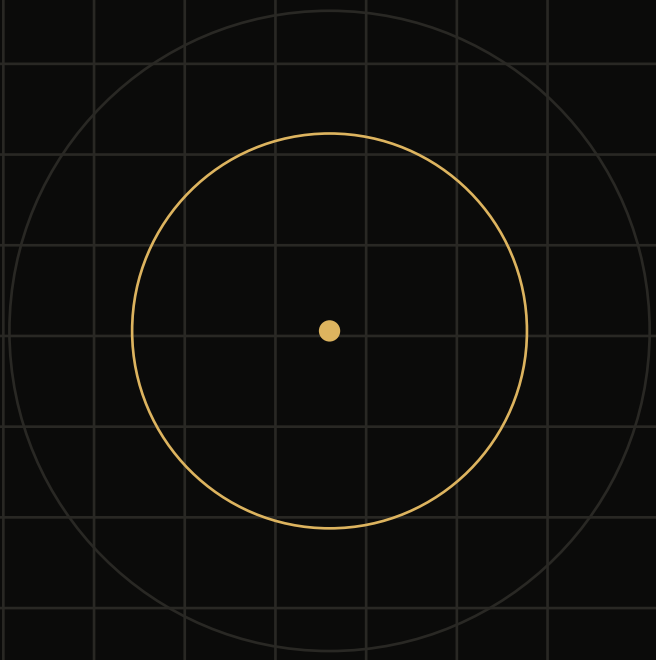
VENTEX

CONNECT / WHITEPAPER 01



SECURITY & ARCHITECTURE

A technical whitepaper for the controlled MVP

EDITION 01 / 09 AUGUST 2026

NOT EXTERNALLY AUDITED

01

Executive summary

VENTEX Connect is a European-oriented communication platform for operational teams. This paper deliberately separates implemented controls, pilot capabilities and planned assurance.

01

DEVICES AS A SECURITY BOUNDARY

Sessions, keys and revocation are associated with a visible device.

02

CONTENT PROTECTION BEFORE TRANSPORT

Messages and attachments are encrypted on the endpoint.

03

EVIDENCE BEFORE CLAIMS

Tests and boundaries are recorded; external certification is never implied.

This document is a technical product description, not an audit report or certification.

02

System boundary

The public product site, installable PWA and API are separate applications. Only the TLS edge is public. Data stores and internal services remain on a private network.

03

Threat model

The current design considers stolen credentials, lost endpoints, unauthorised API calls, compromised transport layers and an inquisitive service operator. A fully compromised endpoint remains outside the protection boundary.

ACCOUNT

Credential stuffing

Rate limits by IP and identifier; rotating refresh tokens.

DEVICE

Lost endpoint

Visible devices, targeted revocation and a local panic function.

SERVICE

Curious server

Ciphertext content; key envelopes for each authorised device.

CLIENT

Injected code

Nonce-based CSP, restrictive delivery and integrity verification.

OUT OF SCOPE

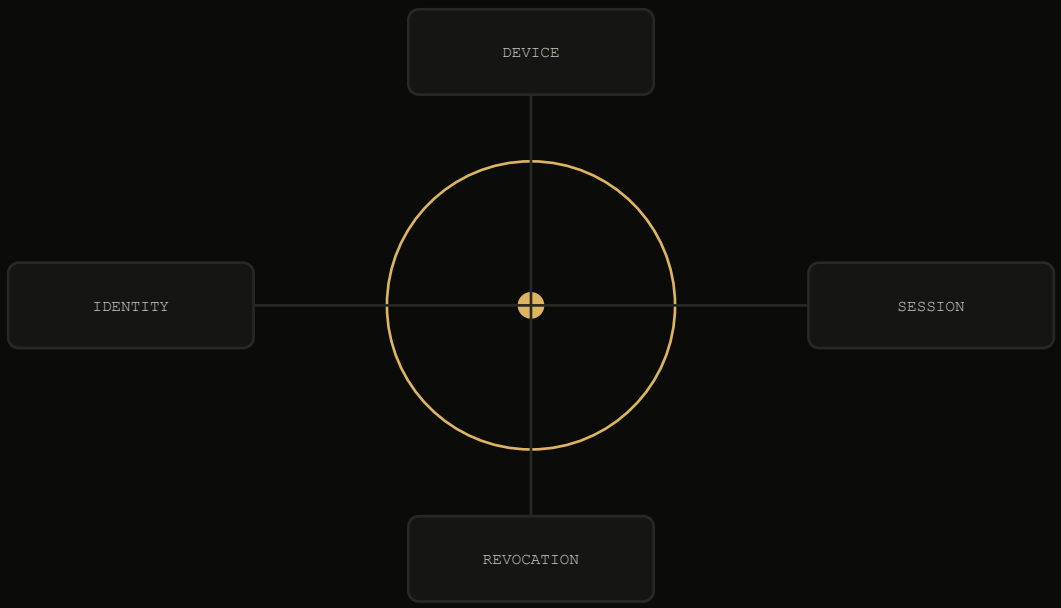
Fully compromised endpoint, coerced authorised user, hardware side channels, and undisclosed platform vulnerabilities.

04

Identity, devices and sessions

Short-lived access tokens and rotating refresh tokens are managed per device. Revocation can target one session. Login history and security-relevant events provide accountability.

- Device-bound refresh sessions
- Reuse detection
- Individual session revocation
- Safety numbers for key changes



05

Content protection

Message bodies and attachments are encrypted on the endpoint with AES-256-GCM. X25519, with P-256 as a fallback, wraps conversation keys for each authorised device through ECDH and HKDF.

- No plaintext message body for encrypted content
- Encrypted editing
- Local decryption into short-lived file URLs
- Filename encrypted; type and ciphertext size visible

06

Ratchet maturity

The active baseline uses forward-moving sender chains with periodic renewal. The Double Ratchet is implemented and browser-tested, but activation remains limited to an explicit pilot allowlist.

ASSURANCE BOUNDARY

No fleet-wide Double Ratchet. No claim of Signal-level assurance or complete post-compromise security.

07

Mission Rooms

Mission Rooms assign communication to an operational context. Members, roles, messages, files and pins stay in one situation. Tasks and the mission record are labelled as a target model in the public simulator.

SIMULATOR

LOCAL PRODUCT PREVIEW

Alarm, channel, tasks and evidence run only in the visitor's browser.

08

Deployment model

Production requires separate public hostnames, private data components, encrypted off-site backups and a tested recovery process.

www.ventex-connect.com	PRODUCT SITE
app.ventex-connect.com	PWA / WEB / API
docs.ventex-connect.com	PUBLIC DOCUMENTATION
status.ventex-connect.com	PUBLIC STATUS / SAME ORIGIN

PRIVATE / POSTGRESQL / REDIS / OBJECT STORAGE / BACKUPS

09

Operations and status

The status portal performs explicit HTTPS origin checks. Unconfigured services appear as not monitored. Production additionally requires an independent external monitor.

- TLS and HSTS at the public edge
- System and application monitoring
- Alerting outside the primary server
- Recovery drill with measured RPO and RTO

STATUS / JSON / RSS

PUBLIC REACHABILITY

Configured HTTPS health endpoints only. Internal URLs and diagnostic details stay private.

10

Assurance roadmap

Internal evidence reduces defects but does not replace independent review. High-security claims require an architecture review, penetration test and cryptography audit with a named scope.

ACTIVE	Automated quality gates
ACTIVE	Browser and multi-device evidence
PLANNED	External penetration test
PLANNED	Independent cryptography audit
LATER	Formal compliance programme

NOT EXTERNALLY AUDITED

11

Pilot checklist

A release begins with synthetic data and a named pilot group. The following points must be observed and recorded in practice.

01	Two accounts on separate devices
02	Secondary device and key change
03	Send, edit, file and voice message
04	Realtime reconnect without duplicates
05	Revoke a device and verify again
06	Restore a backup
07	Accept known boundaries in writing

Security is not an adjective.
It is a verifiable state.

docs.ventex-connect.com / trust-center