

Sichere Organisationskommunikation plus vertraulicher Dokumentenraum

Harpocrypt verbindet Chat, Gruppen und vertraulichen Dokumentenaustausch mit Ende-zu-Ende-Verschlüsselung, Policy-Steuerung, Datei-Limits und kontrolliertem Device-Lifecycle. Der Betreiber kann Nachrichten- und Dateiinhalte nicht lesen.

Fuer wen NGOs, Krisenteams, Rechtsberatung, medizinische und soziale Organisationen, vertrauliche Projektteams.	Problem Private Messenger und E-Mail-Anhaenge geben Organisationen wenig Kontrolle ueber Teilnehmer, Geraete, Policies und Offboarding.
Loesung Einladungsbasierter Chat plus Secure Document Room fuer sensible Dateien im gleichen Sicherheits- und Policy-Modell.	Abgrenzung Kein WhatsApp-Killer fuer alle, kein Cloud-Drive, kein Signaturdienst. Harpocrypt ist kontrollierte Organisationskommunikation.

Was Harpocrypt bietet

- 1:1- und Gruppenchat, Medien, Voice, Dateien und Secure Document Room fuer vertrauliche Uebergaben.
- Ende-zu-Ende-Verschlüsselung mit empfaengerspezifischen Envelopes.
- Policies fuer Screenshot-Schutz, Weiterleiten, Medien, Voice, Dateien, Ablauf und Recall.
- PlatformAdmin- und Policy-Limits fuer Nutzerzahl und maximale Dateigroesse.
- Push ohne Nachrichtentext, Dateiname oder Vorschau.
- Device-Revoke und Remote-Wipe-Unterstuetzung fuer Geraeteverlust und Offboarding.

Sicherheitsmodell

- Server speichern und vermitteln nur verschluesselte Nutzdaten.
- Admins verwalten Organisation, Nutzer, Policies, Geraete und Limits, nicht den Klartext.
- Metadaten wie Organisation, Nutzer, Geraete, Zeitpunkte, technische Objekt-IDs, Dateigroessen und Zustellstatus bleiben personenbezogene Daten.
- Kein Claim wie unhackbar, absolut anonym oder garantiert geloescht.
- Secure Document Room ist kein allgemeiner Cloud-Speicher, keine qualifizierte elektronische Signatur und keine zertifizierte Zustellung.

Pilotangebot

Pilot 20 490 EUR / 30 Tage Bis 20 Nutzer, 1 OrgAdmin, bis 3 Testgruppen, Chat, Dateien, Secure Document Room, Setup-Call und Feedback.	Pilot 50 890 EUR / 30 Tage Bis 50 Nutzer, erweiterte Policy-Abstimmung, Datei-Limits, Zwischencheck, Secure Document Room und Feedback.
---	--

Secure Document Room im Pilot

- Mindestens einen realistischen Dokumentenfall testen: senden, oeffnen, Dateilimit, schlechte Verbindung, Recall/Revoke/Wipe.
- Push bleibt ohne Dateiname, Inhalt oder Vorschau; Metadaten wie Groesse und technische Objekt-ID bleiben sichtbar.

Pilotablauf

- Anfrage und Sicherheitsbedarf klaeren.
- Organisation, OrgAdmin, MFA, Nutzerlimit, Datei-Limit und Policies einrichten.
- Smoke-Test: 1:1, Gruppen, Medien, Voice, Dateien, Secure Document Room, Push, strenge Policy, Recall, Device-Revoke/Wipe.
- Feedback auswerten und Angebot fuer den Betrieb erstellen.

Kontakt: hello@harpocrypt.io | security@harpocrypt.io | Pilot: <https://harpocrypt.io/pilot/anfrage>