
Filum, technisch: was die IT vor der Einführung wissen will

Berechtigungen, Datenwege, Archivformat und Prüfbarkeit.
Ein Blatt für die IT eines Architektur- oder Planungsbüros.

Stand 19.09.2026. Alle Angaben stammen aus dem Code, wie er heute im Baum steht, nicht aus einer Produktbroschüre. Wo eine Quelle im Repo genauer ist, steht sie am Rand. Keine Rechtsberatung.

Filum ist noch nicht veröffentlicht. Die macOS-Fassung ist für den App Store in Vorbereitung, die Windows-Fassung ist zurückgestellt. Dieses Blatt beschreibt den Stand des Programms, nicht einen Liefertermin.

1. Was Filum tut

Ein Architektur- oder Planungsbüro führt seine Projektkorrespondenz in Microsoft 365. Jede Person sortiert ihre Projektmails in einen Outlook-Ordner. Filum liest diesen Ordner über Microsoft Graph und legt den Inhalt in einem Ordner auf dem Büro-NAS ab: die Originale als `.eml`, die Anhänge ausgepackt, die Verläufe als HTML, dazu eine Übersicht mit Suche, die direkt ab Disk funktioniert. Jeder Lauf schreibt einen Nachweis über den gesamten Bestand, verkettet mit dem vorigen und von einem Dritten zeitgestempelt.

Drei Eigenschaften bestimmen alles Weitere:

- Filum betreibt keinen Dienst. Es gibt keinen Server von bimover, auf dem Mails liegen, und keine Datenbank, in der ein Archiv stünde. Das Archiv ist ein Ordner auf einem Träger, den das Büro selbst wählt.
- Filum arbeitet mit der Anmeldung der Person, die den Lauf startet. Es gibt kein Dienstkonto und keinen tenantweiten Lesezugriff.
- Das Archiv ist ohne Filum lesbar und ohne Filum prüfbar. Beides ist keine Absichtserklärung, sondern liegt als Datei im Ordner.

2. Berechtigungen

Delegiert, nicht als Anwendung

Filum meldet sich über die mehrmandantenfähige Registrierung «Filum Mailarchiv» an, einen öffentlichen Client ohne Geheimnis auf dem Arbeitsplatz. Auf Windows läuft ein Gerätecode, auf macOS ein Anmeldefenster. Die App sieht danach genau die Postfächer und Ordner, die die angemeldete Person ohnehin öffnen darf, auch geteilte und freigegebene.

Die Alternative wäre ein Zugriff als Anwendung. Er bräuchte `Mail.Read` für den ganzen Mandanten, also Lesezugriff auf jedes Postfach des Büros, und ein Geheimnis, das irgendwo liegt. Beides gibt es bei Filum nicht, und es ist der Grund, warum die Einführung ohne Projekt auskommt.

Recht	Wofür
<code>Mail.ReadWrite</code>	Projektordner lesen, Rohbytes holen, beim Einsammeln Nachrichten in den Projektordner verschieben
<code>Mail.ReadWrite.Shared</code>	dasselbe für geteilte und freigegebene Postfächer
<code>User.Read</code>	Anzeigename und Adresse der angemeldeten Person, daraus die eigene Domain
<code>offline_access</code>	Anmeldung über den Programmstart hinaus halten

Schreibrecht steht in der Liste, weil das Einsammeln Nachrichten verschiebt. Filum löscht in keinem Postfach etwas, und es schreibt keine Nachricht.

Quelle: `Kern/crates/filum-graph/src/auth.rs` (Rechte), `Kern/crates/filum-kern/src/zugang.rs` (Registrierung).

Wenn der Mandant fremde Apps sperrt

Sperrt eine Organisation die Zustimmung durch Nutzer, scheitert die erste Anmeldung. Dann, und nur dann, zeigt Filum die Aufforderung samt Adresse für die einmalige Freigabe durch die Kontoverwaltung. Danach steht die App als Unternehmensanwendung im eigenen Mandanten und gilt für alle im Büro.

Eine eigene Registrierung je Kunde gibt es bewusst nicht. Sie machte den Zugriff nicht enger, sie verschöbe nur ein Formular auf den Kunden.

3. Datenwege

Filum spricht mit vier Gegenstellen, sonst mit keiner.

Ziel	Was hingeht	Wann
<code>login.microsoftonline.com</code>	Anmeldung, Token-Erneuerung	beim Anmelden und danach im Hintergrund
<code>graph.microsoft.com</code>	Ordner- und Nachrichtenabfragen mit dem Zugriffstoken	während eines Laufs
<code>www.bimover.ch</code>	Lizenznachweis, Anfrage nach freien Plätzen, Meldung nach dem Lauf	vor und nach einem Lauf
Zeitstempeldienst, Vorgabe <code>tsa.swisssign.net</code>	der Hash eines Belegs, nichts sonst	einmal je Lauf

Was an bimover geht, sind Hashes und Zahlen: je archiviertem Postfach ein SHA-256 statt der Adresse, die Zahl der Läufe, die Zahl der Nachrichten, eine Archivkennung ohne Projektnamen. Betreff, Adressen,

Dateinamen und Inhalte sind dort nicht vorgesehen, und eine feste Liste verbotener Feldnamen in den Tests hält es fest (`filum_kern::meldung`).

Die Meldung hat einen zweiten Zweck, der die IT interessieren kann: Alles, was beweist, dass ein Archiv unverändert ist, liegt sonst im selben Ordner, auf den auch schreibt, wer es ändern wollte. Der Server merkt sich je Archiv den Höchststand an Läufen und Nachrichten. Meldet dasselbe Archiv später weniger, sagt Filum das.

Ein Diagnosebericht entsteht nur auf Knopfdruck, geht durch eine eigene Prüfstelle (`filum_kern::austritt`) und nennt weder Betreff noch Adressen; vom Ablagepfad steht darin seit dem 19.09.2026 nur noch der letzte Ordner. Die hausweite Grundlage dazu steht in `PRIVACY.md` im Oberordner.

Anfragen an Microsoft gehen ausschliesslich an `graph.microsoft.com` . Auch die Folgeadresse einer Antwort, über die Filum seitenweise blättert, wird vorher daraufhin geprüft; führt sie woanders hin, folgt Filum ihr nicht und sagt es im Laufbericht (`filum_kern::zugang::zeigt_auf_graph`).

4. Wo das Archiv liegt

Ein eigenes Share auf dem NAS, zum Beispiel `Mailarchiv` . Die Projekte sind darin Unterordner. Berechtigungen je Projekt gibt es nicht, und das ist eine Entscheidung, keine Auslassung: Ein Büro mit sechs Leuten pflegt keine Rechtematrix über vierzig Projekte, und was niemand pflegt, stimmt nach dem zweiten Personalwechsel nicht mehr.

Die vier Regeln der Einrichtung:

1. Ein eigenes Share fürs Archiv, nicht in der Projektablage. Das Archiv wächst nur, darum kosten seine Snapshots wenig Platz und dürfen lange bleiben.
2. Alle schreiben mit dem eigenen Konto, die Belegschaftsgruppe bekommt Lesen und Schreiben. Kein geteiltes Archivkonto: Windows erlaubt keine zwei gleichzeitigen Verbindungen zum selben Server mit verschiedenen Konten.
3. Snapshots laufen automatisch und gehören der NAS-Verwaltung. Für die Belegschaft sind sie unsichtbar, und niemand aus der Belegschaft ist Administrator des NAS.
4. Gelöscht wird nur über die App, weil die Löschfunktion einen Vermerk hinterlässt statt einer Lücke.

Das trägt, weil die Prüfung jede fehlende oder veränderte Datei nennt und der Snapshot sie zurückbringt. Genau so sieht das Recht den Umgang mit veränderbaren Trägern vor. Ein früheres Modell mit Briefkasten-Rechten (anlegen ja, löschen nein) ist am 14.09.2026 aufgegeben worden: aufwendig einzurichten, auf manchen Geräten nur über SMB durchzusetzen, und wer eine Datei selbst angelegt hatte, konnte sie trotzdem löschen.

Während eines Laufs liegt eine Sperrdatei im Archiv, damit nicht zwei Läufe gleichzeitig schreiben. Bricht ein Lauf hart ab, gilt die Sperre nach zwei Stunden als verwaist und der nächste Lauf übernimmt.

Schrittweise Anleitung für Synology und QNAP: `docs/backup-vorgabebblatt.md` .

5. Was im Ordner liegt

2019-0234_neubau-sonnenhof/	
Mails ansehen.html	Übersicht mit Suche und Filtern, der Hauptzugang
Mails/	je Nachricht eine Archivdatei (PDF/A-2u), chronologisch
.filum/	ausgeblendet, alles Übrige:
originale/	die Originale als .eml, unverändert, flach
verlaeufer/	je Gespräch eine lesbare HTML
anhaenge/	ausgepackt, über den Inhalt dedupliziert
verzeichnis.csv	eine Zeile je Nachricht, für Excel oder Texteditor
belege/	Bestandsbelege, Zeitstempel (.tsr), Anker
pruefen.py	prüft das Archiv ohne Filum
verfahren.txt	Verfahrensdokumentation
laeufer/, pruefungen/	Protokolle

Die Trennung, an der alles hängt: Der Nachweis ist allein die `.eml`. Sie ist das Originalste, was von einer Nachricht zu bekommen ist, mit den Anhängen darin. Alles andere ist Lesefassung und aus der `.eml` jederzeit neu erzeugbar: die Archivdatei in `Mails/`, die ausgepackten Anhänge, die Lesesicht, das Verzeichnis. Eine Abweichung am Original ist ein harter Befund, eine neu erzeugte Archivdatei nicht.

Dateinamen sehen so aus:

```
2019-04-02 0914 Eingang – Anna Muster – Baugesuch Sonnenhof a5d21a19.eml
```

Datum und Uhrzeit voran, damit jeder Dateimanager chronologisch sortiert; Ortszeit, weil man nach der Uhrzeit sucht, die in Outlook stand; reines ASCII, weil macOS Dateinamen zerlegt und Windows sie zusammensetzt und das Verhalten über SMB bei gemischten Formen offen ist. Der echte Betreff mit Umlauten steht im HTML und im CSV. Am Ende der Name steht eine Kurzbezeichnung aus der Identität der Nachricht.

Als Option legt Filum neue Nachrichten ohne die Nutzlast ihrer Anhänge ab («Anhänge nur einmal ablegen»). Das Original entsteht dann beim Lesen wieder Byte für Byte aus dem Gerüst und den Teilen unter `.filum/anhaenge`, und Prüfung, Herausziehen und Prüfskript rechnen über das zusammengesetzte Original. Bei einem Büro, in dem dieselbe Planserie in zwölf Postfächern liegt, ist das der Unterschied zwischen zwölf Kopien und einer. Schon abgelegte Nachrichten stellt ein eigener Lauf in beide Richtungen um, ohne dass Kennungen oder Belege sich ändern.

6. Nachweis und Prüfung

Jede Nachricht hat zwei Kennungen. Die Identität ist ein Hash über die kanonisierte Form, nicht über die Bytes: Exchange hält MAPI und baut das MIME bei jedem Abruf neu zusammen, deshalb würde ein Byte-Hash bei jedem Quartalslauf neue Nachrichten erfinden. Daneben steht der Byte-Hash der abgelegten Datei, und der ist es, den die Prüfung nachrechnet.

Jeder Lauf schreibt einen Bestandsbeleg: einen Hash über den gesamten Bestand, beide Kennungen je Nachricht, sortiert, verkettet mit dem Beleg des vorigen Laufs. Auf diesen Beleg holt Filum einen Zeitsstempel nach RFC 3161 und legt ihn roh daneben. Fällt der Zeitstempeldienst aus, läuft der Lauf zu Ende und der nächste stempelt nach.

Geprüft wird auf zwei Wegen, die dasselbe rechnen:

- in der App, auf der Projektseite,
- ohne Filum mit `python3 -I .filum/pruefen.py`, das nur die Standardbibliothek braucht und auch die Signatur der Zeitstempel nachrechnet.

Ein Paritätstest hält beide Prüfer aneinander fest, damit sie nicht auseinanderlaufen. Die Prüfung kennt drei Ergebnisse statt zwei: vorhanden, entfernt mit Löschermerk, fehlend ohne Vermerk. Ohne diese Unterscheidung sähe eine rechtmässige Löschung aus wie eine Manipulation.

7. Löschen

Die Löschung entfernt Original und Lesefassung samt den Anhängen, die keine andere Nachricht braucht, schwärzt die Zeile in der Satzdatei und legt einen Vermerk mit beiden Kennungen daneben. Die Nachricht verschwindet, der Nachweis, dass dort eine lag, bleibt, und die Belegkette bleibt gültig. Hashes ohne Original sind keine Personendaten mehr.

Zwei Eigenschaften, die im Betrieb zählen: Eine Löschung, die mitten im Schreiben abbricht, lässt sich in «Auskunft und Löschung» wählen und mit dem Stempel von damals zu Ende führen. Und liegt auf dem Weg zu einer Datei, die die Löschung anfassen würde, ein symbolischer Verweis, entsteht gar kein Plan, und Filum sagt es. Eine Vorlage für das Löschkonzept des Büros liegt in `docs/loeschkonzept-vorlage.md`.

8. Lesemaske, wenn die Belegschaft im Browser lesen soll

Wer kein Laufwerk einbinden will, stellt auf dem NAS die Lesemaske auf: einen kleinen Dienst, der genau die Lesesicht ausliefert, die ohnehin im Archiv liegt. Sie kann nichts schreiben, es gibt keinen Endpunkt dafür, und sie hält nicht fest, wer wann welche Nachricht liest. Der Zugang ist ein gemeinsames Lesekennwort für das ganze Büro; wer feiner trennen will, trennt am Netz.

Die wichtigste Zusicherung dabei: Fällt der Dienst aus oder wird er nie eingerichtet, bleibt jedes Archiv im Ordner vollständig lesbar. Die Maske ist Komfort, nie Voraussetzung. Einrichtung: `docs/lesemaske-vorgabebblatt.md`.

9. Betrieb

Anforderungen. macOS 14 oder neuer. Die Windows-Fassung setzt Windows 10 Version 1809 voraus, ist aber zurückgestellt und heute nicht erhältlich. Dazu ein Microsoft-365-Konto mit Exchange-Online-Post-

fach, eine Internetverbindung und Schreibzugriff auf das Archiv-Share.

Ein Lauf. Die App listet die gewählten Ordner, holt die Kopfdaten seitenweise, dann die Rohbytes in Stapeln zu zwanzig, baut die Gespräche, schreibt Dateien, Belege und die Lesesicht. Mehrere Postfächer laufen nebeneinander, innerhalb eines Postfachs höchstens drei Anfragen gleichzeitig, weil Outlook dort die Grenze zieht. Drosselt Microsoft, wartet Filum die angegebene Zeit ab und macht weiter. Ein zweiter Lauf erkennt, was schon da ist, und holt nur Neues.

Nach einem Abbruch. Ein abgebrochener Lauf hinterlässt kein halbes Archiv. Geschrieben wird erst, wenn die Datei vollständig ist, und der Archivstand zuletzt. Ein neuer Lauf nimmt die Arbeit auf.

Jahresdurchgang. Einmal im Jahr zeigt die App über alle Projekte, welche Aufbewahrungsfristen abgelaufen sind, und hält den Durchgang als Text fest. Gelöscht wird dabei nie von selbst.

Netz und Konto. Ohne gültige Lizenz beginnt kein neuer Lauf, und ohne Verbindung ebenfalls nicht. Bestehende Archive bleiben davon unberührt: Öffnen, Lesen, Prüfen, Herausziehen, Auskunft und Löschen gehen immer, auch ohne Konto und ohne Netz. Antwortet bimover.ch vorübergehend nicht, trägt ein gespeicherter Lizenznachweis bis zu seiner Gnadenfrist, und die App sagt, wie viele Tage das noch sind.

10. Lizenzierung

Gezählt werden archivierte Postfächer, nicht Personen, die einen Lauf starten. Wer Zugriff auf ein geteiltes Postfach hat und es mitarchiviert, braucht dafür eine Lizenz.

Gerechnet wird gestaffelt wie bei der Steuer: der Satz einer Stufe gilt nur für die Postfächer in dieser Stufe. Damit kann der Gesamtbetrag nicht sinken, wenn ein Postfach dazukommt. Stand 20.09.2026, Quelle ist `Kern/crates/filum-kern/src/lizenz.rs` :

Postfächer	je Postfach und Jahr
1 bis 10	CHF 50
11 bis 20	CHF 40
21 bis 30	CHF 30
ab 31	CHF 25

Der kleinste Rechnungsbetrag ist CHF 250. Ein Büro mit zwanzig Postfächern zahlt CHF 900 im Jahr; drei Jahre im Voraus kosten zweieinhalb Jahresbeiträge. Die Lizenz trägt die Software. Betreuung kostet Stunden, und das erste Jahr bringt zwei davon mit. Gekauft wird auf bimover.ch, nicht in der App.

11. Grenzen, offen benannt

- Teams-Chats sind nicht erfasst.

- Cloud-Anhänge, also OneDrive-Links statt echter Dateianhänge, werden als Link archiviert. Graph liefert dafür keine Bytes.
- Entwürfe werden übersprungen. Sie haben weder Message-ID noch Transport-Header.
- Filum verhindert keine Änderung am Archiv. Es macht sie feststellbar. Der Schutz gegen versehentliches Löschen kommt vom NAS-Snapshot.
- Ein Umstelllauf über sehr viele Nachrichten kann länger dauern als die zwei Stunden, nach denen eine Sperre als verwaist gilt. Übernimmt dann ein anderer Lauf, hält eine Wache den Umstelllauf vor dem Schreiben an, und er muss neu gestartet werden.
- Wer den Verkehr zu Microsoft über einen eigenen Proxy mit eigener Zertifizierungsstelle leitet, kann die Zeitangabe fälschen, an der Filum die Gnadenfrist misst. Das ist Aufwand mit Absicht, keine verstellte Uhr.

12. Wo es genauer steht

Frage	Datei
Archivformat, Identität, Fäden, Lesesicht	README.md
Was Filum rechtlich hält	docs/aufbewahrung.md
Archiv-Share, Snapshots, Wiederherstellen	docs/backup-vorgabebblatt.md
Lesemaske auf dem NAS	docs/lesemaske-vorgabebblatt.md
Löschkonzept des Büros	docs/loeschkonzept-vorlage.md
Manipulationsschutz im Detail	docs/audit-veraenderbarkeit.md
Was bei bimover-Apps als Datenerhebung gilt	../PRIVACY.md