

Harpocrypt Security Review Plan

Stand: 2026-06-16

Status: Plan fuer externe Pruefung vor groesseren Kunden.

Ziel

Vor groesseren NGO-, Enterprise- oder regulierten Kunden soll Harpocrypt ein externes Security-/Crypto-Review durchlaufen. Ziel ist nicht Marketing, sondern echte Risikoreduktion und belastbare Kommunikation.

Review-Phasen

Phase 1: Readiness Review

Zeitpunkt: vor erstem groesseren zahlenden Kunden.

Scope:

- Architekturreview.
- Threat Model Review.
- Key Management und Envelope-Konzept.
- Auth/MFA/AdminWeb.
- Push ohne Inhalte.
- Device-Revoke/Wipe.
- Secrets und Production Configuration.

Ergebnis:

- Findings mit Severity.
- Fixliste.
- Go/No-Go fuer groessere Piloten.

Phase 2: AppSec/Pentest

Zeitpunkt: nach Stabilisierung erster Pilotkunden.

Scope:

- Public Web und AdminWeb.
- Directory/Messaging/Policy/Relay/Gateway APIs.
- Mandantentrennung.
- Rollen/Scopes.
- Mobile API-Flows.
- Rate Limits und Abuse.

Ergebnis:

- Technischer Bericht.
- Management Summary fuer Kunden.
- Re-Test kritischer Findings.

Phase 3: Crypto Review

Zeitpunkt: vor Hochsicherheitskunden oder grossem Rollout.

Scope:

- Clientseitige Verschlüsselung.
- Device Keys.
- Envelope-Erzeugung und Empfängerlogik.
- Passphrase/KDF.
- Media/Voice Encryption.
- Key Verification Roadmap.

Ergebnis:

- Aussage zur Angemessenheit des Designs.
- Konkrete Fixes.
- Restrisiken fuer Whitepaper.

Auswahlkriterien fuer Anbieter

- Erfahrung mit E2E-Messengern oder kryptographischen Protokollen.
- Erfahrung mit .NET, MAUI/Mobile, Azure und Web APIs.
- Bereitschaft zu pragmatischem MVP-Review.
- Bericht darf kundenfaehige Summary enthalten.
- Re-Test inklusive.

Vorbereitung

- Aktuelles Threat Model: docs/threat-model.md.
- Security Whitepaper: docs/security-privacy-whitepaper.md.
- TOMs und AVV-Arbeitsentwurf.
- Architekturdiagramm und Datenflussdiagramm.
- Testaccounts und dedizierte Testorganisation.
- Liste produktiver Secrets getrennt, keine Secrets im Report.
- Aktuelle Deployment-/Migration-Dokumentation.

Anfrage an Security-Anbieter

Kurztext:

Wir suchen ein externes Security-/Crypto-Review fuer Harpocrypt, eine Ende-zu-Ende verschlüsselte Organisationskommunikation mit .NET Services, MAUI Mobile Client, Azure Hosting und AdminWeb.

Gesucht ist zuerst ein pragmatisches Readiness Review mit Threat Model, Architektur, Auth/MFA, Mandantentrennung, Key Management, Envelope-Konzept, Push ohne Inhalte und Device-Revoke/Wipe.

Bitte senden Sie Scope-Vorschlag, Aufwand, Zeitplan, Beispielbericht/Management Summary und Re-Test-Konditionen.

Budgetannahme

Arbeitsannahme fuer Planung:

- Readiness Review: 5.000 bis 12.000 EUR.
- AppSec/Pentest: 8.000 bis 20.000 EUR.
- Crypto Review: 10.000 bis 30.000 EUR.

Diese Werte muessen mit echten Angeboten validiert werden.

Entscheidungspunkt

Ein externes Review wird spaetestens dann eingeplant, wenn einer dieser Punkte eintritt:

- erster Kunde mit mehr als 50 aktiven Nutzern,
- regulierter Kunde,
- Hochrisiko-NGO,
- On-Premise-/Customer-hosted-Anfrage,
- Jahresvertrag ueber 10.000 EUR,
- Kunde verlangt belastbaren externen Nachweis.