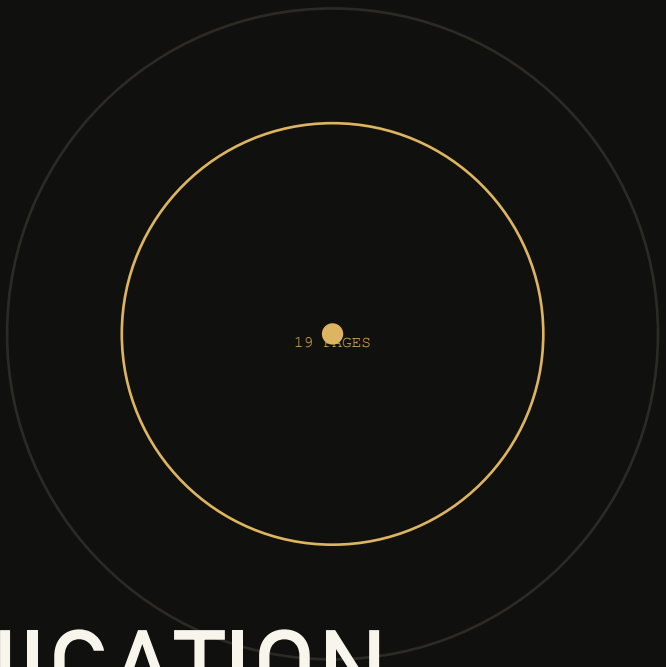
VENTEX CONNECT

PILOT PLAYBOOK / PUBLIC METHOD / 2026



SECURE COMMUNICATION PILOT PLAYBOOK 2026

Eine prüfbare Methode für Einführung, Betrieb und Entscheidung

STATUS / PUBLIC WORKING DOCUMENT

Arbeitsmethode, kein Audit, keine Zertifizierung und keine Rechtsberatung.

VERSION 1.0 / 13 AUGUST 2026 / ventex-connect.com

01

Warum ein Pilot Beweise braucht

Ein sicherer Messenger ist kein isoliertes Interface. Sicherheit entsteht aus Identitäten, Geräten, Rollen, Verhalten, Betrieb und einem getesteten Rückfallweg.

ZIEL

Dieses Playbook übersetzt technische und organisatorische Annahmen in 30 Tage beobachtbare Arbeit.

NICHT-ZIEL

Es ersetzt weder Datenschutzprüfung, Informationssicherheitsmanagement, Penetrationstest noch kryptografisches Audit.

02

Entscheidungsmodell

Der Pilot beantwortet nicht, ob ein Produkt abstrakt 'sicher' ist, sondern ob ein benannter Ablauf unter benannten Bedingungen vertretbar funktioniert.

GO

Kriterien erfüllt, Risiken akzeptiert, Bedingungen und Owner dokumentiert.

ITERATE

Nutzen erkennbar, aber konkrete Lücken verlangen einen weiteren begrenzten Versuch.

STOP

Schutzgrenze, Betrieb oder Nutzen reichen nicht aus.

NO DECISION IST EIN GÜLTIGES ERGEBNIS, WENN EVIDENZ FEHLT

03

Schutzgrenze zeichnen

Vor dem ersten Login wird festgehalten, was innerhalb und außerhalb der Pilotverantwortung liegt.

INNERHALB

- Benannte Konten und Geräte
- Freigegebene Pilotdaten
- Produktfunktionen im definierten Scope
- Support- und Incident-Prozess
- Aufbewahrung und Löschung im Pilot

AUSSERHALB

- Vollständig kompromittiertes Endgerät
- Erzwungene Handlungen berechtigter Nutzer
- Nicht freigegebene Integrationen
- Ungeprüfte Plattformschwachstellen
- Prozesse außerhalb der Charta

04

Bedrohungen als Hypothesen

Das Bedrohungsmodell bleibt praktisch, wenn jede Annahme in eine Übung oder einen überprüfbaren Nachweis übersetzt wird.

BEISPIELE

- Gestohlenes Passwort -> Zweitfaktor und Sitzungsübersicht prüfen
- Verlorenes Gerät -> gezielten Widerruf messen
- Unterbrochene Verbindung -> Reconnect und Duplikate beobachten
- Falscher Empfänger -> Bestätigung und Korrekturablauf testen
- Ausfall Primärkanal -> Kontaktbaum aktivieren

REGEL

Ein Szenario wird nicht heimlich im Produktivbetrieb inszeniert. Zeitpunkt, Testdaten und Abbruchbedingung sind vorab freigegeben.

05

Identität und Geräte

Identität ist ein Lebenszyklus, kein einmaliger Login.

PRÜFPUNKTE

- Registrierung und Einladung
- Gerätename und eindeutige Sitzung
- Passkey oder zweiter Faktor
- Neues Gerät und Schlüsseländerung
- Verlust, Widerruf und Wiederherstellung
- Austritt und Restzugriffe

MESSUNG

Zeit bis zur Erkennung, Zeit bis zum Widerruf, fehlerhafte Wiederholungen und offene Sitzungen nach Abschluss.

06

Workflow vor Featureliste

Der Pilot beginnt mit einem Ablauf, nicht mit einer Tour durch alle Schaltflächen.

ABLAUFKARTE

- Auslöser
- Entscheidung
- benötigte Information
- verantwortliche Rolle
- zulässiger Kanal
- Nachweis
- Rückfallweg

BEISPIEL

Alarm wird bestätigt -> Operator eröffnet Mission Room -> Lageformat wird gepinnt -> Dispatcher weist Aufgabe zu -> Abschlussentscheidung wird protokolliert.

07

Mission-Room-Protokoll

Ein Raum benötigt ein stabiles Lageformat, damit Aktualität und Entscheidung voneinander unterscheidbar bleiben.

LAGEUPDATE

- Zeit / Autor / Rolle
- bestätigte Fakten
- Annahmen
- Entscheidung
- Aufgabe und Owner
- nächster Updatezeitpunkt

VERMEIDEN

- unmarkierte Vermutung
- mehrere parallele Entscheidungsnachrichten
- Datei ohne Kontext
- Screenshot als einziges System of Record

08

Incident-Kommunikation

Während eines Cybervorfalls kann das primäre Identitäts- oder Nachrichtensystem selbst Teil des Problems sein.

AKTIVIERUNG

- Kriterien für Vertrauenswechsel
- unabhängiger Kontaktbaum
- Primär- und Ausweichkanal
- verifizierte Rollen
- fester Update-Takt

RÜCKKEHR

Erst zurückkehren, wenn Identitäten, Geräte, Sitzungen und Integrationen neu bewertet sowie offene Einladungen und Tokens behandelt wurden.

09

30-Tage-Plan

Vier Phasen liefern mehr Erkenntnis als eine lange, unstrukturierte Testperiode.

WOCHE 1 - BASELINE

Onboarding, Kernablauf, zulässige Daten und Messwerte.

WOCHE 2 - REIBUNG

Gerätewechsel, schlechte Verbindung, Datei, Suche und Rollenübergabe.

WOCHE 3 - RESILIENZ

Widerruf, Ausweichkanal und redigierte Incident-Übung.

WOCHE 4 - ENTSCHEIDUNG

Interviews, Evidence Matrix, Risiken und Abschlussbericht.

10

Messwörterbuch

Eine Kennzahl ist nur nützlich, wenn Start, Ende, Einheit, Datenquelle und Owner definiert sind.

KERNMETRIKEN

- Onboarding completion rate
- Median time to first valid message
- Task completion without workaround
- Median device revocation time
- Reconnect duplicates per exercise
- Operator confidence 1-5 mit Begründung

KEINE VANITY-METRIKEN

Anzahl Nachrichten oder Logins belegt allein weder Sicherheit noch operativen Nutzen.

11

Reibungsregister

Umgehung ist wertvolle Evidenz. Sie wird nicht als Nutzerfehler abgetan.

EINTRAG

- Zeit und Rolle
- beabsichtigte Aufgabe
- beobachtete Hürde
- Workaround
- Risiko
- Häufigkeit
- Owner und nächste Prüfung

PRIORISIERUNG

Hohe Häufigkeit plus hohe Schutzwirkung zuerst. Kosmetische Wünsche bleiben getrennt von sicherheitsrelevanter Reibung.

12

Kontrollierte Übungen

Übungen prüfen die Schutzgrenze ohne reale Schäden zu provozieren.

ÜBUNG A

Testgerät als verloren markieren, gezielt widerrufen und alte Sitzung erneut versuchen.

ÜBUNG B

Verbindung trennen, mehrere Nachrichten vorbereiten, wiederverbinden und Reihenfolge/Duplikate prüfen.

ÜBUNG C

Primärkanal als nicht vertrauenswürdig erklären und Kontaktbaum aktivieren.

ABBRUCH

Sofort stoppen bei unerwarteten Produktivdaten, realem Sicherheitsereignis oder unklarer Zuständigkeit.

13

Evidence Matrix und Claim Ledger

Die Evidence Matrix beschreibt, was beobachtet wurde. Das Claim Ledger steuert, was daraus öffentlich gesagt werden darf.

EVIDENCE

- Anforderung
- Test
- Ergebnis
- Artefakt
- Owner
- Datum
- Status

CLAIM

- Formulierung
- Zielgruppe
- tragende Evidence-IDs
- Grenze
- Freigebender
- Ablaufdatum

CLAIMS VERFALLEN, WENN DIE TRAGENDE VERSION ODER EVIDENZ VERALTET

14

Privacy und Beobachtung

Pilotmessung soll Produktentscheidungen ermöglichen, nicht verdeckte Personenprofile erzeugen.

MINIMIERUNG

- nur erforderliche Ereignisse
- möglichst aggregierte Kennzahlen
- kurze Aufbewahrung
- rollenbasierter Zugriff
- Redaktion vor Export

TRANSPARENZ

Teilnehmende wissen vorab, welche Daten zu welchem Zweck erhoben werden, wer sie sieht und wann sie gelöscht werden.

15

Security-Ereignis im Pilot

Ein echter Verdacht unterbricht die Übung. Betriebliches Incident Handling hat Vorrang vor Erkenntnisgewinn.

SOFORT

- Pilot Owner und Security Contact informieren
- betroffenen Ablauf stoppen
- Beweise nicht verändern
- Zugänge nur nach Freigabe widerrufen
- Ausweichkanal nutzen

DANACH

- Timeline und Entscheidungen dokumentieren
- Datenschutz- und Meldepflichten separat bewerten
- Wiederaufnahme ausdrücklich freigeben

16

Abschlussentscheidung

Die Entscheidung wird an Kriterien gebunden, nicht an allgemeine Begeisterung.

ENTSCHEIDUNGSVORLAGE

- Welche Kriterien sind erfüllt?
- Welche sind teilweise oder nicht erfüllt?
- Welche Risiken bleiben und wer akzeptiert sie?
- Welche Bedingungen gelten für die nächste Stufe?
- Welche Daten und Zugänge werden beendet?

SIGN-OFF

Sponsor: _____ Pilot Owner: _____ Security: _____ VENTEX: _____ Datum: _____

17

Transfer in den Betrieb

Ein erfolgreicher Pilot ist noch kein Produktionsbetrieb. Der Übergang benötigt eigene Abnahmen.

VOR PRODUKTION

- Betriebs- und Supportmodell
- Backup und Restore-Test
- Monitoring außerhalb des Primärsystems
- Rollen- und Berechtigungsmodell
- Datenverarbeitung und Verträge
- Penetrationstest und unabhängige Reviews nach Schutzbedarf

CHANGE CONTROL

Pilotkonfiguration und produktive Konfiguration werden versioniert, verglichen und separat freigegeben.

18

Quellen und Review

Die Quellen liefern Orientierung für Authentisierung, Incident Response, Kommunikation, Datenschutz und Gruppenkommunikation.

PRIMÄRQUELLEN

- NIST SP 800-61 Rev. 3
- NIST SP 800-63B-4
- CISA Emergency Communications Guidance
- Regulation (EU) 2016/679
- RFC 9420 Messaging Layer Security
- ENISA Secure Group Communications

REVIEW

Owner: VENTEX Connect Product & Security
Version: 1.0
Stand: 13. August 2026
Nächster Review: bei wesentlicher Produktänderung, spätestens 13. Februar 2027

PUBLIC METHOD / NOT AN AUDIT OR CERTIFICATION