

KATIM



KATIM X4

**UNBREAKABLE COMMUNICATION.
ABSOLUTE PRIVACY.
TOTAL CONTROL.**



SECURING TRUST, EMPOWERING SEAMLESS COLLABORATION

KATIM X4 — a next-generation secure communication and collaboration platform, purpose-built to support custom, national-level cryptography. Designed for elite government agencies and organisations that demand the highest level of privacy, KATIM X4 safeguards your most critical communications — whether messages, voice, video, or file sharing.

Unlike commercial apps, it offers uncompromising security tailored to your unique needs, ensuring full control over your data and protection against even the most advanced threats. When it comes to security, why settle for less?



Encryption & Security

KATIM X4 uses end-to-end encryption with national-level custom cryptography, ensuring only the intended recipient can access messages or calls. Secure storage, encryption at rest, and tamper-resistant architecture further protect against unauthorised access. Each message has unique encryption keys, minimising risks from key compromise. Multi-factor authentication (MFA), self-destructing messages, and anti-surveillance features guarantee privacy and security, even in the most hostile environments.

Administrative capabilities

The KATIM X4 platform offers administrators comprehensive control and customisation to meet organisational needs. Key features include managing internal group communication via User Circles, defining and enforcing security and access policies, comprehensive user management, activity monitoring, and usage analytics. Administrators can also respond to user support requests, receive real-time alerts for critical events, and ensure seamless oversight of the platform's functionalities.

Key Fetures

Voice and Video Calls	Supports high-quality voice and video calls over the internet, making it ideal for secure multimedia communication.
Group Chats	Enables encrypted group chats for secure communication among friends, family, or teams.
Self-Destructing Messages	Allows users to set timers on messages, automatically deleting them after expiration for enhanced privacy.
Pluggable Crypto Support	Offers crypto agility by integrating sovereign cryptographic algorithms, making it adaptable to various encryption needs without exposing the algorithms.
Secure User Search	Verifies contact identities during searches, ensuring users communicate with the right people and preventing man-in-the-middle attacks.
Secure User Onboarding	A secure, seamless registration process, starting with a fully encrypted session. Users authenticate with a one-time code via a secure channel, preventing interception. Cryptographic identity keys are generated to block impersonation, and password rotation policies further strengthen security, reducing exposure to threats.
Cross-Platform Support	Available on iOS, Android, Windows, MacOS, and Linux, ensuring seamless communication across multiple devices.
Multi-point of Presence (MPoP)	Enables users to switch devices without interrupting conversations, with real-time message sync across all connected devices.
Self-Hosting & Data Sovereignty	Offers self-hosting to give organisations full control over data storage, security, and compliance, ensuring adherence to regional regulations and data sovereignty.