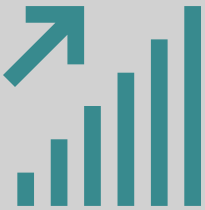
5 Key Elements of a Secure Communication Infrastructure

A security-first architecture embraces the mindset that everything should be scrutinized and authenticated by implementing cutting-edge cybersecurity protocols and operating on the basis of zero-trust. This means enabling electronic communication throughout federal and government agencies with the same level of security and privacy as a face-to-face conversation.



COVID-19 has seen employees bombarded by a staggering volume of attacks with ever-more realistic imitations of messages sent out impersonating well-recognized Government agencies. In fact, FBI data suggests that cyberattacks **have increased by a whopping 400% during the pandemic.**

1. State-of-the-art Encryption

End-to-end encryption (E2EE) is no longer an add-on, it is a fundamental necessity for secure communication. But not all end-to-end encryption is created equal. Using **forward and backward secrecy** ensures that every asset is separately encrypted instead of using one key for everything. Some protocols have also been proven to be more secure than others. A decentralized solution that uses **double-ratchet E2EE** allows for every individual call, message, and file to be separately encrypted on every device, with the keys generated from the device rather than a central server. This protects the information to the smallest possible unit, creating a system that grows more complex - not more valuable - for hackers with every message.

2. Data Sovereignty

Data is crucial in every industry, but for government organizations especially, the pressure is immense and the threats complex. Organizations need to prioritize data sovereignty by implementing **Zero-trust policies** and moving systems that exchange or host data to a **private cloud or on-premise environments**.

3. Continuity of Service

A crucial (and often overlooked) element is the ability to communicate, plan, and update on what's going on should the network be compromised or under attack. If organizations fail to **provide a secure environment for critical/crisis communication** that is independent of their network infrastructure and by invitation only, they can be certain that employees will find their own ways of talking and sharing information. This will put confidential and sensitive information on the radar of third parties, fundamentally eroding the entire cybersecurity defense of the organization, not to mention potential regulatory fines for breach of compliance.

4. Federation & Messaging Layer Security

Wire™ is leading the development of a new, open global standard for secure communication technologies called Messaging Layer Security (MLS).

Partnering with industry leaders, our goal is to create a **secure, interoperable, and federated system that enables users to operate between different messaging systems with the same level of privacy and security that Wire offers.** Alan Duric, Wire's Co-Founder previously helped develop WebRTC and is leading the development of the MLS, which will establish a broader standard for all encryption.

Federation is especially important for government branches to be able to communicate with one another using their own intranet while remaining secure.

5. Hyper-Transparency

Organizations that are interested in implementing platforms that prioritize protecting their digital assets will see security, privacy and transparency go hand-in-hand. There is no true security if there is a violation of privacy, and **the best way to prove real privacy is through an open-source code.** Open source demonstrates that a vendor is truly focused on taking a proactive and less opaque approach in sharing its security measures and enables third-party auditing of the software.

By having the ability to examine the source code of any technology you evaluate, you can determine precisely how the vendor treats data, integrations, encryption key storage, and other potential sources of security risks.