The American Journal of Engineering and Technology
ISSN 2689-0984 Volume 08 - 2026

Architecture of The PRIVATGRAM Secure Corporate Messenger for Critical Infrastructure Based on X3DH And Double Ratchet Protocols

Artur Valiulin
Independent PhD Researcher Tashkent University of Information Technologies named after Muhammad al-Khwarizmi Tashkent, Uzbekistan

Received: 28 Mar 2026 | Received Revised Version: 16 Apr 2026 | Accepted: 06 May 2026 | Published: 31 May 2026

Volume 08 Issue 05 2026 | Crossref DOI: 10.37547/tajet/Volume08Issue05-15

Abstract

The rapid development of mobile messaging applications has significantly transformed internal communications within banks, government institutions, and other critical information infrastructure (CII) facilities. However, the use of foreign public communication platforms creates risks associated with confidential data leakage, metadata exposure, dependence on foreign infrastructure, and insufficient administrative control.

This paper proposes the architecture of PRIVATGRAM, a sovereign secure corporate messenger designed for the banking sector and critical infrastructure organizations. The proposed architecture is based on a modified Signal-class security model and integrates the X3DH key agreement protocol and the Double Ratchet algorithm. Unlike consumer-oriented solutions, PRIVATGRAM implements centralized administration, device-level session isolation, persistent ratchet-state storage, role-based access control, secure session recovery mechanisms, and sovereign on-premises deployment capabilities.

The research demonstrates that sovereign secure messaging systems can significantly reduce cybersecurity risks, enhance digital sovereignty, and ensure compliance with the operational requirements of the banking sector and critical infrastructure facilities.

Keywords: Cybersecurity, corporate messenger, X3DH, Double Ratchet, Signal protocol, banking cybersecurity, digital sovereignty, critical infrastructure, PRIVATGRAM.

Cite This Article: Artur Valiulin. (2026). Architecture of The PRIVATGRAM Secure Corporate Messenger for Critical Infrastructure Based on X3DH And Double Ratchet Protocols. The American Journal of Engineering and Technology, 8(05), 159–164. https://doi.org/10.37547/tajet/Volume08Issue05-15

1. Introduction

Digital transformation has made instant messaging systems one of the primary communication channels within enterprises, financial organizations, and government institutions. Employees increasingly exchange operational data, documents, voice messages, customer information, credentials, and management directives through mobile and desktop applications.

This trend is particularly evident in Uzbekistan, where messaging applications have become dominant tools for both personal and business communications. According to regional analytical studies and communication market surveys, approximately 70% of users in Uzbekistan prefer Telegram as their primary messaging platform,

while WhatsApp accounts for roughly 18% of the market. Other platforms occupy significantly smaller shares.

Such dependence on foreign communication ecosystems creates strategic risks for regulated industries. Financial institutions, telecommunications operators, government agencies, industrial enterprises, and transportation infrastructure require substantially higher guarantees of confidentiality, administrative control, auditability, and infrastructure sovereignty than consumer-oriented platforms can provide.

Modern cyber incidents increasingly demonstrate that secure communication requires more than strong cryptography alone. Corporate communication systems must also address identity lifecycle management, session revocation, device control, metadata minimization, regulatory compliance, and operational resilience.

This paper presents the results of developing PRIVATGRAM, a sovereign secure corporate messenger specifically designed for banking institutions and critical infrastructure organizations.

The proposed architecture is based on a modified Signal-class cryptographic model that combines X3DH, Double Ratchet, Curve25519, HKDF, and AES-GCM with enterprise-grade administration mechanisms and device-oriented infrastructure management.

2. Challenges of Using Public Messengers in Critical Infrastructure

The use of public messaging platforms within regulated sectors creates several categories of risks.

Digital Sovereignty Risk

Confidential communications may traverse foreign infrastructure or become subject to foreign jurisdictions beyond national control. Financial institutions and government agencies cannot fully guarantee geographical and legal isolation of sensitive information.

Insider Threats

Employees may intentionally or accidentally transfer confidential files, screenshots, or internal operational information outside trusted corporate environments. Consumer messaging platforms provide limited corporate governance mechanisms to prevent such incidents.

Lack of Administrative Control

Organizations often cannot centrally manage user lifecycle processes, revoke compromised sessions, enforce data retention policies, monitor device activity, or maintain comprehensive audit trails within public communication platforms.

Metadata Exposure

Even when message content is encrypted, metadata such as communication timestamps, social relationships, network patterns, and session behavior may remain observable and available for analytical processing.

Dependence on External Infrastructure

Geopolitical restrictions, sanctions, service outages, or changes in external policies may directly affect operational communications. For critical infrastructure operators, such dependency represents a systemic operational risk.

It should be noted that existing communication platforms provide different levels of secure messaging capabilities.

Table 1. Overview of Existing Solutions

Platform	End-to-End Encryption	Enterprise Administration	On-Premises Deployment	Sovereign Infrastructure
Telegram	Partial / Optional	Low	No	No
WhatsApp	Yes	Low	No	No
Signal	Yes	Low	No	No
Microsoft Teams	Enterprise-Oriented	Medium	Limited	Partial

Most public messaging platforms are optimized for scalability and mass-market usability. In contrast, banking institutions and critical infrastructure operators require secure communication systems with controlled deployment models and centralized administrative governance.

3. Research Contribution and Proposed Architecture

The scientific novelty of this research lies in the development of a modified enterprise-oriented secure communication architecture based on Signal-class cryptographic principles and adapted to the operational requirements of banking institutions and critical infrastructure facilities.

Unlike conventional consumer implementations, the proposed architecture incorporates: Device-level session isolation; Persistent Double Ratchet state storage;

Corporate administrative governance; Centralized user lifecycle management; Session revocation mechanisms; Sovereign infrastructure deployment; Secure metadata separation; Ciphertext isolation across devices.

Consequently, the research extends the traditional user-centric Signal paradigm toward an enterprise-oriented cybersecurity model.

PRIVATGRAM is designed as a sovereign secure communication ecosystem consisting of several interconnected architectural layers.

Administrative Layer

The upper architectural layer contains the corporate administration subsystem. Administrators interact with the platform through secured workstations connected to the Administration Center.

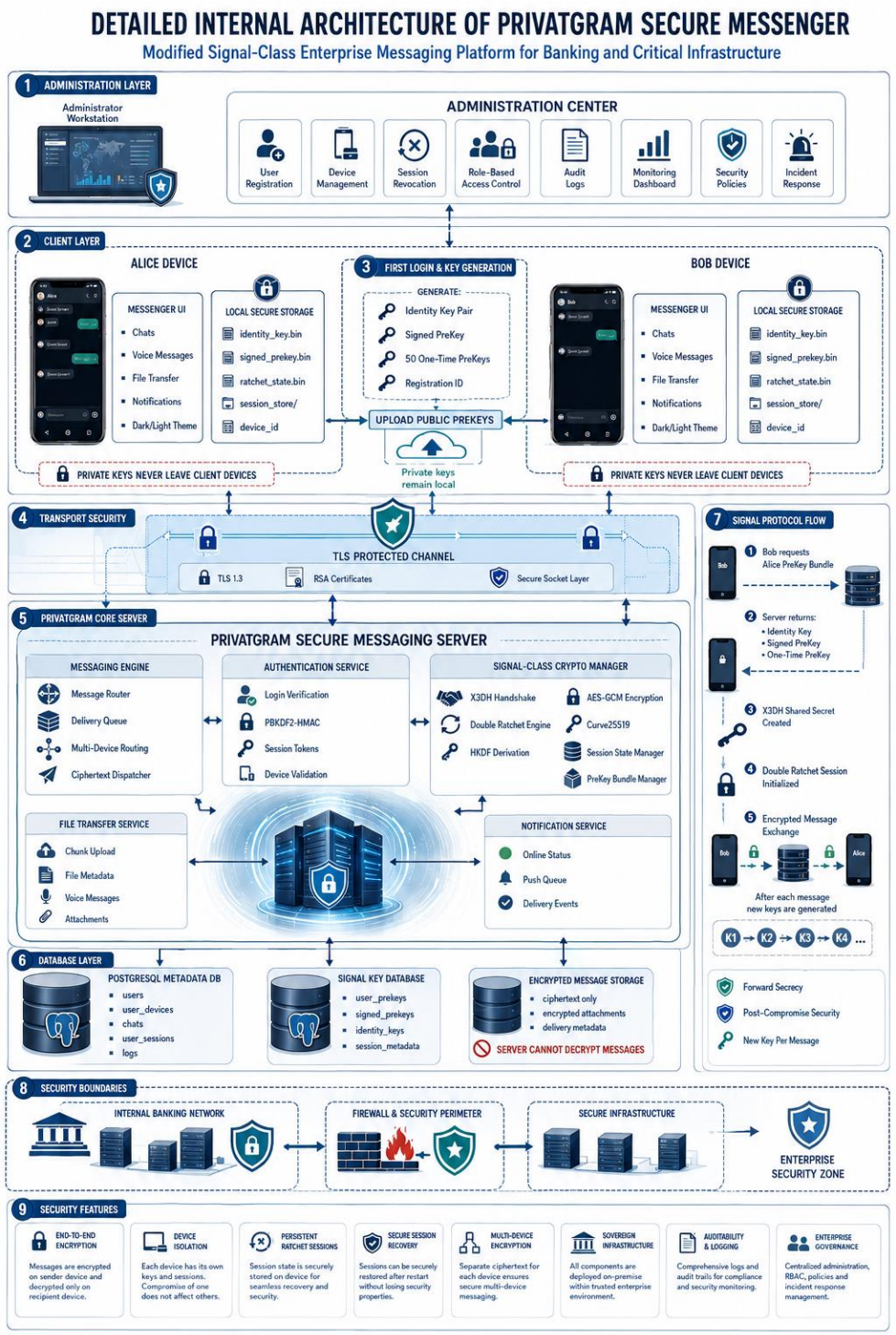

Figure 2. Detailed Internal Architecture of the PRIVATGRAM Secure Messenger

PRIVATGRAM is designed as a sovereign secure communication ecosystem consisting of several interconnected architectural layers.

Administrative Layer

The upper architectural layer contains the corporate administration subsystem. Administrators interact with the platform through secured workstations connected to the Administration Center.

The administrative subsystem supports: User registration; Device management; Session revocation; Role-based access control; Audit logging; Monitoring dashboards; Incident response procedures; Security policy management.

Unlike public messengers, this architecture allows organizations to maintain centralized governance over communication infrastructure.

Client Layer

The client architecture includes desktop and mobile messenger applications operating on isolated endpoint devices.

Each client device maintains: Local secure storage; Identity key storage; Signed prekeys; Ratchet session states; Session persistence modules; Unique device identifiers.

The messenger interface supports encrypted chats, file transfer, voice messaging, notifications, and adaptive user themes.

A fundamental architectural principle is that private cryptographic keys never leave the user's device.

Initial Login and Key Generation

During the first authentication process, the client application generates: Identity Key Pair; Signed PreKey; Fifty One-Time PreKeys; Registration ID.

Only public cryptographic material is uploaded to server infrastructure, while private keys remain exclusively within the local secure storage.

This model significantly reduces the risk of centralized compromise.

Transport Security Layer

Communication between clients and server infrastructure is protected using secure TLS channels.

The transport layer integrates: TLS 1.3; RSA certificates; Secure socket connections; Encrypted transport sessions.

Transport encryption complements end-to-end encryption but does not replace it.

PRIVATGRAM Server Core

The central server infrastructure functions as the primary coordination component of the system.

Message Processing Module

The messaging subsystem provides: Message routing; Delivery queues; Multi-device routing; Ciphertext dispatching.

The server never processes messages in plaintext form.

Authentication Service

Authentication mechanisms implement: Login verification; PBKDF2-HMAC password hashing; Session token validation; Device verification.

Signal-Class Cryptographic Manager

The cryptographic subsystem implements: X3DH asynchronous key agreement; Double Ratchet session evolution; HKDF key derivation; AES-GCM encryption; Curve25519 elliptic-curve cryptography; Session state management; PreKey bundle management.

File Transfer Service

The file-transfer subsystem supports: Chunk-based uploads; Encrypted metadata; Voice messaging; Attachment transmission.

Notification Service

The notification subsystem manages: Online-status synchronization; Push notification queues; Delivery events.

Database Architecture

The database architecture separates operational metadata from encrypted message content. The server infrastructure is incapable of decrypting stored messages.

4. Secure Session Establishment in the PRIVATGRAM Prototype

The PRIVATGRAM prototype was implemented using Python and an enterprise-oriented interface inspired by modern messaging platforms.

Implemented modules include: Authentication; Encrypted messaging; File transfer; Voice and video messaging; Session persistence; Administrative management; Multi-device management; Encrypted data storage.

Particular attention was paid to persistent Double Ratchet state storage. Many experimental secure messengers experience synchronization problems after client restarts, potentially resulting in message loss or chain-key corruption.

The proposed architecture introduces ratchet-state recovery mechanisms designed to preserve secure session continuity.

Additionally, ciphertext isolation between devices has been implemented. This mechanism represents a multi-device cryptographic segmentation model in which each registered device maintains an independent secure session, separate Double Ratchet state, and distinct

ciphertext generation process. This approach enables granular device revocation, compromise localization, and enterprise lifecycle management.

The secure session establishment process follows a modified Signal-class protocol workflow.

Step 1. PreKey Bundle Request

Bob requests Alice's public PreKey Bundle from the server.

Step 2. Bundle Delivery

The server returns: Identity Key; Signed PreKey; One-Time PreKey.

Step 3. X3DH Shared Secret Generation

Bob generates an X3DH shared secret and initializes a secure session.

Step 4. Double Ratchet Initialization

A Double Ratchet session is established between Alice and Bob.

Step 5. Encrypted Message Exchange

Messages are encrypted locally before transmission: «Bob → Ciphertext → Server → Alice»

After each transmitted message, cryptographic keys evolve dynamically.

This mechanism provides: Forward Secrecy; Post-Compromise Security; A "new key for every message" security model.

The proposed architecture offers significant security advantages compared with public communication platforms.

The entire architecture operates within a protected corporate security perimeter and is intended for deployment inside: Internal banking networks; Secure enterprise segments; Sovereign data centers; Isolated governmental infrastructures.

The research demonstrates that strong cryptography alone is insufficient for corporate cybersecurity. Secure communication systems for critical infrastructure must additionally provide centralized governance, device lifecycle management, controlled deployment, local infrastructure ownership, audit capabilities, and regulatory compliance support.

The proposed PRIVATGRAM architecture extends classical Signal-class secure messaging principles toward enterprise-grade operational security and sovereign deployment.

5. Conclusion

Under the conditions of an increasingly digital environment dominated by foreign communication ecosystems, Uzbekistan's critical information infrastructure requires national secure communication platforms.

This paper proposes the architecture of PRIVATGRAM, a sovereign secure corporate messenger designed for banking institutions and critical infrastructure organizations.

The proposed system integrates X3DH asynchronous key agreement, Double Ratchet secure session evolution, AES-GCM authenticated encryption, and HKDF-based key derivation. Unlike consumer messaging platforms, PRIVATGRAM implements device-level session isolation, persistent ratchet recovery mechanisms, sovereign deployment capabilities, and centralized enterprise administration.

The research confirms that combining modern cryptographic protocols with corporate governance mechanisms can significantly improve cybersecurity resilience, support digital sovereignty, and address the operational requirements of critical infrastructure environments.

References

1. Perrin T., Marlinspike M. «The Double Ratchet Algorithm». Signal Foundation. https://signal.org/docs/specifications/doubleratchet/
2. Marlinspike M., Perrin T. «The X3DH Key Agreement Protocol». Signal Foundation. https://signal.org/docs/specifications/x3dh/
3. Signal Foundation. «Signal Protocol Specifications». https://signal.org/docs/
4. Krawczyk H., Eronen P. «HMAC-based Extract-and-Expand Key Derivation Function, RFC 5869». IETF, 2010. https://datatracker.ietf.org/doc/html/rfc5869
5. Dworkin M. «Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC». NIST SP 800-38D. https://csrc.nist.gov/publications/detail/sp/800-38d/final
6. Rescorla E. «The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446». IETF, 2018. https://datatracker.ietf.org/doc/html/rfc8446
7. Cohn-Gordon K., Cremers C., Dowling B., Garratt L., Stebila D. «A Formal Security Analysis of the Signal Messaging Protocol». IEEE European Symposium on Security and Privacy, 2017. https://eprint.iacr.org/2016/1013.pdf
8. Republic of Uzbekistan. Law of the Republic of Uzbekistan “On Cybersecurity” №ZRU-764, April 15, 2022. https://lex.uz/ru/docs/5960609.

9. President of the Republic of Uzbekistan. Resolution № PP-167 “On Additional Measures for Improving the Cybersecurity System of Critical Information Infrastructure Facilities of the Republic of Uzbekistan”, May 31, 2023. https://lex.uz/uz/docs/6479197.

10. President of the Republic of Uzbekistan. Decree № UP-38 “On the Approval of the Cybersecurity Strategy of the Republic of Uzbekistan and the Improvement of the Cybercrime Prevention System”, March 10, 2026. https://lex.uz/ru/docs/8079279.

.