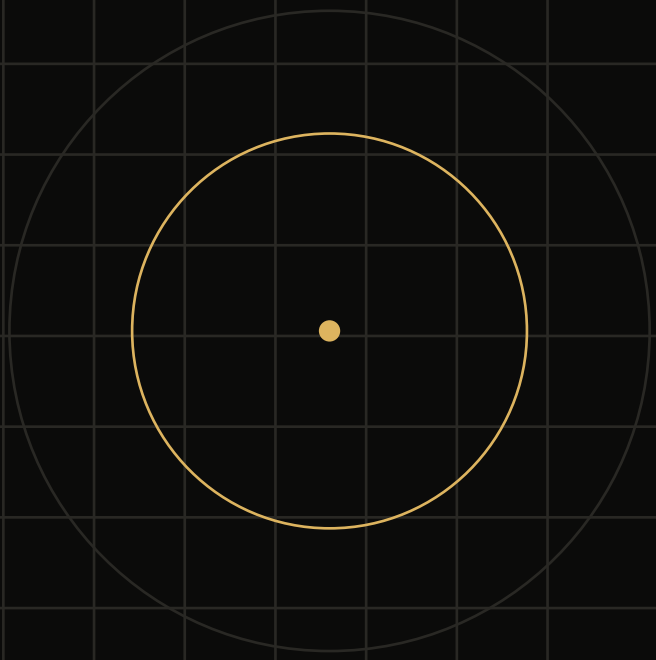
VENTEX

CONNECT / WHITEPAPER 01



SECURITY & ARCHITECTURE

Ein technisches Whitepaper zum kontrollierten MVP

AUSGABE 01 / 09. AUGUST 2026

NICHT EXTERN AUDITIERT

01

Zusammenfassung

VENTEX Connect ist eine europäisch ausgerichtete Kommunikationsplattform für operative Teams. Dieses Papier trennt implementierte Kontrollen, Pilotfunktionen und geplante Assurance bewusst voneinander.

01

GERÄTE ALS SICHERHEITSGRENZE

Sitzungen, Schlüssel und Widerruf werden einem sichtbaren Gerät zugeordnet.

02

INHALTSSCHUTZ VOR TRANSPORT

Nachrichten und Anhänge werden auf dem Endgerät verschlüsselt.

03

NACHWEIS VOR CLAIM

Tests und Grenzen werden dokumentiert; externe Zertifizierung wird nicht vorgetäuscht.

Dieses Dokument ist eine technische Produktbeschreibung, kein Auditbericht und keine Zertifizierung.

02

Systemgrenze

Die oeffentliche Produktseite, die installierbare PWA und die API sind getrennte Anwendungen. Nur die TLS-Kante ist oeffentlich. Datenhaltung und interne Dienste bleiben in einem privaten Netz.

PUBLIC BOUNDARY

INTERNAL SERVICES / PRIVATE NETWORK / NO PUBLIC ADMIN PORTS

03

Bedrohungsmodell

Der aktuelle Entwurf betrachtet gestohlene Zugangsdaten, verlorene Endgeräte, unberechtigte API-Aufrufe, kompromittierte Transportschichten und einen neugierigen Dienstbetreiber. Ein vollständig kompromittiertes Endgerät bleibt außerhalb der Schutzwirkung.

ACCOUNT

Credential stuffing

Ratenbegrenzung nach IP und Kennung; rotierende Refresh Tokens.

DEVICE

Verlorenes Gerät

Sichtbare Geräte, gezielter Widerruf und lokale Panikfunktion.

SERVICE

Neugieriger Server

Inhalte als Chiffrat; Schlüsselumschläge je berechtigtem Gerät.

CLIENT

Eingeschleuster Code

CSP mit Nonce, restriktive Auslieferung und Integritätsprüfung.

OUT OF SCOPE

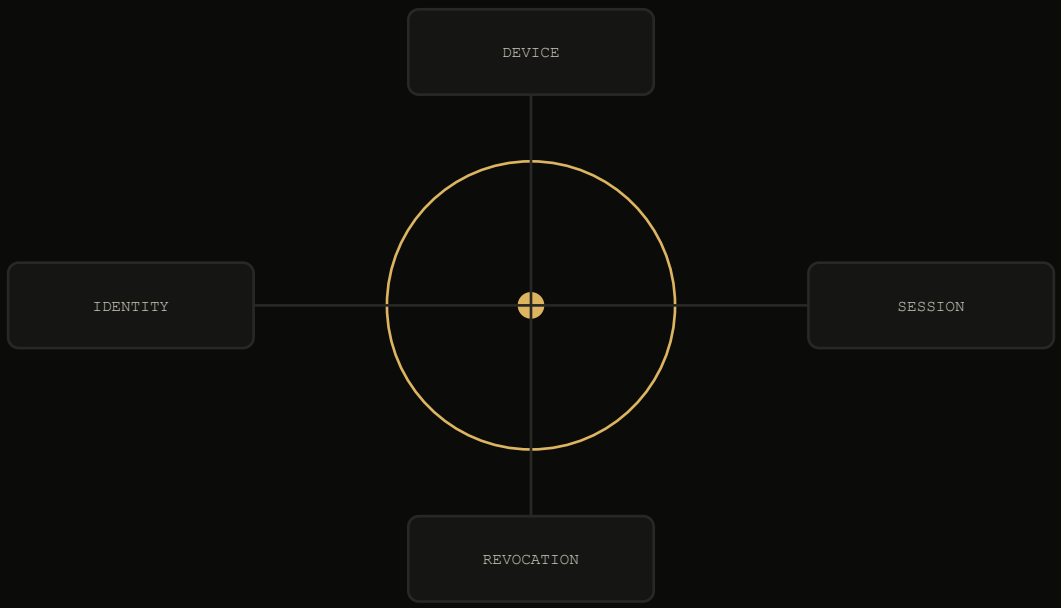
Fully compromised endpoint, coerced authorised user, hardware side channels, and undisclosed platform vulnerabilities.

04

Identität, Geräte und Sitzungen

Kurze Access Tokens und rotierende Refresh Tokens werden pro Gerät verwaltet. Ein Widerruf kann gezielt erfolgen. Login-Historie und sicherheitsrelevante Ereignisse schaffen Nachvollziehbarkeit.

- Gerätegebundene Refresh-Sitzungen
- Wiederverwendungserkennung
- Individueller Sitzungswiderruf
- Sicherheitsnummern für Schlüsselwechsel



05

Inhaltsschutz

Nachrichtentexte und Anhänge werden auf dem Endgerät mit AES-256-GCM verschlüsselt. X25519, mit P-256 als Rückfall, verpackt Conversation-Schlüssel pro berechtigtem Gerät über ECDH und HKDF.

- Kein Klartext-Nachrichtenfeld für verschlüsselte Inhalte
- Verschlüsselte Bearbeitung
- Lokale Entschlüsselung kurzlebiger Datei-URLs
- Dateiname verschlüsselt; Typ und Chiffratgröße sichtbar

06

Ratchet-Reifegrad

Der aktive Basisschutz nutzt vorwärts laufende Senderketten mit regelmäßiger Erneuerung. Der Double Ratchet ist implementiert und im Browser erprobt, wird aber nur über eine explizite Pilotfreigabe aktiviert.

ASSURANCE BOUNDARY

Kein flächenweiter Double Ratchet. Keine Behauptung von Signal-Niveau oder vollständiger Post-Compromise Security.

07

Mission Rooms

Mission Rooms ordnen Kommunikation einem operativen Kontext zu. Mitglieder, Rollen, Nachrichten, Dateien und Pins bleiben in einer gemeinsamen Lage. Aufgaben und Einsatzakte sind im oeffentlichen Simulator als Zielmodell gekennzeichnet.

SIMULATOR

LOCAL PRODUCT PREVIEW

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

08

Deployment-Modell

Produktion erfordert getrennte öffentliche Hostnamen, private Datenkomponenten, verschlüsselte Offsite-Backups und einen getesteten Wiederherstellungsprozess.

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

Betrieb und Status

Das Statusportal führt explizite HTTPS-Origin-Checks aus. Nicht konfigurierte Dienste erscheinen als nicht überwacht. Für Produktion ist zusätzlich ein unabhängiger externer Monitor erforderlich.

- TLS und HSTS an der öffentlichen Kante
- System- und Applikationsmonitoring
- Alarmierung außerhalb des primären Servers
- Restore-Test mit gemessenem RPO und RTO

STATUS / JSON / RSS

PUBLIC REACHABILITY

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

10

Assurance-Roadmap

Interne Belege reduzieren Fehler, ersetzen aber keine unabhängige Prüfung. Vor Hochsicherheitsclaims sind Architekturreview, Penetrationstest und Kryptografieaudit mit benanntem Umfang erforderlich.

AKTIV	Automatisierte Qualitätsgates
AKTIV	Browser- und Multi-Device-Belege
GEPLANT	Externer Penetrationstest
GEPLANT	Unabhängiges Kryptografieaudit
SPÄTER	Formales Compliance-Programm

NICHT EXTERN AUDITIERT

11

Pilot-Checkliste

Eine Freigabe beginnt mit künstlichen Daten und einer benannten Pilotgruppe. Die folgenden Punkte müssen praktisch beobachtet und dokumentiert werden.

01	Zwei Konten auf getrennten Geräten
02	Zweitgerät und Schlüsselwechsel
03	Senden, Bearbeiten, Datei und Sprachnachricht
04	Realtime-Reconnect ohne Duplikate
05	Gerät entziehen und erneut prüfen
06	Backup wiederherstellen
07	Bekannte Grenzen schriftlich bestätigen

Sicherheit ist kein Adjektiv.
Sie ist ein nachprüfbarer Zustand.

docs.ventex-connect.com / trust-center