

S/MIME an Hochschulen: Nutzerzertifikate aus GÉANT TCS in Outlook und Exchange Online

Microsoft 365 · Hochschule · S/MIME

S/MIME an Hochschulen: Nutzerzertifikate aus GÉANT TCS in Outlook und Exchange Online

Ein Zertifikat ist schnell beantragt. Der private Schlüssel überlebt seinen Besitzer meist nicht.

GÉANT TCS HARICA DFN-AAI Outlook im Web Intune Schlüsselsicherung Funktionspostfächer

Erneuerung

boddenberg.de

WISSEN

Alle Beiträge der Serie zu Microsoft 365 in Hochschule und Forschung an einem Ort.

› [Microsoft 365 in Hochschule und Forschung](#)

BERATUNG

S/MIME-Konzept mit Schlüsselsicherung, Verteilung und Austrittsprozess, abgestimmt mit Datenschutz und Personalrat.

› [Beratung für Hochschulen und Forschung](#)

SCHULUNG

Für Exchange- und Client-Teams: S/MIME in Exchange Online, Outlook und Intune sicher betreiben.

› [Schulungen für Hochschulen und Forschung](#)

Fragen Sie in einem Hochschulrechenzentrum, ob man S/MIME-Zertifikate bekommen kann, lautet die Antwort seit Jahrzehnten: selbstverständlich. Fragen Sie dann, wie viele Mitarbeiterinnen und Mitarbeiter ihre Mails tatsächlich signieren, wird es still. Und fragen Sie schließlich, wer die verschlüsselten Mails eines Professors lesen kann, der vor drei Jahren emeritiert wurde, bekommen Sie den Blick, den man sonst nur von Leuten kennt, die gerade gemerkt haben, dass das Backup seit Monaten leer ist.

Das S/MIME-Hochschulzertifikat ist ein merkwürdiges Wesen. Der Zugang ist über den DFN-Verein geregelt, die Zertifikate sind in jedem gängigen Mailprogramm verankert, der Antrag dauert wenige Minuten. Trotzdem nutzen es an den meisten Hochschulen nur das Rechenzentrum selbst, ein paar Kryptografie-Lehrstühle und jene Einzelkämpfer, die ihre Signatur für eine Frage der Ehre halten. Flächig eingeführt wird es selten, und wenn doch, dann meist ohne das, was den Betrieb erst tragfähig macht: eine zentrale Sicherung der privaten Schlüssel, einen sauberen Verteilweg auf alle Geräte und einen Prozess für den Tag, an dem jemand die Hochschule verlässt.

Dieser Beitrag gehört zur Serie [Microsoft 365 in Hochschule und Forschung](#). Er richtet sich an Leitungen von Hochschulrechenzentren, CIOs, Kanzlerinnen und Kanzler, Datenschutzbeauftragte und Personalräte an Universitäten, Hochschulen für angewandte Wissenschaften, Kunst- und Musikhochschulen sowie an IT-Leitungen außeruniversitärer Forschungseinrichtungen. Es geht um die aktuelle Lage des Zertifikatsdienstes über DFN und GÉANT, um Antrag und Ausstellung, um die Verteilung auf Outlook, Outlook im Web und Mobilgeräte, um das Verzeichnis, um Schlüsselsicherung, Funktionspostfächer, Ablauf und Erneuerung. Universitätsklinika haben mit Gesundheitsdaten und KRITIS-Pflichten eigene Anforderungen und bleiben hier außen vor.

FAKTEN · Das Wichtigste in fünf Sätzen

Die DFN-PKI im Sicherheitsniveau Global stellt seit August 2023 keine neuen Zertifikate mehr aus; Nachfolger für browser- und mailclientverankerte Zertifikate ist GÉANT TCS, das der DFN-Verein über GÉANT bezieht.

Im TCS hat Sectigo seinen Dienst zum 10. Januar 2025 beendet; seit 2025 ist HARICA, ein Vertrauensdiensteanbieter aus dem griechischen Hochschulnetz, der Anbieter.

Nutzer beantragen ihr S/MIME-Zertifikat im HARICA Certificate Manager, idealerweise per Academic Login über DFN-AAI und eduGAIN; mit passendem Entitlement wird ohne zusätzliche Freigabe ausgestellt.

Exchange Online braucht für S/MIME eine virtuelle Zertifikatssammlung und die öffentlichen Zertifikate im Verzeichnis; Outlook im Web benötigt zusätzlich eine Browser-Erweiterung per Richtlinie.

Ohne zentrale Sicherung der privaten Schlüssel sind verschlüsselte Mails nach Geräteverlust, Erneuerung oder Austritt dauerhaft unlesbar.

Vom DFN-PKI-Zertifikat zu GÉANT TCS: Die Lage im Herbst 2026

Wer die Geschichte der Nutzerzertifikate an deutschen Hochschulen erzählt, muss mit der DFN-PKI anfangen. Jahrzehntlang war sie die Instanz, bei der Rechenzentren über eigene Registrierungsstellen Zertifikate für ihr Personal ausstellten, inklusive persönlicher Identitätsprüfung am Schalter und Ausweis auf dem Tresen. Das Sicherheitsniveau Global war in Browsern und Mailprogrammen verankert und damit für S/MIME im Austausch mit der Außenwelt brauchbar.

Was aus der DFN-PKI Global geworden ist

Bis August 2023 konnten im Sicherheitsniveau Global Zertifikate mit Browser- und Betriebssystemverankerung ausgestellt werden. Seitdem ist es im Erhaltungsbetrieb: Neue Zertifikate gibt es nicht mehr, auch keine Erneuerungen. Ausgestellte Zertifikate bleiben bis zum regulären Ablauf gültig und können gesperrt werden, Sperrlisten und OCSP laufen weiter. Je nach Anwendungsfall nennt der DFN als Nachfolger GÉANT TCS oder die DFN-Verein Community-PKI. Für S/MIME mit externen Partnern ist TCS der relevante Weg, weil nur dessen Wurzelzertifikate in den gängigen Mailprogrammen von Haus aus vertraut werden.

Der Anbieterwechsel im Trusted Certificate Service

TCS ist ein PKI-Angebot, das der DFN-Verein über GÉANT bezieht, die Dachorganisation der europäischen Forschungsnetze. Den eigentlichen Betrieb leistet ein kommerzieller oder halbkommerzieller Vertrauensdiensteanbieter. Von 2020 bis 2024 war das Sectigo. Der Anbieter kündigte seinen Vertrag mit GÉANT, der Dienst endete am 10. Januar 2025. Der DFN-Verein beauftragte Anfang Dezember 2024 HARICA, einen Vertrauensdiensteanbieter aus dem Umfeld des griechischen Hochschulnetzes GUnet; GÉANT hat anschließend selbst einen Vertrag mit HARICA geschlossen. Seit dem 6. März 2025 stammen alle S/MIME-Zertifikate aus eigens dafür betriebenen GÉANT-TCS-S/MIME-Zwischenzertifizierungsstellen unterhalb der HARICA-Client-Wurzeln für RSA und ECC.

Für den Betrieb heißt das: Sectigo-Zertifikate laufen bis zu ihrem Ablaufdatum weiter, neue Zertifikate kommen ausschließlich über HARICA. Wer seine Anleitungen, Wiki-Seiten und Vorlagen seit 2024 nicht angefasst hat, schickt Nutzer gerade zu einem Portal, das ihnen nichts mehr ausstellt. Das ist kein Sicherheitsproblem, aber eine verlässliche Quelle für Helpdesk-Tickets mit dem Betreff »Zertifikat geht nicht«.

WICHTIG · Schnelllebig: vor jeder Entscheidung gegenprüfen

Anbieter, Zwischenzertifikate, verfügbare Profile und Laufzeiten im TCS haben sich in den letzten Jahren mehrfach geändert, getrieben von den S/MIME Baseline Requirements des CA/Browser Forums und vom Anbieterwechsel. Maßgeblich ist die Dokumentation des DFN zu TCS und die Information der DFN-PCA an die teilnehmenden Einrichtungen. Dieser Beitrag beschreibt den Stand vom Herbst 2026.

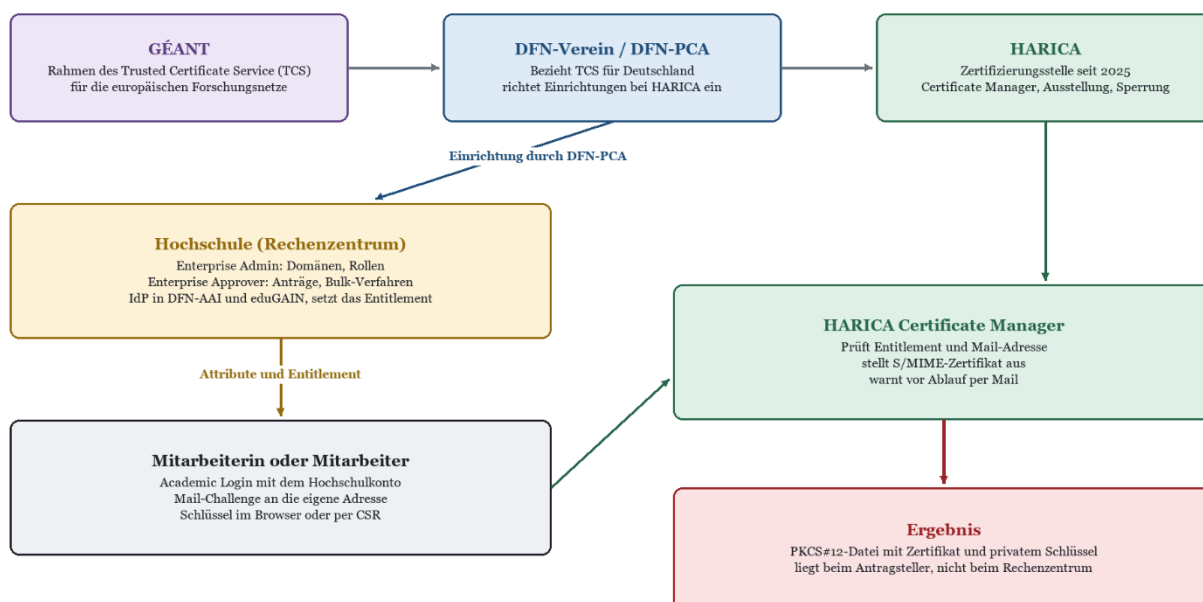
Wie eine Hochschule teilnimmt

Einrichtungen werden nicht per Selbstbedienung angelegt, sondern von der DFN-PCA direkt im HARICA-System eingerichtet. Danach gibt es drei Rollen: normale Nutzer, die persönliche Zertifikate beantragen, Enterprise Approver, die Anträge genehmigen, und Enterprise Admins, die Domänen verwalten und Rollen vergeben. Wer zum Approver oder Admin befördert wird, muss vorher in seinem Profil die Zwei-Faktor-Anmeldung per TOTP einschalten. Eine Organisationsvalidierung braucht es nur für Zertifikate mit Organisationsangaben; reine Mail-Zertifikate kommen auch ohne sie aus.

Der eigentliche Hebel ist die Anbindung an die DFN-AAI. Ist der Identity Provider der Hochschule in eduGAIN eingebunden und gibt er die nötigen Attribute frei, melden sich Nutzer im HARICA Certificate Manager per Academic Login mit ihrem Hochschulkonto an. Setzt der IdP zusätzlich ein Entitlement für S/MIME-Selbstbedienung, übernimmt HARICA Vor- und Nachnamen aus der AAI und stellt nach erfolgreicher Mail-Challenge ohne separate Genehmigung aus. Wer seinen IdP ohnehin gerade mit Entra ID verheiratet, findet die Grundlagen im Beitrag [Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden](#).

Wer bei einem Nutzerzertifikat mit wem redet

DFN-Verein, GÉANT, HARICA, Hochschule: vier Beteiligte, ein Zertifikat



Skizze 1: Self-Service ist bequem. Die .p12-Datei landet dabei genau dort, wo niemand sie sichert

Welche Zertifikatstypen es gibt

Typ	Inhalt	Antragsweg	Geeignet für
Email-only	nur die Mail-Adresse, kein	Mail-Challenge, keine weitere	Funktions- und Rollenadressen, schneller

	Personenname	Genehmigung	Einstieg
IV+OV (Personal)	validierter Vor- und Nachname plus Organisationsangaben	Academic Login mit Entitlement oder Freigabe durch Enterprise Approver	Personal, das nach außen signiert und verschlüsselt
Bulk über Approver	wie oben, bis zu drei Mail-Adressen je Zertifikat	CSV-Upload durch Approver, Schlüssel im System oder per CSR	zentrale Ausstellung mit Schlüsselsicherung
Client-Auth	nur Client-Authentifizierung	nach Profil	Anmeldung an vorbereiteten Systemen, nicht für Mail

WARNUNG · Keine Gruppennamen, keine Pseudonyme

HARICA erlaubt keine Zertifikate für Gruppennamen oder Pseudonyme im Namensfeld; solche Zertifikate werden nachträglich gesperrt. Mail-Adressen von Rollen und Funktionen sind ausdrücklich zulässig. Ein Zertifikat für »Team Prüfungsamt« als Personenname ist also tabu, eines für die Adresse des Prüfungsamts als Email-only-Zertifikat nicht. Das betrifft auch Testkonten im IdP: Wer »Test Testmann« durch die AAI schickt, testet vor allem den Sperrprozess.

Antrag, Ausstellung und Verteilung auf alle Clients

S/MIME ist im Kern simpel: Jeder hat ein Schlüsselpaar. Der öffentliche Teil steckt im Zertifikat und muss dorthin, wo andere ihn finden. Der private Teil muss auf jedes Gerät, auf dem der Besitzer signiert oder verschlüsselte Mails liest, und sonst nirgendwohin. Fast alle Probleme im Betrieb entstehen, weil eine dieser beiden Bewegungen nicht organisiert ist.

Selbstbedienung oder zentrale Ausstellung

Im Self-Service-Weg erzeugt der Browser des Antragstellers das Schlüsselpaar, HARICA signiert, und am Ende steht eine passwortgeschützte PKCS#12-Datei auf dem Rechner des Nutzers. Das ist datensparsam und schnell. Es hat aber eine Konsequenz, die in keiner Anleitung fett gedruckt steht: Weder das Rechenzentrum noch HARICA hat danach eine Kopie des privaten Schlüssels. Die Datei liegt im Download-Ordner, das Passwort im Kopf des Nutzers oder auf einem Klebezettel.

Der Gegenentwurf ist die zentrale Ausstellung. Approver können im Bulk-Verfahren per CSV bis zu fünfzig Zeilen auf einmal beantragen und dabei Schlüssel im System erzeugen lassen oder eigene Zertifikatsanforderungen hochladen. Erzeugt das Rechenzentrum die Schlüssel selbst, kann es sie vor der Auslieferung in einen Tresor legen. Dafür trägt es die Verantwortung für einen Bestand an privaten Schlüsseln, also für genau das Gut, um das sich die ganze Konstruktion dreht.

Kriterium	Self-Service mit Browser-Schlüssel	Zentrale Ausstellung mit Sicherung
Aufwand im Rechenzentrum	gering, einmalige AAI-Konfiguration	laufend: Erzeugung, Tresor, Auslieferung, Wiederherstellung
Kopie des privaten Schlüssels	nur beim Nutzer	beim Nutzer und im Tresor
Verschlüsselte Mails nach Austritt	in der Regel unlesbar	nach geregelter Verfahren lesbar
Verteilung auf Mobilgeräte	manuell, .p12 per Mail an sich selbst	automatisiert über Intune möglich
Mitbestimmung und Datenschutz	wenig Regelungsbedarf	Zugriffsregeln, Protokollierung, Dienstvereinbarung

Eignung	Signatur, Einzelpersonen, Pilotgruppen	flächiger Einsatz mit Verschlüsselung
----------------	--	---------------------------------------

TIPP · Signieren und Verschlüsseln getrennt denken

Für die reine Signatur braucht niemand eine Schlüsselsicherung: Geht der Schlüssel verloren, beantragt man einen neuen, alte Signaturen bleiben prüfbar. Erst die Verschlüsselung macht den privaten Schlüssel zum Archivgut. Viele Hochschulen fahren gut damit, flächig mit Signatur anzufangen und Verschlüsselung nur dort freizugeben, wo Schlüsselsicherung und Verfahren stehen.

Exchange Online vorbereiten

Exchange Online prüft S/MIME-Zertifikate gegen eine virtuelle Zertifikatssammlung. Dafür exportieren Sie die Wurzel- und Zwischenzertifikate, die zur Prüfung der Nutzerzertifikate nötig sind, als SST-Datei und laden sie mit Set-SmimeConfig und dem Parameter SMIMECertificateIssuingCA in den Tenant. Gehören noch Sectigo- oder DFN-PKI-Zertifikate zum Bestand, gehören deren Ketten für die Restlaufzeit mit in die Sammlung. Die Sperrlisten der Zertifizierungsstellen müssen aus dem Internet erreichbar sein; Exchange Online verwirft Zertifikate, deren Sperrstatus es nicht prüfen kann.

Outlook klassisch, neues Outlook, Outlook im Web

Das klassische Outlook für Windows nutzt den Zertifikatsspeicher des Betriebssystems. Das neue Outlook unterstützt S/MIME inzwischen ebenfalls; Digitale IDs werden in den Einstellungen unter Mail und S/MIME importiert, die Einstellungen werden mit Outlook im Web synchronisiert. Outlook im Web unterstützt S/MIME auf Windows-Clients in Edge und Chrome. Dafür müssen Sie per Richtlinie ExtensionInstallForcelist die S/MIME-Erweiterung erzwingen, was nach Microsofts Dokumentation domänen- oder Entra-gebundene Geräte voraussetzt; zusätzlich installieren Nutzer beim ersten Einsatz das S/MIME-Steuerelement. Auf dem privaten Mac einer Lehrbeauftragten oder am Rechner im Lesesaal funktioniert das also nicht.

Eine Eigenheit sollten Sie kennen, bevor jemand ein Ticket schreibt: Sind auf einer Mail Vertraulichkeitsbezeichnungen mit Schutzaktionen gesetzt, schaltet Outlook im Web S/MIME für diese Mail ab, weil die Labels serverseitig, S/MIME aber im Client wirken. Wer parallel Sensitivity Labels für Drittmittelprojekte einführt, sollte die beiden Verfahren nicht auf dieselbe Mail ansetzen.

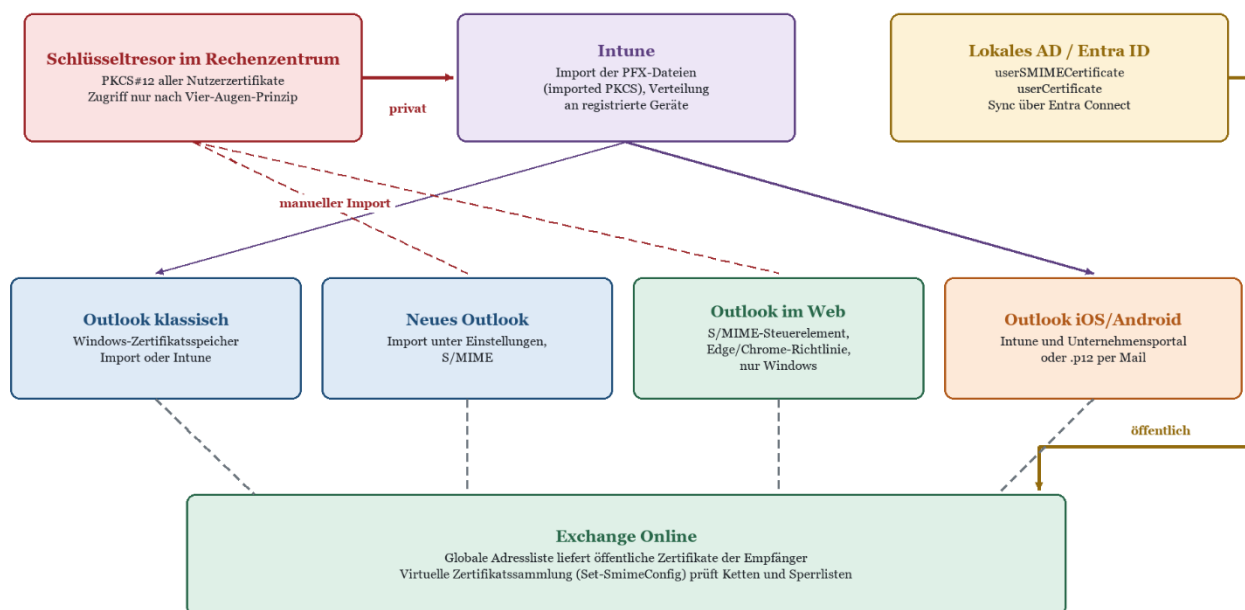
Mobilgeräte

Outlook für iOS und Android kennt zwei Wege. Manuell schickt sich der Nutzer die exportierte, passwortgeschützte .p12-Datei per Mail und installiert sie in der App. Automatisiert geht es nur mit Intune als Verwaltungsdienst: Verschlüsselungszertifikate werden als importierte PKCS-Zertifikate in Intune hochgeladen, über den PFX-Connector bereitgestellt und an jedes registrierte Gerät des Nutzers ausgeliefert; auf iOS holt das Unternehmensportal sie in den Microsoft-Schlüsselbund. Für Signaturen kann SCEP ein gerätespezifisches Zertifikat erzeugen, das braucht allerdings eine eigene Zertifizierungsstelle im Hintergrund. Die App gleicht die primäre SMTP-Adresse mit dem Zertifikat ab; passen sie nicht zusammen, meldet sie schlicht, es sei kein Zertifikat vorhanden. Ab dreißig Tagen vor Ablauf warnt Outlook mobil beim Signieren und Verschlüsseln.

Der automatisierte Weg setzt voraus, dass das Rechenzentrum die PKCS#12-Dateien besitzt. Self-Service und Intune-Verteilung schließen sich damit praktisch aus. Das ist der Moment, in dem viele Hochschulen merken, dass die Frage der Schlüsselsicherung keine Kür ist, sondern die Voraussetzung für alles Weitere.

Ein Zertifikat, vier Clients, drei Verteilwege

Privater Schlüssel auf jedes Gerät, öffentlicher Schlüssel ins Verzeichnis



Skizze 3: Der öffentliche Schlüssel will ins Verzeichnis, der private auf jedes Gerät und in genau einen Tresor

Client	Privater Schlüssel	Empfängerzertifikate	Einschränkungen
Outlook klassisch (Windows)	Windows-Zertifikatsspeicher, Import oder Verteilung	GAL, Kontakte, empfangene Signaturen	Profilpflege bei Erneuerung
Neues Outlook	Import unter Einstellungen, Mail, S/MIME	GAL	Funktionsumfang wächst noch, vor Rollout testen
Outlook im Web	S/MIME-Steuerelement, Zertifikat lokal	GAL	nur Windows, Edge/Chrome, Richtlinie und verwaltetes Gerät nötig
Outlook iOS/Android	manuell per .p12 oder Intune (imported PKCS)	GAL, lokaler Speicher, optional LDAP	nur klar signierte Mails, S/MIME in der App standardmäßig aus
Fremde Clients (Thunderbird, Apple Mail)	eigener Speicher je Programm	eigenes Adressbuch, LDAP	kein Zugriff auf die GAL, Koexistenz einplanen

Veröffentlichung im Verzeichnis

Damit jemand an Sie verschlüsselt, braucht er Ihren öffentlichen Schlüssel. Innerhalb des Tenants liefert ihn die globale Adressliste. In hybriden Umgebungen ist das lokale Active Directory die Quelle: Das Zertifikat wird in die Attribute userSMIMECertificate oder userCertificate geschrieben, Entra Connect synchronisiert beide nach Microsoft 365. Wer Konten aus dem Identity Management provisioniert, sollte das Veröffentlichen dort einbauen und nicht dem Zufall überlassen, ob ein Nutzer in Outlook irgendwann auf »In GAL veröffentlichen« klickt. Bei synchronisierten Konten überschreibt die nächste Synchronisation, was nicht aus dem lokalen Verzeichnis kommt.

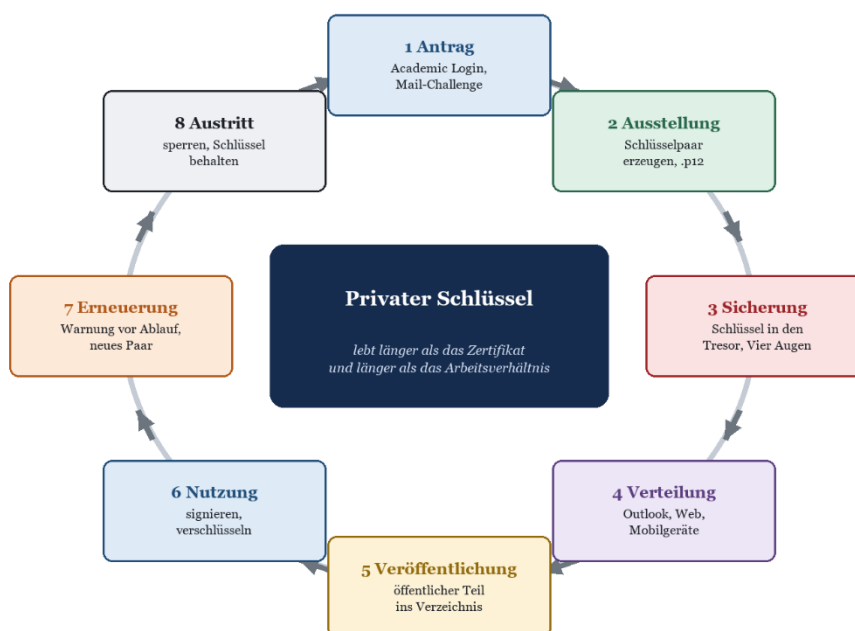
Nach außen hilft die GAL nicht. Externe Partner bekommen Ihren öffentlichen Schlüssel am einfachsten mit der ersten signierten Mail. Das ist ein gutes Argument, standardmäßig zu signieren: Jede signierte Mail verteilt nebenbei den Schlüssel, den der Empfänger für die Antwort braucht. Ein öffentliches LDAP-Verzeichnis für Zertifikate ist möglich, aber eine eigene Entscheidung mit Datenschutzfolgen, weil es Namen und Adressen nach außen preisgibt. Wie Mailfluss, Hybrid und Alt-Mailserver am Campus zusammenspielen, beschreibt der Beitrag [Exchange an der Hochschule: Hybrid, Alt-Mailserver und die Studenten-Mail](#).

Schlüsselsicherung, Austritt und Erneuerung

Ein Zertifikat hat ein Ablaufdatum. Der private Schlüssel nicht, jedenfalls nicht in dem Sinn, der für ein Archiv zählt. Jede mit einem Schlüssel verschlüsselte Mail bleibt genau so lange lesbar, wie dieser Schlüssel irgendwo existiert und jemand befugt ist, ihn zu benutzen. Das ist der Punkt, an dem S/MIME aufhört, ein Client-Thema zu sein, und zu einer Frage der Aktenführung wird.

Lebenszyklus eines Nutzerzertifikats

Vom Antrag bis zur Archivierung des Schlüssels, der das Zertifikat überlebt



Skizze 2: Der Kreis schließt sich bei der Erneuerung. Der alte Schlüssel fällt dabei nicht heraus, er wandert ins Archiv

WARNUNG · Verschlüsselte Mails ohne Schlüsselsicherung sind ein Archivproblem mit Ansage

S/MIME verschlüsselt Ende zu Ende. Exchange Online speichert die Mail so, wie sie ankommt: verschlüsselt. Die Inhaltssuche findet keinen Text darin, Aufbewahrungsrichtlinien bewahren den verschlüsselten Datensalat sorgfältig auf, und eDiscovery liefert Ihnen im Ernstfall formvollendet ein Paket unlesbarer Anhänge. Ist der private Schlüssel mit dem alten Laptop entsorgt worden, hilft weder Microsoft noch HARICA noch das Rechenzentrum. Das ist kein Fehler im System, das ist das System.

Wer Verschlüsselung erlaubt, muss vorher klären, wo die Schlüssel liegen, wer sie wiederherstellen

darf und wie lange sie aufbewahrt werden. Wer das nicht klärt, betreibt kein Archiv, sondern einen sehr gut gesicherten Papierkorb.

Wie eine Schlüsselsicherung aussieht

Bewährt hat sich ein schlichter Aufbau: Das Rechenzentrum erzeugt Schlüsselpaare zentral oder sammelt die PKCS#12-Dateien beim Erstantrag ein, legt sie verschlüsselt in einem dafür vorgesehenen Tresor ab und dokumentiert jedes Ein- und Auslesen. Der Zugriff auf den Tresor folgt dem Vier-Augen-Prinzip, die Wiederherstellung einer fremden Schlüsseldatei braucht einen dokumentierten Anlass, zum Beispiel einen Antrag der Dienststelle nach Austritt oder eine Anfrage im Rahmen eines Verfahrens. Alle Schlüssel eines Nutzers bleiben im Tresor, auch die abgelaufenen: Eine Mail von 2024 wurde mit dem Schlüssel von 2024 verschlüsselt, nicht mit dem aktuellen.

Für Signaturschlüssel gilt das Gegenteil. Eine Kopie im Tresor schwächt die Aussage, dass nur der Besitzer signiert haben kann. Wer sauber trennen will, gibt für Signatur und Verschlüsselung getrennte Schlüssel aus; wer ein Kombizertifikat nutzt, sollte dokumentieren, dass die Sicherung ausschließlich der Entschlüsselung dient und nicht zum Signieren verwendet wird.

HINWEIS · Kein Rechtsrat: Landesrecht und Mitbestimmung

Ob und unter welchen Bedingungen eine Hochschule auf dienstliche Mails ausgeschiedener Mitarbeiterinnen und Mitarbeiter zugreifen darf, regeln Landesdatenschutzgesetze, Hochschulgesetze, Personalvertretungsgesetze, Archivgesetze und örtliche Dienstvereinbarungen, und zwar je Bundesland unterschiedlich. Hinzu kommt die Frage, ob die private Nutzung des dienstlichen Postfachs erlaubt ist. Ein zentraler Schlüsseltresor ist eine technische Einrichtung, die sich zur Kontrolle eignen kann; der Personalrat wird das zu Recht wissen wollen. Klären Sie Zugriffsregeln, Anlässe und Protokollierung mit Datenschutz, Personalrat und Justizariat, bevor der erste Schlüssel im Tresor liegt.

› [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#)

› [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#)

Was passiert, wenn der Mitarbeiter geht

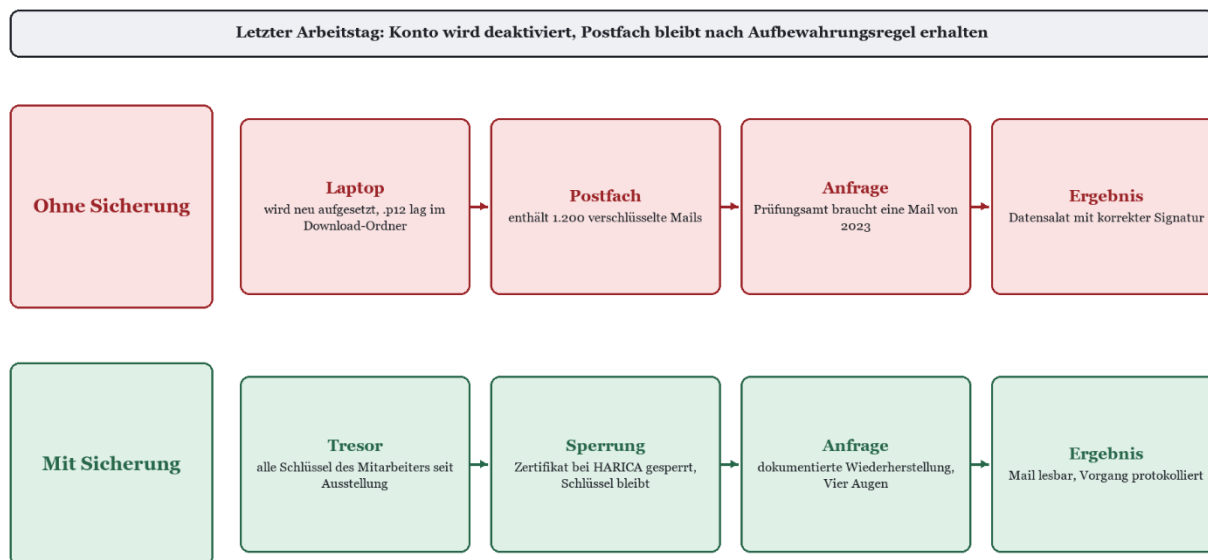
Austritte sind an Hochschulen keine Ausnahme, sondern Geschäftsmodell. Befristete Stellen in Drittmittelprojekten, Gastwissenschaftler, die nach einem Semester weiterziehen, Emeriti, die ihr Postfach behalten wollen, studentische Hilfskräfte mit Rollenadresse: Der Identitätsprozess muss für jede dieser Gruppen wissen, was mit Zertifikat und Schlüssel passiert. Die Grundlagen dafür stehen in den Beiträgen [Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto](#) und [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#).

- **Zertifikat sperren:** Mit dem Austritt verliert die Adresse ihre Bindung an die Person. Das Zertifikat wird bei HARICA gesperrt, damit niemand mehr mit einer Hochschulidentität signiert, die es nicht mehr gibt.
- **Schlüssel behalten:** Gesperrt heißt nicht gelöscht. Der private Schlüssel bleibt im Tresor, solange das Postfach oder seine Inhalte aufbewahrt werden.

- **Postfach und Schlüssel koppeln:** Die Aufbewahrungsfrist für Schlüssel richtet sich nach der längsten Frist für Inhalte, die damit verschlüsselt wurden, nicht nach dem Ablaufdatum des Zertifikats.
- **Geräte einsammeln:** Auf Intune-verwalteten Geräten verschwinden die Zertifikate mit dem Entfernen der Registrierung. Private Geräte mit manuell importierter .p12-Datei bleiben eine Restgröße, die Sie nur organisatorisch abdecken.
- **Emeriti und Weiterbeschäftigte:** Wer seine Adresse behält, braucht weiter ein gültiges Zertifikat. Das setzt voraus, dass die AAI ihn noch mit passendem Entitlement führt.

Wenn der Mitarbeiter geht: zwei Wege, ein Archiv

Mit und ohne Schlüsselsicherung, fünf Jahre nach dem letzten Arbeitstag



Skizze 4: Die Signatur ist gültig, der Inhalt ist weg. Kryptografie funktioniert, Organisation nicht

TYPISCHE SITUATION · Typische Situation aus der Projekterfahrung

In einem kommunalen Zweckverband hatte die Personalabteilung jahrelang Unterlagen an das Rechnungsprüfungsamt verschlüsselt verschickt, vorbildlich und auf eigene Initiative. Als der zuständige Sachbearbeiter in Rente ging und sein Rechner turnusgemäß ersetzt wurde, fragte niemand nach dem Zertifikat. Zwei Jahre später brauchte die Prüfung einen Vorgang aus seinem Postfach. Das Postfach war da, die Mails waren da, der Inhalt nicht. Am Ende wurden die Unterlagen in Papierform aus dem Keller rekonstruiert, was immerhin bewies, dass das Papierarchiv die robustere Kryptografie hatte.

Übertragen auf die Hochschule: Ersetzen Sie das Rechnungsprüfungsamt durch das Prüfungsamt, den Sachbearbeiter durch die Vorsitzende eines Prüfungsausschusses und den Keller durch nichts, weil es kein Papier mehr gibt.

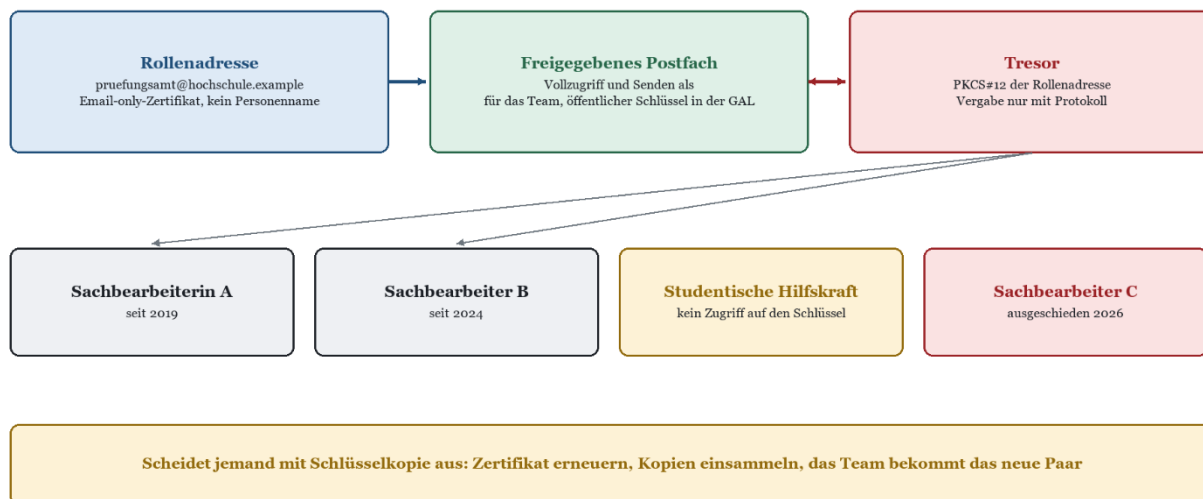
Funktions- und Gruppenpostfächer

Prüfungsamt, Dekanat, Studienberatung, Berufungskommission, Geschäftsstelle eines Verbundprojekts: Viele schutzwürdige Mails gehen nicht an Personen, sondern an Rollen. Für deren Adressen eignet sich das Email-only-Zertifikat, das nur die Mail-Adresse enthält und ausdrücklich für Funktionspostfächer gedacht ist. Das freigegebene Postfach in Exchange Online bekommt den öffentlichen Schlüssel in der GAL, der private Schlüssel geht an alle, die mit Vollzugriff im Postfach arbeiten.

Genau hier wird es organisatorisch: Jede Person, die den Schlüssel hat, kann alle jemals an diese Adresse verschlüsselten Mails lesen, auch nach ihrem Wechsel in eine andere Abteilung, sofern sie die Datei behalten hat. Scheidet jemand aus dem Team aus, gehört zum Austritt deshalb die Erneuerung des Rollenzertifikats; der alte Schlüssel wandert in den Tresor, das Team bekommt den neuen. Studentische Hilfskräfte, die im Funktionspostfach Routinepost sortieren, brauchen in der Regel keinen Entschlüsselungsschlüssel.

Funktionspostfach mit eigenem Zertifikat

Ein Email-only-Zertifikat für die Rollenadresse, verteilt an das wechselnde Team



Skizze 5: Rollenadressen sind erlaubt, Gruppennamen im Namensfeld nicht

Ablauf und Erneuerung

Für S/MIME-Zertifikate aus den Self-Service-Wegen verschickt HARICA Ablaufwarnungen dreißig, fünfzehn, fünf Tage und einen Tag vor Ablauf an die Adressen im Zertifikat. Das ist hilfreich für Einzelpersonen und nutzlos für Funktionspostfächer, in denen solche Warnungen zwischen Prüfungsanmeldungen untergehen. Die zulässigen Laufzeiten sind durch die S/MIME Baseline Requirements begrenzt und deutlich kürzer als die Zertifikate aus der alten DFN-PKI, an die sich manche Lehrstühle noch erinnern. Erneuerung ist damit kein seltenes Ereignis, sondern Routine.

Bei der Erneuerung entsteht ein neues Schlüsselpaar. Das neue Zertifikat muss ins Verzeichnis, auf alle Geräte und in den Tresor, das alte bleibt zum Entschlüsseln auf den Geräten und im Tresor. Wer das alte Zertifikat vom Rechner löscht, weil es »abgelaufen« ist, kann die Mails der letzten Jahre nicht mehr öffnen. Das passiert erstaunlich oft, meistens durch besonders ordentliche Menschen.

Aufgaben im Lebenszyklus: manuell oder automatisiert

Aufgabe	Manuell	Automatisiert	Risiko
Antrag	Nutzer meldet sich im Certificate Manager an	Entitlement aus dem IdM, Bulk-Antrag durch Approver	Wildwuchs an Einzelanträgen ohne Überblick
Schlüsselerzeugung	im Browser des Nutzers	zentral im System oder per CSR aus dem Rechenzentrum	Schlüssel existiert nur auf einem Gerät
Schlüsselsicherung	Nutzer sichert .p12 selbst	Ablage im Tresor mit Protokoll und Vier-Augen-Zugriff	verschlüsselte Mails dauerhaft unlesbar
Verteilung Desktop	Import durch Nutzer	Intune-Profil (imported)	Zertifikat fehlt auf

		PKCS) oder Softwareverteilung	Zweitgerät
Verteilung mobil	.p12 per Mail an sich selbst	Intune und Unternehmensportal	Schlüsseldatei liegt dauerhaft im Postfach
Veröffentlichung	In GAL veröffentlichen in Outlook	Attribut im AD aus dem IdM, Sync über Entra Connect	Sync überschreibt manuelle Werte, Empfänger findet keinen Schlüssel
Erneuerung	Nutzer reagiert auf Ablaufmail	Ablaufbericht aus dem Bestand, Bulk-Erneuerung	Signatur bricht ab, alter Schlüssel wird gelöscht
Austritt	Ticket an das Rechenzentrum	Sperrung und Archivierung als Schritt im Austrittsprozess	fremde Identität signiert weiter, Schlüssel geht verloren
Funktionspostfach	Schlüssel per Weitergabe im Team	Zuordnung über Gruppenmitgliedschaft, Rotation bei Wechsel	Ehemalige lesen weiter mit

FAKTEN • Merkposten für das Betriebskonzept

Virtuelle Zertifikatssammlung in Exchange Online mit allen Ketten, die noch im Umlauf sind, inklusive Restbestände aus Sectigo und DFN-PKI.

Erreichbare Sperrlisten und OCSP; Exchange Online und Outlook mobil verwerfen Zertifikate, deren Status sie nicht prüfen können.

Tresor für Entschlüsselungsschlüssel mit Aufbewahrungsfrist, die sich an den Inhalten orientiert, nicht an den Zertifikaten.

Austrittsprozess mit Sperrung, Archivierung und Geräte-Bereinigung.

Verantwortliche für Enterprise Admin und Approver, beide mit TOTP-Zweifaktor.

Flächig einführen ohne Helpdesk-Kollaps

Warum nutzen Hochschulen ihre Zertifikate so selten flächig? Nicht aus Unwissen. Die Rechenzentren wissen genau, was S/MIME kann. Es fehlt meist der Anlass, der den Aufwand rechtfertigt, und es fehlt jemand, der den organisatorischen Teil verantwortet. Die Technik ist an einem Nachmittag eingerichtet. Die Klärung, wer im Ernstfall einen fremden Schlüssel aus dem Tresor holen darf, dauert länger als manches Berufungsverfahren.

Wo S/MIME sich lohnt und wo nicht

Einsatz	Nutzen	Empfehlung
Signatur für alle Mitarbeiterinnen und Mitarbeiter	Phishing-Abwehr, Absenderprüfung, verteilt nebenbei öffentliche Schlüssel	guter Einstieg, auch ohne Schlüsselsicherung
Verschlüsselung in Verwaltung und Prüfungswesen	Vertraulichkeit Ende zu Ende, auch gegenüber dem Mailbetreiber	nur mit Schlüsselsicherung und Austrittsprozess
Kommunikation mit Verbundpartnern in Drittmittelprojekten	funktioniert über Organisations- und Ländergrenzen hinweg	sinnvoll, Partner müssen S/MIME selbst beherrschen
Interne Vertraulichkeit im Tenant	auch über Purview Message Encryption oder Labels erreichbar	Verfahren abwägen, nicht doppelt auf dieselbe Mail
Studenten	selten echter Bedarf, hoher	in der Regel nicht flächig

	Supportaufwand	
--	----------------	--

Microsoft selbst bezeichnet Purview Message Encryption als direkte Alternative zu S/MIME: richtlinienbasiert, ohne eigene PKI, mit dem Nachteil, dass die Schlüssel beim Dienst liegen. S/MIME hat den umgekehrten Vor- und Nachteil. Wer an der Hochschule ohnehin mehrere Mailsysteme und Clients parallel betreibt, wird S/MIME kaum ersetzen wollen, weil es als offener Standard auch mit Thunderbird, Apple Mail und dem Unix-Mailserver des Instituts funktioniert. Koexistenz ist auch hier der Normalfall.

Reihenfolge, die sich bewährt

- **Bestand aufnehmen:** Welche Zertifikate sind im Umlauf, von welcher CA, mit welchem Ablaufdatum? Wer verschlüsselt heute schon, und wo liegen diese Schlüssel?
- **AAI anbinden:** IdP-Attribute und Entitlement für den HARICA Certificate Manager konfigurieren, Approver und Admins benennen.
- **Signatur ausrollen:** Mit Pilotgruppen in Rechenzentrum, Verwaltung und einer Fakultät beginnen, Outlook-Clients, Outlook im Web und Mobilgeräte testen.
- **Tresor und Verfahren:** Schlüsselsicherung aufbauen, Regeln mit Datenschutz und Personalrat abstimmen, Austrittsprozess ergänzen.
- **Verschlüsselung freigeben:** Zunächst für Funktionspostfächer und Bereiche mit klarem Bedarf, dann schrittweise ausweiten.

TIPP · Dezentrale Administratoren einbinden

An vielen Hochschulen betreuen Fakultäts- und Lehrstuhl-Admins die Arbeitsplätze. Sie sind die natürlichen Ansprechpartner für Zertifikatsimport und Gerätewechsel, sollten aber keinen Zugriff auf den zentralen Schlüsseltresor bekommen. Wie man Rollen in einem gemeinsamen Tenant schneidet, beschreibt der Beitrag zur dezentralen IT.

› [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#)

TYPISCHE SITUATION · Typische Situation aus der Projekterfahrung

In einem Krankenhausverbund in kirchlicher Trägerschaft sollten Befundberichte an einweisende Praxen per S/MIME gehen. Technisch war alles in zwei Wochen fertig. Monate kostete die Frage, wer die Schlüssel des Sekretariats verwahrt, wenn die Chefärztin wechselt, und wie die Mitarbeitervertretung den Tresor bewertet. Übertragen auf die Hochschule: Planen Sie die Zeit für Verfahren und Mitbestimmung großzügiger ein als die für die Technik. Die Technik wartet geduldig.

FAQ: S/MIME-Zertifikate an der Hochschule

Bekommen wir über den DFN überhaupt noch Nutzerzertifikate?

Ja. Die DFN-PKI Global stellt seit August 2023 nichts mehr aus, aber über GÉANT TCS erhalten teilnehmende Einrichtungen weiterhin S/MIME-Zertifikate. Anbieter ist seit 2025 HARICA, beantragt wird im HARICA Certificate Manager.

Sind unsere alten Sectigo- und DFN-PKI-Zertifikate jetzt ungültig?

Nein. Sie bleiben bis zu ihrem regulären Ablauf gültig und können weiter gesperrt werden. Ihre Ketten gehören bis dahin in die virtuelle Zertifikatssammlung von Exchange Online, und die zugehörigen privaten Schlüssel gehören dauerhaft in den Tresor, solange damit verschlüsselte Mails existieren.

Brauchen wir für S/MIME eine eigene Zertifizierungsstelle?

Für Zertifikate aus TCS nicht. Eine eigene CA brauchen Sie nur, wenn Sie etwa per SCEP gerätespezifische Signaturzertifikate über Intune ausgeben wollen.

Funktioniert S/MIME in Outlook im Web auf jedem Rechner?

Nein. Microsoft unterstützt es auf Windows-Clients in Edge und Chrome; die S/MIME-Erweiterung wird per Richtlinie erzwungen, was verwaltete Geräte voraussetzt. Am privaten Rechner von Lehrbeauftragten oder im Lesesaal ist S/MIME im Browser damit in der Praxis nicht verfügbar.

Kann der Mailbetreiber verschlüsselte Mails lesen?

Nein, das ist der Sinn der Sache. Weder Exchange Online noch das Rechenzentrum kann den Inhalt ohne privaten Schlüssel lesen. Das gilt auch für Inhaltssuche, eDiscovery und Schadsoftwareprüfung des Inhalts.

Was ist mit Funktionspostfächern wie dem Prüfungsamt?

Dafür gibt es Email-only-Zertifikate, die nur die Rollenadresse enthalten. Gruppennamen als Personennamen sind nicht zulässig. Wichtig ist die Rotation, wenn jemand mit Schlüsselkopie das Team verlässt.

Sollen Studenten S/MIME-Zertifikate bekommen?

Möglich ist es, flächig sinnvoll selten. Der Supportaufwand ist hoch, der Bedarf gering, und die Frage der Schlüsselsicherung stellt sich bei Exmatrikulation genauso wie beim Austritt von Personal.

Brauchen wir eine Dienstvereinbarung für den Schlüsseltresor?

Das hängt vom Personalvertretungsrecht Ihres Landes und von der Ausgestaltung ab. Weil ein Tresor mit Wiederherstellungsmöglichkeit Zugriff auf dienstliche Kommunikation eröffnet, sollten Sie den Personalrat frühzeitig beteiligen. Rechtsverbindlich beurteilen kann das nur Ihr Justizariat.

Fazit: Erst den Schlüssel organisieren, dann das Zertifikat

Der Zugang zu S/MIME-Zertifikaten ist an Hochschulen gelöst. Über DFN und GÉANT TCS stellt HARICA seit 2025 aus, die Anbindung an die DFN-AAI macht den Antrag zu einer Sache von Minuten, und Exchange Online, Outlook und Intune bringen alles mit, was für die Verteilung nötig ist. Was fehlt, ist selten Technik, sondern Organisation: ein Tresor für Entschlüsselungsschlüssel, klare Regeln für den Zugriff darauf, ein Austrittsprozess, der Zertifikate sperrt und Schlüssel behält, und eine Erneuerung, die alte Schlüssel nicht wegwirft.

Wer klein anfangen will, beginnt mit der Signatur. Sie kostet wenig, schützt gegen gefälschte Absender und verteilt ganz nebenbei die öffentlichen Schlüssel. Verschlüsselung folgt, wenn die Schlüsselsicherung steht. In dieser Reihenfolge ist S/MIME ein solides Werkzeug. In umgekehrter Reihenfolge ist es eine Zeitkapsel, deren Schlüssel man beim Vergraben gleich mit vergraben hat. Wenn Sie dabei Unterstützung beim Konzept wollen, hilft unsere [Microsoft-365-Beratung für Hochschulen und Forschung](#); für Ihre Exchange- und Client-Teams gibt es die [Microsoft-365-Schulung für Hochschulen und Forschung](#).

WEITERLESEN • Weiterlesen

Die Serie zu Microsoft 365 in Hochschule und Forschung. Für diesen Beitrag besonders passend:

- › [Microsoft 365 in Hochschule und Forschung](#)
- › [Exchange an der Hochschule: Hybrid, Alt-Mailserver und die Studenten-Mail](#)

- › [Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden](#)
- › [Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto](#)
- › [Gastwissenschaftler, Lehrbeauftragte, Emeriti: Sonderrollen in Entra ID sauber abbilden](#)
- › [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#)
- › [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#)
- › [Microsoft 365 an Hochschulen: Wo der Campus anders tickt als Verwaltung und Wirtschaft](#)