UDKS.

WHITEPAPER · FASSUNG 1.3 · NOVEMBER 2026

Vertrauliche Dokumente lenken, nachweisen und über Jahrzehnte schützen

Wie UDKS gebaut ist: Verschlüsselung im Browser, Schutzklassen, Nachweiskette, Migration des Altbestands und Betrieb in der Schweiz.

CH-PRD-UDK-TEC-Whitepaper-1.3.0-S1
C&W SOFTWARE LABS AG
BUNDESPLATZ 4 · 6300 ZUG · SCHWEIZ
UDKS.CUNDW.CH

S1 ÖFFENTLICH

AUF EINEN BLICK

UDKS und der Gegenstand dieses Dokuments

UDKS ist ein browserbasierter Dienst zur Lenkung, Freigabe, Kenntnisnahme, Aufbewahrung und zum kontrollierten Versand vertraulicher Dokumente. Dokumentinhalte werden im Browser verschlüsselt, bevor sie den Dienst erreichen.

Dieses Whitepaper beschreibt den Aufbau von UDKS und die Gründe dafür. Es richtet sich an Geschäftsleitungen und an Verantwortliche für Informationssicherheit, Compliance, Revision und Informatik in Unternehmen, die vertrauliche Unterlagen lange aufbewahren und ihren Umgang damit belegen müssen. Es benennt die eingesetzten Verfahren und die Grenzen des Systems.

> **Begriffe.** «Der Dienst» bezeichnet UDKS als laufende Anwendung auf den Servern. «Die Betreiberin» ist die C&W Software Labs AG, die den Dienst betreibt. «Das Unternehmen» ist die Kundin, die UDKS nutzt; die Anrede «Sie» meint ihre Personen. Alle weiteren Begriffe erklärt das Glossar im Anhang.

01

Verschlüsselt, bevor es Ihr Gerät verlässt

Dokumente, Arbeitsstände und Notizen werden im Browser verschlüsselt und signiert. Der Dienst speichert Chiffrat. Die Betreiberin hat im vorgesehenen Betrieb keine privaten Schlüssel, keine Passphrasen und keinen berechtigten Zugriff auf Klartexte.

02

Verfahren nach FIPS 203, 204 und 197

Schlüsselkapseln mit ML-KEM-768 (FIPS 203), Signaturen mit ML-DSA-65 (FIPS 204), Inhalte mit AES-256-GCM (FIPS 197). Die beiden Post-Quanten-Verfahren sind seit August 2024 als Standards veröffentlicht und in UDKS produktiv.

03

Ordnung, die Rechte trägt

Jedes Dokument hat ein sprechendes Kennzeichen und einen Datenpass. Die Schutzklasse S1 bis S5 ist Bestandteil des Kennzeichens und entscheidet, wer das Dokument sieht, versendet und freigibt.

04

Ein Nachweis für jeden Schritt

Upload, Freigabe, Versand, Kenntnisnahme und jede Verweigerung stehen als Ereignis in einer verketteten, signierten Folge, die sich nachrechnen und exportieren lässt.

05

Der Altbestand kommt geführt ins System

Dokumenteninventar, Zuordnung, Testimport, Abnahme mit Gegenzeichnung. Verschlüsselt wird bei Ihnen. Bis zur Abnahme bleibt die Quelle führend.

06

Betrieb in der Schweiz, Kopie bei Ihnen

Die Produktionsinstanz läuft bei Exoscale in Zürich. Eine verschlüsselte Sicherung liegt auf Ihrer NAS, der Notfallschlüssel offline bei Ihrer Geschäftsführung. Der vollständige Export steht Ihnen während der ganzen Vertragsdauer offen.

Inhaltsverzeichnis

1 Ausgangslage: zwei Fristen
2 Das Prinzip: speichern, nicht lesen
3 Kryptografie im Einzelnen
4 Kennzeichen, Datenpass, Schutzklassen
5 Lenkung bis zur verbindlichen Revision
6 Nachweis: die Kette
7 Migration des Altbestands
8 Betrieb, Sicherung und Ausstieg
9 Regulatorische Einordnung
10 Grenzen des Systems
11 Funktionsstand, Quellen, Kontakt
A Anhang: Glossar

KAPITEL 1

Ausgangslage: zwei Fristen, die länger laufen als jede Software

Verträge, Personalakten, Mandatsunterlagen und weitere geschäftskritische Dokumente werden zehn Jahre und länger aufbewahrt und bleiben über diese Zeit hinaus vertraulich. Mit der Ablage von heute fallen zwei Entscheidungen, deren Folgen sich erst in vielen Jahren zeigen.

Die erste betrifft die Vertraulichkeit: ob in Zukunft jemand mitlesen kann, dem das heute nicht möglich ist. Die zweite betrifft den Nachweis: ob sich dann noch belegen lässt, welche Person welche Fassung freigegeben, versendet und zur Kenntnis genommen hat.

Vertraulichkeit über Jahrzehnte

Die heute verbreiteten Verfahren für Schlüsselaustausch und Signatur, RSA und elliptische Kurven, lassen sich mit einem ausreichend grossen Quantencomputer brechen. Symmetrische Verfahren wie AES sind davon nicht in gleicher Weise betroffen. Wann ein solcher Rechner existiert, weiss niemand. Für lange vertrauliche Daten zählt das Datum aber weniger, als es scheint: Verschlüsselte Daten lassen sich heute kopieren und später entschlüsseln. Was heute mit einem brechbaren Verfahren geschützt wird, bleibt in diesem Szenario nur so lange vertraulich, wie der Angreifer warten muss.

Die Antwort sind Verfahren, die auf anderen mathematischen Problemen beruhen. Das US-Institut NIST hat die ersten davon im August 2024 als Standards veröffentlicht: ML-KEM für den Schlüsselaustausch (FIPS 203) und ML-DSA für Signaturen (FIPS 204). Seither haben Aufsicht und Normgeber Fristen genannt.

STELLE	AUSSAGE	DATUM
NIST, FIPS 203 und 204	ML-KEM und ML-DSA sind als Standards veröffentlicht.	13.8.2024
EU, koordinierter Fahrplan der NIS-Kooperationsgruppe	Mitgliedstaaten beginnen die Umstellung; Anwendungen mit hohem Risiko sind umgestellt; möglichst alle übrigen Systeme folgen.	Ende 2026 · Ende 2030 · 2035
FINMA, Aufsichtsmitteilung 05/2026 «Quantum Computing»	Die FINMA legt eine Roadmap für Post-Quanten-Kryptografie bis spätestens Mitte 2027 nahe, getragen von einer Strategie, die das Oberleitungsorgan verabschiedet. Sie regt eine Risikoanalyse mit Inventar der eingesetzten Kryptografie an und empfiehlt den Einbezug der Dienstleister und Kryptoagilität. In ihrer Umfrage unter 60 Instituten hatten 72 % noch keine Massnahmen geplant oder umgesetzt; 8 % hatten eine konkrete Roadmap.	9.7.2026
NIST, IR 8547	RSA und elliptische Kurven gelten nach 2030 als veraltet und sind nach 2035 nicht mehr zulässig.	2030 · 2035
BSI, TR-02102-1	Das BSI empfiehlt ML-KEM und ML-DSA, kombiniert mit einem klassischen Verfahren (hybrid).	laufend

Nachweis statt Behauptung

Die zweite Frist ist die Beweisfrist. Das Obligationenrecht verlangt, Geschäftsbücher und Buchungsbelege zehn Jahre aufzubewahren (Art. 958f OR); die Geschäftsbücherverordnung verlangt dafür Integrität und Nachvollziehbarkeit. Für beaufsichtigte Institute, für Träger eines Berufsgeheimnisses und für alle, die Personendaten bearbeiten, kommen eigene Pflichten dazu. Gemeinsam ist ihnen: Im Streitfall, in der Revision und gegenüber der Aufsicht zählt nicht, dass eine Regel galt. Es zählt, dass sich ihre Einhaltung zeigen lässt: welche Fassung gültig war und welche Personen sie freigegeben, erhalten und bestätigt haben.

Ein Dateiserver leistet das nicht. Er kennt Ordner und Zugriffsrechte, aber keine verbindliche Fassung, keine Freigabe und keinen Empfänger. Wer den Nachweis später braucht, muss ihn heute mit der Arbeit erzeugen.

FOLGERUNGEN

- **Dokumente zuerst.** Sie haben die längste Schutzdauer. Wo ein Unternehmen mit Post-Quanten-Verfahren beginnt, sind sie der naheliegende erste Anwendungsfall.
- **Schlüssel beim Unternehmen.** Wer mitlesen kann, ist ein Risiko und ein Geheimnisträger. Der Betreiber eines Dienstes soll deshalb nichts entschlüsseln können.
- **Nachweis aus der Arbeit.** Jeder Schritt erzeugt sein Ereignis selbst. Niemand führt nachträglich ein Protokoll.

KAPITEL 2

Das Prinzip: Der Dienst speichert und lenkt, lesen kann er nicht

UDKS trennt zwei Dinge, die in den meisten Systemen am selben Ort liegen: den Inhalt eines Dokuments und die Angaben, die für seine Lenkung nötig sind. Der Inhalt wird auf Ihrem Gerät verschlüsselt. Lenken, prüfen und nachweisen kann der Dienst trotzdem.

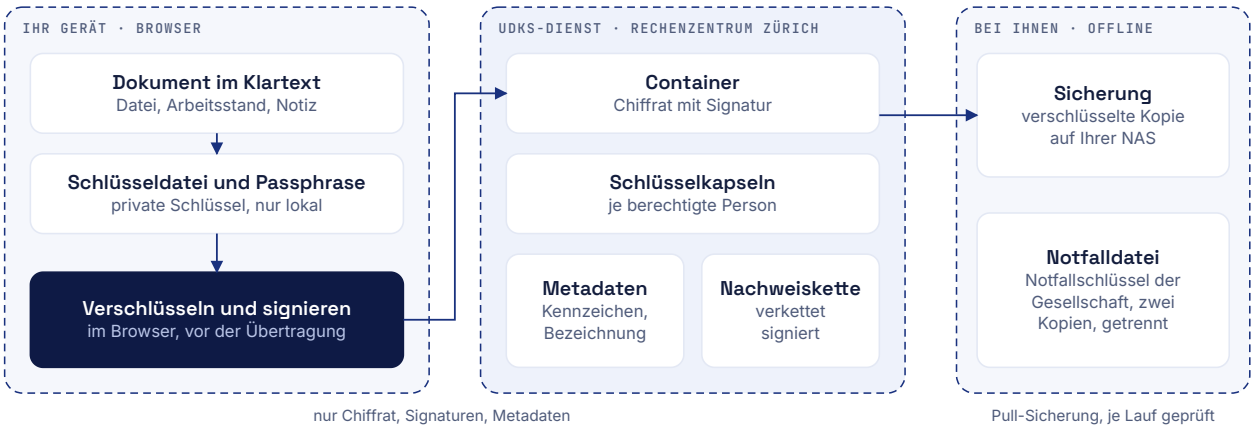


Bild 1 · Speicherort von Klartext und Chiffrat: Inhalte und Schlüssel bleiben bei Ihnen, der Dienst erhält Chiffrat, Signaturen und Metadaten.

Wenn Sie ein Dokument ablegen, erzeugt Ihr Browser einen zufälligen Schlüssel für dieses eine Dokument, verschlüsselt den Inhalt damit und signiert das Ergebnis mit Ihrem persönlichen Schlüssel. Für jede Person, die das Dokument nach den Regeln sehen darf, verpackt der Browser den Dokumentenschlüssel in eine eigene Kapsel, die Schlüsselkapsel. Erst dann wird übertragen. Der Dienst erhält den verschlüsselten Container, die Kapseln und die Angaben, die er zum Lenken braucht.

Beim Öffnen läuft es umgekehrt: Der Dienst prüft, ob Sie berechtigt sind, und liefert Container und Kapsel. Ihr Browser öffnet die Kapsel mit Ihrem privaten Schlüssel und entschlüsselt den Inhalt lokal. Auch das gemeinsame Bearbeiten in Echtzeit folgt diesem Muster: Die Änderungen der Beteiligten laufen verschlüsselt über den Dienst.

Klartext und Chiffrat nach Speicherort

GEGENSTAND	IHR GERÄT	UDKS-DIENST
Dokumentinhalt, Arbeitsstände, Änderungsnotizen	Klartext	nur Chiffrat
Private Schlüssel und Passphrase	ja	nie
Öffentliche Schlüssel, Kapseln, Signaturen	ja	ja
Kennzeichen mit Schutzklasse, Bezeichnung, Dateiname, Stand, Grösse Metadaten: Mit ihnen lenkt, filtert und sucht der Dienst.	ja	ja
Handlungen mit Person, Zeitpunkt und Aktion	Ansicht nach Recht	Nachweiskette

Die Aussage zur Verschlüsselung gilt für Dokumentinhalte. Konten-, Kontakt- und Metadaten, gewöhnliche E-Mails mit dem Support sowie Bestell- und Zahlungsdaten gehören nicht dazu. Wer Vertrauliches nicht im Dateinamen oder in der Bezeichnung führen will, wählt beide entsprechend.

DIE KONSEQUENZ

Im vorgesehenen Betrieb kann die Betreiberin ein Dokument nicht im Klartext herausgeben, weil sie die Schlüssel dazu nicht hat. Aus demselben Grund kann sie es auch nicht wiederherstellen, wenn alle Schlüssel dazu verloren sind. Die Schlüsselhoheit liegt beim Unternehmen, mit der Verantwortung, die dazugehört. Kapitel 3 beschreibt, wie UDKS dafür vorsorgt.

KAPITEL 3

Kryptografie im Einzelnen

UDKS verwendet veröffentlichte, standardisierte Verfahren auf dem aktuellen Stand der Normung, eingebunden aus einer offenen Bibliothek. Eigene kryptografische Verfahren kommen nicht vor.

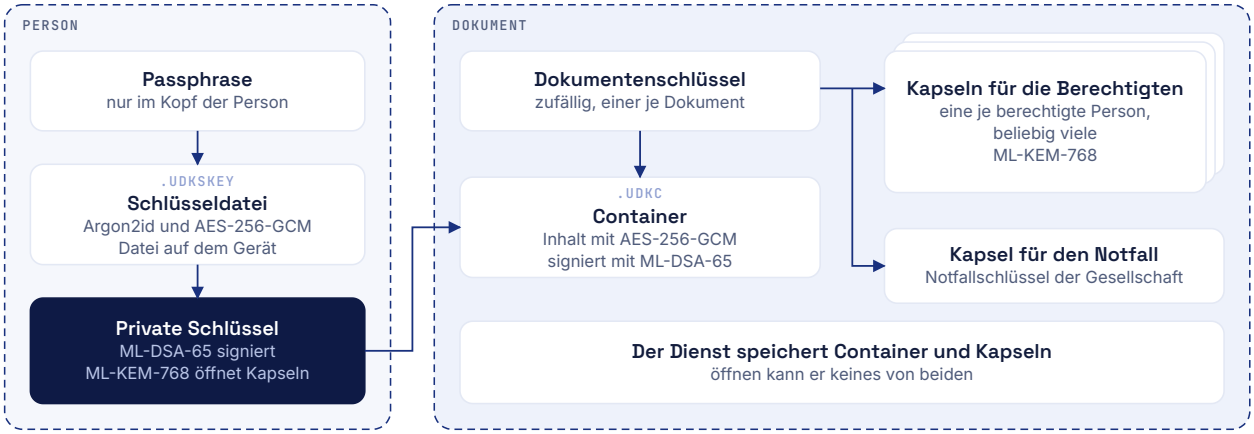


Bild 2 · Ein Schlüssel je Dokument, eine Kapsel je berechtigte Person. Die privaten Schlüssel liegen in der Schlüsseldatei auf Ihrem Gerät.

ZWECK	VERFAHREN	NORM
Inhalt eines Dokuments ein zufälliger Schlüssel je Dokument	AES-256-GCM	FIPS 197, NIST SP 800-38D
Schlüsselkapsel je berechtigte Person	ML-KEM-768	FIPS 203
Signatur Container, Anmeldung, Arbeitsstände, Kenntnisnahme, Nachweiskette, Sicherungsmanifest	ML-DSA-65	FIPS 204
Schutz der Schlüsseldatei aus der Passphrase abgeleitet	Argon2id, danach AES-256-GCM	RFC 9106
Verkettung der Nachweise	SHA-512	FIPS 180-4

Die Post-Quanten-Verfahren stammen aus der Bibliothek liboqs des Projekts Open Quantum Safe. Im Browser läuft sie als WebAssembly; der Server verwendet dieselbe Bibliothek, um Signaturen zu prüfen und die Nachweise zu signieren. Drei automatisierte Kreuzprüfungen laufen bei jeder Änderung und stellen sicher, dass beide Seiten dieselben Ergebnisse liefern: Eine im Browser-Kern erzeugte Signatur wird mit der Bibliothek des Servers geprüft. Ein im Browser-Kern gebauter Container wird auf der Serverseite verifiziert und entschlüsselt, und eine dort erzeugte Schlüsselkapsel wird hier geöffnet. Die Ableitung des Schlüssels aus der Passphrase liefert im Browser dasselbe Ergebnis wie die Referenzimplementierung.

Anmelden ohne Passwort

Ein Konto hat kein Passwort, das der Dienst kennen oder verlieren könnte. Bei der Aktivierung erzeugt der Browser zwei Schlüsselpaare, eines zum Signieren und eines zum Öffnen von Kapseln, und legt die privaten Teile in eine Schlüsseldatei, geschützt mit Ihrer Passphrase. Zur Anmeldung signiert der Browser eine einmalige Anfrage des Dienstes; der Dienst prüft die Signatur mit Ihrem öffentlichen Schlüssel. Eine Sitzung dauert 60 Minuten. Ein zweites Gerät koppeln Sie per QR-Code.

Wenn ein Schlüssel verloren geht

Verliert eine Person Schlüsseldatei oder Passphrase, setzt der Key-User des Unternehmens das Konto zurück. Die Person aktiviert es neu und erhält ein neues Schlüsselpaar. Kolleginnen und Kollegen, die die betroffenen Dokumente noch öffnen können, versorgen sie in ihrem Browser mit neuen Kapseln. Die alte Passphrase stellt niemand wieder her, und die Betreiberin erhält dabei keinen Zugang zu Inhalten.

Für den Fall, dass niemand mehr einen passenden Schlüssel hat, gibt es den Notfallschlüssel der Gesellschaft. Eine berechtigte Person des Unternehmens erzeugt ihn in einer Zeremonie im Browser, bevor das erste echte Dokument entsteht. Im Dienst liegt nur der öffentliche Teil; jedes neue Dokument erhält damit eine zusätzliche Kapsel. Die Datei mit dem privaten Teil verwahrt das Unternehmen offline in zwei Kopien an getrennten Orten, die Passphrase dazu gesondert. Die Betreiberin nimmt weder die Datei noch die Passphrase entgegen und hat keinen Generalschlüssel.



Beide Wege laufen im Browser des Unternehmens. Die Betreiberin nimmt weder Schlüsseldatei noch Passphrase entgegen.
Jeder Zugriff auf eine Notfall-Kapsel steht als Ereignis in der Nachweiskette.

Bild 3 · Zwei Wege zurück zum Zugang: das Zurücksetzen eines Kontos durch den Key-User und, wenn kein passender Schlüssel mehr vorhanden ist, der Notfallschlüssel der Gesellschaft.

Heutige und nächste Fassung des Formats

Das heutige Format setzt ML-KEM und ML-DSA ohne zweites, klassisches Verfahren ein. Mehrere Fachstellen empfehlen, beide zu kombinieren, damit ein Fehler im neuen Verfahren nicht allein über die Vertraulichkeit entscheidet. Die zweite Fassung des Formats sieht das vor: Kapseln aus X25519 und ML-KEM-768, Signaturen aus Ed25519 und ML-DSA-65, dazu Schlüsselwechsel und Widerruf. Sie ist nicht Teil des heutigen Produkts; der Funktionsfahrplan führt sie als `Welle 3, Termin offen`.

Jeder Container nennt die Fassung des Formats und die verwendeten Verfahren. Das ist die Voraussetzung dafür, ein Verfahren später abzulösen. Die Formatspezifikation mit Versionen und Testvektoren ist VERFÜGBAR.

KAPITEL 4

Ordnung: Kennzeichen, Datenpass, Schutzklassen

Verschlüsselung regelt die Vertraulichkeit des Inhalts. Art, Zugehörigkeit und zulässige Verwendung eines Dokuments regelt sie nicht. Diese Angaben tragen in UDKS der Datenpass und das Kennzeichen.

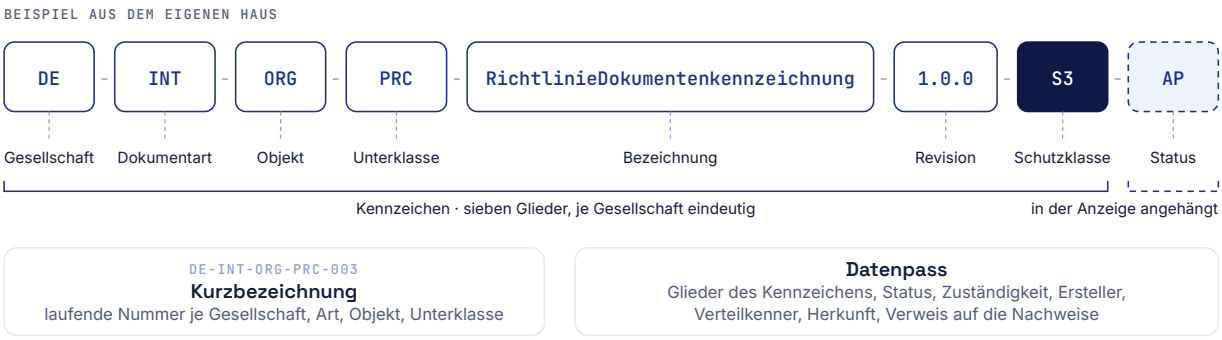


Bild 4 · Kennzeichen, Statusanzeige und Kurzbezeichnung am Beispiel. Rechte und Regeln folgen dem Kennzeichen; der Datenpass führt alle Angaben zum Dokument.

Der Datenpass ist der vollständige Satz der Angaben zu einem Dokument. Er enthält die sieben Glieder, aus denen das Kennzeichen entsteht: Gesellschaft, Dokumentart, Objektbezug, Unterklasse, Bezeichnung, Revision und Schutzklasse. Darüber hinaus führt er den Status im Lebenszyklus, die Zuständigkeit, die erstellende Person, einen allfälligen Verteilkenner, die Herkunft (im System angelegt, von aussen erhalten oder importiert) und den Verweis auf die Nachweise zum Dokument.

Das Kennzeichen ist die Kurzform dieses Passes: für Menschen lesbar und je Gesellschaft eindeutig. In der Anzeige folgt ihm der aktuelle Status als achtes Glied, zum Beispiel AP für «freigegeben»; er wechselt mit dem Lebenszyklus, die sieben Glieder davor bleiben. Zusätzlich vergibt der Dienst eine Kurzbezeichnung mit laufender Nummer. Welche Dokumentarten, Objektbezüge und Unterklassen es gibt, legt jede Gesellschaft in ihrem Rahmen fest. Wer lieber in Ordnern denkt, legt eigene Ordner als zweite Sicht an; die Rechte folgen weiter dem Kennzeichen.

Fünf Schutzklassen

KLASSE	BEDEUTUNG	SICHTBARKEIT DER FREIGEGEBENEN REVISION	DOWNLOAD-LINK NACH AUSSEN
S1	Öffentlich	alle Personen der Gesellschaft	direkt
S2	Gebundener Empfänger	alle Personen der Gesellschaft; an einen benannten Empfänger gebunden	direkt
S3	Intern	alle Personen der Gesellschaft	mit Autorisierung
S4	Arbeitsgruppe	die Mitglieder der zugeordneten Arbeitsgruppe	mit Autorisierung
S5	Einzeln Berechtigte	namentlich benannte Personen	mit Autorisierung

Die Klasse wirkt zweifach. Der Dienst zeigt ein Dokument nur den Personen, denen die Klasse es erlaubt, und der Browser verpackt den Dokumentenschlüssel nur für diese Personen. Wer ein Dokument nach den Regeln nicht sieht, erhält auch keine Kapsel dazu. Entwürfe sehen bis zur Freigabe nur die Beteiligten: die erstellende, die zuständige, die mitschreibenden und die prüfenden Personen.

Rollen und Prüfung

Rollen gelten je Gesellschaft: Geschäftsführung, Leitung, Sachbearbeitung, Qualitätsmanagement, Informationssicherheit und die Verwaltung der Kundin. Die Geschäftsführung wirkt als Key-User in ihrem eigenen Zugriffsrahmen. Das Qualitätsmanagement prüft und gibt nie frei. Das Konto der Betreiberin richtet Gesellschaften ein und sieht kein Dokument. Wer jemanden vertritt, handelt sichtbar «im Auftrag von».

Jeder Aufruf des Dienstes läuft durch dieselbe Prüfung: Subjekt, Aktion, Objekt. Was nicht ausdrücklich erlaubt ist, wird verweigert, und jede Verweigerung ist selbst ein Ereignis in der Nachweiskette. Das Regelwerk trägt eine Version; jedes Ereignis hält fest, welche Fassung galt. Dienstkonten und Schnittstellen gehen durch dieselbe Prüfung wie Menschen.

KAPITEL 5

Lenkung: vom Entwurf zur verbindlichen Revision

Ein gelenktes Dokument hat zu jedem Zeitpunkt genau eine gültige Fassung, und es ist belegt, welche Personen diese Fassung geprüft, freigegeben und erhalten haben.

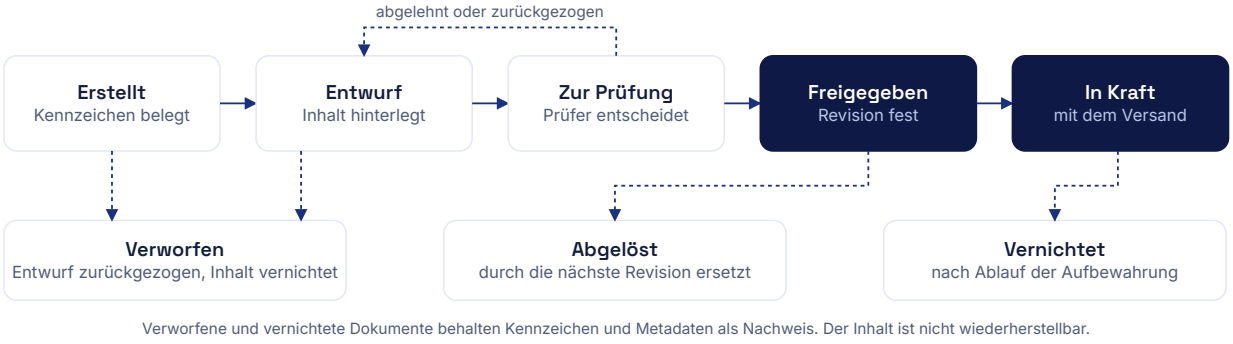


Bild 5 · Vom Entwurf zur verbindlichen Revision. Jede Stufe wechselt nur, wer dafür die Rolle hat, und jeder Wechsel ist ein Ereignis in der Nachweiskette.

Bearbeiten

Wer ein Dokument bearbeitet, sperrt es, arbeitet lokal im Klartext und lädt den neuen Stand verschlüsselt zurück. Jeder Arbeitsstand trägt Urheber, Zeit und Signatur; der Verlauf bleibt erhalten. Textentwürfe lassen sich im Browser gemeinsam bearbeiten, mit Mitautoren und Konfliktanzeige.

Prüfen und freigeben

Der Weg zur Freigabe trennt die Rollen: Eine Person legt vor, eine prüft, eine gibt frei. Wer erstellt hat, gibt nicht selbst frei. Für kleine Teams gibt es einen vereinfachten Modus; eine Selbstfreigabe ist dort möglich und wird als solche vermerkt. Mit der Freigabe ist die Revision unveränderlich. Eine Änderung führt zu einer neuen Revision, die alte bleibt als abgelöst erhalten. Der Teamabschluss mit Mehrheit und Fristen, auch über mehrere Dokumente eines Projekts, ist VERFÜGBAR.

Versenden und Kenntnisnahme einholen

Nach aussen führen zwei Wege mit unterschiedlichem Zweck. Die **Versandmappe** ist der förmliche Versand an einen registrierten Empfänger: Sie fasst ein oder mehrere freigegebene Dokumente der Klassen S1 und S2 zusammen, trägt ein Begleitschreiben und wird unveränderlich archiviert. Mit dem Versand tritt die Revision in Kraft. Der **Download-Link** stellt ein einzelnes freigegebenes Dokument einer Person ohne Konto zum Abruf bereit. Er erlischt nach einer Frist und nach einer festgelegten Zahl von Abrufen, das Passwort dazu geht auf einem getrennten Weg, und ab Schutzklasse S3 braucht er die Autorisierung durch die Leitung oder die Geschäftsführung. Externe Empfänger erhalten nur die Revisionen, die ihnen zugewiesen sind. Wo es auf die Kenntnis ankommt, bestätigt jede Person «Gelesen und verstanden» mit ihrer Signatur, je Revision. Offene Kenntnisnahmen stehen im Arbeitsplatz der Person.

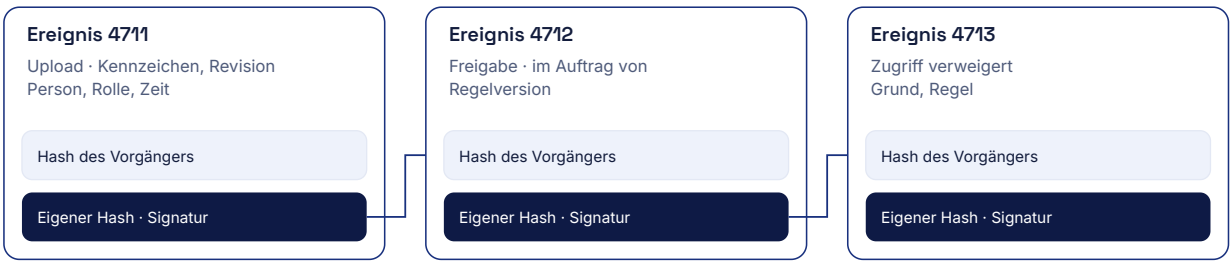
Aufbewahren und vernichten

Aufbewahrungsregeln gelten je Dokumentart und Gesellschaft und zeigen die fälligen Dokumente an. Vernichtet wird ein Dokument, indem seine Schlüsselkapseln und sein verschlüsselter Inhalt gelöscht werden. Kennzeichen und Metadaten bleiben als Nachweis der Vernichtung bestehen. Die Löschanforderung mit festgelegtem Umfang, von Ständen und Revisionen bis zu den Sicherungen, und der Status gesperrter Kopien sind VERFÜGBAR.

KAPITEL 6

Nachweis: eine Kette, die sich nachrechnen lässt

Der Nachweis entsteht in UDKS nicht als Bericht am Ende, sondern als Nebenprodukt jeder Handlung. Jede Aktion schreibt ein Ereignis, und jedes Ereignis hängt am vorherigen.



Hash: SHA-512 über Vorgänger-Hash und Ereignis · Signatur: ML-DSA-65 mit dem Schlüssel des Dienstes · Datenbankrolle der Anwendung: nur anhängen
Geprüft wird jede Nacht und auf Wunsch sofort. Der Prüfexport trägt ein Manifest, das sich ausserhalb des Dienstes nachrechnen lässt.

Bild 6 · Jedes Ereignis trägt den Hash seines Vorgängers und eine Signatur des Dienstes. Wer ein Ereignis ändert oder entfernt, bricht die Kette an dieser Stelle.

Ein Ereignis hält die Aktion, das betroffene Objekt und dessen Stand fest: Kennzeichen, Revision, Status. Es nennt die handelnde Person oder den Dienst, ihre Rolle, eine allfällige Vertretung, die geltende Fassung des Regelwerks und die Zeit. Aus dem Hash des vorherigen Ereignisses und dem eigenen Inhalt entsteht der eigene Hash, den der Dienst signiert.

Drei Eigenschaften machen die Kette belastbar. Die Anwendung arbeitet mit einer Datenbankrolle, die Nachweise nur anhängen kann, nicht ändern und nicht löschen. Die ganze Kette wird jede Nacht nachgerechnet, und die Administration kann die Prüfung jederzeit selbst auslösen. Und der Prüfexport enthält ein Manifest, mit dem sich die Integrität ausserhalb des Dienstes prüfen lässt.

Ausgewertet werden die Nachweise in einer Ansicht mit Filtern nach Gesellschaft, Objekt, Person, Zeitraum und Aktion. Revision und Qualitätsmanagement prüfen damit den Ablauf, zum Beispiel Freigaben, Versand und Kenntnisnahmen, ohne die Dokumente selbst zu öffnen: Die Ansicht zeigt die Ereignisse mit ihren Metadaten, keinen Inhalt.

INHALT UND GRENZEN DES NACHWEISES

Die Kette hält Metadaten fest, keinen Inhalt. Sie zeigt, dass eine bestimmte Revision freigegeben, versendet oder bestätigt wurde, und sie zeigt jeden abgewiesenen Versuch. Sie beweist nicht, dass jemand einen Text verstanden hat; sie beweist, dass die Person es mit ihrer Signatur erklärt hat.

KAPITEL 7

Migration: der Altbestand kommt geführt ins System

Kaum ein Unternehmen beginnt bei null. Die Unterlagen liegen auf einem Dateiserver, gewachsen über Jahre, ohne Kennzeichen und ohne Schutzklasse. Die Migration bringt diesen Bestand in die Ordnung von UDKS, ohne dass Klartext Ihr Haus verlässt.



Bild 7 · Die Migration in sechs Schritten. Bis zur Abnahme bleibt die Quelle führend und der Import abgeschottet.

Dafür läuft bei Ihnen eine Importkapsel: ein abgeschlossenes Programm, das die Quelle mit einem Lesekonto liest, das Sie selbst anlegen. Die Importkapsel verändert an der Quelle nichts. Sie erfasst, schlägt vor und verschlüsselt vor Ort mit den Schlüsseln der berechtigten Personen. An den Dienst gehen Chiffrat und Metadaten.

01 **Dokumenteninventar.** Alle Dateien eines Ordnerzweigs werden mit Pfad, Grösse und Typ erfasst, Duplikate erkannt. Der Bestand ist damit bekannt, bevor eine Datei übertragen wird.

02 **Zuordnung.** Regeln bilden Ordner auf den Datenpass ab. Für jede Datei entsteht ein Kennzeichnungsvorschlag mit Begründung: Dokumentart, Bezeichnung und Schutzklasse. Unsichere Fälle entscheidet eine Person, gebündelt je Ordner statt Datei für Datei.

03 **Testimport.** Die Dokumente entstehen verschlüsselt in der Zielgesellschaft, bleiben aber abgeschottet: Ablage, Suche und Versand kennen sie noch nicht.

04 **Prüfung.** Der Dienst zieht eine Stichprobe, die eine Fachperson gegen die Quelle prüft. Ein Delta-Bericht zeigt jede Abweichung zwischen Quelle und Import.

05 **Umschalten.** Erst wenn keine Abweichung offen ist, schaltet eine zweite Person mit ihrer Gegenzeichnung um; im vereinfachten Modus für kleine Teams darf es dieselbe Person, mit Vermerk. Das Abnahmeprotokoll steht in der Nachweiskette.

06 **Betrieb.** Die Dokumente sind für die Berechtigten sichtbar, wahlweise in einer Ordner-Sicht, die der alten Struktur entspricht.

RÜCKFALL JE LAUF · VERFÜGBAR

Bis zum Umschalten bleibt die Quelle führend. Ein umgeschalteter Lauf lässt sich innerhalb einer festgelegten Frist zurücknehmen und erneut abnehmen, ohne dass ein Dokument verloren geht.

KEIN ERFUNDENER VERLAUF

Importierte Dokumente tragen die Herkunft «Import». Ihre Geschichte in UDKS beginnt mit dem Import; eine frühere Freigabe wird nicht nachgebildet. Nach der Abnahme wird die Importkapsel entfernt, und das Lesekonto entziehen Sie.

KAPITEL 8

Betrieb, Sicherung und Ausstieg

Die C&W Software Labs AG betreibt UDKS in einer Instanz mit Datenstandort Schweiz. Das Angebot richtet sich an Kunden in der Schweiz und in Liechtenstein.

THEMA	UMSETZUNG
Standort	Produktionsinstanz bei Exoscale, Zone Zürich, ohne US-Hyperscaler. Das Rechenzentrum ist nach ISO 27001 zertifiziert; die Zertifizierung gilt dem Rechenzentrum, nicht UDKS. Dokumente, Konten und Nachweise bleiben in der Schweiz.
Aufbau	Von aussen erreichbar sind nur die Ports 80 und 443, mit automatischem HTTPS. Anwendung und Datenbank stehen in einem internen Netz. Die Anwendung läuft ohne Root-Rechte und mit einer eingeschränkten Datenbankrolle.
Lieferung	Die Umgebungen sind als Code beschrieben. Vor jeder Lieferung laufen über 1'100 automatisierte Tests, Browser-Suiten gegen PostgreSQL und eine Prüfung der Abhängigkeiten auf bekannte Schwachstellen. Staging folgt automatisch, die Produktion nur aus einem markierten Stand und mit Freigabe. Vor jeder Bereitstellung entsteht ein Schnappschuss; der Rückweg ist ein eigenes, dokumentiertes Verfahren.
Verfügbarkeit	Zielverfügbarkeit 99,5 % im Monatsmittel, gemessen je Kalendermonat. Reguläre Wartung liegt sonntags zwischen 00 und 04 Uhr und wird mindestens sieben Kalendertage vorher angekündigt.
Sicherung bei Ihnen	Ihre NAS holt die Sicherung selbst ab. Die Kopie ist verschlüsselt wie der Bestand, trägt ein signiertes Manifest und wird bei jedem Lauf gegen den öffentlichen Schlüssel des Dienstes geprüft, den Sie vorab auf einem getrennten Weg erhalten haben. Der zweite Standort steht unter Ihrer Kontrolle. Die Wiederherstellung in einer Testzone mit Protokoll, der Wiederanlauf und Sicherungspakete auf buchbarem Archivspeicher sind VERFÜGBAR.
Ausstieg	Während der Vertragsdauer und 30 Kalendertage danach steht der vollständige Export offen: die Inhalte nach Entschlüsselung bei Ihnen im ursprünglichen Dateiformat, Metadaten und Nachweise maschinenlesbar mit Prüfanleitung. Danach werden die aktiven Daten und anschliessend die Sicherungskopien gelöscht.

Einführung

Die Einrichtung geschieht aus der Ferne: Gesellschaften, Rollen, Freigaberegeln und der Rahmen für die Kennzeichen. Jede Person durchläuft einen geführten Lernpfad mit sechs Einheiten, in dem sie die Schritte an Übungsdokumenten selbst ausführt. Die Schlüssel-Zeremonie mit der Geschäftsführung findet vor dem ersten echten Dokument statt. Ein Unternehmen ist innerhalb von fünf Arbeitstagen nach dem Start produktiv, sofern es Teilnehmerliste, Zuständigkeiten und Termine rechtzeitig bereitstellt. Das versionierte Konfigurationspaket mit Pflichtfeldern, Rollen und Freigabemodus, bestätigt und mit Rückfall, ist VERFÜGBAR.

KAPITEL 9

Regulatorische Einordnung

UDKS unterstützt die Umsetzung der einschlägigen Anforderungen. Eine Zertifizierung durch FINMA, BaFin oder BSI existiert für Software dieser Art nicht, und wir behaupten keine.

Die folgende Übersicht ordnet ein, welche Funktion zu welcher Anforderung beiträgt. Sie ersetzt keine Rechtsberatung. Ob eine Anforderung im Einzelfall erfüllt ist, hängt vom Unternehmen, seinen Abläufen und seiner Aufsicht ab; die Verantwortung dafür bleibt bei ihm. Eine allgemeine regulatorische Eignung für jeden Einsatzfall und eine allgemeine DORA-Konformität sagen wir nicht zu.

GRUNDLAGE	ANFORDERUNG	BEITRAG VON UDKS
Aufbewahrung Art. 958f OR, GeBüV	Geschäftsbücher und Belege zehn Jahre aufbewahren, integer und nachvollziehbar	Unveränderliche Revisionen, Aufbewahrungsregeln mit Fälligkeit, Nachweiskette, Sicherung mit signiertem Manifest
Datensicherheit Art. 8 DSG, DSV	Angemessene technische und organisatorische Massnahmen	Verschlüsselung im Browser, Schutzklassen, Prüfung bei jedem Aufruf, protokollierte Verweigerung
Berufs- und Bankkundengeheimnis Art. 321 StGB, Art. 47 BankG	Schutz der Geheimnisse gegenüber Dritten, auch gegenüber Dienstleistern	Die Betreiberin hat im vorgesehenen Betrieb keinen Zugriff auf Klartexte; die Schlüssel liegen beim Unternehmen
Operationelle Resilienz FINMA-RS 2023/1	Umgang mit kritischen Daten, Kontrollen und Wiederherstellung	Getrennte Rollen bei der Freigabe, Nachweise, Sicherung an einem zweiten Standort, Vollexport
Post-Quanten-Kryptografie FINMA-Aufsichtsmitteilung 05/2026	Roadmap, Inventar der Kryptografie, Einbezug der Dienstleister, Kryptoagilität	Für den Anwendungsfall Dokumente sind ML-KEM-768 und ML-DSA-65 produktiv. Verfahren, Schlüsselorte und Formatfassung sind dokumentiert und lassen sich ins Inventar übernehmen.
Europäische Union DORA Art. 9 und 28, DSGVO Art. 28 und 32	Schutz der Daten, Register und Ausstiegsstrategie je IKT-Dienstleister, Auftragsverarbeitung	Dieselben Mechanismen; Vertrag zur Auftragsbearbeitung, Angaben für das Register, dokumentierter Ausstieg. Der EU-Rollout startet ab dem 04.01.2027.

UDKS wird nach Schweizer Datenschutzrecht betrieben; eine Vereinbarung zur Auftragsbearbeitung ist Teil jeder Bestellung. Das Vertragspaket mit Leistungsbeschreibung, Servicevereinbarung und der Vereinbarung «Schlüssel und Wiederherstellung» ist auf udks.cundw.ch einsehbar.

KAPITEL 10

Grenzen des Systems

Ein System, das Inhalte nicht lesen kann, bietet einige Funktionen nicht, die andere Systeme bieten. Diese Grenzen sind die Kehrseite des Prinzips und sollten vor einer Entscheidung bekannt sein.

GRENZE	BEDEUTUNG
Der Dienst durchsucht keine Inhalte	Die Suche arbeitet über Kennzeichen, Bezeichnungen und Merkmale, mit Platzhaltern und Filtern. Eine Suche im Text der Dokumente findet im Dienst nicht statt, weil er den Text nicht kennt. Gute Bezeichnungen und Merkmale ersetzen sie.
Metadaten sind sichtbar	Kennzeichen, Bezeichnung, Dateiname, Grösse, Zeitpunkte und beteiligte Konten liegen dem Dienst vor. Sie sind durch Zugriffsregeln geschützt, nicht durch die Verschlüsselung der Inhalte.
Schlüssel sind Sache des Unternehmens	Ohne Schlüsseldatei und Passphrase einer berechtigten Person und ohne nutzbaren Notfallschlüssel ist ein Dokument verloren. Die Betreiberin kann es nicht wiederherstellen. Dokumente, die vor der Schlüssel-Zeremonie entstehen, haben keine Kapsel für den Notfall.
Das Endgerät zählt	Der Klartext entsteht und endet auf dem Gerät der berechtigten Person, in der Anwendung, die ihr Browser vom Dienst lädt. Wer das Gerät beherrscht, sieht dieselben Inhalte wie die berechtigte Person. Der Schutz der Endgeräte bleibt Aufgabe des Unternehmens.
Kein Prüfsiegel	UDKS ist von keiner Aufsichts- oder Zertifizierungsstelle zertifiziert, geprüft oder zugelassen. Die Zertifizierung nach ISO 27001 betrifft das Rechenzentrum.
Kein absoluter Schutz	Die eingesetzten Verfahren gelten nach heutigem Stand als geeignet, auch gegen Angriffe mit Quantencomputern. Eine Zusage für alle Zeit gibt es in der Kryptografie nicht; deshalb trägt das Format eine Versionsnummer und lässt sich ablösen.

KAPITEL 11

Funktionsstand, Quellen, Kontakt

Massgebend für den Stand jeder einzelnen Funktion ist der Funktionsfahrplan auf udks.cundw.ch. Er führt jede Funktion in einem von zwei Ständen: VERFÜGBAR oder Welle 3, Termin offen. Die sechzehn Funktionen der Welle 2 sind seit dem 20.11.2026 verfügbar. Wo dieses Dokument eine Funktion nennt, die der Funktionsfahrplan noch nicht als verfügbar führt, trägt sie die Marke ihres Stands.

IM FUNKTIONSFAHRPLAN · WELLE 2 · VERFÜGBAR SEIT DEM 20.11.2026

Teamabschluss mit Mehrheit und Fristen · Konfigurationspaket mit Pflichtfeldern, Rollen, Modus, Versionen und Rückfall · Löschanforderung mit Umfang und Status gesperrter Kopien · Formatspezifikation mit Versionen und Testvektoren · Wiederherstellung in einer Testzone mit Protokoll und Wiederanlauf · Sicherungspakete auf Archivspeicher; Zusatz- und Archivspeicher buchbar · Rückfall je Lauf und Delta-Automatik im Import.

IM FUNKTIONSFAHRPLAN · WELLE 3, TERMIN OFFEN

Eigene Ausführungsumgebung je Kunde für Anwendungen, Datenbanken, Texterkennung und KI, die Klartext brauchen, mit Geheimnissen und Automationsaufträgen · zweite Fassung des Formats mit Schlüsselwechsel und Widerruf · Offline-Client · Ordner- und Programmbrücke · Penetrationstests.

Ausserhalb der Wellen. Der EU-Rollout startet ab dem 04.01.2027.

Der Funktionsfahrplan dient der Information. Er begründet keine Liefer- oder Terminpflicht; eine Funktion, die er noch nicht als verfügbar führt, ist nicht Teil der heutigen Leistung.

Quellen

01 NIST, FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, und FIPS 204, Module-Lattice-Based Digital Signature Standard, 13.8.2024. csrc.nist.gov/pubs/fips/203/final · csrc.nist.gov/pubs/fips/204/final

02 NIST, IR 8547, Transition to Post-Quantum Cryptography Standards. csrc.nist.gov/pubs/ir/8547/final

03 NIS-Kooperationsgruppe, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 23.6.2025. digital-strategy.ec.europa.eu

04 FINMA, Aufsichtsmitteilung 05/2026 «Quantum Computing», 9.7.2026. finma.ch/de/news/2026/07/20260709-mm-am-05-26

05 BSI, Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen. bsi.bund.de

06 Obligationenrecht, Art. 958f (SR 220); Geschäftsbücherverordnung (SR 221.431); Datenschutzgesetz, Art. 8 (SR 235.1). fedlex.admin.ch

07 FINMA, Rundschreiben 2023/1 «Operationelle Risiken und Resilienz – Banken». finma.ch

08 Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA). eur-lex.europa.eu/eli/reg/2022/2554/oj

09 Open Quantum Safe, liboqs. openquantumsafe.org · Argon2: RFC 9106. rfc-editor.org/rfc/rfc9106

10 C&W Software Labs AG, Leistungsbeschreibung und Servicevereinbarung 1.1, Vereinbarung «Schlüssel und Wiederherstellung» 1.0, Funktionsfahrplan. udks.cundw.ch

KONTAKT

C&W Software Labs AG
Bundesplatz 4 · 6300 Zug · Schweiz
techsupport@cundw.ch · udks.cundw.ch
Funktionsfahrplan:
udks.cundw.ch/funktionsfahrplan

Fragen zur Kryptografie, zum Betrieb und zum Vertragspaket beantworten wir schriftlich.

ZU DIESEM DOKUMENT

Whitepaper 1.3, November 2026.
Herausgeberin: C&W Software Labs AG, Zug.
Fassung 1.3 ersetzt 1.2: Welle 2 verfügbar seit dem 20.11.2026, EU-Rollout ab dem 04.01.2027.

Dieses Dokument beschreibt den Stand der Technik von UDKS zum Zeitpunkt der Herausgabe. Es ist kein Angebot und keine Zusicherung. Massgebend sind die mit der Bestellung vereinbarten Vertragsunterlagen.

ANHANG

Glossar

Die Begriffe dieses Dokuments in alphabetischer Folge.

BEGRIFF	BEDEUTUNG
Arbeitsgruppe	Personenkreis innerhalb einer Gesellschaft. Dokumente der Schutzklasse S4 gehören einer Arbeitsgruppe; nur ihre Mitglieder sehen die freigegebene Revision.
Betreiberin	Die C&W Software Labs AG. Sie betreibt den Dienst und richtet Gesellschaften ein. Im vorgesehenen Betrieb hat sie keine privaten Schlüssel und keinen Zugriff auf Klartexte.
Chiffrat	Verschlüsselter Inhalt. Ohne den passenden Schlüssel ist er nicht lesbar.
Container	Die verschlüsselte und signierte Datei eines Dokuments oder Arbeitsstands, so wie der Dienst sie speichert.
Datenpass	Der vollständige Satz der Angaben zu einem Dokument: die Glieder des Kennzeichens, Status, Zuständigkeit, erstellende Person, Verteilkenner, Herkunft und der Verweis auf die Nachweise.
Dienst	UDKS als laufende Anwendung auf den Servern der Betreiberin, im Unterschied zum Browser auf Ihrem Gerät. Der Dienst speichert, prüft Berechtigungen und führt die Nachweise.
Dokumentenschlüssel	Zufälliger Schlüssel, mit dem genau ein Dokument verschlüsselt ist (AES-256-GCM).
Download-Link	Befristeter, passwortgeschützter Abruf eines einzelnen freigegebenen Dokuments für eine Person ohne Konto.
Ereignis	Eintrag der Nachweiskette zu einer Handlung oder zu einer Verweigerung.
Gesellschaft	Rechtliche Einheit des Unternehmens in UDKS, mit eigenem Rahmen, eigenen Rollen und eigenen Freigaberegeln.
Importkapsel	Abgeschlossenes Programm, das bei der Migration beim Unternehmen läuft, die Quelle liest und vor Ort verschlüsselt. Nicht zu verwechseln mit der Schlüsselkapsel.
Kenntnisnahme	Die mit der eigenen Signatur bestätigte Erklärung «Gelesen und verstanden» zu einer bestimmten Revision.
Kennzeichen	Sprechender, je Gesellschaft eindeutiger Name eines Dokuments aus sieben Gliedern. In der Anzeige folgt der aktuelle Status als achtes Glied.
Key-User	Die Geschäftsführung einer Gesellschaft in ihrer Rolle als Schlüsselverantwortliche. Sie setzt Konten zurück und führt die Schlüssel-Zeremonie durch.
Kurzbezeichnung	Kurzform eines Kennzeichens mit laufender Nummer, zum Beispiel DE-INT-ORG-PRC-003.
Nachweiskette	Die verkettete und signierte Folge aller Ereignisse. Jedes Ereignis trägt den Hash seines Vorgängers.
Notfallschlüssel	Schlüsselpaar der Gesellschaft für den Fall, dass keine Person mehr einen passenden Schlüssel hat. Der private Teil liegt offline beim Unternehmen.

Passphrase	Schützt die Schlüsseldatei. Nur die Person selbst kennt sie; der Dienst erhält sie nie.
Rahmen	Die Dokumentarten, Objektbezüge und Unterklassen, die eine Gesellschaft für ihre Kennzeichen festlegt.
Revision	Fassung eines Dokuments, zum Beispiel 1.0.0. Mit der Freigabe ist sie unveränderlich.
Schlüsseldatei	Datei mit den privaten Schlüsseln einer Person, geschützt mit ihrer Passphrase.
Schlüsselkapsel	Kurz «Kapsel»: der Dokumentenschlüssel, verpackt für genau eine berechtigte Person (ML-KEM-768).
Schlüssel-Zeremonie	Das Erzeugen des Notfallschlüssels im Browser durch eine berechtigte Person des Unternehmens, vor dem ersten echten Dokument.
Schutzklasse	S1 bis S5. Sie ist ein Glied des Kennzeichens und bestimmt Sichtbarkeit, Versand und Freigabe.
Unternehmen	Die Kundin, die UDKS nutzt. Die Anrede «Sie» meint ihre Personen.
Versandmappe	Förmlicher Versand eines oder mehrerer freigegebener Dokumente der Klassen S1 und S2 an einen registrierten Empfänger, mit Begleitschreiben und unveränderlich archiviert.
Verteilkenner	Zusatz zur Schutzklasse für Personal- und Managementdokumente. Er sperrt jeden Versand nach aussen.