Technical and Organisational Measures

Stand: 2026-06-08

Status: Pilot-Arbeitsdokument, keine Rechtsberatung.

Diese TOMs beschreiben den aktuellen Zielzustand fuer Harpocrypt-Piloten. Sie muessen vor produktiven Kunden mit tatsaechlicher Infrastruktur, Rollen und Lieferanten abgeglichen werden.

Vertraulichkeit

- Ende-zu-Ende-Verschluesselung fuer Chat-Inhalte und Medien.
- Server speichert keine Chat-Klartexte.
- Private Device-Schluessel verbleiben auf Endgeraeten.
- AdminWeb ist MFA-geschuetzt fuer PlatformAdmins und OrgAdmins.
- Rollen und Scopes begrenzen Admin-Operationen.
- Produktive Secrets duerfen nicht im Repository liegen.
- Secret Storage ueber Azure App Settings, Key Vault oder vergleichbaren Secret Store.
- Logging ohne Passphrases, private Keys, Tokens, Klartextnachrichten oder Connection Strings.

Integritaet

- Signatur-/KEX-Public-Keys sind device-gebunden.
- Device-Revoke verhindert kuenftige Zustellung an widerrufene Geraete.
- MessageRecipients-Envelopes begrenzen Entschluesselbarkeit pro Empfaenger.
- Policy-Versionen steuern Nutzungsregeln wie Weiterleiten, Screenshots, Medien und Ablauf.
- Migrationen werden vor Pilotfreigabe geprueft.
- Releases werden versioniert und dokumentiert.

Verfuegbarkeit

- /health und /health/ready je Service.
- Azure Availability Tests fuer alle produktiv gehosteten Services.
- Backup/Restore-Runbook mit RPO/RTO-Zielen.
- Migrationsprozess mit Backup vor Schemaaenderungen.
- Incident-Runbook fuer Deviceverlust, Org-Sperre, Sendefehler und Migrationen.

Belastbarkeit und Wiederherstellung

- PostgreSQL-Backups fuer Directory, Policy, Messaging und Relay.
- Blob/Object-Storage-Sicherung fuer verschluesselte Medien, falls genutzt.
- Restore-Test mindestens monatlich oder vor relevanten Piloten.
- Tageskontrolle fuer Demo-Anfragen, abgelaufene Piloten und Service-Readiness.

Zugriffskontrolle

- Einladungsbasierte Registrierung.
- Org-Code aus Einladung mit kurzer Gueltigkeit.
- OrgAccessStatus Pilot, Active, Suspended, Closed.
- Gesperrte/geschlossene Organisationen erhalten keine neuen Tokens und koennen keine neuen Geraete registrieren.
- OrgAdmin-MFA-Enrollment mit zeitlich begrenztem Token.
- Device-Revoke und Offboarding im AdminWeb.

Mandantentrennung

- OrgId ist zentrale Mandantengrenze fuer User, Devices, Invites, Policies, Threads und Messages.
- AdminWeb OrgAdmin-Zugriff ist auf die eigene Organisation begrenzt.
- PlatformAdmin-Aktionen sind fuer Pilotbetrieb vorgesehen und muessen betrieblich protokolliert werden.

Monitoring und Protokollierung

- Strukturierte Events fuer Readiness, Policy fehlt, Key-Lookup-Fehler, Sendefehler, Pushfehler, Demo-Anfragen und Org-Zugang.
- AuditService ist fuer externe/zahlende Piloten empfohlen.
- Audit- und Betriebslogs duerfen keine Chat-Inhalte enthalten.
- Audit-Retention ist konfigurierbar; Export ist fuer Incident Review vorgesehen und darf nur Metadaten enthalten.

Datenschutz by Design und Default

- Push-Benachrichtigungen ohne Nachrichtentext, Absendernamen oder Dateinamen.
- Keine serverseitige Klartextsuche ueber Chat-Inhalte.
- Keine Nutzung von Chat-Inhalten fuer Profiling, Werbung oder KI-Training.
- Metadateninventar und Retention-Konzept separat dokumentiert.

Noch offen vor groesseren Kunden

- Externes Security-/Crypto-Review.
- Vollstaendige Key-Verifikation/Safety Numbers.
- Automatisierter Retention-Job und formaler Audit-Export-Prozess.
- Produktive Retention technisch erzwingen.
- SBOM/Dependency-Scanning in CI.
- Formale Access Reviews fuer Admins und Subprozessoren.