SecurityNet

Technical Architecture & Security Model Overview

Version 1.1
March 2026

Prepared by
Ian Zatman
Founder & Architect, SecurityNet

SecurityNet is a privately licensed, owner-controlled encrypted communication environment designed for small, high-trust networks.

Table of Contents

`

SecurityNet

Technical Architecture & Security Model Overview

This document provides a high-level architectural overview of SecurityNet's communication and governance model.

Executive Summary

SecurityNet is a licensed, owner-controlled encrypted communication platform designed for small, high-trust networks requiring controlled, private coordination without reliance on cloud infrastructure.

The system architecture incorporates:

- Mediated peer-to-peer session establishment
- Ephemeral per-connection encryption
- Per-delivery encryption keys
- Explicit permission-based identity pairing
- Default-deny administrative governance
- Runtime digital signature verification

SecurityNet does not store message content centrally and does not retain persistent communication metadata beyond active session requirements.

It is designed for controlled encrypted coordination within defined networks — not for anonymity or public social messaging.

1. Design Principles

SecurityNet is designed around four core principles:

1. Direct device-to-device encrypted communication
2. No centralised storage of message or file content
3. Explicit permission-based network membership
4. Ephemeral session encryption with controlled lifecycle

SecurityNet is not a cloud messaging platform. It operates as a licensed, owner-controlled encrypted communication environment for small, high-trust networks. Communication requires both endpoints to be online simultaneously. SecurityNet does not queue or store messages centrally.

---

2. Network Model

SecurityNet uses a mediated peer-to-peer connection model.

A lightweight mediator (relay) is used only to:

- Determine whether a recipient is online
- Facilitate initial session establishment
- Exchange encrypted session material during connection setup

Once the encrypted tunnel is established:

- File and chat data flow directly through the encrypted session
- No message or file content is stored on any central server
- The relay does not retain metadata beyond the active session lifecycle
- After establishment, active transfers proceed directly between devices and do not depend on the mediator.

The mediator is not a data repository and does not store communication history.

---

3. Session Establishment & Key Exchange

When a user initiates communication:

1. Session-level encryption material is generated dynamically for each connection.
2. During the initial connection process, the recipient's availability is confirmed.
3. If no connection is established, the generated session key is discarded.
4. If the recipient is online, the session key is securely exchanged via the mediator.
5. This key becomes the symmetric encryption key protecting the session tunnel.

The session tunnel exists only for the duration of the active transfer.

Upon completion:

- The tunnel is destroyed.
- The session encryption key is no longer active.

4. Per-Connection and Per-Delivery Encryption

SecurityNet derives encryption material per connection.

Within an active session:

- Multiple files may be transmitted.
- Each transfer uses independently generated encryption material, ensuring cryptographic isolation between deliveries.
- That delivery key is exchanged securely during the session “Link” phase.
- The recipient stores the delivery key locally to enable later decryption.

This design ensures:

- Compromise of one delivery key does not expose other files.
- Encryption material is not reused across sessions.
- Delivery-specific keys are cryptographically independent of one another.

---

5. Authentication & Permission Model

SecurityNet uses a layered permission model:

Identity Pairing

Communication requires mutual exchange of SecurityNet IDs.

- User A must explicitly add User B.
- User B must explicitly add User A.
- Without pairing, communication cannot occur.

No unsolicited inbound communication is possible.

License Owner Governance

Each licensed network has a designated License Owner.

- New internal users must be explicitly authorised before they can log in.
- Permissions such as “Invite External” and “Create Groups” are disabled by default.
- The License Owner must deliberately enable these permissions.

SecurityNet does not currently implement device binding as an authentication factor.
Authentication is based on:

- SecurityNet ID pairing
- License Owner approval
- Session-based encrypted tunnel establishment

6. Metadata Handling

During active sessions:

- No message or file content is transmitted through the SecurityNet website infrastructure.
- No content is stored centrally.
- The mediator temporarily handles routing metadata necessary for session establishment.

This metadata is:

- Used only during the active session
- Not retained after session termination
- Not logged persistently

Local activity logs exist only on sender and recipient machines.

These logs:

- Record SecurityNet IDs only
- Do not record IP addresses
- Do not record ports
- Do not include message or file content

---

7. External Users

External users:

- Hold their own independent SecurityNet license
- May be invited only if permission is granted by the License Owner
- Are isolated from internal groups
- Communicate only with the inviting user

External connections do not expand internal network access.

---

8. Runtime Integrity Verification

All SecurityNet executables are digitally signed.

At startup:

- Each executable verifies its own digital signature.
- If the binary is modified, unsigned, or corrupted, execution is refused.

This prevents tampered binaries from operating within the network.

Signature validation is performed locally at application startup.

9. Operational Boundaries

SecurityNet operates under the following assumptions:

- Endpoints are trusted and not compromised by malware.
- Users protect their local systems with standard security practices.

SecurityNet does not:

- Protect against local device compromise
- Provide anonymity against network-level surveillance
- Act as a censorship circumvention tool

It is designed for controlled encrypted coordination within defined, permission-governed networks.