VENTEX

RESEARCH / BASELINE 01

SECURE ENTERPRISE COMMUNICATION BASELINE 2026

Twelve verifiable controls for resilient operational communication

EDITION 01 / 15 AUGUST 2026

OPEN EVIDENCE SYNTHESIS / NOT A CERTIFICATION

01

Executive baseline

Secure enterprise communication is not a single encryption feature. It emerges from an evidenced chain of governance, identity, endpoint, session, authorisation, content protection, revocation, recovery and auditability.

01

SCOPE

Every claim states its system boundary, attacker model and exposed metadata.

02

TRANSITIONS

Loss, role change, revocation and recovery are exercised in practice.

03

EVIDENCE

Negative tests and maxima remain visible; averages never hide a blocker.

This baseline is a normative synthesis. It is not a market ranking, legal advice, product certification or evidence that VENTEX Connect already satisfies every control described.

02

Method and source logic

VENTEX maps current primary sources to a complete communication workflow. The documents are not treated as equivalent certification catalogues: governance, identity, cryptography, incident response and operations contribute different requirements to the same safe state.

01 / GOVERN

GOVERN

Define objective, owner and protection scope

02 / OBSERVE

OBSERVE

Measure technical state and user belief separately

03 / DISRUPT

DISRUPT

Exercise controlled disruption and negative paths

04 / EVIDENCE

EVIDENCE

Publish artefact, deviation and decision

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

03

The twelve controls

01

Governance

Scope, risk and accountable owner

02

Identity binding

Enrolment and evidence

03

Authentication

Phishing resistance and recovery

04

Device trust

Register, state and revocation

05

Sessions

Binding, rotation and reauth

06

Authorisation

Roles and least privilege

07

Content protection

E2EE boundary and metadata

08

Keys

Lifecycle and group changes

09

Integrity

Delivery and synchronisation

10

Incident response

Detect, revoke and preserve

11

Continuity

Alternate channel and recovery

12

Audit & privacy

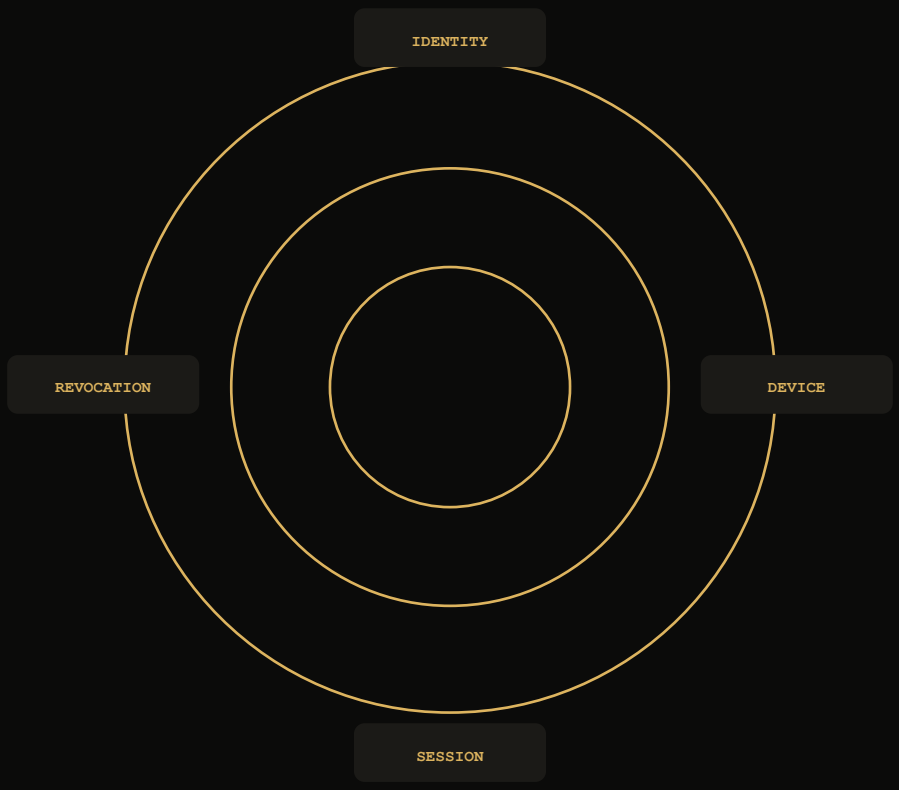
Evidence, retention and rights

04

Identity, devices and sessions

The safe state starts before sign-in and does not end after successful MFA. Enrolment, additional authenticators, reauthentication, recovery, invalidation and lifecycle records must be assessed as one control chain.

- Admit a new device only through a traceable binding path
- Promptly invalidate a stolen authenticator and one device session
- Reject old API, realtime, file and refresh paths after revocation
- Reconcile technical state with visible user confirmation
- Complete recovery without silently lowering assurance



05

Cryptography with a stated boundary

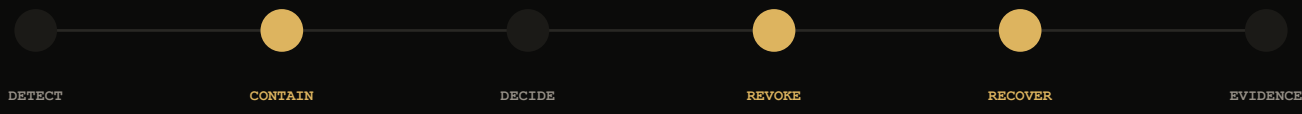
TLS, local encryption and end-to-end protection solve different problems. Groups add membership, asynchronous key establishment, forward secrecy and recovery after compromise. A verifiable claim names content, metadata, key path and remaining trust assumptions.

TRANSPORT	**Authenticated channel**	Network path and service endpoint
CONTENT	**Content protection**	Messages, files and names
GROUP	**Membership**	Add, remove and device change
RECOVERY	**New safe state**	Rotation and rejoin

06

Communication during an incident

Incident communication must be part of ongoing risk management. Roles, alternate channels, timelines, stop criteria and the controlled return to normal operation are defined before an incident and exercised with synthetic data.



STOP / CONTROL

Safe abort is a control

A test pauses on ambiguous identity, ineffective revocation, data loss, uncontrolled authorisation or prohibited data. Cause, correction and re-run remain documented.

07

The evidence pack

A screenshot does not prove a control. A defensible assessment connects expected state, visible observation, technical measurement, negative tests, deviation and release decision.

E-01

System boundary and data flow

Observable / reproducible / release-bound

E-02

Role model and test accounts

Observable / reproducible / release-bound

E-03

Scenario scripts and targets

Observable / reproducible / release-bound

E-04

Maximum revocation latency

Observable / reproducible / release-bound

E-05

Recovery and deviation record

Observable / reproducible / release-bound

E-06

Claim ledger tied to the current release

Observable / reproducible / release-bound

EXPECTATION + OBSERVATION + MEASUREMENT + DEVIATION + DECISION

08

Maturity without false precision

00

UNDEFINED

No objective, owner or acceptance

01

DEFINED

Control objective and ownership recorded

02

OBSERVED

Technical positive path is reproducible

03

VERIFIED

Negative path and disruption tested to target

Next step: independent application to synthetic scenarios with pre-defined targets and publishable negative results.

09

Primary sources and evidence boundary

This baseline is a normative synthesis. It is not a market ranking, legal advice, product certification or evidence that VENTEX Connect already satisfies every control described.

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

Security begins where claims become verifiable.

VENTEX-CONNECT.COM / RESEARCH / VRB-004