GUIDE TECHNIQUE

Tixeo 18.2 : comment fonctionne la protection post-quantique

Plateforme Tixeo, version 18.2 · 20 octobre 2026



Introduction

Avec la version 18.2, le chiffrement de bout en bout de Tixeo s'enrichit, dans le navigateur, d'une protection post-quantique : l'échange qui établit les clés d'une réunion combine le mécanisme classique déjà en place et ML-KEM-768, un mécanisme normalisé conçu pour résister aux ordinateurs quantiques. Cette protection s'applique à l'ensemble des flux de la réunion, s'active automatiquement et ne demande aucun réglage.

Établi avec la R&D de Tixeo, ce guide rassemble les éléments techniques qui permettent de comprendre ce que recouvre cette protection, comment elle fonctionne et où s'arrête son périmètre dans la version 18.2.

L'essentiel en six points

1. **Ce qui change** : l'établissement des clés d'une réunion devient **hybride**, X25519 + ML-KEM-768 (norme FIPS 203). Rien n'est remplacé : le mécanisme post-quantique s'ajoute au mécanisme classique.
2. **Pourquoi « protection » et non « chiffrement » post-quantique** : la menace quantique vise l'échange des clés, pas le chiffrement des flux. Les flux restent chiffrés en ChaCha20-Poly1305 avec une clé de 256 bits, déjà considéré comme résistant.
3. **Pourquoi l'hybridation** : le référentiel de l'ANSSI l'impose pour tout produit visant une sécurité post-quantique. La construction de Tixeo correspond au mode qu'il désigne comme le plus souhaitable, au niveau de paramètres qu'il préfère.
4. **Ce qui est protégé** : en réunion, l'audio, la vidéo, le partage d'écran, la messagerie instantanée et le transfert de fichiers ; dans les Workspaces, la messagerie, le stockage et le partage de fichiers. À condition que tous les participants soient connectés depuis un navigateur avec la version 18.2, quel que soit leur nombre.
5. **Portée par le moteur de Tixeo** : les outils de chiffrement intégrés aux navigateurs ne proposent aujourd'hui aucun mécanisme post-quantique. Tixeo n'en a pas besoin : ML-KEM-768 est intégré à son propre moteur cryptographique, qui s'exécute dans le navigateur.
6. **Sans réglage** : la protection est active par défaut, sans configuration ni option à activer.

1 Pourquoi une protection post-quantique, et pourquoi maintenant ?

Une menace qui commence avant l'ordinateur quantique

Aucun ordinateur quantique n'est aujourd'hui en mesure de casser les mécanismes de chiffrement en usage. Le risque est pourtant déjà présent, sous une forme que les spécialistes nomment *harvest now, decrypt later* : collecter aujourd'hui des communications chiffrées, les conserver, et attendre de disposer de la puissance de calcul nécessaire pour les déchiffrer.

Le risque concerne d'abord les organisations dont les échanges doivent rester confidentiels pendant des décennies.

Ce que l'ordinateur quantique menace, et ce qu'il ne menace pas

Deux algorithmes quantiques structurent le sujet :

- **l'algorithme de Shor** casse la cryptographie asymétrique (RSA, échange Diffie-Hellman, courbes elliptiques), celle qui sert à établir et à authentifier les clés. C'est là que se concentre le risque réel ;
- **l'algorithme de Grover** affaiblit la cryptographie symétrique, celle qui chiffre les flux, mais ne fait que diviser par deux sa robustesse effective. Une clé de 256 bits conserve un niveau de sécurité de 128 bits, considéré comme suffisant.

La conséquence est directe : pour protéger une communication contre la menace quantique, c'est l'établissement des clés qu'il faut renforcer.

Un calendrier désormais fixé

Date	Étape
Août 2024	Le NIST publie la norme **FIPS 203**, qui standardise ML-KEM, mécanisme d'encapsulation de clé post-quantique
20 mars 2026	L'ANSSI publie la version 3.00 de son référentiel sur les mécanismes cryptographiques (**ANSSI-PG-083**), qui fixe les règles d'hybridation
16 juin 2026	L'ANSSI annonce qu'à partir de **2027**, elle ne certifiera plus les produits de sécurité dépourvus de mécanismes résistants au quantique, et fixe à **2030** l'horizon auquel les organisations concernées devront n'employer que des solutions résistantes
2030 et 2035	Échéances de la transition post-quantique fixées par la feuille de route européenne (groupe de coopération NIS)

La version 18.2 s'inscrit dans cette trajectoire : elle intègre la protection post-quantique avant que l'exigence de certification n'entre en vigueur.

2 Pourquoi parle-t-on de « protection » et non de « chiffrement » post-quantique ?

Une réunion chiffrée de bout en bout repose sur deux opérations distinctes.

L'établissement de la clé. Avant d'échanger le moindre contenu, les participants doivent convenir, sans jamais la transmettre en clair, de la clé qui protégera leurs échanges. Cette opération fait appel à la cryptographie asymétrique : c'est elle que l'algorithme de Shor menace, et c'est elle que la version 18.2 renforce.

Le chiffrement des flux. Une fois la clé établie, chaque échantillon audio, chaque image vidéo, chaque message et chaque fichier est scellé avec cette clé. Chez Tixeo, ce chiffrement repose sur **ChaCha20-Poly1305**, avec une clé de **256 bits** : un algorithme symétrique, que l'algorithme de Grover ne ramène qu'à 128 bits de sécurité. Il est donc déjà considéré comme résistant, et la version 18.2 ne le modifie pas.

D'où l'expression juste : un **chiffrement de bout en bout qui s'enrichit d'une protection post-quantique**. La protection porte sur l'échange qui établit les clés, et cet échange protège à son tour l'intégralité des flux.



Schéma 1 : les deux couches d'une réunion chiffrée de bout en bout

3 Comment fonctionne l'échange hybride ?

Une clé par participant

Dans une réunion Tixeo, chaque participant génère **sa propre clé de média**, celle qui scelle ce qu'il publie. Pour déchiffrer un interlocuteur, un participant va chercher la clé de celui-ci, directement auprès de lui, au moyen d'un échange de clés de pair à pair. Le serveur et le relais transportent ces échanges sans pouvoir en extraire les clés.

Deux mécanismes combinés

Avec la version 18.2, cet échange devient hybride. Deux mécanismes travaillent en parallèle, et chacun produit un secret partagé :

Composant	Mécanisme
Mécanisme classique	**X25519**, échange Diffie-Hellman sur courbe elliptique (Curve25519), éphémère par session
Mécanisme post-quantique	**ML-KEM-768**, mécanisme d'encapsulation de clé normalisé par la norme FIPS 203, éphémère par session
Combinaison	**HKDF-SHA-256**, fonction de dérivation de clé appliquée aux deux secrets, les clés publiques et les chiffrés des deux mécanismes étant liés dans le contexte de dérivation
Authentification de l'échange	**RSA-4096** (RSASSA-PKCS#1 v1.5 + SHA-256), signature liée au certificat de l'appareil, inchangée

La clé obtenue, qui protège la clé de média, est dérivée **des deux secrets à la fois**. Elle reste donc secrète tant que **l'un des deux** problèmes mathématiques résiste : celui des courbes elliptiques, sur lequel repose

X25519, ou celui des réseaux euclidiens, sur lequel repose ML-KEM. Un attaquant qui casserait l'un des deux mécanismes n'obtiendrait rien sans casser aussi l'autre.

Rien n'est remplacé, et **ML-KEM-768 n'est pas un algorithme de signature.** C'est un mécanisme d'encapsulation de clé, au niveau de sécurité 3 de la norme FIPS 203 : il sert à établir un secret partagé, rien d'autre. La signature de l'échange reste assurée par RSA-4096.

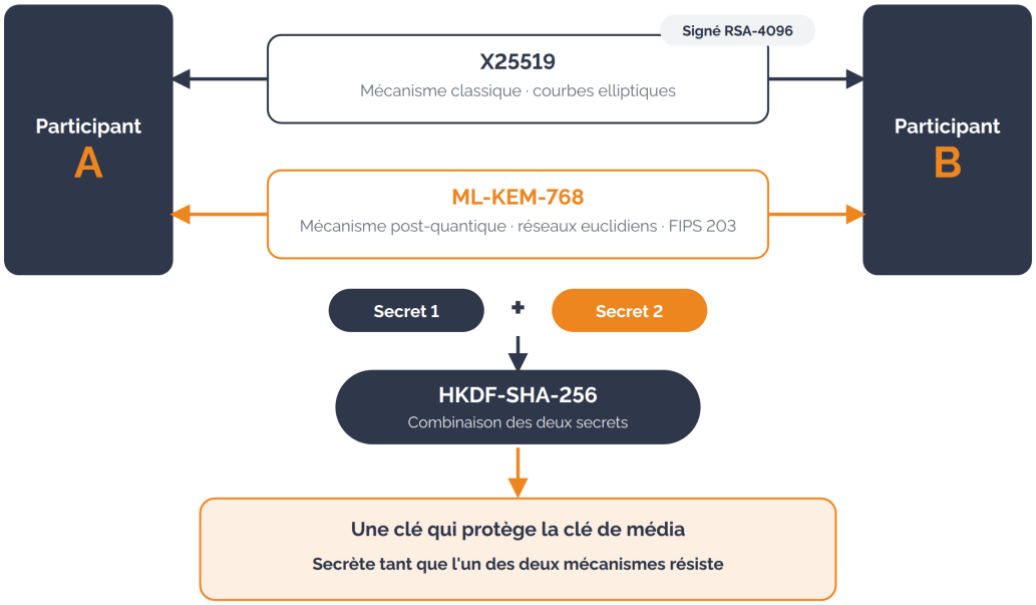


Schéma 2 : l'échange hybride

4 Pourquoi l'hybridation ?

Parce que le référentiel de l'ANSSI l'impose

L'hybridation n'est pas une précaution de Tixeo : le référentiel de l'ANSSI (ANSSI-PG-083 v3.00) l'impose, et il écarte explicitement un mécanisme post-quantique utilisé seul :

> *« Un produit visant une sécurité post-quantique doit satisfaire les règles RègleSécuAsym **et** RèglePQSécuAsym, afin d'assurer une non-régression de la sécurité. » (§2.2.1)*

> *« Les mécanismes dont la sécurité repose uniquement sur les problèmes de réseaux euclidiens […] ne sont pas conformes à la règle RègleSécuAsym. » (§2.2.1)*

Lues ensemble, ces deux règles signifient qu'un mécanisme à réseaux euclidiens, comme ML-KEM, satisfait l'exigence post-quantique mais échoue à l'exigence classique. **Utiliser ML-KEM seul aurait donc constitué une régression**, et non un choix plus audacieux.

Le mode que le référentiel juge le plus souhaitable

> *« La méthode la plus souhaitable consiste à hybrider un mécanisme d'encapsulation de clé asymétrique classique avec un mécanisme d'encapsulation de clé asymétrique post-quantique. Les clés issues des décapsulations […] peuvent être combinées, éventuellement avec des données supplémentaires comme les chiffrés et les clés publiques de ces deux mécanismes, à l'aide d'une fonction de dérivation de clés bien choisie. » (§2.2.1)*

> *« Il est toutefois préférable d'utiliser le niveau de sécurité supérieur, ML-KEM-768. » (§2.2.2)*

La construction de la version 18.2 reprend chacun de ces éléments, au niveau ML-KEM-768. C'est aussi la combinaison que déploie le protocole TLS sous le nom `X25519MLKEM768`.

Cette conformité porte sur la construction du mécanisme ; elle ne vaut pas certification du produit, qui relève d'une évaluation distincte.

5 Comment évaluer une protection post-quantique en visioconférence ?

Les annonces post-quantiques se multiplient dans la visioconférence et les communications sécurisées. Elles recouvrent des réalités techniques très différentes : le même mot peut désigner la protection du seul trajet entre un poste et un serveur, ou celle d'une réunion de bout en bout. Cinq questions permettent de les distinguer. Elles s'appliquent à n'importe quelle solution ; le tableau y apporte les réponses de Tixeo.

Question à poser	Ce que l'on observe	La réponse de Tixeo 18.2
Quelle couche est protégée ?	Une partie des annonces porte sur le chiffrement du transport (TLS) : la protection couvre alors le trajet entre le poste et le serveur, pas le contenu de bout en bout	Le cœur du chiffrement de bout en bout : l'échange de clés entre participants, dont dépend la protection de tous les flux de la réunion
Dépend-elle du système ou du navigateur ?	Lorsqu'elle repose sur les primitives du système d'exploitation ou du navigateur, sa couverture suit leurs versions et leur calendrier. Les navigateurs ne proposent à ce jour aucune primitive post-quantique, et le post-quantique n'est pas standardisé dans WebRTC	Aucune dépendance : ML-KEM-768 est compilé dans le propre moteur cryptographique de Tixeo, y compris dans le navigateur
Le mécanisme est-il hybride ?	Plusieurs approches coexistent : hybridation d'un mécanisme classique et d'un mécanisme post-quantique, mécanisme post-quantique seul, ou superposition de deux mécanismes post-quantiques	Hybride, X25519 + ML-KEM-768 : la construction qu'exige le référentiel de l'ANSSI

Question à poser	Ce que l'on observe	La réponse de Tixeo 18.2
Repose-t-il sur la version normalisée ?	Les premiers déploiements en visioconférence ont été lancés avant la publication de la norme FIPS 203 (août 2024), sur sa version préliminaire, Kyber	ML-KEM-768, dans sa version normalisée FIPS 203
Est-il actif par défaut ?	Le chiffrement de bout en bout, et la protection post-quantique qui s'y rattache, est souvent un mode à activer, dont l'activation peut restreindre des fonctions de collaboration	Actif par défaut, sans réglage, sans renoncement aux fonctions de collaboration

Ces critères ne classent pas les solutions dans l'absolu. Ils permettent de savoir précisément ce qu'une annonce protège, et à quelles conditions.

6 Qu'est-ce qui est protégé ?

Le périmètre de la version 18.2

Modalité d'accès	L'accès par navigateur
Contexte	En réunion et dans les Workspaces
Flux couverts	En réunion : audio, vidéo, partage d'écran, messagerie instantanée et transfert de fichiers instantané. Dans les Workspaces : messagerie, stockage et partage de fichiers, en et hors réunion
Condition	Tous les participants connectés depuis un navigateur avec la version 18.2
Non couvert en 18.2	L'application native et l'application mobile

En réunion, tous les flux couverts sont scellés sous **la même clé de média par participant**, celle que l'échange hybride protège.

Le multipoint couvert comme le point à point

Il n'existe pas, chez Tixeo, de clé de groupe : une réunion à N participants repose sur N clés de média et sur des échanges deux à deux. Le multipoint est donc protégé exactement comme le point à point.

Entre deux clients web 18.2

La protection s'établit entre deux participants qui utilisent tous deux le client web de la version 18.2. Face à un participant qui ne porte pas ce mécanisme, par exemple depuis une version antérieure ou depuis l'application native, l'échange s'établit avec le mécanisme classique, qui reste en place. La réunion se déroule normalement, et son chiffrement de bout en bout reste entier.

Actif par défaut, sans réglage

La protection post-quantique n'est soumise à aucun réglage, à aucune option de profil, à aucun prérequis côté serveur. Elle prolonge le chiffrement de bout en bout de Tixeo, qui n'est pas un mode : actif par défaut sur l'ensemble des échanges, il n'impose aucun renoncement aux fonctions de collaboration.

7 Pourquoi dans le navigateur, et comment l'accès navigateur porte-t-il cette protection ?

Aucune dépendance au navigateur

WebCrypto, l'interface cryptographique des navigateurs, ne propose aujourd'hui **aucun mécanisme post-quantique**. ML-KEM-768 est donc compilé dans **le propre moteur cryptographique de Tixeo**, exécuté en WebAssembly dans le navigateur, avec le reste de son chiffrement. Ce choix lui donne l'**agilité cryptographique** : la capacité à changer ou à ajouter un algorithme sans attendre les éditeurs de navigateurs.

L'architecture de l'accès navigateur

- **Un cœur Rust unique, compilé en WebAssembly.** C'est une implémentation indépendante du protocole Tixeo, et non un portage de l'application installée.
- Le protocole, le chiffrement des flux et la décision de qualité s'exécutent dans ce code compilé. Les clés propres à l'appareil sont gardées par le navigateur, sans pouvoir en être extraites. Le navigateur prend aussi en charge la capture de la caméra et du micro, l'encodage et le décodage, le rendu, l'interface et les connexions réseau.
- Le relais n'a jamais accès au contenu des échanges : audio, vidéo, messages et fichiers restent chiffrés de bout en bout.
- **Un participant dans un navigateur et un participant sur l'application installée se retrouvent dans la même réunion**, avec le même chiffrement de bout en bout des flux.

Deux couches réseau, choisies automatiquement. Le navigateur se connecte d'abord en **WebTransport** (UDP 443) : chaque flux y circule séparément ce qui garde la réunion fluide même sur un réseau instable. Si l'UDP est bloqué, il bascule en **WebSocket** (TCP 443), qui passe partout où passe le web, sans réglage de la part de l'utilisateur.

Le navigateur ne se connecte qu'aux serveurs Tixeo de l'organisation : le serveur de gestion, l'API et les notifications, et le relais de réunion. Aucune télémétrie, aucun service tiers : polices, scripts, moteurs et modèles d'IA sont servis par le serveur de l'organisation.

Un coût négligeable

La protection ajoute environ un kilo-octet à chaque échange de clés, une fois par participant et par session, sans aller-retour supplémentaire. Elle ne coûte rien sur les flux audio et vidéo eux-mêmes.

La maîtrise reste à l'organisation

L'accès navigateur ne s'impose pas à l'organisation : il s'active côté serveur, depuis la console d'administration de Tixeo, puis s'autorise profil par profil. Il ne demande aucun composant supplémentaire à héberger : le client web est un ensemble de fichiers statiques servi par le serveur Tixeo de l'organisation, y compris lorsque celui-ci est installé sur sa propre infrastructure.

Prérequis et compatibilité

Navigateurs	Chrome, Firefox, Safari
Serveur	Version 18.2, requise pour l'accès navigateur
Protection post-quantique	Aucun prérequis supplémentaire : ni réglage, ni option de profil, ni modification du serveur. Elle s'établit entre deux clients web 18.2

8 Contre quelle menace la version 18.2 protège-t-elle précisément ?

La menace qui pèse dès aujourd'hui

Un échange de clés remplit deux fonctions distinctes :

- **garder la clé secrète**, pour que seuls les participants puissent la connaître. C'est ce que renforce l'échange hybride X25519 + ML-KEM-768 ;
- **authentifier l'interlocuteur**, pour s'assurer que la clé reçue vient bien de lui. Ce rôle revient à la signature RSA-4096, un mécanisme classique.

Ces deux fonctions répondent à deux scénarios d'attaque différents :

Scénario d'attaque	Ce qu'il suppose	Possible aujourd'hui ?	Protection post-quantique en 18.2
Enregistrer une réunion aujourd'hui pour la déchiffrer demain	Stocker les échanges chiffrés, puis disposer un jour d'un ordinateur quantique	**Oui** : la collecte peut commencer dès maintenant	**Oui** : il faudrait casser à la fois X25519 et ML-KEM-768
S'interposer dans une réunion en cours en se faisant passer pour un participant	Disposer d'un ordinateur quantique opérationnel **au moment même** de la réunion	**Non, impossible à ce jour** : aucun ordinateur quantique capable de casser RSA-4096 n'existe	Non : ce scénario relève de l'authentification, qui reste classique

Le premier scénario est celui qui motive la migration post-quantique : la collecte peut commencer dès maintenant, sans attendre l'ordinateur quantique. Le second est **impossible à ce jour** : il exige une machine qui n'existe pas, et il ne peut être mené qu'en direct, pendant la réunion. Un enregistrement ne permet pas de le conduire après coup.

Autrement dit, ce qui est échangé aujourd'hui dans une réunion protégée le restera demain.

Un périmètre : l'accès navigateur, en réunion et dans les Workspaces

La protection post-quantique s'établit dès lors que tous les participants, en réunion comme dans un Workspace, utilisent le client web 18.2. Dans cette version, elle ne s'étend pas à l'application native ni à l'application mobile.

Les échanges qui impliquent l'une de ces applications conservent le chiffrement de bout en bout de Tixeo, avec l'échange de clés classique. La protection post-quantique sera étendue dans les prochains mois à l'application mobile, puis au client natif.

En pratique : bénéficier de la protection post-quantique

1. **Mettre à jour le serveur Tixeo en version 18.2,** requise pour l'accès navigateur.
2. **Activer l'accès navigateur** depuis la console d'administration de Tixeo, puis l'autoriser profil par profil.
3. **Rejoindre les réunions et les Workspaces depuis un navigateur** (Chrome, Firefox, Safari) : un simple lien suffit, sans installation.

La protection post-quantique s'applique alors automatiquement, sans réglage ni option à activer, dès lors que tous les participants sont connectés depuis un navigateur avec la version 18.2.

Glossaire

Terme	Définition
Chiffrement de bout en bout	Chiffrement réalisé sur le poste de l'émetteur et levé uniquement sur celui des destinataires : les serveurs intermédiaires n'ont jamais accès au contenu des échanges
Échange de clés	Opération par laquelle deux parties conviennent d'un secret commun sans jamais le transmettre en clair
Mécanisme d'encapsulation de clé (KEM)	Mécanisme asymétrique qui permet de transmettre un secret protégé à un destinataire disposant de la clé privée correspondante
ML-KEM-768	Mécanisme d'encapsulation de clé post-quantique fondé sur les réseaux euclidiens, normalisé par le NIST dans la norme FIPS 203 (niveau de sécurité 3)
X25519	Échange Diffie-Hellman sur la courbe elliptique Curve25519, mécanisme classique largement déployé
Hybridation	Combinaison d'un mécanisme classique et d'un mécanisme post-quantique, de sorte que la sécurité tienne tant que l'un des deux résiste
HKDF-SHA-256	Fonction de dérivation de clé qui produit une clé à partir d'un ou plusieurs secrets

Terme	Définition
ChaCha20-Poly1305	Algorithme de chiffrement authentifié symétrique, utilisé ici avec une clé de 256 bits
RSA-4096	Mécanisme asymétrique classique, utilisé ici pour signer et authentifier l'échange de clés
Harvest now, decrypt later	Stratégie consistant à collecter des communications chiffrées aujourd'hui pour les déchiffrer lorsque la puissance de calcul le permettra
Algorithmes de Shor et de Grover	Algorithmes quantiques : le premier casse la cryptographie asymétrique actuelle, le second affaiblit la cryptographie symétrique sans la casser
WebAssembly	Format de code compilé exécuté par les navigateurs, qui permet d'y faire tourner un moteur écrit dans un autre langage que JavaScript, ici Rust
WebCrypto	Interface de programmation cryptographique fournie par les navigateurs
Workspace Tixeo	Espace de collaboration persistant, partagé par une équipe ou autour d'un projet. Il réunit une salle de visioconférence permanente, la messagerie, le stockage et le partage de fichiers, accessibles en réunion comme en dehors, et fait office d'open space virtuel. Les échanges et les documents y sont conservés : un nouveau membre a accès à l'historique, y compris aux échanges antérieurs à son arrivée.
Primitive	Brique cryptographique élémentaire (algorithme de chiffrement, de signature, d'échange de clés)

Références

- **ANSSI-PG-083 v3.00** (20 mars 2026), *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*, §2.2.1 et §2.2.2 : https://messervices.cyber.gouv.fr/documents-guides/anssi-guide-mecanismes-crypto-3.00.pdf
- **NIST FIPS 203**, *Module-Lattice-Based Key-Encapsulation Mechanism Standard* (août 2024) : https://csrc.nist.gov/pubs/fips/203/final
- **NIST IR 8547**, *Transition to Post-Quantum Cryptography Standards*
- **Groupe de coopération NIS** (juin 2025), feuille de route coordonnée de la transition post-quantique dans l'Union européenne
- **RFC 7748** (X25519), **RFC 5869** (HKDF), **RFC 8439** (ChaCha20-Poly1305)

Contact

Pour toute question sur la protection post-quantique ou sur l'activation de l'accès navigateur, rapprochez-vous de votre interlocuteur Tixeo.