Zusammenfassung · Whitepaper 1.3 · November 2026

UDKS auf einen Blick

Dokumentenlenkung mit Post-Quanten-Kryptografie

WAS IST UDKS?

UDKS ist ein browserbasierter Dienst zur Lenkung, Freigabe, Kenntnisnahme, Aufbewahrung und zum kontrollierten Versand vertraulicher Dokumente. Dokumente werden bereits im Browser verschlüsselt und signiert, bevor sie den Dienst erreichen. Der Dienst speichert die Inhalte als Chiffrat; Signaturen und Metadaten liegen ihm vor. Die Betreiberin (C&W Software Labs AG) hat im vorgesehenen Betrieb keine privaten Schlüssel, keine Passphrasen und keinen berechtigten Zugriff auf Klartexte. Das Angebot richtet sich an Unternehmen in der Schweiz und in Liechtenstein, die vertrauliche Unterlagen langfristig aufbewahren und den Umgang damit belegen müssen. Der EU-Rollout startet ab dem 04.01.2027.

ZWECK UND ZIELE

- **Vertraulichkeit über Jahrzehnte:** Klassische Verfahren (RSA, elliptische Kurven) lassen sich mit einem ausreichend grossen Quantencomputer brechen; heute kopierte Chiffrate liessen sich später entschlüsseln. UDKS setzt deshalb produktiv auf Post-Quanten-Kryptografie.
- **Nachweis statt Behauptung:** Aufbewahrungspflichten (Art. 958f OR, GeBüV) verlangen Integrität und Nachvollziehbarkeit über zehn Jahre. UDKS erzeugt den Nachweis als Nebenprodukt jeder Handlung.

KERNINHALTE

- **Kryptografie:** ML-KEM-768 (FIPS 203) für Schlüsselkapseln, ML-DSA-65 (FIPS 204) für Signaturen, AES-256-GCM (FIPS 197) für Inhalte, dazu Argon2id und SHA-512; die Post-Quanten-Verfahren stammen aus der offenen Bibliothek liboqs. Ein Schlüssel je Dokument, eine Kapsel je berechtigte Person.
- **Ordnung:** Jedes Dokument trägt ein siebengliedriges Kennzeichen inklusive Schutzklasse S1–S5 sowie einen Datenpass; die Klasse steuert Sichtbarkeit, Versand und Freigabe.
- **Lenkung:** Lebenszyklus vom Entwurf über Prüfung und Freigabe bis zur unveränderlichen Revision; Rollentrennung (Erstellen, Prüfen, Freigeben); Versandmappe für den förmlichen Versand, befristeter Download-Link für Externe; signierte Kenntnisnahme je Revision.
- **Nachweiskette:** Jede Aktion — auch jede Verweigerung — ist ein verkettetes, signiertes Ereignis (nur anhängbar); nächtliche Nachrechnung und Prüfexport mit Manifest.
- **Migration:** Die Migration läuft in sechs Schritten. Eine Importkapsel verschlüsselt den Altbestand beim Unternehmen; bis zur Abnahme mit Gegenzeichnung bleibt die Quelle führend.
- **Wiederherstellung:** Der Key-User setzt Konten zurück; ein Notfallschlüssel der Gesellschaft liegt offline beim Unternehmen.

FUNKTIONSSTAND

- **Welle 2, verfügbar seit dem 20.11.2026:** Teamabschluss, Konfigurationspaket, Löschanforderung, Formatspezifikation, Wiederherstellung in einer Testzone, Archivspeicher sowie Rückfall je Lauf und Delta-Automatik im Import.
- **Welle 3, Termin offen:** Eigene Ausführungsumgebung je Kunde, zweite Fassung des Formats mit Schlüsselwechsel und Widerruf, Offline-Client, Ordner- und Programmbrücke, Penetrationstests.
- Massgebend ist der Funktionsfahrplan auf udks.cundw.ch. Eine Funktion, die er noch nicht als verfügbar führt, ist nicht Teil der heutigen Leistung.

BETRIEB UND WICHTIGE FAKTEN

- Produktionsinstanz bei Exoscale, Zürich (ISO-27001-zertifiziertes Rechenzentrum — die Zertifizierung gilt dem Rechenzentrum, nicht UDKS); Dokumente, Konten und Nachweise bleiben in der Schweiz.
- Zielverfügbarkeit 99,5 % im Monatsmittel; verschlüsselte Sicherung auf der NAS des Kunden; vollständiger Export während der Vertragsdauer und 30 Kalendertage danach.
- Produktiv innerhalb von fünf Arbeitstagen nach dem Start, sofern das Unternehmen Teilnehmerliste, Zuständigkeiten und Termine rechtzeitig bereitstellt.
- **Regulatorischer Rahmen:** NIST-Standards FIPS 203/204 seit 13.8.2024; NIST IR 8547 (RSA/ECC gelten nach 2030 als veraltet und sind nach 2035 nicht mehr zulässig); die FINMA-Aufsichtsmitteilung 05/2026 legt eine Roadmap für Post-Quanten-Kryptografie bis spätestens Mitte 2027 nahe.

GRENZEN

Keine Volltextsuche in Inhalten; Metadaten sind dem Dienst sichtbar. Schlüsselhoheit und Endgeräteschutz liegen beim Unternehmen: Ohne Schlüsseldatei und Passphrase einer berechtigten Person und ohne nutzbaren Notfallschlüssel ist ein Dokument verloren; die Betreiberin kann es nicht wiederherstellen. UDKS ist von keiner Aufsichts- oder Zertifizierungsstelle zertifiziert, geprüft oder zugelassen. Eine Zusage für alle Zeit gibt es in der Kryptografie nicht.

C&W Software Labs AG · Bundesplatz 4 · 6300 Zug
udks.cundw.ch · Funktionsfahrplan · Sicherheitsmodell
Stand: 20. November 2026. Massgebend ist der Wortlaut des Whitepapers 1.3.