VENTEX

RESEARCH / BASELINE 01

# SECURE ENTERPRISE COMMUNICATION BASELINE 2026

Zwölf überprüfbare Kontrollen für belastbare operative Kommunikation

AUSGABE 01 / 15. AUGUST 2026

OFFENE EVIDENZSYNTHESE / KEINE ZERTIFIZIERUNG

01

# Executive Baseline

Sichere Unternehmenskommunikation ist kein einzelnes Verschlüsselungsmerkmal. Sie entsteht aus einer nachweisbaren Kette von Governance, Identität, Endgerät, Sitzung, Berechtigung, Inhaltsschutz, Widerruf, Wiederanlauf und Auditierbarkeit.

01

**SCHUTZUMFANG**

Jeder Claim nennt Systemgrenze, Angreifermodell und offene Metadaten.

02

**ÜBERGÄNGE**

Verlust, Rollenwechsel, Widerruf und Wiederanlauf werden praktisch geprüft.

03

**EVIDENZ**

Negative Tests und Maximalwerte bleiben sichtbar; Durchschnittswerte verdecken keinen Blocker.

Diese Baseline ist eine normative Synthese. Sie ist kein Marktranking, keine Rechtsberatung, keine Produktzertifizierung und kein Nachweis, dass VENTEX Connect jede beschriebene Kontrolle bereits erfüllt.

02

# Methode und Quellenlogik

VENTEX ordnet aktuelle Primärquellen einem vollständigen Kommunikationsablauf zu. Die Dokumente werden nicht als gleichwertige Zertifizierungskataloge behandelt: Governance, Identität, Kryptografie, Incident Response und Betrieb liefern unterschiedliche Anforderungen an denselben sicheren Zustand.

01 / GOVERN

### GOVERN

Ziel, Eigentümer und Schutzumfang definieren

02 / OBSERVE

### OBSERVE

Technischen Zustand und Nutzerannahme getrennt messen

03 / DISRUPT

### DISRUPT

Kontrollierte Störung und negative Pfade ausführen

04 / EVIDENCE

### EVIDENCE

Artefakt, Abweichung und Entscheidung veröffentlichen

PRIMARY SOURCES -> CONTROL OBJECTIVES -> NEGATIVE TESTS -> RELEASE EVIDENCE

03

# Die zwölf Kontrollen

01

**Governance**

Schutzumfang, Risiko, Eigentümer

02

**Identitätsbindung**

Enrollment und Nachweis

03

**Authentisierung**

Phishing-Resistenz und Recovery

04

**Gerätevertrauen**

Register, Zustand, Widerruf

05

**Sitzungen**

Bindung, Rotation, Reauth

06

**Berechtigung**

Rollen und Least Privilege

07

**Inhaltsschutz**

E2EE-Grenze und Metadaten

08

**Schlüssel**

Lebenszyklus und Gruppenwechsel

09

**Integrität**

Zustellung und Synchronisation

10

**Incident Response**

Erkennen, widerrufen, sichern

11

**Kontinuität**

Ausweichkanal und Wiederanlauf

12

**Audit & Privacy**

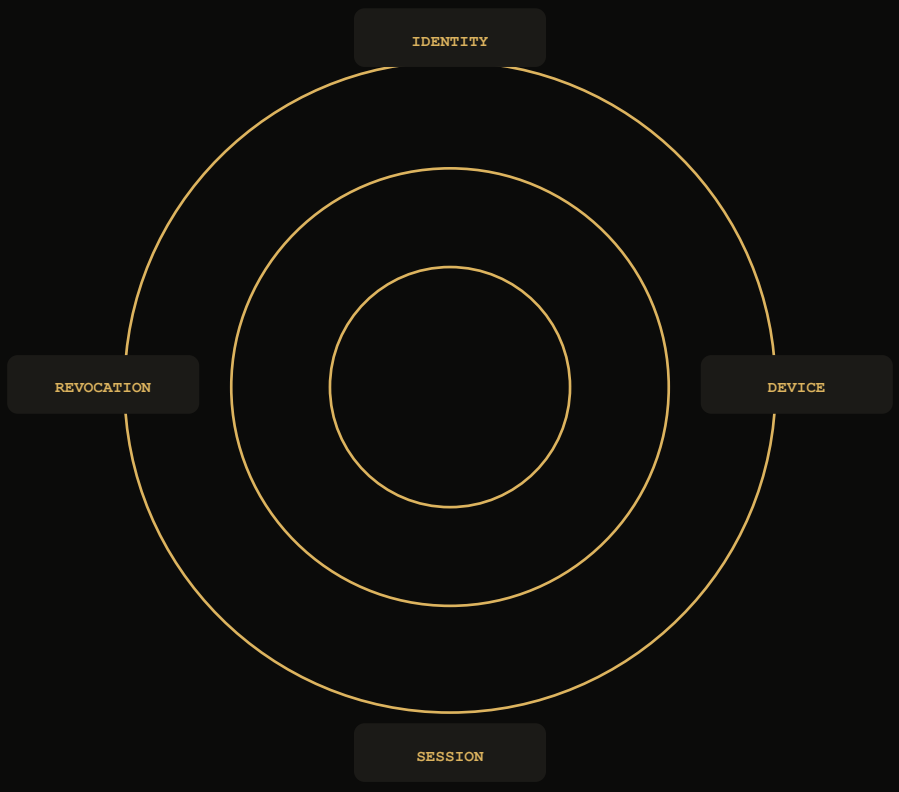
Nachweis, Aufbewahrung, Rechte

04

# Identität, Geräte und Sitzungen

Der sichere Zustand beginnt vor dem Login und endet nicht nach erfolgreicher MFA. Enrollment, zusätzliche Authentikatoren, Reauthentisierung, Recovery, Invalidierung und Lebenszyklusprotokolle müssen als eine Kontrollkette geprüft werden.

- Neues Gerät nur über einen nachvollziehbaren Bindungsweg zulassen
- Gestohlenen Authentikator und einzelne Gerätesitzung zeitnah invalidieren
- Alte API-, Realtime-, Datei- und Refresh-Pfade nach Widerruf ablehnen
- Technischen Zustand und sichtbare Nutzerbestätigung abgleichen
- Recovery ohne stille Herabstufung der Assurance durchführen



05

# Kryptografie mit benannter Grenze

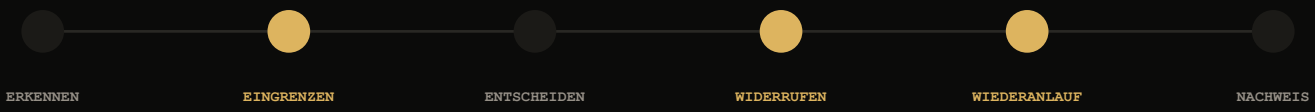
TLS, lokale Verschlüsselung und Ende-zu-Ende-Schutz lösen unterschiedliche Probleme. In Gruppen kommen Mitgliedschaft, asynchroner Schlüsselaufbau, Forward Secrecy und Wiederherstellung nach Kompromittierung hinzu. Ein überprüfbarer Claim benennt Inhalt, Metadaten, Schlüsselpfad und verbleibende Vertrauensannahmen.

| | | |
|---|---|---|
| TRANSPORT | **Authentisierter Kanal** | Netzpfad und Dienstendpunkt |
| CONTENT | **Inhaltsschutz** | Nachrichten, Dateien, Namen |
| GROUP | **Mitgliedschaft** | Add, Remove, Gerätewechsel |
| RECOVERY | **Neuer sicherer Zustand** | Rotation und Rejoin |

06

# Kommunikation während eines Vorfalls

Incident-Kommunikation muss Teil des laufenden Risikomanagements sein. Rollen, Ausweichkanäle, Zeitlinien, Stopkriterien und der kontrollierte Rückweg in den Normalbetrieb werden vor dem Ernstfall festgelegt und mit synthetischen Daten geübt.




STOP / CONTROL

**Sicherer Abbruch ist eine Kontrolle**

Der Test pausiert bei unklarer Identität, unwirksamem Widerruf, Datenverlust, unkontrollierter Berechtigung oder unzulässigen Daten. Ursache, Korrektur und Wiederholung bleiben dokumentiert.

07

# Das Evidenzpaket

Ein Screenshot beweist keine Kontrolle. Eine belastbare Bewertung verbindet erwarteten Zustand, sichtbare Beobachtung, technische Messung, negative Tests, Abweichung und Freigabeentscheidung.

E-01

**Systemgrenze und Datenfluss**

Observable / reproducible / release-bound

E-02

**Rollenmodell und Testkonten**

Observable / reproducible / release-bound

E-03

**Szenarioskripte und Sollwerte**

Observable / reproducible / release-bound

E-04

**Maximale Widerrufslatenz**

Observable / reproducible / release-bound

E-05

**Recovery- und Abweichungsprotokoll**

Observable / reproducible / release-bound

E-06

**Claim-Ledger mit aktuellem Release-Bezug**

Observable / reproducible / release-bound

EXPECTATION + OBSERVATION + MEASUREMENT + DEVIATION + DECISION

08

# Reifegrad ohne Scheingenauigkeit

00

**NICHT DEFINIERT**

Kein Ziel, kein Eigentümer, keine Abnahme

01

**DEFINIERT**

Kontrollziel und Verantwortlichkeit dokumentiert

02

**BEOBACHTET**

Technischer Positivpfad reproduzierbar

03

**VERIFIZIERT**

Negativpfad und Störung gegen Sollwert geprüft

Nächster Schritt: unabhängige Anwendung auf synthetische Szenarien mit vorab definierten Sollwerten und veröffentlichbaren negativen Ergebnissen.

09

# Primärquellen und Evidenzgrenze

Diese Baseline ist eine normative Synthese. Sie ist kein Marktranking, keine Rechtsberatung, keine Produktzertifizierung und kein Nachweis, dass VENTEX Connect jede beschriebene Kontrolle bereits erfüllt.

01 / BSI
**Sicherheit von Messenger-Systemen (2026)**
bsi.bund.de/Publikationen/DVS-Berichte/messenger.pdf

02 / BSI
**VS-AP-0024 - Sichere Messenger und Videokonferenzsysteme**
bsi.bund.de/Zulassung/VS-Anforderungsprofile/BSI-VS-AP-0024

03 / ENISA
**NIS2 Technical Implementation Guidance**
enisa.europa.eu/publications/nis2-technical-implementation-guidance

04 / NIST
**Cybersecurity Framework 2.0**
doi.org/10.6028/NIST.CSWP.29

05 / NIST
**SP 800-63B-4 - Authentication and Authenticator Management**
pages.nist.gov/800-63-4/sp800-63b.html

06 / NIST
**SP 800-61 Rev. 3 - Incident Response**
doi.org/10.6028/NIST.SP.800-61r3

07 / IETF
**RFC 9420 - Messaging Layer Security**
rfc-editor.org/rfc/rfc9420

## Sicherheit beginnt dort, wo Behauptungen prüfbar werden.

VENTEX-CONNECT.COM / RESEARCH / VRB-004