Harpocrypt Security and Privacy Whitepaper

Stand: 2026-06-15

Status: MVP-Arbeitsdokument, keine Rechtsberatung

Dieses Dokument beschreibt, was Harpocrypt im aktuellen MVP technisch schuetzt, welche Daten der Server weiterhin sieht und welche Punkte vor NGO-Piloten oder produktivem EU-Einsatz noch geschlossen werden muessen.

Kurzfassung

Harpocrypt ist als sichere Kommunikationsplattform mit clientseitiger Verschluesselung aufgebaut. Chat-Inhalte werden vor dem Upload auf dem Endgeraet verschluesselt. Der Server soll Inhalte weiterleiten, speichern und Berechtigungen pruefen, aber keine Chat-Klartexte entschluesseln koennen.

Die starke Aussage fuer NGOs lautet deshalb nicht "wir speichern keine Daten", sondern:

- Der Server soll keine Chat-Inhalte im Klartext erhalten.
- Schluesselmaterial fuer Nachrichten bleibt auf den Endgeraeten.
- Server-seitig notwendige Metadaten werden minimiert, dokumentiert und mit definierten Loeschfristen betrieben.
- Push-Benachrichtigungen enthalten keine Chat-Inhalte.
- Sicherheitsgrenzen und Restrisiken werden transparent offengelegt.

Aktueller technischer Stand

Clientseitige Verschluesselung

Nachrichten werden im Mobile Client in ein MessagePayload serialisiert und mit einem zufaelligen Data Encryption Key verschluesselt. Der Data Encryption Key wird fuer Empfaengergeraete ueber ein Envelope-Verfahren verpackt. Die eigentlichen verschluesselten Objekte werden ueber Relay/Gateway transportiert.

Relevante Codebereiche:

- src/clients/mobileApp/smedia.harpocrypt.clients.mobileApp/Services/ChatService.cs
- src/libs/CryptoCore/StreamAead.cs
- src/libs/CryptoCore/CryptoClient.cs
- src/libs/Contracts/MessagingContracts.cs

Lokale Schluessel

Device-Schluessel werden clientseitig erzeugt. Private Schluessel und lokale Auth-/Crypto-Zustaende werden ueber die Plattform-Secure-Storage-Mechanismen verwaltet. Fuer lokale Ableitungen wird Argon2id eingesetzt.

Relevante Codebereiche:

- src/clients/mobileApp/smedia.harpocrypt.clients.mobileApp/Services/DeviceKeysService.cs
- src/clients/mobileApp/smedia.harpocrypt.clients.mobileApp/Services/CryptoStateStore.cs
- src/libs/CryptoCore/Argon2Kdf.cs
- src/libs/CryptoCore/IHardwareKeyProvider.cs

Messaging und Metadaten

Der Messaging-Service speichert Nachrichten-Metadaten wie Organisation, Thread, Absender, Empfaenger, Policy, Objekt-ID, Envelope und Read-State. Diese Daten sind fuer Zustellung, Berechtigungspruefung und Synchronisation notwendig, bleiben aber personenbezogene Daten.

Relevante Codebereiche:

- src/services/MessagingService/Infra/MessagingDb.cs
- src/services/MessagingService/Endpoint/MessagesEndpoints.cs
- src/services/MessagingService/Endpoint/ThreadsEndpoints.cs

Realtime und Push

Der MVP enthaelt Realtime-Benachrichtigungen ueber SignalR sowie Android Push ueber Firebase Cloud Messaging. Push-Benachrichtigungen sollen generisch bleiben und keine Chat-Inhalte enthalten.

Relevante Codebereiche:

- src/services/MessagingService/Notifications/MessageHub.cs
- src/services/MessagingService/Notifications/MessageNotifier.cs
- src/services/MessagingService/Notifications/FcmPushNotificationSender.cs
- src/services/MessagingService/Endpoint/PushEndpoints.cs
- src/clients/mobileApp/smedia.harpocrypt.clients.mobileApp/Platforms/Android/Push/

Was Harpocrypt nicht sehen soll

Bei korrekter Client-Implementierung und nicht kompromittierten Endgeraeten soll der Server nicht sehen koennen:

- Chat-Nachrichtentext im Klartext
- Anhaenge im Klartext
- Voice-Nachrichten im Klartext
- Lokale Passphrase
- Private Device-Schluessel
- Data Encryption Keys im Klartext

Diese Aussage haengt an der Integritaet der Clients, der korrekten Schluesselverwaltung und der korrekten Envelope-Implementierung. Sie ersetzt kein externes Security Audit.

Was Harpocrypt weiterhin sehen kann

Auch bei Ende-zu-Ende-Verschluesselung fallen Metadaten an. Diese Daten sind in der EU in der Regel personenbezogene Daten, wenn sie direkt oder indirekt einer Person zugeordnet werden koennen.

Datenkategorie	Beispiel	Zweck	Risiko	MVP-Status
Organisation	OrgId	Mandantentrennung	Organisationszuordnung	vorhanden
Nutzer	UserId, Absender, Empfaenger	Zustellung, Rechte	Kommunikationsbeziehungen	vorhanden
Geraet	DeviceId, Plattform	Device Binding, Push	Geraeteprofil	vorhanden
Public Keys	Signatur-/KEX-Public-Key	Verschluesselung, Identitaet	Key-Historie	vorhanden

Datenkategorie	Beispiel	Zweck	Risiko	MVP-Status
Nachrichtenmetadaten	Thread, Objekt-ID, Policy, Zeitstempel	Sync, Threadliste	Kommunikationsmuster	vorhanden
Read-State	ReadAt	Lesestatus	Nutzungsverhalten	vorhanden
Push Tokens	FCM Token	Push-Zustellung	Drittanbieterbezug	Android vorhanden
IP/Logs	Server- und Infrastruktur-Logs	Betrieb, Security	Standort-/Nutzungsdaten	noch zu definieren
Audit Events	Admin-/Security-Ereignisse	Nachvollziehbarkeit	Profilbildung bei zu viel Logging	vorhanden, Retention/Export konfigurierbar

Datenschutzprinzipien fuer den MVP

Datenminimierung

Nur Daten speichern, die fuer Zustellung, Sicherheit, Betrieb oder gesetzliche Anforderungen wirklich notwendig sind. Chat-Inhalte duerfen nicht serverseitig entschluesselt oder indiziert werden.

Privacy by Design und Default

Sichere Defaults muessen die Voreinstellung sein:

- Push ohne Nachrichtentext
- kurze Standard-Loeschfristen fuer technische Logs
- minimale Admin-Einsicht
- keine Klartextsuche ueber Chat-Inhalte
- keine Analyse von Kommunikationsinhalten
- Mandantentrennung auf jeder Datenbankabfrage

Zweckbindung

Metadaten duerfen nur fuer definierte Zwecke verwendet werden:

- Zustellung
- Synchronisation
- Missbrauchs-/Sicherheitsabwehr
- Abrechnung, falls spaeter erforderlich
- Support nur mit minimal notwendigem Zugriff

Nicht vorgesehen im MVP:

- Werbeprofiling
- Verkauf von Daten
- inhaltliche Auswertung von Chats
- serverseitiges Training von KI-Modellen auf Chat-Inhalten

Push-Benachrichtigungen

Push ist fuer Akzeptanz wichtig, erzeugt aber neue Datenschutz- und Betriebsfragen.

MVP-Leitlinie:

- Push-Payload enthaelt nur technische Routingdaten: Ereignistyp und Thread-ID zum Oeffnen des richtigen Chats.
- Push-Titel/Text ist fest generisch: Harpocrypt / Neue Nachricht.
- Keine Absendernamen, Nachrichtenvorschau, Dateinamen, Attachment-Arten oder Nachrichtenzahlen in Push.
- Push Tokens werden device- und org-gebunden gespeichert.
- Deaktivierte oder abgelehnte Tokens werden invalidiert.
- Deaktivierte Push Tokens werden nach konfigurierbarer Frist geloescht.
- Firebase Cloud Messaging wird als Subprozessor/Drittanbieter dokumentiert.

Noch offen:

- iOS Push ueber APNs/FCM Bridge
- Opt-out je Organisation oder Nutzer
- Admin-Dokumentation fuer Push-Metadaten

EU-/NGO-Readiness

Vor NGO-Piloten sollten diese Punkte als Paket vorliegen:

- Datenschutzinformation fuer Nutzer und Organisationen
- Auftragsverarbeitungsvertrag, falls Harpocrypt als Processor betrieben wird
- Technische und organisatorische Massnahmen
- Subprozessorenliste, z.B. Hosting, Push, Monitoring
- Metadateninventar mit Zweck und Loeschfrist
- Incident-Response-Prozess
- Responsible-Disclosure-/Vulnerability-Policy
- Backup-, Restore- und Datenloeschkonzept
- Admin-Rollenmodell mit minimalen Rechten
- Externer Security Review vor produktivem Einsatz in sensiblen Gruppen

Rechtliche Einordnung in der EU

GDPR/DSGVO

Auch verschluesselte oder pseudonymisierte Daten koennen personenbezogene Daten bleiben, wenn eine Re-Identifikation moeglich ist. Deshalb muessen Metadaten, Device IDs, IP-Adressen, Push Tokens und Logs wie personenbezogene Daten behandelt werden.

Wichtige Arbeitspakete:

- Rechtsgrundlagen je Verarbeitung definieren
- Betroffenenrechte technisch unterstuetzen
- Loesch- und Exportfaehigkeit klaeren
- Data Protection Impact Assessment fuer sensible NGO-Einsaetze vorbereiten
- Privacy by Design und Default dokumentieren

DPIA/DSFA

Fuer NGOs, Aktivisten, Journalisten oder besonders gefaehrdete Gruppen ist eine Datenschutz-Folgenabschaetzung naheliegend, auch wenn die Pflicht im Einzelfall juristisch bewertet werden muss. Harpocrypt sollte eine technische DPIA-Zuarbeit liefern: Datenfluesse, Risiken, Schutzmassnahmen, Restrisiken.

NIS2

Ob NIS2 direkt greift, haengt von Betreiber, Groesse, Sektor und Rolle ab. Harpocrypt sollte trotzdem NIS2-kompatible Betriebspraktiken vorbereiten: Risikomanagement, Incident Handling, Lieferkettensicherheit, Logging-Minimierung und klare Security-Verantwortung.

Cyber Resilience Act

Der Cyber Resilience Act betrifft Produkte mit digitalen Elementen und wird fuer Softwareprodukte im EU-Markt relevant. Fuer Harpocrypt sollten jetzt schon vorbereitet werden:

- Secure Development Lifecycle
- Vulnerability Handling
- Security Updates
- technische Dokumentation
- SBOM/Dependency-Inventar
- Konformitaets- und Release-Nachweise

Sicherheitsgrenzen

Harpocrypt sollte diese Grenzen offen kommunizieren:

- Kompromittierte Endgeraete koennen Klartext vor oder nach Verschluesselung auslesen.
- Metadaten koennen Kommunikationsmuster sichtbar machen.
- Push-Infrastruktur sieht Zustellungsmetadaten.
- Server kann Verfuegbarkeit, Accounts, Policies und Zustellung beeinflussen.
- Ohne Key-Verifikation bleibt ein Risiko durch falsche oder ausgetauschte Public Keys.
- Der aktuelle MVP ist noch nicht extern auditiert.

Empfohlene naechste technische Schritte

- Key-Verifikation/Safety Numbers fuer 1:1 Chats
- Saubere Retention-Konfiguration fuer Messages, Objekte, Logs und Push Tokens
- Automatisierten Retention-Job fuer Audit Events und Betriebslogs entscheiden
- Subprozessoren und Betriebsregionen konfigurierbar dokumentieren
- iOS Push implementieren
- Security Headers, Rate Limits und Abuse Controls pruefen
- Secrets aus Repo/Appsettings entfernen und Secret Management erzwingen
- Dependency Scanning und SBOM in CI aufnehmen
- Backup/Restore-Test dokumentieren

- Externes Kryptographie- und AppSec-Review einplanen

Betriebsunterlagen

- Security-Unterlagen-Index: docs/security-documentation-index.md
- Threat Model: docs/threat-model.md
- DPA/AVV-Arbeitsentwurf: docs/data-processing-agreement-working-draft.md
- TOMs: docs/technical-organisational-measures.md
- Retention/Loeschkonzept: docs/data-retention-deletion-concept.md
- Subprozessoren: docs/subprocessors.md
- Backup/Restore: docs/backup-restore-runbook.md
- Incident Response: docs/incident-response-runbook.md
- Azure Alerts: docs/azure-alerts-runbook.md
- AuditService-Entscheidung: docs/audit-service-operations.md
- Production Configuration: docs/production-configuration.md

Quellen

- European Commission: Data protection in the EU

https://commission.europa.eu/law/law-topic/data-protection_en

- European Commission: Data protection by design and by default

https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en

- European Commission: What is personal data?

https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

- European Data Protection Board: Data Protection Impact Assessment

https://www.edpb.europa.eu/sme-data-protection-guide/faq-frequently-asked-questions/answer/what-data-protection-impact_en

- European Commission: NIS2 Directive

https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

- European Commission: Cyber Resilience Act summary

https://digital-strategy.ec.europa.eu/en/policies/cra-summary