EXTRA SAFE

EXTRA SAFE

Technical White Paper

JANUARY 2026

Contents

Introduction

EXTRA SAFE is a secure communication system designed around cryptographic identity, end-to-end encryption, and strict data minimization. Rather than relying on centralized accounts, passwords, or trusted intermediaries, EXTRA SAFE uses user-controlled cryptographic keys as the foundation for identity, authentication, and access control.

The system treats ownership of cryptographic material as the sole source of authority. User identities are derived from Hierarchical Deterministic wallets, and all authentication is performed through verifiable digital signatures. This approach eliminates the need for credential storage, reduces centralized attack surfaces, and ensures that control over an account cannot be separated from control over its private keys.

This document describes the technical architecture of EXTRA SAFE, including its identity model, encryption mechanisms, data handling principles, and real-time communication design.

Cryptographic Identity and Authorization

In EXTRA SAFE, user identity is based on **cryptographic ownership** rather than centralized credentials. Each user is identified by ownership of a Hierarchical Deterministic (HD) wallet generated from a mnemonic phrase in accordance with **BIP-32** and **BIP-39** standards.

In EXTRA SAFE, a user's Hierarchical Deterministic wallet (HD wallet) functions as their core identity. Instead of usernames and passwords, the system relies on cryptographic signatures to authenticate users and authorize actions.

When a user interacts with the system, their client generates a digital signature using the private key derived from their HD wallet. This signature proves ownership of the private key without revealing it. EXTRA SAFE verifies the signature using the corresponding public key, ensuring that the request was created by the legitimate wallet owner.

The system follows the **ERC-191 Signed Data Standard** and uses a proof-of-private-key-ownership model for authentication. Private keys are generated and stored exclusively on the user's device and are never transmitted to EXTRA SAFE servers.

All actions that require authentication - including registration, login, updating user data, and initiating calls—must be accompanied by a valid digital signature. Only requests with successfully verified signatures are accepted, guaranteeing that no action can be performed without cryptographic control of the associated wallet.

User Types

EXTRA SAFE supports two distinct user types: guest user and registered user.

Guest users operate without a persistent identity or stored user data. No personal or identifying information is stored on EXTRA SAFE servers, and no HD wallet is associated with an EXTRA SAFE number. Access for guest users is limited to browser-based meetings only.

Registered users have a **persistent cryptographic identity** linked to their HD wallet.

User Registration Process

To become a registered user, a client submits a registration request **signed with the user's private key**. Upon successful signature verification:

1. The user's HD wallet public key is associated with a unique **ES Number (EXTRA SAFE Number)**. **Used as user primary identifier, check "Registered user data" section).**
2. The ES Number becomes the **primary identifier** within the EXTRA SAFE ecosystem.
3. The user gains access to more features and services.

Registered User Capabilities:

- Store encrypted associated data
- Initiate and receive phone-like calls with other registered users
- Participate in encrypted chats and meetings
- Use EXTRA SAFE across web and mobile applications

All associated data remains cryptographically bound to the user's wallet identity, ensuring that **control over the account is inseparable from control over the private keys.**

End-to-End Encryption

EXTRA SAFE implements true end-to-end encryption (E2EE), ensuring that only the communicating users can access the contents of messages, files, and calls. No plaintext data or private keys are ever transmitted to or stored on EXTRA SAFE servers.

Key Derivation

Each EXTRA SAFE user is the owner of a Hierarchical Deterministic (HD) wallet generated from a mnemonic phrase according to **BIP-32** and **BIP-39** standards.
From this wallet, EXTRA SAFE deterministically derives cryptographic key material used for encryption.

- **Elliptic curve:** secp256k1
- **Key source:** HD wallet private keys
- **Derivation:** Keys used for encryption are derived locally on the client and never leave the user's device.

This allows key rotation and forward secrecy without requiring additional key storage or centralized key management.

Key Exchange (ECDH)

To establish a secure communication channel between two users, EXTRA SAFE uses **Elliptic-curve Diffie–Hellman (ECDH)** over the secp256k1 curve.

1. Each participant shares their **public key** (derived from their HD wallet).
2. Each participant computes a **shared secret** locally using:
   - Their own private key
   - The other participant’s public key
3. The resulting shared secret is identical on both sides but cannot be derived by third parties.

Encryption (AES-256-GCM)

The shared secret produced by ECDH is used as input to a key derivation function (KDF) to generate a symmetric encryption key. EXTRA SAFE uses AES-256 in Galois/Counter Mode (AES-256-GCM) with a 256-bit key for data encryption.

Registered User Data

- **ES ID (EXTRA SAFE Number):** A globally unique identifier generated at registration. It is public, not encrypted on the server, and used exclusively for user discovery and addressing. The ES ID contains no personal data and cannot be used to derive cryptographic keys.
- **Optional Displayed Name:** A non-unique label associated with an ES ID. It is stored in plaintext and used only for human-readable identification during contact exchange. It plays no role in authentication or authorization.
- **Contacts:** Associated via ES IDs. User-defined contact names and metadata are end-to-end encrypted using keys derived from the user's HD wallet. Servers can observe contact relationships for routing purposes but cannot access contact labels or user annotations.
- **Chat Messages:** Between registered users, these are fully end-to-end encrypted. Encryption keys are derived via ECDH from wallet-based keys and used with authenticated symmetric encryption. Servers act only as message relays and temporary storage and cannot decrypt message contents.
- **Chat Files:** Encrypted on the client prior to upload. File contents are encrypted using symmetric encryption (AES-CTR), while file encryption keys are end-to-end encrypted and unique for each file. Servers store only encrypted file blobs and have no access to file contents or keys.

- **Calls/Meetings History Metadata:** Servers may store minimal call metadata (e.g., timestamps, durations, participant ES IDs) but never have access to media content or encryption keys.

Key Security Principle: All encrypted data remains cryptographically bound to the user’s HD wallet. Control over private keys is required to access associated data, ensuring that user data ownership and access cannot be separated.

Calls (voice and video meetings)

EXTRA SAFE implements peer-to-peer audio and video communication using WebRTC. Connections are established directly between participants whenever possible, with TURN servers used strictly as a relay when network conditions prevent direct P2P connectivity. A signaling server is used only for session coordination and never processes media content.

All calls operate in the form of meetings identified by a unique meeting identifier. To join a meeting, a user initiates an HTTP request to establish a WebSocket connection, authenticated at the handshake level by a digitally signed payload proving ownership of the user's cryptographic identity. The protocol is upgraded to WebSocket only after successful signature verification; invalid or unauthenticated requests are rejected with a forbidden response and no WebSocket connection is established. Upon successful authentication, the user joins the meeting associated with the provided meeting ID.

Audio and video streams are transmitted via RTCPeerConnection. When relayed through TURN, media data is forwarded without being stored or processed by the server. Media streams are protected using WebRTC's built-in security mechanisms, including encrypted transport.

In-meeting messaging is implemented using WebRTC DataChannels and does not persist data on the server. All messages and files exchanged via the in-meeting chat are end-to-end encrypted, as described in the end-to-end encryption section.

Web version & mobile app

The web version allows guest users to join meetings but does not provide the full feature set available in the mobile application. Advanced features - including contact management, chat messaging, call history, and calls with push notifications are available exclusively to registered users. Access to the mobile application is limited to registered users only.

Conclusion

EXTRA SAFE demonstrates an approach to secure communication in which trust is derived from cryptography rather than institutional control. By anchoring identity, authentication, and authorization to user-owned cryptographic keys, the system removes reliance on centralized credentials and reduces systemic attack surfaces.

End-to-end encryption is enforced at the protocol level, ensuring that messages, files, and real-time media remain accessible only to intended participants. Servers are intentionally constrained to coordination and relay roles and are unable to access user content or cryptographic material. This separation of responsibilities limits the impact of server compromise and enables a verifiable zero-knowledge architecture.

This design illustrates how secure communication systems can be constructed to minimize trust, reduce misuse potential, and enforce privacy by default through technical means.

EXTRA SAFE

Try it now

and let us know what you think at

hello@extrasafe.chat

Download on the App Store

GET IT ON Google Play