

Tixeo lance la version 18.2 de sa plateforme de collaboration : la protection post-quantique arrive dans le navigateur

L'accès le plus ouvert de la plateforme devient le plus protégé.



(ci-dessus, une illustration de la V18.2 de Tixeo ; crédit photo @Tixeo.)

Tixeo, éditeur français de solutions de visioconférence collaborative sécurisée, dont la technologie a été certifiée CSPN à quatre reprises par l'ANSSI, dévoile sa version 18.2 qui allie un haut niveau de sécurité à une grande fluidité d'accès. Accessible en un clic depuis le navigateur, la plateforme enrichit son chiffrement de bout en bout d'une protection post-quantique. Française et souveraine, elle s'adresse tout particulièrement aux secteurs critiques et sensibles (défense, industrie, énergie, administrations, santé, finance, etc.).

La V18.2 ne nécessite aucune nouvelle installation, tant pour les collaborateurs que pour les intervenants extérieurs. Un simple lien permet de rejoindre la réunion et d'accéder aux fonctionnalités de collaboration de la plateforme (transcription et traduction en temps réel, partage de fichiers, chat, Workspaces, etc.).



*“L’ANSSI prévoit de conditionner ses certifications à l’intégration de mécanismes post-quantiques à partir de 2027. Tixeo a choisi d’anticiper cette échéance”, déclare **Renaud Ghia, Président de Tixeo.***

“Dans la plupart des solutions de visioconférence, le navigateur est l’endroit où le chiffrement de bout en bout s’efface. Chez Tixeo, il devient celui où il va le plus loin”, poursuit-il.

Un chiffrement de bout en bout enrichi d’une protection post-quantique

Tixeo renforce le chiffrement de bout en bout de sa plateforme d’une protection post-quantique dans le navigateur. L’échange qui établit la clé d’une réunion combine le mécanisme habituel X25519 au mécanisme post-quantique ML-KEM-768 conçu pour résister aux ordinateurs quantiques de demain.

Cet échange hybride protège l’intégralité des flux de la réunion (audio, vidéo, partage d’écran, chat, transfert de fichiers) ainsi que les Workspaces (open-space virtuel, messagerie, stockage et partage de fichiers en et hors réunion). Il est porté par le propre moteur de chiffrement de Tixeo sans dépendre d’aucune primitive du navigateur ou du système d’exploitation.

La protection post-quantique s’applique dès lors que les participants, en réunion comme dans un Workspace, sont tous connectés depuis un navigateur avec la V18.2. Lorsque l’un d’eux utilise l’application ou une version antérieure, l’échange repose sur le mécanisme de chiffrement de bout en bout classique.

*“Sur le marché de la visioconférence d’entreprise, les rares protections post-quantiques proposées aujourd’hui viennent d’acteurs américains. Or ceux-ci restent soumis au Cloud Act, qui peut les contraindre à répondre aux demandes d’accès des autorités américaines. Avec la V18.2, Tixeo apporte cette protection post-quantique à une plateforme française et souveraine, sans aucune exposition à une législation extraterritoriale”, souligne **Renaud Ghia.***

Une expérience fluide et intuitive, depuis le navigateur

*“Les organisations sensibles veulent des outils de collaboration aussi simples à utiliser que ceux auxquels elles sont habituées, sans faire de compromis sur la sécurité de leurs échanges. C’est cette double exigence qui a guidé le développement de notre V18.2 : offrir une interface familière et une prise en main immédiate, tout en maintenant le niveau de protection indispensable à leurs activités”, ajoute **Renaud Ghia.***

Pendant l’échange, le mode incrustation vidéo (Picture-in-Picture) affiche les participants dans une fenêtre flottante dès que l’utilisateur passe sur un autre onglet. La messagerie s’affiche en mode étendu sur tout ou partie de l’écran et devient un espace d’échange à part entière. Le mode Fusion et les Workspaces gagnent encore en fluidité, comme dans un véritable open space. Fichiers et historique restent accessibles : réunion, espace de travail et documents tiennent dans un seul onglet.

Tixeo enrichit cette expérience avec la transcription et la traduction en temps réel des échanges, affichées en sous-titres et portées par une IA souveraine. Lors d'une réunion internationale, chaque participant peut ainsi suivre en direct l'échange dans sa langue.

“Avec la V18.2, nous appliquons un principe qui guide notre R&D depuis plus de vingt ans : traiter les exigences de sécurité de demain comme des contraintes d'aujourd'hui, sans complexifier les usages. À mesure que la doctrine de l'ANSSI se précisera d'ici 2027, Tixeo continuera d'élargir le périmètre post-quantique”, déclare Renaud Ghia.

Accessible depuis le navigateur, la protection post-quantique sera étendue dans les prochains mois à l'ensemble de l'écosystème Tixeo, à commencer par l'application mobile puis le client natif, en gardant cette même exigence de simplicité d'accès et d'utilisation. Le déploiement de la version 18.2 débutera dans les tout prochains jours.

Pour aller plus loin...

Les fondamentaux du chiffrement Tixeo

- **Les clés sont générées et conservées sur les postes des participants.** Le serveur ne les détient à aucun moment.
- **Les flux sont chiffrés sur le poste de l'émetteur et déchiffrés uniquement sur ceux des destinataires.** Le serveur achemine des données scellées qu'il ne peut pas lire.
- **Un chiffrement propriétaire développé par Tixeo**, éditeur français : aucune dépendance à un tiers, aucune porte dérobée, aucune soumission à une législation extraterritoriale.
- **Actif par défaut sur l'ensemble des échanges** (audio, vidéo, partage d'écran, messagerie, fichiers, Workspaces), quel que soit le nombre de participants, sans configuration de sécurité à effectuer.
- **Cette même technologie opère dans le navigateur avec la V18.2** : le chiffrement s'exécute côté client, dans le propre moteur de Tixeo.
- **Un intervenant extérieur, sans compte ni installation, bénéficie de la même protection.**
- **L'organisation garde la maîtrise** : l'accès navigateur s'active côté serveur et s'autorise par profil de sécurité.

Protection post-quantique Tixeo : le mécanisme en bref

- **L'établissement de la clé de chaque réunion devient hybride : X25519** (courbes elliptiques) + **ML-KEM-768** (norme FIPS 203). Rien n'est remplacé : le mécanisme classique reste en place, le post-quantique s'y ajoute.
- **Aligné sur la doctrine de l'ANSSI** : le référentiel ANSSI-PG-083 impose l'hybridation pour un produit visant une sécurité post-quantique. La construction de Tixeo correspond au mode que ce référentiel juge le plus souhaitable. Tixeo peut donc s'appuyer sur le référentiel lui-même.
- **Le périmètre** : navigateur uniquement à ce stade, en réunion (audio, vidéo, partage d'écran, chat, transfert de fichiers instantané) et dans les Workspaces (open-space

virtuel, messagerie, stockage et partage de fichiers en et hors réunion), à condition que tous les participants soient connectés depuis un navigateur.

- **Actif par défaut, sans mode dégradé.** Rien à activer, aucun prérequis de configuration. La protection s'applique entre deux clients web 18.2 ; face à un participant connecté depuis l'application ou équipé d'une version antérieure, l'échange revient au mécanisme classique.

Pour en savoir plus sur le fonctionnement de la protection post-quantique et l'architecture de l'accès navigateur, une annexe technique est disponible à ce [lien](#). Vous trouverez des visuels HD de la V18.2 à ce [lien](#) (crédit photo @Tixeo).

CONTACTS PRESSE | OXYGEN

Eliot Granveau - eliot.g@oxygen-rp.com - 06 26 36 41 17

Caroline Hoffmann - caroline.h@oxygen-rp.com

À propos de Tixeo

Depuis plus de 20 ans, Tixeo, éditeur français de solutions de visioconférence collaborative sécurisée, accompagne les organisations stratégiques (défense, industrie, énergie...) pour garantir l'efficacité et la sécurité de leurs échanges en ligne dans le cadre de leurs activités critiques.

Disponible en cloud ou On-premise, Tixeo propose sa propre technologie de visioconférence certifiée CSPN à quatre reprises par l'ANSSI et vient compléter les solutions de collaboration standard pour encore plus de confidentialité. Conçue selon une approche Secure by Design, sa technologie intègre un véritable chiffrement de bout en bout des flux (vidéo, audio, données) quel que soit le nombre de participants.

Avec un niveau de sécurité sans précédent, Tixeo permet de limiter le risque cyber, renforcer la cyber-résilience ou aider à se conformer aux réglementations. De nombreuses organisations européennes lui font ainsi confiance telles que Naval Group, Dassault Aviation, Orange, Orano, Aéroport de Bordeaux, etc.

Tixeo est :

- Labellisé « France Cybersecurity », « Cybersecurity Made in Europe » et « Utilisé par les Armées Françaises »
- Membre du GICAT, de l'Alliance pour la Confiance Numérique, du CLUSIF et d'HEXATRUST.

En savoir plus : www.tixeo.com