Pressemitteilung
Montpellier, 12. Oktober 2026

Tixeo stellt Version 18.2 seiner Kollaborationsplattform vor: Post-Quanten-Schutz jetzt auch im Browser

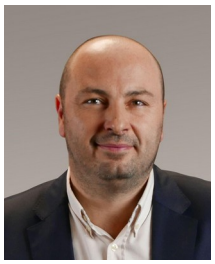
Der offenste Zugang zur Plattform wird zum am besten geschützten.



(Oben: Illustration der Version 18.2 von Tixeo; Bildnachweis @Tixeo.)

Tixeo, europäischer Anbieter sicherer Lösungen für kollaborative Videokonferenzen, hat für seine Technologie bereits viermal die Sicherheitszertifizierung der ersten Stufe (Certification de Sécurité de Premier Niveau, CSPN) der französischen Cybersicherheitsbehörde ANSSI (Agence nationale de la sécurité des systèmes d'information) erhalten. Diese Zertifizierung wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt. Nun stellt das Unternehmen die Version 18.2 seiner Plattform vor, die ein hohes Sicherheitsniveau mit einem besonders einfachen Zugang verbindet. Die Plattform ist mit einem Klick im Browser erreichbar und ergänzt ihre Ende-zu-Ende-Verschlüsselung um einen Post-Quanten-Schutz. Als europäische und souveräne Lösung richtet sie sich insbesondere an kritische und sensible Sektoren (Verteidigung, Industrie, Energie, öffentliche Verwaltung, Gesundheitswesen, Finanzwesen usw.).

Version 18.2 erfordert keine neue Installation, weder für Mitarbeitende noch für externe Teilnehmende. Ein einfacher Link genügt, um an einer Besprechung teilzunehmen und die Kollaborationsfunktionen der Plattform zu nutzen (Echtzeit-Transkription und -Übersetzung, Dateifreigabe, Chat, Workspaces usw.).



„Die ANSSI plant, ihre Zertifizierungen ab 2027 an die Integration von Post-Quanten-Mechanismen zu knüpfen. Tixeo hat sich entschieden, dieser Frist zuvorzukommen“, erklärt **Renaud Ghia, CEO von Tixeo**.

„In den meisten Videokonferenzlösungen ist der Browser der Ort, an dem die Ende-zu-Ende-Verschlüsselung endet. Bei Tixeo ist er der Ort, an dem sie am weitesten reicht“, fährt er fort.

Ende-zu-Ende-Verschlüsselung, ergänzt um einen Post-Quanten-Schutz

Tixeo ergänzt die Ende-zu-Ende-Verschlüsselung seiner Plattform im Browser um einen Post-Quanten-Schutz. Der Austausch, mit dem der Schlüssel einer Besprechung vereinbart wird, kombiniert das etablierte Verfahren X25519 mit dem Post-Quanten-Verfahren ML-KEM-768, das darauf ausgelegt ist, den Quantencomputern von morgen standzuhalten.

Dieser hybride Schlüsselaustausch schützt sämtliche Datenströme der Besprechung (Audio, Video, Bildschirmfreigabe, Chat, Dateiübertragung) sowie die Workspaces (virtuelles Großraumbüro, Messaging, Speicherung und Freigabe von Dateien innerhalb und außerhalb von Besprechungen). Er beruht auf der eigenen Verschlüsselungs-Engine von Tixeo und ist von keinerlei Primitiven des Browsers oder des Betriebssystems abhängig.

Der Post-Quanten-Schutz greift, sobald alle Teilnehmenden, ob in einer Besprechung oder in einem Workspace, über einen Browser mit Version 18.2 verbunden sind. Nutzt eine teilnehmende Person die Anwendung oder eine frühere Version, beruht der Austausch auf dem klassischen Verfahren der Ende-zu-Ende-Verschlüsselung.

„*Auf dem Markt für Videokonferenzen im Unternehmensumfeld stammen die wenigen heute verfügbaren Post-Quanten-Schutzmechanismen von US-Anbietern. Diese unterliegen jedoch dem CLOUD Act, der sie verpflichten kann, Zugriffsanfragen von US-Behörden nachzukommen. Mit Version 18.2 bringt Tixeo diesen Post-Quanten-Schutz auf eine europäische und souveräne Plattform, ohne jede Exposition gegenüber extraterritorialer Gesetzgebung*“, betont **Renaud Ghia**.

Ein flüssiges, intuitives Nutzungserlebnis direkt im Browser

„Sensible Organisationen wünschen sich Kollaborationswerkzeuge, die so einfach zu bedienen sind wie die, die sie gewohnt sind, ohne Abstriche bei der Sicherheit ihrer Kommunikation. Diese doppelte Anforderung hat die Entwicklung unserer Version 18.2 geleitet: eine vertraute Oberfläche, die sich sofort nutzen lässt, bei gleichbleibend hohem Schutzniveau, wie es ihre Tätigkeit erfordert“, ergänzt **Renaud Ghia**.

Während des Gesprächs zeigt der Bild-in-Bild-Modus (Picture-in-Picture) die Teilnehmenden in einem schwebenden Fenster an, sobald in einen anderen Tab gewechselt wird. Der Chat lässt sich im erweiterten Modus über den gesamten Bildschirm oder einen Teil davon anzeigen und wird so zu einem vollwertigen Kommunikationsraum. Der Fusion-Modus und die Workspaces werden noch flüssiger, wie in einem echten Großraumbüro. Dateien und Verlauf bleiben jederzeit zugänglich: Besprechung, Arbeitsbereich und Dokumente finden in einem einzigen Tab Platz.

Ergänzt wird dieses Nutzungserlebnis durch die Echtzeit-Transkription und -Übersetzung der Gespräche, die als Untertitel angezeigt werden und auf einer souveränen KI beruhen. In internationalen Besprechungen kann so jede teilnehmende Person das Gespräch live in ihrer eigenen Sprache verfolgen.

„Mit Version 18.2 setzen wir ein Prinzip um, das unsere Forschung und Entwicklung seit mehr als zwanzig Jahren leitet: die Sicherheitsanforderungen von morgen als Vorgaben von heute zu behandeln, ohne die Nutzung zu verkomplizieren. In dem Maße, in dem die ANSSI ihre Doktrin bis 2027 präzisiert, wird Tixeo den Post-Quanten-Schutz weiter ausbauen“, erklärt **Renaud Ghia**.

Der im Browser verfügbare Post-Quanten-Schutz wird in den kommenden Monaten auf das gesamte Tixeo-Ökosystem ausgeweitet, beginnend mit der mobilen App und anschließend dem nativen Client, mit demselben Anspruch an einfachen Zugang und einfache Bedienung. Die Auslieferung der Version 18.2 beginnt in den nächsten Tagen.

Weiterführende Informationen

Die Grundlagen der Tixeo-Verschlüsselung

- **Die Schlüssel werden auf den Endgeräten der Teilnehmenden erzeugt und gespeichert**. Der Server verfügt zu keinem Zeitpunkt über sie.
- **Die Datenströme werden auf dem Endgerät des Senders verschlüsselt und ausschließlich auf den Endgeräten der Empfänger entschlüsselt.** Der Server leitet versiegelte Daten weiter, die er nicht lesen kann.
- **Eine von Tixeo entwickelte proprietäre Verschlüsselung**, aus der Hand eines europäischen Anbieters: keine Abhängigkeit von Dritten, keine Hintertür, keine Unterwerfung unter extraterritoriale Gesetzgebung.
- **Standardmäßig für die gesamte Kommunikation aktiv** (Audio, Video, Bildschirmfreigabe, Messaging, Dateien, Workspaces), unabhängig von der Zahl der Teilnehmenden und ohne Sicherheitskonfiguration.
- **Dieselbe Technologie arbeitet mit Version 18.2 im Browser**: Die Verschlüsselung erfolgt clientseitig in der eigenen Engine von Tixeo.
- **Externe Teilnehmende ohne Konto und ohne Installation profitieren vom gleichen Schutz.**
- **Die Organisation behält die Kontrolle**: Der Browserzugang wird serverseitig aktiviert und je Sicherheitsprofil freigegeben.

Post-Quanten-Schutz von Tixeo: der Mechanismus im Überblick

- **Die Schlüsselvereinbarung jeder Besprechung wird hybrid: X25519** (elliptische Kurven) + **ML-KEM-768** (Standard FIPS 203). Nichts wird ersetzt: Das klassische Verfahren bleibt bestehen, das Post-Quanten-Verfahren kommt hinzu.
- **Im Einklang mit der Doktrin der ANSSI**: Der Leitfaden ANSSI-PG-083 schreibt für Produkte, die Post-Quanten-Sicherheit anstreben, die Hybridisierung vor. Die Konstruktion von Tixeo entspricht dem Modus, den dieser Leitfaden als den wünschenswertesten einstuft. Tixeo kann sich damit auf den Leitfaden selbst stützen.

- **Umfang**: derzeit ausschließlich im Browser, in Besprechungen (Audio, Video, Bildschirmfreigabe, Chat, sofortige Dateiübertragung) und in den Workspaces (virtuelles Großraumbüro, Messaging, Speicherung und Freigabe von Dateien innerhalb und außerhalb von Besprechungen), sofern alle Teilnehmenden über einen Browser verbunden sind.
- **Standardmäßig aktiv, ohne eingeschränkten Modus**. Nichts zu aktivieren, keine Konfigurationsvoraussetzungen. Der Schutz greift zwischen zwei Web-Clients der Version 18.2; ist eine teilnehmende Person über die Anwendung oder mit einer früheren Version verbunden, wird auf das klassische Verfahren zurückgegriffen.

Weitere Informationen zur Funktionsweise des Post-Quanten-Schutzes und zur Architektur des Browserzugangs enthält ein technischer Anhang, der unter diesem Link abrufbar ist.

PRESSEKONTAKT | OXYGEN (französische PR-Agentur)
Eliot Granveau - eliot.g@oxygen-rp.com - +33 6 26 36 41 17
Caroline Hoffmann - caroline.h@oxygen-rp.com

Über Tixeo

Seit mehr als 20 Jahren unterstützt Tixeo, europäischer Anbieter sicherer Lösungen für kollaborative Videokonferenzen, strategische Organisationen (Verteidigung, Industrie, Energie usw.) dabei, die Effizienz und Sicherheit ihrer Online-Kommunikation im Rahmen ihrer kritischen Tätigkeiten zu gewährleisten.

Tixeo ist in der Cloud oder On-Premises verfügbar und bietet eine eigene Videokonferenztechnologie, die von der ANSSI viermal mit der CSPN zertifiziert wurde. Sie ergänzt Standard-Kollaborationslösungen für noch mehr Vertraulichkeit. Nach dem Secure-by-Design-Ansatz entwickelt, bietet die Technologie eine echte Ende-zu-Ende-Verschlüsselung der Datenströme (Video, Audio, Daten), unabhängig von der Zahl der Teilnehmenden.

Mit einem beispiellosen Sicherheitsniveau hilft Tixeo, Cyberrisiken zu begrenzen, die Cyberresilienz zu stärken und regulatorische Anforderungen zu erfüllen. Zahlreiche europäische Organisationen vertrauen Tixeo, darunter Naval Group, Dassault Aviation, Orange, Orano und der Flughafen Bordeaux.

Tixeo trägt das Label „Cybersecurity Made in Europe“.

Mehr erfahren: www.tixeo.com