

Tixeo 18.2: how post-quantum protection works

Technical appendix to the press release of 12 October 2026



Introduction

Tixeo is giving a first look at version 18.2 of its secure videoconferencing platform. With this version, Tixeo's end-to-end encryption gains post-quantum protection in the browser: the exchange that establishes a meeting's keys combines the classical mechanism already in place with ML-KEM-768, a standardised mechanism designed to withstand quantum computers. This protection covers every stream in the meeting, is enabled automatically and requires no configuration.

This document is intended for journalists who wish to go further than the press release. Prepared with Tixeo's R&D team, it brings together the technical elements needed to understand what this protection covers, how it works and where its scope ends in version 18.2.

Key points at a glance

- 1 **What changes:** a meeting's key establishment becomes **hybrid**, X25519 + ML-KEM-768 (FIPS 203 standard). Nothing is replaced: the post-quantum mechanism is added to the classical one.
- 2 **Why "protection" rather than post-quantum "encryption":** the quantum threat targets the key exchange, not the encryption of the streams. Streams remain encrypted with ChaCha20-Poly1305 using a 256-bit key, which is already considered resistant.
- 3 **Why hybridisation:** the guidelines of ANSSI, France's Cybersecurity Agency, require it for any product aiming for post-quantum security. Tixeo's construction matches the mode those guidelines describe as the most desirable, at the parameter level they prefer.
- 4 **What is protected:** in meetings, audio, video, screen sharing, instant messaging and file transfer; in Workspaces, messaging, file storage and file sharing. This applies provided that all participants are connected from a browser running version 18.2, however many there are.
- 5 **Powered by Tixeo's own engine:** the encryption tools built into browsers do not currently offer any post-quantum mechanism. Tixeo does not need them: ML-KEM-768 is built into its own encryption engine, which runs in the browser.
- 6 **No configuration:** the protection is enabled by default, with no settings or options to activate.

1 Why post-quantum protection, and why now?

A threat that starts before the quantum computer exists

No quantum computer today is capable of breaking the encryption mechanisms in use. Yet the risk is already present, in a form specialists call *harvest now, decrypt later*: collecting encrypted communications today, storing them, and waiting until the computing power needed to decrypt them becomes available.

The risk primarily concerns organisations whose exchanges must remain confidential for decades.

What the quantum computer threatens, and what it does not

Two quantum algorithms frame the issue:

- **Shor's algorithm** breaks asymmetric cryptography (RSA, Diffie-Hellman key exchange, elliptic curves), which is used to establish and authenticate keys. This is where the real risk lies;
- **Grover's algorithm** weakens symmetric cryptography, which encrypts the streams, but only halves its effective strength. A 256-bit key retains a 128-bit security level, which is considered sufficient.

The consequence is clear: to protect a communication against the quantum threat, its key establishment must be strengthened.

A timetable now set

Date	Milestone
August 2024	NIST publishes the FIPS 203 standard, which standardises ML-KEM, a post-quantum key encapsulation mechanism
20 March 2026	ANSSI publishes version 3.00 of its guidelines on cryptographic mechanisms (ANSSI-PG-083), which set the rules for hybridisation
16 June 2026	ANSSI announces that from 2027 it will no longer certify security products lacking quantum-resistant mechanisms, and sets 2030 as the horizon by which the organisations concerned must use only resistant solutions
2030 and 2035	Post-quantum transition milestones set by the European roadmap (NIS Cooperation Group)

Version 18.2 is part of this trajectory: it integrates post-quantum protection before the certification requirement comes into force.

2 Why “protection” rather than post-quantum “encryption”?

An end-to-end encrypted meeting relies on two distinct operations.

Key establishment. Before exchanging any content, participants must agree, without ever transmitting it in clear, on the key that will protect their exchanges. This operation relies on asymmetric cryptography: this is what Shor’s algorithm threatens, and this is what version 18.2 strengthens.

Stream encryption. Once the key is established, every audio sample, video frame, message and file is sealed with that key. At Tixeo, this encryption relies on **ChaCha20-Poly1305**, with a **256-bit** key: a symmetric algorithm that Grover’s algorithm only reduces to 128 bits of security. It is therefore already considered resistant, and version 18.2 does not change it.

Hence the accurate wording: **end-to-end encryption strengthened with post-quantum protection**. The protection applies to the exchange that establishes the keys, and that exchange in turn protects every stream.

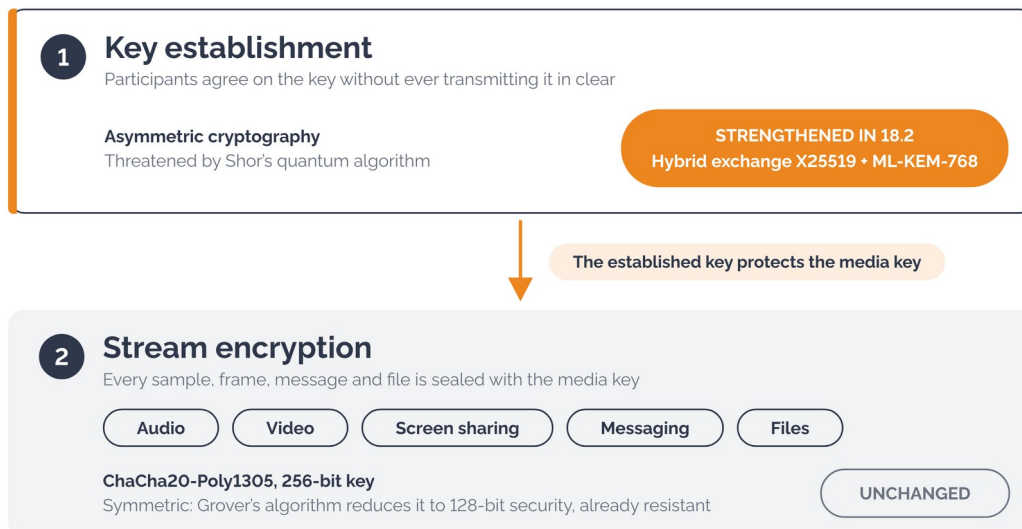


Diagram 1: the two layers of an end-to-end encrypted meeting

3 How does the hybrid exchange work?

One key per participant

In a Tixeo meeting, each participant generates **their own media key**, which seals what they publish. To decrypt another participant, a participant retrieves that participant's key directly from them, through a peer-to-peer key exchange. The server and the relay carry these exchanges without being able to extract the keys from them.

Two mechanisms combined

With version 18.2, this exchange becomes hybrid. Two mechanisms work in parallel, and each produces a shared secret:

Component	Mechanism
Classical mechanism	X25519, elliptic-curve Diffie-Hellman exchange (Curve25519), ephemeral per session
Post-quantum mechanism	ML-KEM-768, key encapsulation mechanism standardised by FIPS 203, ephemeral per session
Combination	HKDF-SHA-256, key derivation function applied to both secrets, with the public keys and ciphertexts of both mechanisms bound into the derivation context
Exchange authentication	RSA-4096 (RSASSA-PKCS#1 v1.5 + SHA-256), signature bound to the device certificate, unchanged

The resulting key, which protects the media key, is derived **from both secrets at once**. It therefore remains secret as long as **either** mathematical problem holds: the elliptic-curve problem on which X25519 relies, or the lattice problem on which ML-KEM relies. An attacker who broke one of the two mechanisms would gain nothing without also breaking the other.

Nothing is replaced, and **ML-KEM-768 is not a signature algorithm**. It is a key encapsulation mechanism, at security level 3 of the FIPS 203 standard: it is used to establish a shared secret and nothing else. The exchange is still signed with RSA-4096.

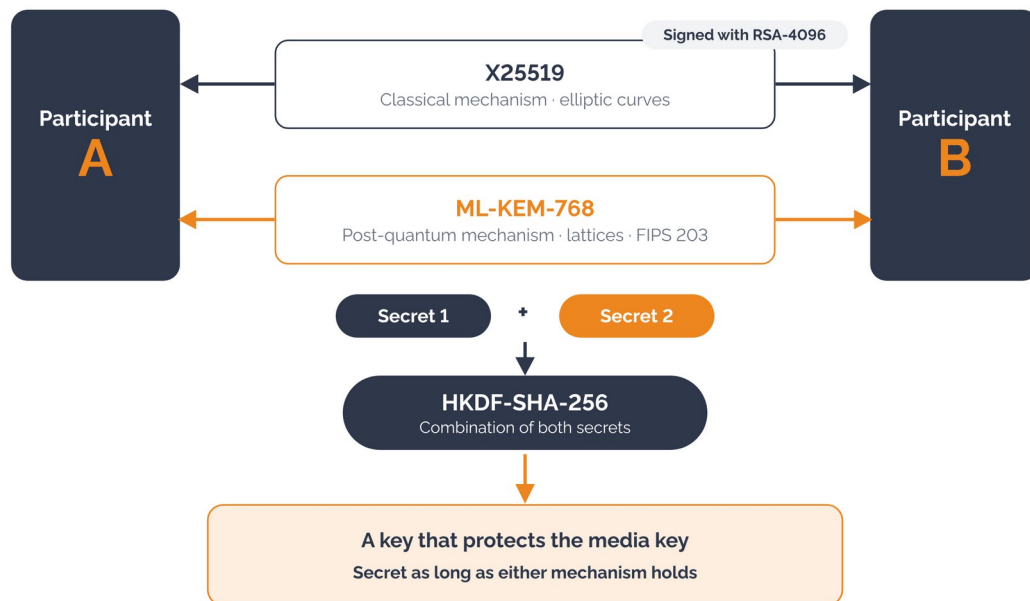


Diagram 2: the hybrid exchange

4 Why hybridisation?

Because ANSSI's guidelines require it

Hybridisation is not a precaution taken by Tixeo: ANSSI's guidelines (ANSSI-PG-083 v3.00) require it, and explicitly rule out a post-quantum mechanism used on its own (quotations translated from the French original):

*"A product aiming for post-quantum security must satisfy the rules RègleSécuAsym **and** RèglePQSécuAsym, in order to ensure non-regression of security." (§2.2.1)*

"Mechanisms whose security relies solely on lattice problems [...] do not comply with the rule RègleSécuAsym." (§2.2.1)

Read together, these two rules mean that a lattice-based mechanism such as ML-KEM meets the post-quantum requirement but fails the classical one. **Using ML-KEM on its own would therefore have been a regression**, not a bolder choice.

The mode the guidelines consider most desirable

"The most desirable method is to hybridise a classical asymmetric key encapsulation mechanism with a post-quantum asymmetric key encapsulation mechanism. The keys resulting from the decapsulations [...] may be combined, possibly with additional data such as the ciphertexts and public keys of both mechanisms, using a well-chosen key derivation function." (§2.2.1)

"It is nevertheless preferable to use the higher security level, ML-KEM-768." (§2.2.2)

The construction of version 18.2 follows each of these elements, at the ML-KEM-768 level. It is also the combination deployed by the TLS protocol under the name X25519MLKEM768.

This compliance concerns the construction of the mechanism; it does not amount to product certification, which is subject to a separate evaluation.

5 How to assess post-quantum protection in videoconferencing

Post-quantum announcements are multiplying in videoconferencing and secure communications. They cover very different technical realities: the same word may refer to protecting only the path between a device and a server, or protecting a meeting end to end. Five questions help tell them apart. They apply to any solution; the table gives Tixeo's answers.

Question to ask	What we observe	Tixeo 18.2's answer
Which layer is protected?	Some announcements concern transport encryption (TLS): the protection then covers the path between the device and the server, not the content end to end	The core of end-to-end encryption: the key exchange between participants, on which the protection of every stream in the meeting depends

Question to ask	What we observe	Tixeo 18.2's answer
Does it depend on the operating system or the browser?	When it relies on primitives from the operating system or the browser, its coverage follows their versions and release schedule. Browsers do not currently offer any post-quantum primitive, and post-quantum mechanisms are not standardised in WebRTC	No dependency: ML-KEM-768 is compiled into Tixeo's own encryption engine, including in the browser
Is the mechanism hybrid?	Several approaches coexist: hybridising a classical mechanism with a post-quantum one, a post-quantum mechanism on its own, or layering two post-quantum mechanisms	Hybrid, X25519 + ML-KEM-768: the construction required by ANSSI's guidelines
Is it based on the standardised version?	The first deployments in videoconferencing were launched before the FIPS 203 standard was published (August 2024), on its preliminary version, Kyber	ML-KEM-768, in its standardised FIPS 203 version
Is it enabled by default?	End-to-end encryption, and the post-quantum protection attached to it, is often a mode that has to be enabled, and enabling it may restrict collaboration features	Enabled by default, with no configuration and no loss of collaboration features

These criteria do not rank solutions in absolute terms. They make it possible to know precisely what an announcement protects, and under what conditions.

6 What is protected?

The scope of version 18.2

Access mode	Browser access
Context	In meetings and in Workspaces
Streams covered	In meetings: audio, video, screen sharing, instant messaging and instant file transfer. In Workspaces: messaging, file storage and file sharing, during and outside meetings
Condition	All participants connected from a browser running version 18.2
Not covered in 18.2	The native application and the mobile application

In meetings, all covered streams are sealed under **the same media key per participant**, the one protected by the hybrid exchange.

Multipoint covered just like point-to-point

Tixeo does not use a group key: a meeting with N participants relies on N media keys and on pairwise exchanges. Multipoint meetings are therefore protected in exactly the same way as point-to-point calls.

Between two 18.2 web clients

The protection is established between two participants who are both using the version 18.2 web client. With a participant who does not support this mechanism, for example one using an earlier version or the native application, the exchange is established with the classical mechanism, which remains in place. The meeting proceeds normally, and its end-to-end encryption remains fully intact.

Enabled by default, no configuration

Post-quantum protection is not subject to any setting, profile option or server-side prerequisite. It extends Tixeo's end-to-end encryption, which is not a mode: enabled by default across all exchanges, it does not require giving up any collaboration feature.

7 Why in the browser, and how does browser access deliver this protection?

No dependency on the browser

WebCrypto, the browsers' cryptographic interface, does not currently offer **any post-quantum mechanism**. ML-KEM-768 is therefore compiled into **Tixeo's own encryption engine**, which runs as WebAssembly in the browser, together with the rest of its encryption. This choice gives it **crypto-agility**: the ability to change or add an algorithm without waiting for browser vendors.

Browser access architecture

- **A single Rust core, compiled to WebAssembly.** It is an independent implementation of the Tixeo protocol, not a port of the installed application.
- The protocol, stream encryption and quality decisions run in this compiled code. Device-specific keys are held by the browser and cannot be extracted. The browser also handles camera and microphone capture, encoding and decoding, rendering, the user interface and network connections.
- The relay never has access to the content of exchanges: audio, video, messages and files remain end-to-end encrypted.
- **A participant in a browser and a participant on the installed application can join the same meeting**, with the same end-to-end encryption of streams.

Two network layers, selected automatically. The browser first connects over **WebTransport** (UDP 443): each stream travels separately, which keeps the meeting smooth even on an unstable network. If UDP is

blocked, it switches to **WebSocket** (TCP 443), which works wherever the web works, with no action required from the user.

The browser connects only to the organisation's Tixeo servers: the management server, the API and notifications, and the meeting relay. No telemetry, no third-party services: fonts, scripts, engines and AI models are all served by the organisation's server.

A negligible overhead

The protection adds around one kilobyte to each key exchange, once per participant and per session, with no additional round trip. It adds nothing to the audio and video streams themselves.

The organisation stays in control

Browser access is not imposed on the organisation: it is enabled server-side, from the Tixeo administration console, then authorised profile by profile. It requires no additional component to host: the web client is a set of static files served by the organisation's Tixeo server, including when that server is installed on the organisation's own infrastructure.

Requirements and compatibility

Browsers	Chrome, Firefox, Safari
Server	Version 18.2, required for browser access
Post-quantum protection	No additional requirement: no setting, no profile option, no server change. It is established between two 18.2 web clients

8 Which threat does version 18.2 protect against, exactly?

The threat that exists today

A key exchange performs two distinct functions:

- **keeping the key secret**, so that only the participants can know it. This is what the hybrid X25519 + ML-KEM-768 exchange strengthens;
- **authenticating the other party**, to make sure the key received really comes from them. This role falls to the RSA-4096 signature, a classical mechanism.

These two functions address two different attack scenarios:

Attack scenario	What it requires	Possible today?	Post-quantum protection in 18.2
Record a meeting today to decrypt it tomorrow	Store the encrypted exchanges, then one day gain access to a quantum computer	Yes: collection can start right now	Yes: both X25519 and ML-KEM-768 would have to be broken
Intercept a meeting in progress by impersonating a participant	Have an operational quantum computer at the very time of the meeting	No, impossible to date: no quantum computer capable of breaking RSA-4096 exists	No: this scenario concerns authentication, which remains classical

The first scenario is what drives the post-quantum migration: collection can begin right now, without waiting for the quantum computer. The second is **impossible to date**: it requires a machine that does not exist, and it can only be carried out live, during the meeting. A recording cannot be used to carry it out after the fact.

In other words, what is exchanged today in a protected meeting will remain protected tomorrow.

One scope: browser access, in meetings and in Workspaces

Post-quantum protection is established whenever all participants, in a meeting or in a Workspace, use the 18.2 web client. In this version, it does not extend to the native application or the mobile application.

Exchanges involving either of these applications retain Tixeo's end-to-end encryption, with the classical key exchange.

Going further

Renaud Ghia, CEO of Tixeo, is available for interviews. Requests via the Oxygen agency.

Five topics he can discuss

- 1 2027, the year post-quantum becomes a requirement.** What the certification requirement announced by ANSSI concretely changes for public administrations and critical infrastructure operators, and why they need to prepare before it becomes enforceable.
- 2 Meetings, the forgotten target of “harvest now, decrypt later”.** Board meetings, defence programmes, industrial negotiations: why exchanges thought of as ephemeral are just as exposed as stored data.
- 3 Owning the encryption chain.** Why a vendor that owns its encryption engine moves at its own pace, rather than waiting for browsers and operating systems, and what this says about technological sovereignty.
- 4 The browser, from weak link to most protected access point.** How to reconcile openness to external participants, with no installation, with the security requirements of sensitive organisations.
- 5 Migrating without disruption.** How an organisation can carry out its post-quantum transition without interrupting its operations or switching its entire estate at once, at a time when Europe is asking every Member State to inventory its encryption mechanisms.

Glossary

Term	Definition
End-to-end encryption	Encryption performed on the sender’s device and removed only on the recipients’ devices: intermediate servers never have access to the content of exchanges
Key exchange	Operation by which two parties agree on a shared secret without ever transmitting it in clear
Key encapsulation mechanism (KEM)	Asymmetric mechanism used to transmit a protected secret to a recipient holding the corresponding private key
ML-KEM-768	Lattice-based post-quantum key encapsulation mechanism, standardised by NIST in FIPS 203 (security level 3)
X25519	Diffie-Hellman exchange on the Curve25519 elliptic curve, a widely deployed classical mechanism

Term	Definition
Hybridisation	Combination of a classical mechanism and a post-quantum mechanism, so that security holds as long as either one resists
HKDF-SHA-256	Key derivation function that produces a key from one or more secrets
ChaCha20-Poly1305	Symmetric authenticated encryption algorithm, used here with a 256-bit key
RSA-4096	Classical asymmetric mechanism, used here to sign and authenticate the key exchange
Harvest now, decrypt later	Strategy of collecting encrypted communications today in order to decrypt them once computing power allows
Shor's and Grover's algorithms	Quantum algorithms: the first breaks today's asymmetric cryptography, the second weakens symmetric cryptography without breaking it
WebAssembly	Compiled code format executed by browsers, which allows them to run an engine written in a language other than JavaScript, here Rust
WebCrypto	Cryptographic programming interface provided by browsers
Tixeo Workspace	Persistent collaboration space shared by a team or around a project. It brings together a permanent videoconferencing room, messaging, file storage and file sharing, available both during and outside meetings, and acts as a virtual open-plan office. Exchanges and documents are retained: a new member has access to the history, including exchanges that predate their arrival.
Primitive	Basic cryptographic building block (encryption, signature or key exchange algorithm)

References

- **ANSSI-PG-083 v3.00** (20 March 2026), *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* (rules and recommendations for the selection and sizing of cryptographic mechanisms), §2.2.1 and §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* (August 2024):
<https://csrc.nist.gov/pubs/fips/203/final>
- **NIST IR 8547**, *Transition to Post-Quantum Cryptography Standards*
- **NIS Cooperation Group** (June 2025), coordinated roadmap for the post-quantum transition in the European Union
- **RFC 7748** (X25519), **RFC 5869** (HKDF), **RFC 8439** (ChaCha20-Poly1305)

Press contacts

Oxygen (French PR agency)

Eliot Granveau · eliot.g@oxygen-rp.com · +33 6 26 36 41 17

Caroline Hoffmann · caroline.h@oxygen-rp.com · +33 6 77 51 58 42