Wire **for Parliaments**

Wire is a comprehensive secure workspace for parliaments. Wire provides integrated and frictionless productivity with audio and video conferencing, messaging, and file sharing protected by the industry's most stringent security. Wire makes it possible to foster fast, seamless and productive collaboration that users want while ensuring the secrecy, resilience, and data protection that legislative bodies need.

wire

Meeting Complex Secure Communications Needs

Secure parliamentary communication requires nuanced support for varying levels of trust and openness between various parties. Discussions of sensitive legislative matters must be protected from outside cyber threats, and internal threats such as inappropriate information access and data leaks. Political factions must be able to communicate freely internally, coordinate with allies, communicate with constituents, negotiate with rivals, and conduct business with parliamentary administration, all while retaining control over access, security, and privacy. Legislatures must also comply with regulatory and legal frameworks such as GDPR, NIS2, and FOIA.

Security and privacy can't come at the expense of user-friendliness. Secure collaboration must be accessible, integrated, and easy-to-use across various user types and roles.

Wire eliminates these challenges by providing a seamless, secure, and scalable collaboration platform designed for government agencies. It is the only enterprise-class solution secured at scale by the Messaging Layer Security (MLS) standard*[1], while ensuring end-to-end encryption, privacy compliance, and support for thousands of teams. Wire is built for privacy and complies with the most rigorous data protection laws including those of the EU and Switzerland. And Wire makes security delightfully invisible. End users just experience an integrated, full-featured collaboration suite that reduces app fatigue and raises their productivity.

10+
Years of experience

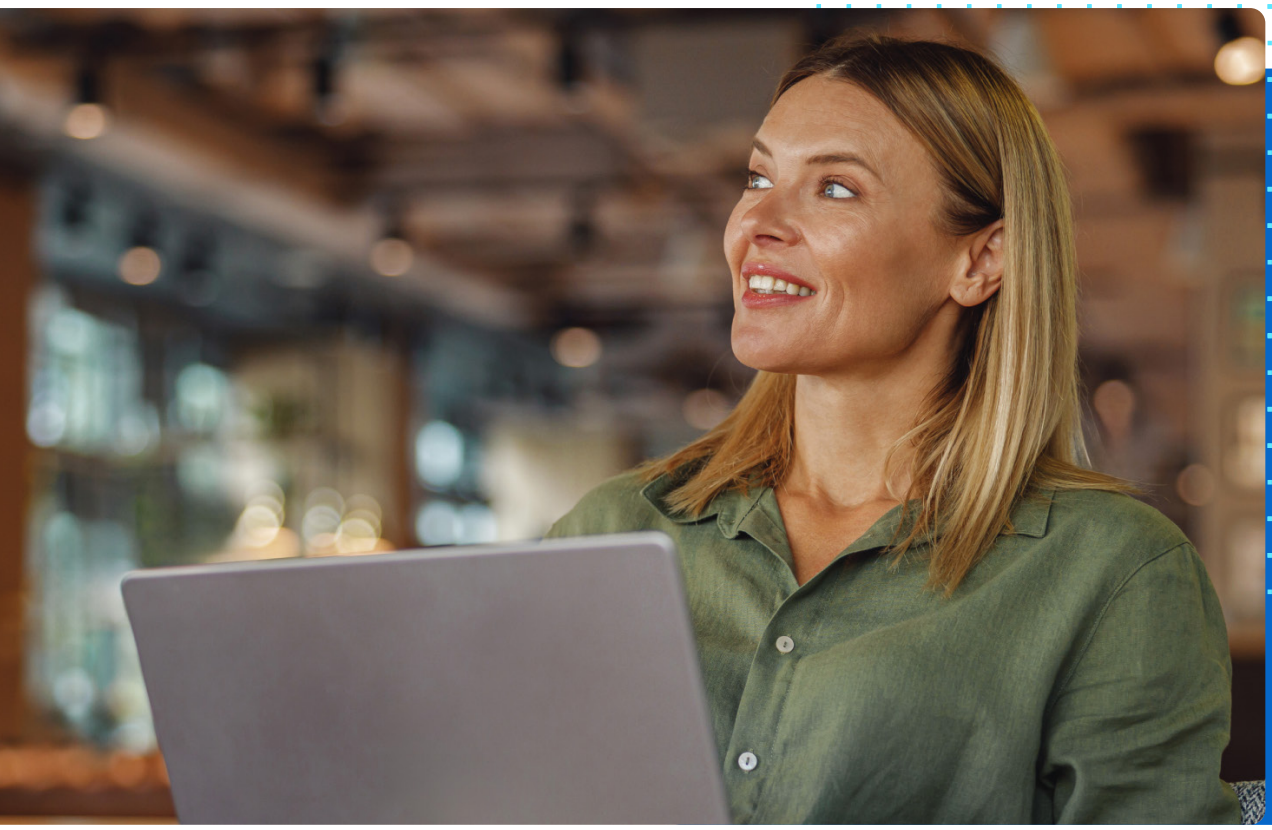
>1800
Customers world wide

Zero
Knowledge Architecture

100%
Ease of use

[1]* Messaging Layer Security (MLS) is the only global open standard for end-to-end encrypted communication. Wire, along with other organizations like Meta, Google, Mozilla, Oxford University, co-founded MLS as the standard for next-gen information security and efficiency for groups in the tens of thousands.

For more information go to: **wire.com/en/security**



Key Features for Parliaments

Secure, Encrypted, and Seamless Communication

Always-On End-to-End Encryption
All features - chat, conferencing, file sharing, reactions, and message timestamps - are always end-to-end encrypted. Whether sending a location, a GIF, or a document, only the intended recipient can access the information. Team admins and operators have no access to any of the information shared, enabling them to manage the team without risking sensitive information.

Multi-tenancy
Maintain separate teams within the same server infrastructure while ensuring role-based segregation. Multiple teams can operate independently without interference. Temporary teams can be set up for employees stationed abroad or for private communication between an employee and their spouse. Security clearance banners within conversations provide clear visibility into participants' authorization levels for discussing sensitive topics.

Federation
Each agency can operate their own independent Wire instances with full administrative control while enabling seamless connections through Wire federation. Users across different backends can communicate as if on a shared infrastructure, ensuring external parties cannot identify federated users or backends. Administrators can regulate federation access and control search visibility, allowing options such as no search, exact handle, or email address only.

ID Shield
Wire offers a painless identity and device verification function called ID Shield, ensuring that users only communicate with intended recipients. Automatic device verification through the organization's Identity Provider (IdP) allows teams to certify, renew, or revoke the verified status of a user's device. Status displays within conversations and calls show who is joining on a trusted device.

Real-World Use Cases

Confidential Legislative Deliberations
Wire facilitates private discussions on sensitive policy proposals, political strategies, and legislative negotiations, ensuring that internal debates remain protected from external scrutiny.

Secure Committee Meetings
Wire allows parliamentary committees to hold virtual meetings where classified documents and sensitive information are exchanged safely, enhancing the integrity of discussions on national security or other critical issues.

Inter-Parliamentary Collaboration
Wire federation enables secure communication channels for coordinating with other legislative bodies, both domestically and internationally, fostering the sharing of confidential insights, comparative policy analysis, and joint initiatives.

Crisis Management and Emergency Coordination
Wire provides a reliable, encrypted medium for urgent communications during national emergencies or crises, ensuring that decision-makers can coordinate responses without risk of information breaches.

Secure Document Sharing and Archival
Wire supports the transmission and storage of sensitive legislative drafts, amendments, and confidential reports, ensuring that all critical documents are exchanged and archived in compliance with strict data protection standards.

The Wire Secure Communications Promise

No matter the use case, Wire always brings you these benefits

E2EE Everything

Next-gen End-to-end encrypted (E2EE) makes security invisible and easy for large and complex orgs

Every piece of data is encrypted, no one – not even Wire – can access your content

Productivity without Risks

Enjoy all the features of well-known collaboration platforms, without the pitfalls of compromised security design choices, and it's configurable to meet your needs

Wire is the only workspace that provides security and productivity in one app

Open Source Transparency

Don't just "trust us", Wire's source code is available on GitHub, frequently independently audited

Transparent by design, the only collaboration platform endorsed by the German government

Zero Trust Architecture

Every piece of data is fully authenticated, authorized, and encrypted before granting access

Never trust, always verified – protects against impersonators and other bad actors

For more information go to: **wire.com/en/government**