees a 1000 cles par session pour borner la memoire)

11.6 Conteneur de message

Chaque evenement de chat televerse sur le serveur est un texte chiffre autonome :

MessageContainer (encode base64, stocke dans chat_events.payload) :

```
+-----+
| ratchet_pub      : Cle publique KEM hybride (etape actuelle)|
| prev_chain_len   : Nombre de messages dans la chaine preced.|
| msg_number       : Compteur dans la chaine actuelle         |
| ciphertext       : AES-256-GCM(MK_n, plaintext || header)    |
| tag              : Tag d'authentification AES-256-GCM       |
+-----+
```

Le header dans le plaintext AEAD contient : login expediteur, content_type (text/quote/file-reference), timestamp, reply_to_event_uuid optionnel.

Le conteneur est opaque pour le serveur — y compris le type de message, le format du nom d'affichage de l'expediteur, et tout contexte de reponse cite. La base de donnees d'Aionda stocke le conteneur tel quel dans chat_events.payload.

11.7 Conversations de groupe — Sender Keys par destinataire

Pour les conversations de salon (3+ participants), AAR utilise un modele de **fan-out par destinataire**. L'expediteur derive une chaine sender-key par paire de pair et chiffre un message une fois par destinataire. Chaque destinataire recoit donc un texte chiffre personnellement adresse, decchiffable uniquement avec les cles derivees de sa propre session AAR avec l'expediteur.

Compromis : Le cout du fan-out est $O(N)$ en destinataires — acceptable pour les tailles d'equipe typiques (≤ 25 participants). Pour des groupes plus grands, un futur mode base sur MLS est prevu (voir Roadmap). Le modele actuel est preferable a une seule cle de groupe partagee parce que : (a) il preserve la forward secrecy par paire, (b) il ne necessite pas de rotation de cles au-dela du niveau bilateral lors du retrait d'un membre, et (c) il herite des garanties post-quantiques de l'AAR par paire sans modification.

11.8 Conteneur de conversation initial

Quand Alice démarre un nouveau salon avec Bob, Carol et Dan, le premier message a chaque participant est emballé comme un **conteneur de handshake initial** qui transporte (a) le matériel de handshake X3DH consomme contre le bundle de ce participant et (b) le premier message lui-même. Le destinataire dispatche sur le champ discriminateur :

```
{
  "type": "initial",
  "initialMessage": { /* metadonnees du handshake, OPK id consommee */,
    "encryptedMessage": "<base64 MessageContainer>"
  }
}
```

Les messages suivants dans le même salon réutilisent la session AAR établie et ne contiennent que la partie encryptedMessage.

11.9 Transport — API chiffree + Mercure SSE + WebSocket

Le plan de chat utilise trois canaux orthogonaux :

Canal	Direction	Objectif	Plaintext vu par le serveur
API chiffree /e	Client -> Serveur	Envoi de message, récupération d'historique, opérations key-bundle (11 endpoints)	Aucun — tous les 11 endpoints chat utilisent le même transport hybrid-KEM documenté en Section 8
Mercure SSE	Serveur -> Client	Push de livraison de nouveaux événements (chat.event_received, chat.read_receipt)	Aucun — le serveur pousse le même MessageContainer opaque qu'il a stocké
WebSocket /chat/ws	Bidirectionnel	Backfill de reconnexion (sync_request), heartbeat, presence	Booleen de présence (en ligne/hors ligne) et chaîne de login uniquement — jamais le contenu des messages

La présence est tenue dans une carte en mémoire sur `aionda_chat_realtime` ; un seul endpoint HTTP intranet expose une recherche login -> online pour le sélecteur d'équipe afin que les utilisateurs puissent voir si un pair est joignable. Aucun historique, aucun état de lecture, aucun contenu ne traverse jamais le canal de présence.

11.10 Accuses de lecture

Les accuses de lecture sont un paramètre opt-in par compte (`chat_participants.send_read_receipts`). S'ils sont actifs, marquer un message comme lu publie un événement `chat.read_receipt` contenant :

```
{ conversation_uuid, last_read_event_uuid, account_login }
```

Notez que `last_read_event_uuid` n'est **pas** le contenu du message — c'est un identifiant alloué par le serveur déjà connu de lui. Aucune information supplémentaire ne fuit au-delà de « Alice a maintenant vu les messages jusqu'à l'événement X. » Les destinataires qui désactivent les accusés de lecture (`send_read_receipts = false`) n'émettent jamais de tels événements, et le serveur applique le toggle.

11.11 Intégration de la chaîne d'audit

Pour les comptes Enterprise, chaque opération de chat est ajoutée au journal d'audit infalsifiable existant (`enterprise_audit_log`, chaîne de hash SHA3-256 — voir §18). Les types d'action réservés sont :

`CHAT_CONVERSATION_CREATED`, `CHAT_PARTICIPANT_ADDED`, `CHAT_PARTICIPANT_REMOVED`, `CHAT_MESSAGE_SENT`, `CHAT_MESSAGE_READ`, `CHAT_KEYBUNDLE_PUBLISHED`, `CHAT_KEYBUNDLE_ROTATED`, `CHAT_OPK_TOPPED_UP`, `CHAT_CONVERSATION_LEFT`.

L'enregistrement d'audit ne contient que l'UUID de conversation, le login de l'acteur et un timestamp — **jamais** le payload chiffré, les clés de ratchet ou les contenus de messages.

11.12 Ce que le serveur voit

Visible pour le serveur	Non visible
<code>conversation_uuid</code> , liste des participants (par <code>mail_account.name</code>)	Contenu des messages en clair
Payloads <code>MessageContainer</code> chiffrés (textes chiffrés opaques)	Clés de ratchet, clés de chaîne, clés de message
Moitiés publiques de IK, SPK, OPK ; signatures Ed25519 sur SPK	Moitiés privées de toute paire de clés
Compteur et timestamp de consommation OPK	Quelle OPK a été consommée pour quelle conversation (corrélation empêchée par la liaison HKDF-info uniquement côté client)
Cadence de conversation (timestamps des lignes <code>chat_events</code>)	Chaînes de réponses citées, pièces jointes dans le conteneur
Booleen de présence (en ligne/hors ligne)	Indicateurs de frappe (peer-to-peer, n'atteignent jamais le serveur)
Entrées de la chaîne d'audit pour les comptes Enterprise	Contenus en clair des entrées d'audit

11.13 Audits cryptographiques

Le protocole AAR a été implémenté à partir de zéro en TypeScript et a subi trois audits indépendants assistés par IA, documentés dans `typescript/manager/chat/crypto/AUDIT.md`, `AUDIT_SECOND_OPINION.md` et `AUDIT_THIRD_OPINION.md`. Les conclusions de chaque tour ont été intégrées avant le déploiement public. Les surfaces principales auditées étaient : symétrie du handshake, réservation OPK sous concurrence, deep-cloning de l'état immuable du ratchet, et le framing AEAD du `MessageContainer`.

11.14 Limites d'implémentation

La base de code chat vit dans `typescript/manager/chat/` (~9 000 lignes de TypeScript) et `includes/classes/Api/Services/Chat/` (couche service PHP). Artefacts d'audit clés :

crypto/aar-types.ts	– declarations de types uniquement, aucune logique
crypto/aar-keybundle.ts	– creation, rotation, serialisation du KeyBundle
crypto/aar-x3dh.ts	– Handshake (chemins initiateur + repondeur)
crypto/aar-double-ratchet.ts	– Root chain, sending chain, receiving chain

La separation propre entre logique de protocole (crypto/) et transport/UI (chat-store.ts, chat-panel.ts, ...) garantit que le coeur cryptographique peut etre re-audite sans derive de portee UI.

12. Appels video Aionda — visioconference E2EE post-quantique

Aionda Mail inclut des appels video de groupe chiffres de bout en bout (suite cryptographique AIONDA_PQ_CALL_V1). Le relais de medias ne voit jamais l'audio ou la video en clair — il ne transfere que des trames chiffrees. Les cle de groupe sont negociees par un handshake **hybride post-quantique**.

12.1 Objectifs de securite & modele de confiance

Dans le perimetre — le protocole fournit :

- **Confidentialite** des medias audio et video, de bout en bout.
- **Authenticite** du groupe — chaque participant est cryptographiquement membre du meme groupe MLS, verifie hors-bande via la Short Authentication String (Section 12.5).
- **Forward secrecy** — les medias passes restent secrets meme si les cle actuelles sont compromises ulterieurement.
- **Post-compromise security** — le groupe recouvre la confidentialite apres le retrait d'un membre compromis et le renouvellement des cle du groupe.
- **Confidentialite post-quantique** — l'etablissement du groupe utilise le KEM hybride X-Wing.
- **Independance du serveur** — une SFU, un serveur de signalisation ou une couche de stockage malveillants ou compromis ne peuvent ni lire ni injecter de medias.

Hors perimetre (explicitement *non* defendu) :

- L'analyse de trafic — le timing des paquets, les tailles des paquets, le nombre de participants et la duree de l'appel sont observables (Section 12.9).
- La compromission du terminal (voir l'hypothese de confiance ci-dessous).
- Les logiciels malveillants au niveau du systeme d'exploitation ou la saisie physique de l'appareil.

Hypothese de confiance sur le terminal. Le modele suppose un navigateur et un systeme d'exploitation non compromis. Les trames sont scellees a l'interieur de la pipeline media du navigateur (RTCRtpScriptTransform), mais un terminal compromis peut lire les medias en clair *avant* le chiffrement ou *apres* le dechiffrement. Le modele de confiance de la livraison web et ses mesures d'attenuation (signature des reponses Guardian) sont couverts en Section 18 et Section 23.

12.2 Pourquoi un protocole dedie ?

La visioconference temps reel a deux exigences que les couches e-mail et chat n'ont pas :

1. **Chiffrement par trame au debit de la ligne.** Les trames audio/video doivent etre chiffrees

individuellement afin qu'une Selective Forwarding Unit (SFU) puisse les router, les supprimer et les reordonner sans jamais les déchiffrer. C'est le rôle de **SFrame** (RFC 9605).

2. **Negotiation dynamique de cle de groupe.** Les participants rejoignent et quittent l'appel en cours. Chaque changement de composition doit renouveler la cle du groupe avec forward secrecy et post-compromise security. C'est le rôle de **MLS** (RFC 9420).

La SFU cote serveur (mediasoup) est traitée comme une **infrastructure non fiable** : c'est un routeur de paquets a connaissance nulle, exactement comme la couche de stockage pour les e-mails.

12.3 Suite cryptographique — AIONDA_PQ_CALL_V1 (0xFF01)

Le profil MLS substitue les primitives classiques d'une suite MLS standard par des hybrides post-quantiques.

Role	Algorithme	Notes
HPKE KEM	X-Wing (ML-KEM-768 + X25519)	Hybrid;
Signatures	ML-DSA-65	draft-connelly-cfrg-xwing-kem NIST FIPS 204 (Dilithium), Level 3
KDF	HKDF-SHA-256	RFC 5869
AEAD (HPKE + SFrame)	AES-256-GCM	AES-256 offre une marge confortable contre les attaques de recherche quantique connues (Grover)

Aucun downgrade. Il n'existe aucun repli purement classique. Si le handshake post-quantique ne peut pas être mené à terme, l'appel échoue de manière fermée (fail closed) — un downgrade est une erreur dure, jamais un affaiblissement silencieux.

Maturité de X-Wing. X-Wing est actuellement un draft IETF/CFRG (draft-connelly-cfrg-xwing-kem). Le profil actuel l'adopte comme KEM hybride préféré ; de futures révisions du protocole pourront migrer vers un KEM hybride finalisé et standardisé par le CFRG/NIST, tout en préservant inchangées les couches MLS et SFrame.

Agilité cryptographique. L'identifiant de la suite cryptographique (0xFF01) détermine entièrement le KEM, l'algorithme de signature, le KDF et l'AEAD. Une future suite AIONDA_PQ_CALL_V2 peut remplacer n'importe quelle primitive sans modifier les couches supérieures du protocole ; les suites sont sélectionnées par identifiant et ne sont jamais négociées silencieusement vers le bas.

12.4 Negotiation de cle de groupe (MLS, RFC 9420)

Chaque participant est représenté dans l'arbre à ratchet MLS par un **KeyPackage** (cle KEM publique X-Wing + identifiant ML-DSA-65). Le groupe évolue à travers des *epochs* :

- **Welcome / Commit** — un membre rejoignant est ajouté avec un secret de chemin encapsulé par X-Wing ; l'arbre à ratchet avance vers une nouvelle epoch.
- **Renouvellement de cle à chaque changement de composition.** Tout changement — une arrivée, un départ, un remplacement d'appareil ou une rotation de cle d'identité —

fait avancer le groupe vers une nouvelle epoch. C'est ce qui assure la forward secrecy (un nouveau participant ne peut lire les medias passes) et la post-compromise security (un membre retire ne peut lire les medias futurs).

- **Remove-Commit.** Lorsqu'un participant quitte (ou qu'un pair perime/zombie est detecte), le propriétaire emit un Remove-Commit qui renouvelle la cle du groupe, de sorte qu'un membre parti ne puisse pas dechiffrer les trames ulterieures meme s'il a conserve l'ancien materiel de cle.

La construction hybride est concue de sorte que la compromission d'un **seul** composant — ML-KEM-768 *ou* X25519 — ne revele pas a elle seule le secret de groupe.

12.5 Identite & authentication

- **Identifiants.** Chaque membre porte un **Credential** MLS qui lie une identite de participant a sa cle de signature ML-DSA-65. Chaque message de handshake MLS (Welcome / Commit / Update) est signe avec cette cle, de sorte que la SFU ou le serveur de signalisation ne peut pas falsifier les operations de groupe.
- **Short Authentication String (SAS).** Le lien de la salle transporte un **secret pre-partage** a haute entropie dans le fragment d'URL, qui n'est jamais envoye au serveur en clair. L'exportateur du groupe MLS et ce secret sont melanges ensemble dans une Short Authentication String, dont le client **epingle** l'empreinte. Une divergence — par exemple un serveur de signalisation ou une SFU tentant d'insérer un participant malveillant — declenche un **abandon dur sans repli souple**. Cela lie le groupe cryptographique au secret de salle hors-bande et fait echec a un man-in-the-middle cote serveur.
- **Facteur d'authentification.** Pour une salle invite, *la possession du lien de salle equivaut a la possession de l'identifiant de salle* — le secret de salle est le seul facteur d'authentification. Les participants Aionda authentifies echangent en outre un jeton de signalisation signe et limite au compte (Section 12.8).

12.6 Chiffrement des medias (SFrame, RFC 9605)

Chaque piste media est chiffrée trame par trame **avant** d'atteindre la SFU. Le cycle de vie de la cle :

```

MLS group secret
  | MLS Exporter (RFC 9420 §8)
  v
SFrame base key
  | HKDF(base_key, KID = sender || epoch)
  v
per-sender key
  | AES-256-GCM(nonce = frame counter, aad = sframe_header)
  v
per-frame ciphertext || tag    -> wire = sframe_header || ciphertext || tag

```

- La cle SFrame est derivee de l'**exportateur MLS**, donc elle n'existe que sur les membres authentifies du groupe — jamais sur le serveur.
- Le chiffrement s'exécute dans un Worker RTCTransform dedie (l'API standardisee Encoded-Transform, disponible dans Chromium et Safari/WebKit), de sorte que les trames sont scellees sur la pipeline media du navigateur.
- Le codec est VP8 ; la SFU effectue le routage des keyframes uniquement sur les meta-donnees — elle n'inspecte jamais la charge utile chiffrée.

12.7 Protection contre le rejeu

Chaque trame chiffrée porte un **compteur** SFrame monotone dans son en-tête authentifié, et est liée à l'époque MLS courante. Les récepteurs suivent le compteur le plus élevé vu par émetteur (un magasin de compteurs côté réception persistant). Une trame avec un compteur dupliqué ou régresse, ou liée à une époque périmée, est rejetée — un texte chiffré capturé ne peut pas être rejoué dans la session.

12.8 Signalisation et modèle d'accès

- **La signalisation** s'effectue sur un WebSocket authentifié (`aionda_signaling`). Chaque session est protégée par un **JWT** à courte durée de vie, émis par le serveur applicatif après que le client a échangé le secret de la salle via l'API chiffrée /e (voir Section 8). Le jeton est symétrique (HS256) et n'est valide qu'entre le serveur applicatif et l'unique service de signalisation ; il autorise l'établissement de la session et ne transporte jamais de médias ni de secrets de groupe. Le serveur de signalisation relaie les messages MLS Welcome/Commit mais ne peut pas les lire.
- **Lien de salle = justificatif au porteur.** Quiconque détient le lien complet (UUID de salle + secret du fragment) peut rejoindre — le modèle est intentionnellement « celui qui a le lien ». Les identifiants de base de données ne sont jamais exposés ; les salles sont adressées uniquement par des UUID non devinables.
- **Contrôle par le propriétaire.** Le propriétaire de la salle (vérifié côté serveur par la propriété du compte) peut marquer une salle comme *terminée* pour bloquer les futures connexions, et peut retirer un participant présent via un MLS Remove-Commit (Section 12.4).

12.9 Ce que la SFU / le serveur voit — et les limites des métadonnées

L'infrastructure PEUT voir	L'infrastructure NE PEUT PAS voir
Tailles des trames chiffrées, timing, métadonnées de routage	Le contenu audio ou vidéo (les trames sont scellées par AES-256-GCM)
Texte chiffré du handshake MLS (Welcome/Commit)	Les secrets de groupe ou les clés SFrame (dérivées côté client depuis l'exportateur MLS)
UUID de salle, nombre de participants, sujet du JWT	Le secret du lien de salle (réside dans le fragment d'URL)
Candidats ICE / adresses de transport	Tout texte en clair qui lui permettrait de rejoindre ou déchiffrer la session

Métadonnées que le système ne cache pas intentionnellement : les adresses IP exposées à l'infrastructure ICE / STUN / TURN, le timing des paquets, les tailles des paquets, le nombre de participants et la durée de l'appel. La résistance à l'analyse de trafic n'est pas un objectif de conception (Section 12.1).

12.10 Propriétés de sécurité (résumé)

Propriété	Garantie
Confidentialité	Seuls les membres actuels du groupe MLS possèdent les clés SFrame.

Propriete	Garantie
Authentification	Tous les messages MLS sont signes avec ML-DSA-65 ; le groupe est lie au secret de salle via la SAS epinglee.
Forward secrecy	La compromission des secrets actuels ne revele pas les medias passes.
Post-compromise security	Le renouvellement des clees restaure la confidentialite apres le retrait d'un membre.
Independance du serveur	La compromission du serveur de signalisation, de la SFU ou du stockage n'expose pas les medias.
Post-quantique	L'etablissement du groupe repose sur le KEM hybride X-Wing (ML-KEM-768 + X25519).

Ces proprietes decrivent la *conception* du protocole. Un audit cryptographique independant par un tiers du sous-systeme d'appel est prevu ; tant qu'il n'est pas publie, les garanties ci-dessus constituent une auto-evaluation.

13. Taches Aionda - Gestion de taches chiffree de bout en bout

Aionda Mail integre un gestionnaire de taches chiffre : listes de taches, sous-taches, notes, echeances, rappels et taches recurrentes. Il suit les memes regles zero-knowledge que la boite aux lettres. Tout ce que l'utilisateur ecrit est chiffre dans le navigateur ; le serveur ne stocke que du chiffre, plus un petit ensemble de champs de planification volontairement laisses en clair.

13.1 Une cle par tache

Chaque tache et chaque liste de taches recoit sa propre cle de 32 octets (AES-256-GCM), generee dans le navigateur avec le generateur d'aleas de l'API WebCrypto. Les champs de contenu sont chiffres avec cette cle ; la cle elle-meme est ensuite enveloppee avec la cle maitresse du coffre :

```

cle de tache aleatoire de 32 octets
  | AES-256-GCM, IV de 96bits frais pour chaque champ
  v
encrypted_title / encrypted_notes / encrypted_steps / encrypted_metadata

cle maitresse du coffre
  | HKDF-SHA-256(salt = 32 octets aleatoires, info = "trashmail-tasks-v1")
  v
cle d'enveloppement
  | AES-256-GCM
  v
wrapped_key = version(1) || salt(32) || IV(12) || chiffre || tag

```

Le serveur ne stocke que wrapped_key et les colonnes chiffrees. Il ne recoit ni la cle de tache, ni la cle maitresse, ni aucun texte en clair. Sans la cle maitresse, qui ne quitte jamais le navigateur, la cle enveloppee ne peut pas etre ouverte.

Separation de domaine. L'étiquette HKDF `trashmail-tasks-v1` est propre au module de tâches. Sans une telle étiquette, une clé enveloppée produite par un autre module (agenda, contacts) serait interchangeable avec une clé de tâche. L'étiquette lie chaque clé enveloppée au module qui l'a créée.

Dechiffrement independant. Les tâches et les listes sont déchiffrées une par une. Un enregistrement illisible est journalisé et ignoré au lieu de faire échouer toute la vue : un chiffrement endommagé ne peut donc pas priver l'utilisateur de ses autres tâches.

13.2 Ce qui est chiffré

Champ	Contenu	Protection
<code>encrypted_title</code>	Titre de la tâche	AES-256-GCM avec la clé de la tâche
<code>encrypted_notes</code>	Note en texte libre	AES-256-GCM avec la clé de la tâche
<code>encrypted_steps</code>	Tableau JSON des sous-tâches (texte et état d'achèvement)	AES-256-GCM avec la clé de la tâche
<code>encrypted_metadata</code>	JSON, y compris la règle de récurrence (RRULE)	AES-256-GCM avec la clé de la tâche
<code>encrypted_name</code>	Nom d'une liste de tâches	AES-256-GCM avec la clé de la liste

Chaque champ est scellé avec son propre IV de 96 bits frais : un même texte en clair ne produit jamais un même chiffre.

Les noms de listes sont eux aussi chiffrés. Une liste nommée "Acquisition Contoso" est du contenu, pas une métadonnée, et elle est traitée comme telle. Le serveur voit qu'un compte possède cinq listes, mais pas comment elles s'appellent.

13.3 Métadonnées volontairement en clair

Un petit ensemble de champs de planification est stocké en clair, afin que le serveur puisse filtrer, trier, compter et déclencher les rappels sans rien déchiffrer :

Champ en clair	Objectif
Date d'échéance	Liste intelligente "Planifie", détection des retards, tri
Heure de rappel	Déclenchement du rappel au bon moment
Indicateur "important"	Liste intelligente "Important"
Indicateur "termine" et heure d'achèvement	Séparation des tâches ouvertes et terminées
Date "Ma journée"	Liste intelligente "Ma journée", valable uniquement pour le jour courant
Position	Tri manuel à l'intérieur d'une liste
Rattachement à une liste (UUID)	Regroupement des tâches sous leur liste
E-mail lié (UUID)	Référence vers l'e-mail à l'origine de la tâche

Le serveur apprend quand quelque chose est du, jamais de quoi il s'agit. Il peut constater qu'un compte compte quatorze tâches ouvertes, dont trois pour le 3 août et une marquée comme importante. Il ne peut lire aucun titre, aucune note, aucune sous-tâche, aucune règle de récurrence et aucun nom de liste.

C'est le même compromis que celui déjà accepté pour les horaires des rendez-vous de l'agenda, et il est exposé plutôt que dissimulé. L'alternative - chiffrer aussi la date d'échéance - obligerait le client à télécharger et déchiffrer l'intégralité des tâches pour chaque filtre, chaque compte et chaque rappel. Les champs de planification ne portent aucun contenu, et les objets auxquels ils appartiennent ne sont adressés que par UUID.

13.4 La liste "E-mail marquée"

La liste "E-mail marquée" n'est pas un second entrepôt de données. C'est une vue sur l'étoile qui existe déjà sur les e-mails de la boîte aux lettres : aucune donnée en clair supplémentaire n'est créée pour elle.

Les objets affichés dans cette liste sont déchiffrés exclusivement côté client, via le chemin de déchiffrement habituel des e-mails (Section 7.2) : la clé de l'e-mail concerne est déballée dans le navigateur et l'objet y est déchiffré. Le module de tâches ne manipule jamais une clé d'e-mail et ne demande jamais un objet au serveur.

13.5 Transport, adressage et mode supervision

- **Transport chiffré.** Tous les points d'entrée des tâches passent par la couche de transport chiffré /e (Section 8). Requête et réponse sont scellées avec le KEM hybride : un CDN ou tout autre intermédiaire ne voit qu'un POST /e avec une charge utile opaque, et non quelle tâche a été créée, renommée ou terminée.
- **Uniquement des UUID.** Les tâches, les listes et les e-mails liés sont adressés exclusivement par UUID. Les identifiants internes de base de données ne sont jamais exposés, ce qui supprime l'énumération comme voie d'attaque.
- **Mode supervision.** Lorsqu'un propriétaire administre la boîte d'un collaborateur ou d'un agent IA, le module de tâches applique la même séparation des clés que le reste du coffre : les clés de tâche sont enveloppées avec la clé maîtresse du contexte supervisé, et non avec celle du propriétaire. Si cette clé de contexte n'est pas disponible, l'opération échoue franchement. Aucun repli sur la clé du propriétaire n'est prévu, et c'est délibéré - un repli silencieux écrirait les tâches d'un collaborateur avec la mauvaise clé. Il s'agirait d'un affaiblissement cryptographique, et un affaiblissement doit échouer bruyamment plutôt que réussir en silence.

13.6 Validation des entrées contre la troncature silencieuse

La longueur de chaque bloc chiffré est vérifiée côté serveur avant écriture :

Champ	Limite
Titre de tâche, nom de liste	2 048 octets
Note	1 Mio
Sous-tâches	256 Kio
Metadonnées	256 Kio
Clé enveloppée	60 à 1 700 octets

Les valeurs trop grandes sont rejetées avec une erreur explicite. Il s'agit d'un contrôle d'intégrité

aux consequences directes sur la confidentialite : selon son mode SQL, la base de donnees tronquerait sinon silencieusement une valeur trop grande. Un chiffre AES-GCM tronque echoue a l'authentification et son contenu devient definitivement illisible, y compris pour l'utilisateur. Refuser l'écriture est le seul comportement sur.

13.7 Ce que le serveur voit - et ce qu'il ne voit pas

Le serveur PEUT voir	Le serveur NE PEUT PAS voir
Dates d'echeance, heures de rappel, dates "Ma journee"	Titres des taches, notes, sous-taches
Indicateurs "important" et "termine", heure d'achevement	Le nom d'une liste de taches
Nombre de taches et de listes, leur ordre et leur regroupement	Regles de recurrence et toutes les autres metadonnees
L'UUID d'un e-mail lie	Le contenu ou l'objet de cet e-mail
Tailles des chiffres, dates de creation et de modification	Tout materiel de cle - cles de tache, de liste et cle maitresse

14. Protections contre les canaux auxiliaires

14.1 Bucket Padding

Problematiche : les tailles des e-mails chiffres peuvent reveler des informations. Un attaquant observant les longueurs de texte chiffre pourrait en deduire le contenu (par exemple, un e-mail de 50 octets est probablement « OK, merci » tandis qu'un e-mail de 500 Ko contient des pieces jointes).

Solution : toutes les donnees sont remplies jusqu'a des « buckets » de taille fixe avant le chiffrement :

Bucket sizes: 256B, 512B, 1KB, 2KB, 4KB, 8KB, 16KB, 32KB,
64KB, 128KB, 256KB, 512KB, 1MB, 2MB, 4MB, 8MB, 16MB

Format: [0xDEAD magic][4-byte length][actual data][random padding to bucket boundary]

Exemple : un e-mail de 523 octets est rempli jusqu'a 1 024 octets. Un observateur ne voit qu'un « e-mail de 1 Ko » — pas la taille réelle de 523 octets.

14.2 Compression avant chiffrement

Les donnees sont compressees avec gzip (niveau 6) **avant** le chiffrement. C'est le seul ordre correct :

- La compression apres le chiffrement echouerait (les donnees chiffrees ont une entropie maximale)
- Le Bucket Padding apres la compression empeche les attaques de type CRIME/BREACH qui exploitent les taux de compression

14.3 Confidentialite du regroupement

Les fils d'e-mails utilisent des hachages SHA-256 des en-tetes Message-ID au lieu d'identifiants en clair. Le serveur peut regrouper les e-mails lies par egalite de hachage sans connaitre les

identifiants de messages reels.

15. Gestion et cycle de vie des clés

15.1 Hierarchie des clés

Vault Master Key (32 bytes, generated once per account)

```

|
|--- Vault Keypair (Hybrid KEM)
|   |-- X25519 public key (32 bytes) – stored plaintext on server
|   |-- X25519 private key (32 bytes) – encrypted with master key
|   |-- ML-KEM-1024 public key (1568 bytes) – stored plaintext on server
|   |-- ML-KEM-1024 private key (3168 bytes) – encrypted with master key
|
|--- Per-Email Ephemeral Keys (32 bytes each)
|   |-- Wrapped with recipient's Hybrid KEM public keys
|
|--- Per-Attachment Ephemeral Keys (32 bytes each)
|   |-- Wrapped independently per attachment
|
|--- Folder Keys (derived via HKDF per folder)
|   |-- Shared via Hybrid KEM encapsulation per recipient
|
|--- Signature Encryption Key (derived from master key)
|   |-- Encrypts email signature templates

```

15.2 Stockage des clés

Cle	Emplacement de stockage	Protection
Cle maitre	Nulle part (reconstruite a la demande a partir des parts Shamir)	Shamir 2-of-3
Cles privees du coffre-fort	Serveur (chiffrees)	AES-256-GCM avec cle maitre
Cles publiques du coffre-fort	Serveur (en clair)	Non sensibles — publiques par definition
Cles ephemeres d'e-mail	Serveur (encapsulees)	Encapsulation Hybrid KEM
Enregistrements OPAQUE	Serveur (chiffres au repos)	AES-256-GCM avec cle serveur
Parts Shamir chiffrees	Serveur	XOR avec les cle derivees du mot de passe/passkey/recuperation

Cle	Emplacement de stockage	Protection
Cles de transport API	Serveur (pool pre-generé)	Usage unique, durée de vie 24h

15.3 Empreintes de clés

Chaque paire de clés du coffre-fort possède une empreinte SHA-256 stockée sur le serveur. Cela permet :

- Une piste d'audit des rotations de clés
- La détection de changements de clés non autorisés
- La vérification de l'intégrité des clés côté client

16. Mécanisme de récupération

16.1 Cle de récupération (mnémonique BIP39)

Lors de la configuration du coffre-fort, l'utilisateur reçoit une **phrase de récupération de 24 mots** générée à partir de 256 bits d'entropie, encodée selon le standard BIP39 :

Exemple: apple river mountain sunset golden bridge falcon ocean
 crystal thunder meadow silver dolphin forest marble castle
 velvet compass harbor window ancient pepper rocket shield

16.2 Derivation de la cle de récupération

1. Generate: 256 bits random entropy
2. Encode: BIP39 mnemonic (24 words, 11 bits per word)
3. Derive: `verificationKey = HKDF-SHA3-256(entropy, salt = accountId, info = "trashmail-recovery-verify")`
4. Hash: `verificationHash = SHA3-256(verificationKey)`
5. Store: Server stores ONLY verificationHash (32 bytes)

16.3 Ce que le serveur stocke

Le serveur ne stocke **que le hachage SHA3-256** d'une clé de vérification dérivée. Il ne stocke pas :

- Les mots de récupération
- L'entropie
- La clé de vérification elle-même

16.4 Processus de récupération

1. L'utilisateur saisit la phrase de récupération de 24 mots
2. Le client dérive l'entropie -> HKDF-SHA3-256 -> SHA3-256 -> hachage de vérification
3. Le client envoie le hachage de vérification au serveur (jamais la clé en clair)

4. Le serveur compare avec le hachage stocke
5. En cas de correspondance : toutes les methodes 2FA sont desactivees, l'utilisateur configure une nouvelle authentication
6. La cle de recuperation est revoquee apres un seul usage

16.5 Limitation de debit

- Maximum 3 tentatives de verification par heure
- Verrouillage de 60 minutes apres depassement de la limite
- Usage unique : la cle de recuperation est definitivement revoquee apres une utilisation reussie

16.6 Pas de recuperation de mot de passe

Il n'y a pas de reinitialisation du mot de passe par e-mail. Si un utilisateur perd son mot de passe ET tous les autres facteurs d'authentification (passkey + cle de recuperation), ses donnees sont definitivement inaccessibles. C'est une decision de conception intentionnelle qui prouve l'integrite du modele Zero-Knowledge — si le serveur pouvait recuperer les donnees, il pourrait aussi les lire.

17. Authentification sans mot de passe (Passkeys)

17.1 Extension WebAuthn PRF

Aionda Mail prend en charge les passkeys FIDO2 (cles de securite materielles, authenticateurs biometriques) pour la connexion sans mot de passe et le deverrouillage du coffre-fort.

L'**extension WebAuthn PRF (Pseudo-Random Function)** fournit une sortie deterministe de 32 octets liee a la passkey et au credential specifiques. Cette sortie est utilisee pour proteger la Part Shamir 2.

17.2 Fonctionnement

1. Registration:
 - User creates passkey via `navigator.credentials.create()`
 - PRF extension generates hardware-bound output
 - Output XOR'd with Shamir Share 2 -> encrypted share stored on server
2. Authentication:
 - User authenticates with passkey (biometric/PIN)
 - PRF extension reproduces same 32-byte output
 - Output XOR'd with encrypted share -> Shamir Share 2 recovered
 - Combined with Share 1 (password) -> Master Key reconstructed
3. Vault Unlock (passwordless):
 - If both passkey (Share 2) and password (Share 1) available -> immediate unlock
 - Password verified via OPAQUE (separate from passkey auth)

17.3 Passkeys multiples

Les utilisateurs peuvent enregistrer plusieurs passkeys (par exemple, Touch ID MacBook, Face ID iPhone, YubiKey). Chaque passkey protege independamment sa propre copie de la Part 2.

Une seule passkey combinee au mot de passe suffit a deverrouiller le coffre-fort.

18. Guardian : protection MITM & signature des reponses

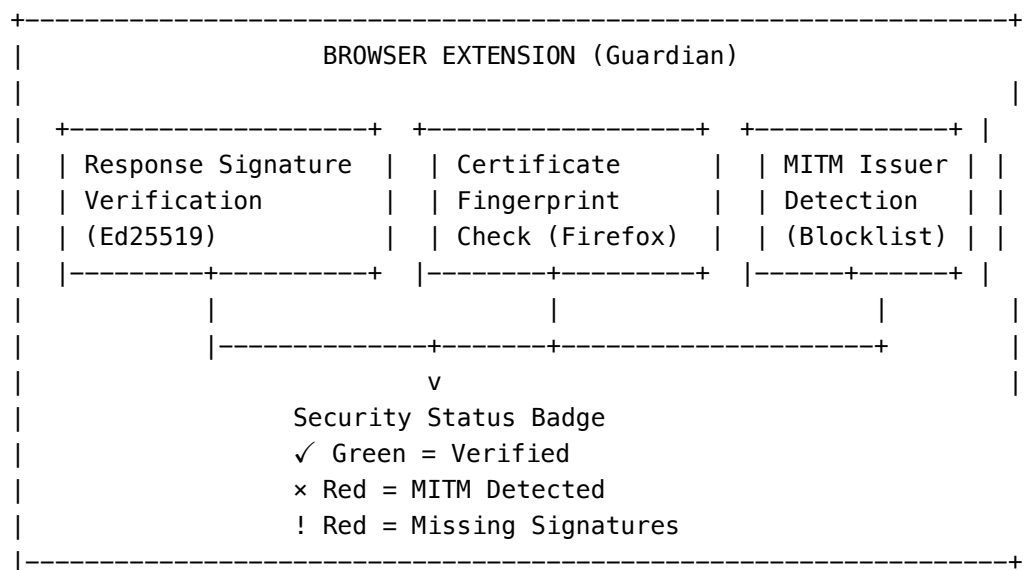
18.1 Le probleme des applications web

Toute application web a un probleme de confiance inherent : le navigateur telecharge du JavaScript depuis le serveur a chaque visite. Un attaquant de type « homme du milieu » (MITM) — qu'il s'agisse d'un CDN compromis, d'un proxy d'entreprise ou d'un FAI malveillant — pourrait theoriquement injecter du code modifie qui exfiltre les cle de chiffrement.

Aionda Mail répond a ce probleme avec le **module Guardian**, un composant d'extension de navigateur (disponible pour Chrome et Firefox) qui verifie independamment l'integrite du serveur.

18.2 Vue d'ensemble de l'architecture

Le module Guardian fonctionne au sein du Service Worker de l'extension de navigateur — complètement independant du JavaScript de l'application web. Il effectue trois types de verification :



18.3 Verification de la signature des reponses (Ed25519)

Chaque reponse API du serveur d'Aionda Mail est signee cryptographiquement a l'aide d'**Ed25519** (Edwards-curve Digital Signature Algorithm).

Processus de signature (cote serveur) :

1. Server generates API response body (JSON)
2. Construct signing input: responseBody + "|" + unixTimestamp
3. Sign with Ed25519 private key -> 64-byte signature
4. Attach HTTP headers:
X-Aionda-Signature: <base64(signature)>
X-Aionda-Timestamp: <unix_timestamp>
X-Aionda-Key-Id: <key_identifier>

Processus de verification (extension de navigateur) :

1. Extract signature, timestamp, and key ID from HTTP headers
2. Look up Ed25519 public key by key ID (bundled in extension)
3. Verify key has not expired (valid_from / valid_until)
4. Check timestamp freshness: $|\text{now} - \text{timestamp}| \leq 300$ seconds
5. Reconstruct signing input: responseBody + "|" + timestamp
6. crypto.subtle.verify("Ed25519", publicKey, signature, data)
7. If invalid -> MITM alert, red badge

Proprietes essentielles :

- **Protection contre la relecture** : la fenetre de 5 minutes sur l'horodatage empeche la relecture d'anciennes reponses
- **Detection d'alteration** : toute modification du corps de la reponse invalide la signature
- **Isolation des cles** : les cles publiques sont integrees dans l'extension (non telechargees depuis le serveur)
- **Separation des environnements** : les cles de developpement (dev-2026-01) ne peuvent pas etre utilisees sur les URL de production et vice versa

18.4 Gestion des cles publiques Ed25519

Les cles publiques sont distribuees avec l'extension de navigateur dans public_key.json :

```
{
  "keys": {
    "prod-2026-01": {
      "algorithm": "Ed25519",
      "public_key": "<base64 SPKI DER>",
      "valid_from": "2026-01-13T00:00:00Z",
      "valid_until": "2027-01-13T00:00:00Z"
    }
  }
}
```

- **Format de cle** : SPKI DER (Subject Public Key Info, Distinguished Encoding Rules)
- **Taille de cle** : 32 octets (cle publique Ed25519 de 256 bits)
- **Taille de signature** : 64 octets (fixe)
- **Rotation** : de nouvelles cles sont ajoutees avant l'expiration des anciennes ; les mises a jour de l'extension livrent les nouvelles cles
- **Aucune confiance envers le serveur** : les cles sont integrees dans le binaire de l'extension, non recuperees depuis le serveur

18.5 Verification des certificats TLS (Firefox)

Sur Firefox, le module Guardian effectue une verification supplementaire des certificats TLS a l'aide de l'API `browser.webRequest.getSecurityInfo()` (non disponible sur Chrome en raison des limitations de Manifest V3).

Flux de verification :

1. Browser extension intercepts HTTPS response
2. Extract TLS certificate chain from browser's security info:
 - Leaf certificate fingerprint (SHA-256)

- Issuer Distinguished Name (O=, CN=)
 - Subject (CN=)
3. Check against known MITM issuers (hardcoded blocklist):
ZScaler, Netskope, Fortinet, Palo Alto, Blue Coat,
Check Point, Barracuda, Sophos, WatchGuard, Cisco Umbrella
-> If match: MITM detected, show warning
 4. Check against trusted issuers:
Google Trust Services, Cloudflare, Let's Encrypt,
DigiCert, Sectigo
-> If match AND subject matches expected domain: OK
 5. If unknown issuer: Fetch server's own certificate fingerprint
 - Server connects to itself via external routing (prevents spoofing)
 - Response is Ed25519 signed (prevents MITM from lying about cert)
 - Compare issuer organization with browser's certificate issuer
 - > If mismatch: MITM suspected, show warning

Pourquoi la validation basee sur l'emetteur plutot que le pinning ? CloudFlare (utilise comme CDN) effectue une rotation des certificats feuille entre les serveurs de bordure. Le pinning de certificat traditionnel (correspondance exacte des empreintes) provoquerait des faux positifs. La validation basee sur l'emetteur est plus robuste : l'autorite de certification emettrice est stable meme lorsque les certificats feuille changent.

18.6 Recuperation automatique du certificat (anti-usurpation)

Le point d'entree de certificat du serveur utilise une technique anti-usurpation ingenieuse :

Server connects to cert.trashmail.com (or cert-subdomain.domain)
with SNI = mail.aionda.com

- > Forces external routing through CloudFlare
- > Receives the actual certificate that users see
- > Prevents localhost spoofing
- > Response signed with Ed25519 to prevent tampering

Le serveur demande essentiellement « quel certificat le monde exterieur voit-il pour mon domaine ? » — et signe la reponse pour que l'extension puisse lui faire confiance.

18.7 Indicateurs d'etat de securite

L'extension affiche un badge dans la barre d'outils du navigateur :

Badge	Couleur	Signification
✓	Vert	Toutes les reponses verifiees — signatures valides
!	Orange	Utilisation d'une cle de signature obsolete (rotation en attente)
×	Rouge	MITM detecte — echec de la verification de signature

Badge	Couleur	Signification
!	Rouge	Signatures manquantes — réponses non signées
[Shield]	Bleu	Mode protege — aucune verification effectuee pour l'instant

18.8 Couverture des menaces

Attaque	Methode de detection	Navigateur
Proxy MITM d'entreprise (ZScaler, Fortinet)	Liste de blocage des emetteurs de certificats	Firefox
Reponses API modifiees	Verification de signature Ed25519	Chrome + Firefox
Attaques par relecture	Fenetre d'horodatage de 5 minutes	Chrome + Firefox
Compromission du CDN (CloudFlare)	Discordance de la signature de reponse	Chrome + Firefox
Substitution de certificat	Comparaison de l'emetteur + auto-verification du serveur	Firefox
Confusion cles dev/prod	Identifiants de cles lies a l'environnement	Chrome + Firefox

18.9 Limites

- **Chrome Manifest V3** : impossible d'inspecter les certificats TLS — seule la verification de signature de reponse est disponible
- **Extension requise** : les utilisateurs sans l'extension ne beneficent pas des protections Guardian
- **Ed25519 n'est pas post-quantique** : la verification de signature utilise la cryptographie classique. Un ordinateur quantique suffisamment puissant pourrait theoriquement forger des signatures Ed25519.

19. Archive e-mail d'entreprise (Blockchain)

19.1 Vue d'ensemble

Le plan Entreprise d'Aionda Mail inclut une **archive e-mail conforme GoBD** securisee par une chaine de hachage cryptographique (blockchain). Chaque e-mail archive devient un bloc immuable dans une chaine propre a l'entreprise. Toute alteration — modification, suppression ou insertion de blocs — est detectee cryptographiquement.

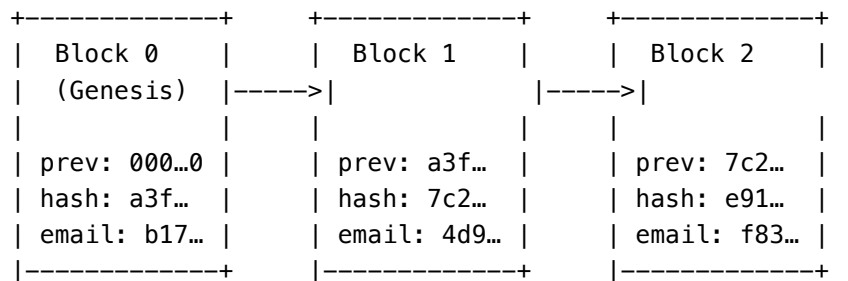
L'archive combine deux couches de securite independantes :

1. **Chaine de hachage (SHA3-256)** : garantit l'integrite et l'immutabilite — prouve qu'aucun e-mail n'a ete modifie ou supprime apres l'archivage

2. **Chiffrement Hybrid KEM (CAK)** : garantit la confidentialite — le serveur ne peut pas lire le contenu des e-mails archives

19.2 Architecture de la chaine de hachage

Chaque e-mail archive devient un bloc dans une chaine sequentielle et inviolable :



Calcul du hachage de bloc :

```
block_hash = SHA3-256(
    prev_block_hash || "|" ||
    timestamp       || "|" ||
    email_hash       || "|" ||
    direction        || "|" ||
    sender_domain    || "|" ||
    recipient_domain
)
```

Proprietes :

- **Algorithme de hachage** : SHA3-256 (NIST FIPS 202)
- **Bloc de genese** : prev_block_hash = 64 zeros, block_number = 0
- **Numerotation sequentielle** : imposee par la contrainte UNIQUE KEY (company_uuid, block_number) en base de donnees
- **Une chaine par entreprise** : isolation complete entre les entreprises
- **Hachage de l'e-mail** : SHA3-256(sender || recipient || timestamp || size) — preuve d'integrite des donnees originales de l'e-mail

19.3 Detection d'alteration

L'algorithme de verification de la chaine detecte toute forme d'alteration :

For each block (ordered by block_number ASC):

1. Verify link: block.prev_block_hash == expected_prev_hash
2. Recalculate: expected = SHA3-256(prev_hash | timestamp | email_hash | ...)
3. Verify content: block.block_hash == expected
4. Advance: expected_prev_hash = block.block_hash

If ANY check fails -> chain is broken at block N

Tentative d'alteration	Detection
Modifier le contenu de l'e-mail	email_hash change -> echec du recalcul de block_hash
Modifier les metadonnees (expediteur, domaine, horodatage)	Incluses dans l'entree du hachage -> discordance de block_hash
Supprimer un bloc	Le prev_block_hash du bloc suivant devient orphelin
Inserer un bloc	Romp le block_number sequentiel + la chaine prev_block_hash
Reordonner les blocs	La contrainte UNIQUE KEY + la verification sequentielle l'empechent
Remplacer toute la chaine	Le hachage du bloc de genese differerait de toute sauvegarde externe

Le resultat de verification indique le numero exact du bloc ou l'alteration a ete detectee, avec les valeurs de hachage attendues et reelles pour l'analyse forensique.

19.4 Cle d'archive d'entreprise (CAK) — Chiffrement Zero-Knowledge

Le contenu de l'archive est chiffre de bout en bout a l'aide d'une **cle d'archive d'entreprise** — une paire de cles Hybrid KEM (X25519 + ML-KEM-1024) generee cote client par le proprietaire de l'entreprise.

Company Owner's Browser

Server

1. Generate Hybrid KEM keypair (client-side):
X25519 keypair (32 + 32 bytes)
ML-KEM-1024 keypair (1568 + 3168 bytes)
2. Derive wrapping key from password:
wrappingKey = HKDF-SHA256(
password,
salt = "trashmail-archive-{account_id}",
info = "trashmail-archive-key-wrap",
length = 32
)
3. Wrap private keys:
AES-256-GCM(x25519_priv || mlkem_priv, wrappingKey)
4. Send to server:
 - Public keys (plaintext)
 - Wrapped private keys (encrypted)

→ Store:
archive_x25519_pub
archive_mlkem_pub

wrapped_archive_key

Distribution de la cle aux autres employes (Administrateur, Responsable conformite) :

1. Le proprietaire dechiffre les cles privees CAK avec son mot de passe
2. Le proprietaire re-encapsule les cles privees avec la cle derivee du mot de passe de l'employe cible
3. Le serveur stocke la copie re-encapsulee sur l'enregistrement de l'employe
4. Chaque employe autorise dispose de sa propre copie encapsulee independamment

Le serveur ne voit jamais les cles privees CAK en clair.

19.5 Ce qui est chiffre

Lorsqu'un e-mail est archive, deux couches de chiffrement sont appliquees :

Metadonnees chiffrees (AES-256-GCM avec Hybrid KEM) :

```
{
  "d": "INBOUND",
  "s": "user@example.com",
  "r": "admin@company.de",
  "sd": "example.com",
  "rd": "company.de",
  "sz": 45000,
  "ts": "2026-02-27T10:30:00Z",
  "ha": true,
  "ac": 3,
  "en": "John Doe"
}
```

Contenu de l'e-mail chiffre (encapsulation Hybrid KEM separee) :

```
{
  "subject": "Meeting notes",
  "body": "<html>...</html>",
  "from": "sender@domain.com",
  "to": "recipient@company.de"
}
```

Application Zero-Knowledge : apres le chiffrement, les champs de metadonnees en clair dans la base de donnees (sender_address, recipient_address, domaines) sont remplaces par leurs hachages SHA3-256. Le serveur ne stocke que des hachages — les valeurs originales n'existent que dans les blobs chiffres.

19.6 Piste d'audit

Chaque action sur l'archive est journalisee dans une **chaîne d'audit independante** (egalement enchainee par hachages SHA3-256) :

Action	Quand elle est journalisee
EMAIL_RECEIVED / EMAIL_SENT / DRAFT_ARCHIVED	E-mail archive
VIEW_EMAIL / VIEW_ATTACHMENT	Un employe lit un e-mail archive

Action	Quand elle est journalisee
SEARCH_ARCHIVE	Recherche effectuee
EXPORT_EMAIL / EXPORT_REPORT	Donnees exportees
VERIFY_CHAIN / CHAIN_VERIFIED_OK / CHAIN_VERIFIED_BROKEN	Verification d'integrite
LEGAL_HOLD_SET / LEGAL_HOLD_RELEASED	Mise en suspens juridique basculee
ARCHIVE_DECRYPT	CAK utilisee pour dechiffrer le contenu
ADMIN_ACCESS	Action administrative

Chaque entree d'audit enregistre : l'acteur (UUID + role), l'adresse IP, l'identifiant de session, le hachage de l'e-mail cible et si la chaine etait valide au moment de l'acces.

19.7 Mise en suspens juridique & retention

- **Duree de retention** : configurable par entreprise (par default : 10 ans), calculee par e-mail comme `archived_at + retention_years`
- **Mise en suspens juridique** : des e-mails individuels peuvent etre places sous mise en suspens juridique, empechant leur suppression jusqu'a la levee. Inclut le motif, l'acteur et l'horodatage.
- **Conformite GoBD** : la combinaison d'une chaine de hachage immuable, d'une piste d'audit complete, d'une retention configurable et d'une mise en suspens juridique satisfait les exigences du GoBD allemand (Grundsätze zur ordnungsmaessigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff).

19.8 Export forensique

Les utilisateurs autorises (Proprietaire, Administrateur) peuvent exporter l'etat complet de la chaine pour une verification independante :

- Donnees completes de la chaine avec tous les hachages de blocs
- Resultat de verification (valide/rompu, numero de bloc rompu le cas echeant)
- Valeurs de hachage attendues et reelles pour l'analyse forensique
- 50 dernieres entrees du journal d'audit
- Format JSON pour une re-verification externe avec toute implementation SHA3-256

20. Ce que le serveur voit — et ce qu'il ne voit pas

Cette section documente explicitement la frontiere Zero-Knowledge.

20.1 Le serveur PEUT voir

Donnees	Raison de la visibilite	Mesure d'attenuation
Adresse IP	Exigence TCP/IP	Utilisation d'un VPN/Tor possible si souhaite
Horodatages	Heure de reception de l'e-mail	Inherent au protocole e-mail
Blobs d'e-mails chiffres	Stockes pour la recuperation	Chiffres avec AES-256-GCM, cle inconnue du serveur
Tailles de texte chiffre rembourrees	Exigence de stockage	Le Bucket Padding masque les tailles reelles
Adresse DEA du destinataire	Exigence de routage	La DEA est jetable, ce n'est pas l'adresse reelle
Existence du compte	Flux d'authentification	Protection contre l'enumeration d'utilisateurs deployee
Cles publiques	Requises pour le chiffrement par le serveur	Publiques par definition, non sensibles
Parts Shamir chiffrees	Stockage pour l'utilisateur	XOR avec des cles que le serveur ne connait pas
Enregistrements OPAQUE	Protocole d'authentification	Pas des hachages de mots de passe, chiffres au repos

20.2 Le serveur NE PEUT PAS voir

Donnees	Raison de l'invisibilite
Contenu de l'e-mail (objet, corps, en-tetes)	Chiffre avec des cles ephemerres encapsulees via Hybrid KEM
Mot de passe de l'utilisateur	OPAQUE — le mot de passe n'est jamais transmis
Cle maitre	Reconstruite uniquement dans le navigateur a partir des parts Shamir
Cles privees du coffre-fort	Chiffrees avec la cle maitre avant le stockage
Cles ephemerres d'e-mail	Encapsulees avec Hybrid KEM, le serveur n'a pas les cles privees
Cle de recuperation / mnemonique	Seul le hachage SHA3-256 de la cle derivee est stocke
Sorties PRF de la passkey	Liees au materiel, ne quittent jamais l'authentificateur
Noms de dossiers	Chiffres avec des cles specifiques aux dossiers
Signatures d'e-mail	Chiffrees avec la cle maitre
Contenu des requetes API	Chiffre via la couche de transport /e
Contenu des reponses API	Chiffre avant la transmission

20.3 Garantie cryptographique

Meme avec un acces complet a :

- La base de donnees complete
- Tout le trafic reseau
- Le code source et la configuration du serveur
- Tous les enregistrements OPAQUE et les cle du serveur

...un attaquant **ne peut pas** dechiffrer un seul e-mail sans le mot de passe de l'utilisateur (ou la passkey + la cle de recuperation). Ce n'est pas une politique — c'est une impossibilite mathematique imposee par la conception cryptographique.

21. Reference des algorithmes

21.1 Tableau complet des algorithmes

Composant	Algorithme	Parametres	Standard
Authentification par mot de passe	OPAQUE	RFC 9807, aPAKE	RFC 9807
Derivation de cle de mot de passe	PBKDF2-SHA256	600 000 iterations, sel de 32 o, sortie de 32 o	NIST SP 800-132
Chiffrement du coffre-fort	AES-256-GCM	Cle de 256 bits, nonce de 96 bits, tag de 128 bits	NIST SP 800-38D
Echange de cle classique	X25519	Curve25519, 256 bits	RFC 7748
KEM post-quantique	ML-KEM-1024	Kyber-1024, NIST Level 5	NIST FIPS 203
Derivation de cle hybride	HKDF-SHA256	IKM de 64 o, info="trashmail-hybrid-kem-v1"	RFC 5869
Partage de secret	Shamir SSS	k=2, n=3, GF(2 ⁸)	Shamir (1979)
Encodage de la cle de recuperation	BIP39	Entropie de 256 bits, 24 mots	BIP-0039
Derivation de la cle de recuperation	HKDF-SHA3-256	Sel lie au compte	NIST FIPS 202
Verification de la cle de recuperation	SHA3-256	Sortie de 32 octets	NIST FIPS 202
Chiffrement des enregistrements OPAQUE	AES-256-GCM	Chiffrement au repos cote serveur	NIST SP 800-38D
Deverrouillage du coffre-fort par passkey	WebAuthn PRF	Base sur HMAC, lie au materiel	WebAuthn Level 2
Compression	gzip	Niveau 6	RFC 1952
Bucket Padding	Personnalise	17 tailles (256 o–16 Mo), magic 0xDEAD	—

Composant	Algorithme	Parametres	Standard
Signature des reponses	Ed25519	Cle de 256 bits, signature de 512 bits	RFC 8032
Chaine de hachage de l'archive	SHA3-256	Hachage par bloc, enchainement sequentiel	NIST FIPS 202
Encapsulation de cle d'archive (CAK)	HKDF-SHA256 + AES-256-GCM	Cle d'encapsulation derivee du mot de passe	RFC 5869 / NIST SP 800-38D
Verification de certificat	SHA-256	Comparaison d'empreinte de certificat TLS	—
Regroupement d'e-mails	SHA-256	Hachage du Message-ID	NIST FIPS 180-4
Cles de groupe d'appel video	MLS + X-Wing	Suite AIONDA_PQ_CALL_V1 (0xFF01), ML-KEM-768 + X25519	RFC 9420 / draft-connolly-cfrg-xwing-kem
Signatures d'appel video	ML-DSA-65	Dilithium, NIST Level 3	NIST FIPS 204
Medias d'appel video	SFrame (AES-256-GCM)	Par trame, cle issue de l'exportateur MLS	RFC 9605

21.2 Niveaux de securite

Algorithme	Securite classique	Securite post-quantique
X25519	128 bits	Casse par l'algorithme de Shor
ML-KEM-1024	Equivalent 256 bits	NIST Level 5 ($\approx$ AES-256)
AES-256-GCM	256 bits	128 bits (algorithme de Grover)
SHA-256	256 bits	128 bits (algorithme de Grover)
SHA3-256	256 bits	128 bits (algorithme de Grover)
Hybrid KEM (combine)	128 bits (borne X25519)	Level 5 (borne ML-KEM)

22. Comparaison avec d'autres fournisseurs

Fonctionnalite	Aionda Mail	Tuta Mail	Proton Mail
Pays	Allemagne (Stuttgart)	Allemagne (Hanovre)	Suisse
Zero-Knowledge	Oui (OPAQUE + cryptographie cote client)	Oui	Oui
Post-quantique	Oui (ML-KEM-1024 + X25519 hybride)	Oui (base sur Kyber)	En developpement

Fonctionnalite	Aionda Mail	Tuta Mail	Proton Mail
Protocole de mot de passe	OPAQUE (RFC 9807) — le mot de passe ne quitte jamais le navigateur	bcrypt (mot de passe envoye au serveur via TLS)	Base sur SRP
Objet chiffre	Oui	Oui	Non
En-tetes chiffres	Oui	Partiel	Non
Noms de contacts chiffres	Oui (dans le coffre-fort)	Oui	Non
Adresses e-mail jetables	Oui (fonctionnalite principale, illimitees pour Plus)	Non	Oui (via SimpleLogin)
Extension de navigateur	Oui (Chrome + Firefox)	Non	Via SimpleLogin
Partage de dossiers	Oui (Hybrid KEM par destinataire)	Limite	Oui
Client open source	Non	Oui	Oui
Audit de securite	Prevu	Oui	Oui
Recuperation de mot de passe	Non (par conception)	Non (par conception)	Non (par conception)
Support des passkeys	Oui (FIDO2 + PRF)	Oui	Oui
Support PGP	Oui (entrant + sortant)	Non (protocole propre)	Oui (OpenPGP)
Archive e-mail conforme GoBD	Oui (chaîne de hachage SHA3-256 + Hybrid KEM)	Non	Non
Detection MITM (ext. navigateur)	Oui (signatures Ed25519 + verification TLS)	Non	Non
Perfect Forward Secrecy (API)	Oui (cles ephemeres par requete)	Inconnu	Inconnu
Masquage de la taille des e-mails	Oui (Bucket Padding)	Inconnu	Non

23. Limites & transparence

23.1 Modele de confiance des applications web

Aionda Mail est une application web. A chaque chargement de page, le navigateur telecharge du JavaScript depuis les serveurs d'Aionda. Un attaquant sophistique qui compromettrait les serveurs pourrait theoriquement servir du JavaScript modifie qui exfiltrer les cles.

Mesures d'attenuation actuelles :

- Hachages d'integrite de sous-ressources (SRI) sur toutes les balises script
- En-tetes Content Security Policy (CSP) restreignant les sources de scripts
- Tout le code cryptographique critique est inclus dans le bundle principal de l'application

- **Extension de navigateur Guardian** (Section 18) : la verification des signatures Ed25519 sur toutes les reponses API detecte les alterations cote serveur ; la verification des certificats TLS (Firefox) detecte les proxys MITM

Mesures d'attenuation prevues :

- Mise en cache par Service Worker pour le fonctionnement hors ligne (reduit la frequence de confiance au chargement)

23.2 Visibilite des metadonnees

Bien que le contenu des e-mails soit entierement chiffre, certaines metadonnees sont visibles par le serveur :

- Quand les e-mails ont ete recus (horodatages)
- Quelle adresse DEA a reçu l'e-mail
- Taille approximative de l'e-mail (dans les limites des buckets)
- Schemas d'activite du compte

23.3 Journal de traitement des e-mails

A des fins de diagnostic, Aionda Mail inclut un **journal de traitement des e-mails** optionnel qui peut stocker temporairement le contenu brut des e-mails entrants. Cette fonctionnalite est configurable par adresse e-mail jetable (DEA) et peut etre activee ou desactivee dans les parametres de la DEA ("Journaliser le contenu des e-mails").

Lorsqu'il est active (par DEA) :

- Le message SMTP brut complet (en-tetes + corps) est stocke en clair sur le serveur
- Suppression automatique apres une courte periode de retention (moins de 7 jours)
- Accessible uniquement au proprietaire du compte via l'API authentifiee
- Objectif : depannage des problemes de livraison, verification du transfert, examen des decisions de filtrage anti-spam

Lorsqu'il est desactive :

- Aucun contenu d'e-mail n'est stocke dans le journal de traitement
- Seules les metadonnees sont journalisees (adresse de l'expediteur, horodatage, statut de livraison)
- Le chiffrement du coffre-fort reste le seul mecanisme de stockage

Important : Ce journal de traitement est independant du coffre-fort chiffre. Les e-mails stockes dans le coffre-fort sont toujours chiffres avec Hybrid KEM, quel que soit le parametre de journalisation. Le journal de traitement existe en tant que fonctionnalite heritee du systeme de transfert d'e-mails et offre une transparence operationnelle. Les utilisateurs necessitant un stockage strictement Zero-Knowledge pour tous les e-mails doivent desactiver cette option.

23.4 Securite des e-mails externes

Les e-mails envoyes ou recus depuis des adresses non-Aionda transitent par l'infrastructure de messagerie standard (SMTP). Bien qu'ils soient stockes chiffres dans le coffre-fort, le contenu de l'e-mail etait visible durant le transit, sauf si le chiffrement PGP etait utilise.

23.5 Pas de sequestre de clés

Il n'existe pas de clé maître, de porte dérobée ou de mécanisme de récupération disponible pour Aionda GmbH. Si un utilisateur perd son mot de passe et toutes les autres méthodes de récupération, ses données sont définitivement perdues. C'est une décision de conception intentionnelle qui prouve l'intégrité du modèle Zero-Knowledge.

24. Feuille de route

Jalon	Statut	Objectif
Architecture Zero-Knowledge	Termine	—
Hybrid KEM post-quantique (ML-KEM-1024)	Termine	—
Authentification OPAQUE (RFC 9807)	Termine	—
Shamir Secret Sharing (2-of-3)	Termine	—
Couche de transport API chiffrée	Termine	—
Support Passkey/WebAuthn PRF	Termine	—
Calendrier chiffré de bout en bout	Termine	—
Tâches chiffrées de bout en bout	Termine	—
Archive e-mail conforme GoBD (Blockchain)	Termine	—
Protection MITM Guardian (Ed25519)	Termine	—
Vérification des certificats TLS (Firefox)	Termine	—

Historique du document

Version	Date	Modifications
1.0	Mars 2026	Publication initiale
1.1	Avril 2026	Nouveau chapitre 10 : Vault Drive (architecture à clé par fichier, partage via re-enveloppement de clé)
1.2	Avril 2026	Section 10.11 : Partage externe — liens publics avec enveloppes KEM hybrides, flow unlock_token, mode mot de passe Argon2id, fragment URL pour link_only, chaîne d'audit infalsifiable (EXT_SHARE_*) et distribution du lien choisie par le propriétaire

Version	Date	Modifications
1.3	Mai 2026	Nouveau chapitre 11 : Aionda Chat — messagerie temps reel E2EE post-quantique via AAR (Aionda Async Ratchet), une variante hybride X25519 + ML-KEM-1024 du Signal X3DH + Double Ratchet. Forward secrecy par message, post-compromise security et integration a la chaine d'audit Enterprise. Chapitres suivants renumerotes 12-22. Traductions PT-BR et PT-PT ajoutees. Bug de double numerotation dans le rendu PDF corrige (numerotation auto LaTeX desactivee ; les numeros de chapitres proviennent uniquement des en-tetes).
1.4	juin 2026	Nouveau chapitre 12 : Appels video Aionda — visioconference de groupe E2EE post-quantique. Accord de cle de groupe MLS (RFC 9420) avec la suite cryptographique AIONDA_PQ_CALL_V1 (X-Wing = ML-KEM-768 + X25519, signatures ML-DSS-65), chiffrement des medias image par image AES-256-GCM SFrame (RFC 9605) avec cle derivee de l'exportateur MLS, liaison SAS, et un relais SFU a connaissance nulle. Chapitres suivants renumerotes 13-23.
1.5	juillet 2026	Nouveau chapitre 13 : Taches Aionda - gestion de taches chiffree de bout en bout. Cle AES-256-GCM par tache et par liste, enveloppees avec la cle maitresse du coffre (HKDF-SHA-256 avec separation de domaine propre au module), titres, notes, sous-taches, noms de listes et regles de recurrence chiffres, expose honnete des metadonnees de planification volontairement laissees en clair, liste des e-mails marques basee sur l'etoile existante, separation des cle en mode supervision et validation de longueur cote serveur contre la troncature silencieuse des chiffres. Chapitres suivants renumerotes 14-24.

Contact

Aionda GmbH Stephan Ferraro Stuttgart, Allemagne

Email: contact-46epp9ba@contact.aionda.com Web: <https://mail.aionda.com>

Ce document décrit l'architecture de sécurité d'Aionda Mail en date de juillet 2026. Les systèmes cryptographiques évoluent — ce document sera mis à jour au fur et à mesure que l'architecture change.