

SMimeManager: S/MIME-Zertifikate zentral verwalten und behalten

Signierte und verschlüsselte E-Mails sind schnell eingeführt. Schwierig wird es danach: Zertifikate laufen ab, Schlüssel gehen verloren, und niemand weiß mehr, wer welches Zertifikat wann bekommen hat. SMimeManager holt die S/MIME-Verwaltung aus der Excel-Liste und macht daraus einen geordneten, nachvollziehbaren Prozess.

Das Problem: S/MIME scheitert selten an der Technik, sondern am Alltag

Kennst du das? Montagmorgen, irgendwo in einer Verwaltung. Eine Sachbearbeiterin schickt wie jede Woche eine verschlüsselte Mail an eine Partnerbehörde. Diesmal kommt ein Rückruf statt einer Antwort: Die Signatur sei ungültig. Ein kurzer Blick zeigt, dass ihr Zertifikat am Freitag abgelaufen ist. Die Erinnerung dazu stand in einer Tabelle, die der Kollege gepflegt hat, der seit drei Monaten in einer anderen Abteilung sitzt. Zwei Tische weiter hat jemand einen neuen Laptop bekommen und kann seine alten verschlüsselten Mails nicht mehr öffnen, weil der private Schlüssel mit dem alten Gerät in der Entsorgung gelandet ist.

Das ist kein exotischer Einzelfall, das ist der Normalzustand in vielen Häusern, die S/MIME ernsthaft betreiben. Die Einführung ist ein Projekt mit Budget und Aufmerksamkeit. Der Betrieb danach ist Kleinarbeit, die niemandem gehört. Und genau dort entstehen die Ausfälle: abgelaufene Zertifikate, verlorene Schlüssel, fehlende Nachweise, wer wann was bekommen hat.

Gleichzeitig wird S/MIME in vielen Branchen Pflicht. Behörden, das Gesundheitswesen und alle, die vertrauliche Informationen per Mail austauschen, kommen um signierte und verschlüsselte Kommunikation kaum noch herum. Mit wachsender Zahl an Postfächern wird aus der Kleinarbeit ein echtes Betriebsrisiko. Manuelles Verwalten scheitert dann an zwei Dingen: Ablaufdaten und Schlüsselverlust.

Schlüssel weg, Mails weg

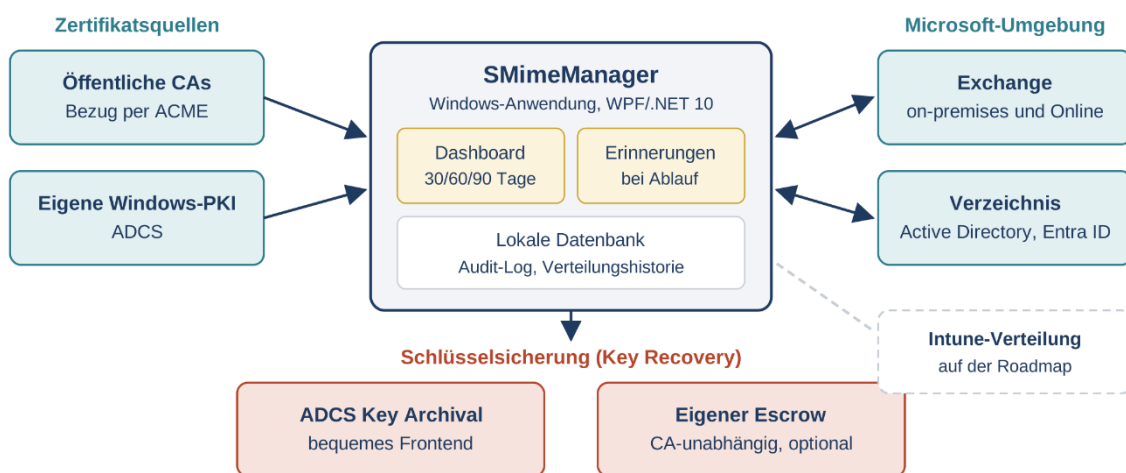
Bei S/MIME-Verschlüsselung wird jede Mail mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Lesen kann sie nur, wer den passenden privaten Schlüssel besitzt. Geht dieser Schlüssel verloren, etwa mit einem defekten Laptop oder einem gelöschten Benutzerprofil, sind alle damit verschlüsselten Mails unlesbar. Nicht schwer lesbar, sondern unlesbar. Ohne Schlüsselsicherung gibt es keinen Plan B.

Was SMimeManager macht

SMimeManager ist eine Windows-Anwendung zur zentralen Verwaltung von S/MIME-Zertifikaten für E-Mail-Signatur und -Verschlüsselung. Statt verteilter Tabellen, Kalendereinträge und Bauchgefühl hast du einen Ort, an dem alle Zertifikate, ihre Laufzeiten und ihre Geschichte zusammenlaufen. Die Anwendung basiert auf WPF und .NET 10 und speichert ihre Daten in einer lokalen Datenbank. Deine Zertifikatsdaten wandern also nicht in irgendeine fremde Cloud, sondern bleiben dort, wo sie hingehören: bei dir.

SMimeManager spricht die Microsoft-Welt in beiden Varianten: on-premises und in der Cloud. Er unterstützt Exchange und Exchange Online beziehungsweise Microsoft 365 ebenso wie Active Directory und Entra ID. Zertifikate bezieht er wahlweise per ACME bei öffentlichen Zertifizierungsstellen oder aus deiner eigenen Windows-PKI mit Active Directory Certificate Services. Wenn du dich tiefer mit dem Unterbau beschäftigen willst, findest du im Kompetenzbereich [PKI mit ADACS](#) das nötige Hintergrundwissen.

SMimeManager: Funktionsprinzip



Alle Daten bleiben in der lokalen Datenbank beim Kunden.

Funktionsprinzip: SMimeManager bündelt Zertifikatsbezug, Microsoft-Umgebung, Schlüsselsicherung und Überwachung an einem Ort mit lokaler Datenbank.

Stell dir SMimeManager wie den Schlüsselkasten im Hausmeisterbüro vor: Jeder Schlüssel hat seinen Haken, ein Schild und einen Eintrag im Buch, wer ihn wann ausgegeben hat. Ohne diesen Kasten liegen die Schlüssel in Schubladen, Jackentaschen und Autos verteilt. Funktioniert auch, bis jemand an einem Freitagabend vor der verschlossenen Tür steht.

Die Funktionen im Detail

Dashboard mit Ablauf-Übersicht 30, 60 und 90 Tage

Das Herzstück im Alltag ist das Dashboard. Es zeigt dir auf einen Blick, welche Zertifikate in den nächsten 30, 60 und 90 Tagen ablaufen. Damit siehst du nicht nur das akute Feuer, sondern auch die Welle, die in zwei Monaten auf dich zurollt. Wer schon einmal erlebt hat, dass bei einer Erstausrüstung alle Zertifikate am selben Tag ausgestellt wurden und deshalb auch am selben Tag ablaufen, weiß, warum der Blick nach vorn so wichtig ist.

Erinnerungen statt Kalendereinträge

SMimeManager erinnert an anstehende Abläufe. Das klingt banal, ist aber der Unterschied zwischen einem geplanten Wechsel am Dienstagvormittag und einem hektischen Notfall am Montagmorgen. Die Erinnerung hängt am Zertifikat und nicht am Outlook-Kalender eines einzelnen Kollegen, der irgendwann den Job wechselt.

Zertifikatsbezug per ACME und aus der eigenen ADCS

Woher die Zertifikate kommen, entscheidest du. SMimeManager bezieht sie per ACME bei öffentlichen Zertifizierungsstellen oder aus deiner eigenen Windows-PKI auf Basis von Active Directory Certificate Services. Beides hat seine Berechtigung: Öffentliche Zertifikate brauchst du typischerweise für die Kommunikation mit externen Partnern, interne Zertifikate reichen oft für den Austausch im eigenen Haus. Mit SMimeManager verwaltest du beide Welten an derselben Stelle.

Exchange, Exchange Online, Active Directory und Entra ID

Viele Organisationen stecken irgendwo zwischen on-premises und Cloud: Exchange im eigenen Rechenzentrum, ein Teil der Postfächer schon in Exchange Online, Identitäten im Active Directory und in Entra ID. SMimeManager ist genau für diese Realität gebaut und unterstützt die Microsoft-Technologien in beiden Varianten. Du musst dich also nicht entscheiden, ob du ein Werkzeug für gestern oder für morgen kaufst.

Key Recovery und Escrow

Hier trennt sich die Spreu vom Weizen. SMimeManager bietet ein Frontend für die Schlüsselarchivierung von ADCS (Key Archival). Die Funktion steckt in der Windows-PKI, ist aber in der Bedienung alles andere als komfortabel. SMimeManager macht sie handhabbar, sodass im Ernstfall nicht erst jemand die Dokumentation von vor sechs Jahren suchen muss.

Auf Wunsch gibt es zusätzlich einen eigenen, CA-unabhängigen Escrow. Das ist vor allem dann interessant, wenn die ausstellende Zertifizierungsstelle irgendwann abgeschaltet wird, etwa bei einer PKI-Migration oder nach einer Umstrukturierung. Die archivierten Schlüssel hängen dann nicht mehr am Schicksal der alten CA, und verschlüsselte Mails aus den vergangenen Jahren bleiben lesbar.

Warum ein CA-unabhängiger Escrow?

Die Schlüsselarchivierung in ADCS ist an die Zertifizierungsstelle gebunden, die das Zertifikat ausgestellt hat. Wird diese CA außer Betrieb genommen, wird auch die Wiederherstellung der Schlüssel schwierig. Ein eigener Escrow in SMimeManager entkoppelt die Schlüsselsicherung vom Lebenszyklus der CA. Gerade bei Umbauprojekten an der PKI ist das ein Sicherheitsgurt, den du erst vermisst, wenn es kracht.

Audit-Log und Verteilungshistorie

Wer hat wann welches Zertifikat bekommen? Wer hat einen Schlüssel wiederhergestellt? SMimeManager führt ein Audit-Log und eine Verteilungshistorie. Das hilft dir bei der nächsten Prüfung durch Revision oder Datenschutz, aber auch ganz praktisch beim Troubleshooting: Wenn ein Partner meldet, dass er eine alte Signatur nicht prüfen kann, siehst du sofort, welches Zertifikat damals im Einsatz war.

Intune-Integration für die Verteilung (Roadmap)

Die Verteilung von Zertifikaten über Intune ist auf der Roadmap. Damit soll SMimeManager künftig auch die Auslieferung auf verwaltete Endgeräte über den Microsoft-Weg unterstützen.

Funktion	Was sie leistet	Was du davon hast
Dashboard 30/60/90 Tage	Zeigt anstehende Abläufe in drei Zeitfenstern	Keine Überraschungen am Montagmorgen
Erinnerungen	Meldet fällige Zertifikate rechtzeitig	Planbare Wechsel statt Notfälle
Bezug per ACME und ADCS	Öffentliche CAs und eigene Windows-PKI	Beide Welten an einer Stelle
Microsoft on-premises und Cloud	Exchange, Exchange Online, AD, Entra ID	Passt zu hybriden Umgebungen
Key Recovery für ADCS	Frontend für ADCS Key Archival	Wiederherstellung ohne Handbuch-Suche
CA-unabhängiger Escrow	Eigene Schlüsselsicherung auf Wunsch	Alte Mails bleiben lesbar, auch ohne alte CA
Audit-Log und Verteilungshistorie	Protokolliert Ausgabe und Änderungen	Nachweis für Revision und Datenschutz
Intune-Verteilung	Auf der Roadmap	Auslieferung auf verwaltete Geräte

SMimeManager auf einen Blick

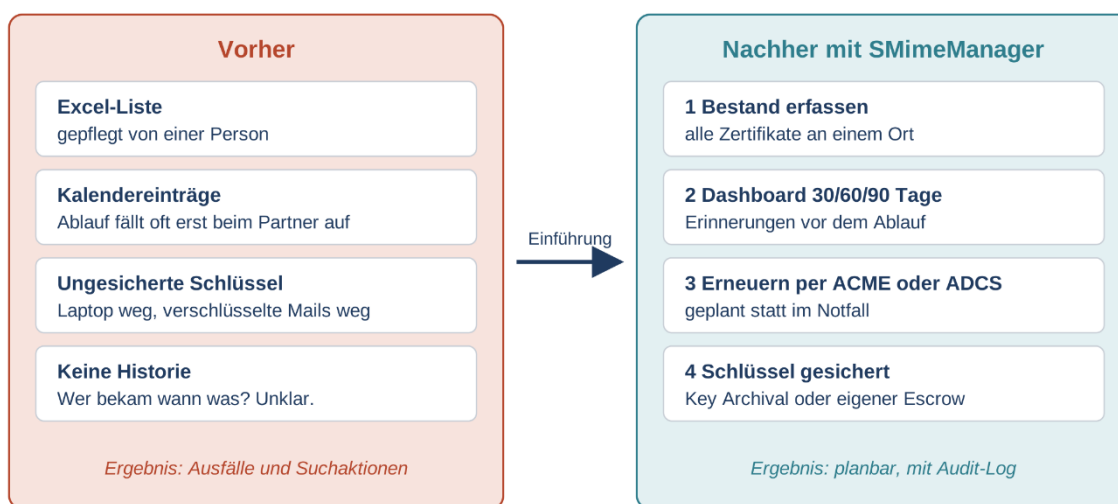
- **Produkttyp:** Windows-Anwendung zur zentralen Verwaltung von S/MIME-Zertifikaten für E-Mail-Signatur und -Verschlüsselung
- **Plattform:** WPF auf .NET 10
- **Datenhaltung:** lokale Datenbank, Daten bleiben beim Kunden
- **Umgebungen:** Exchange, Exchange Online/Microsoft 365, Active Directory, Entra ID; on-premises und Cloud
- **Zertifikatsbezug:** ACME bei öffentlichen CAs sowie eigene Windows-PKI (ADCS)
- **Zielgruppe:** Organisationen mit 20 bis 1.000 Postfächern

- **Lizenzmodell:** Einmallizenz pro verwaltetem Benutzer, Richtpreis 50 € netto; Projekt- und Enterprise-Lizenzen möglich
- **Hersteller:** Eigenentwicklung von boddenberg.de

So sieht der Einsatz in der Praxis aus

Der Unterschied zwischen vorher und nachher ist weniger eine Frage neuer Technik als eine Frage von Ordnung. Die Zertifikate gibt es ja schon, die Postfächer auch. Was fehlt, ist der Ort, an dem alles zusammenläuft, und ein Ablauf, der nicht davon abhängt, dass sich eine einzelne Person an alles erinnert.

S/MIME-Betrieb: vorher und nachher



Vorher und nachher: aus verstreuten Listen, Kalendereinträgen und ungesicherten Schlüsseln wird ein zentraler, nachvollziehbarer Ablauf.

Ein typischer Einstieg sieht so aus: Du erfasst den vorhandenen Bestand und verschaffst dir über das Dashboard einen Überblick, welche Zertifikate wann ablaufen. Dann legst du fest, aus welcher Quelle neue Zertifikate kommen sollen: per ACME von einer öffentlichen CA, aus der eigenen ADCS oder je nach Empfängerkreis aus beiden. Parallel klärst du die Frage der Schlüsselsicherung, also ob du die Key Archival der ADCS nutzt, den eigenen Escrow oder beides.

Im laufenden Betrieb arbeitest du dann mit dem Dashboard und den Erinnerungen. Statt im Krisenmodus reagierst du in Ruhe auf die 90-Tage-Vorschau. Und wenn ein Schlüssel verloren geht, beginnt kein Drama, sondern ein Wiederherstellungsvorgang, der im Audit-Log sauber dokumentiert ist.

Erst die Schlüsselsicherung, dann die Verschlüsselung

Wenn du S/MIME-Verschlüsselung neu einführst, kläre die Schlüsselsicherung, bevor die erste verschlüsselte Mail verschickt wird. Nachträglich lassen sich Schlüssel nur

sichern, die noch irgendwo vorhanden sind. Was mit dem alten Laptop verschwunden ist, holt dir auch das beste Werkzeug nicht zurück.

Für wen SMimeManager gedacht ist

SMimeManager ist für Organisationen mit 20 bis 1.000 Postfächern gebaut. Darunter reicht oft noch die sorgfältig gepflegte Liste, darüber sprechen wir über andere Größenordnungen und meist über Projekt- oder Enterprise-Lizenzen. Im Zielbereich dazwischen ist die Lage typisch: zu viele Zertifikate, um sie im Kopf zu behalten, aber kein eigenes Team, das sich nur um PKI und Mailsicherheit kümmert.

- **Behörden und kommunale Verwaltungen**, in denen signierte und verschlüsselte Kommunikation mit anderen Stellen zum Alltag gehört. Mehr zum Umfeld findest du im Kompetenzbereich [Microsoft 365 in der öffentlichen Verwaltung](#).
- **Einrichtungen im Gesundheitswesen**, die vertrauliche Informationen per Mail austauschen. Hintergründe liefert der Bereich [Microsoft 365 im Krankenhaus](#).
- **Unternehmen mit hohem Vertraulichkeitsbedarf**, etwa in Beratung, Recht oder Entwicklung, die S/MIME aus eigenem Interesse einsetzen.
- **IT-Abteilungen mit hybrider Microsoft-Umgebung**, die Exchange on-premises und Exchange Online parallel betreiben.
- **Systemhäuser und Partner**, die S/MIME als Dienstleistung für ihre Kunden betreuen; dafür gibt es eigene Konditionen auf Anfrage.

Für den IT-Leiter ist die Rechnung einfach: Jeder Ausfall durch ein abgelaufenes Zertifikat kostet Zeit, Nerven und manchmal auch Vertrauen bei externen Partnern. Jeder verlorene Schlüssel kann den Zugriff auf Jahre an Korrespondenz kosten. Für den Admin ist der Gewinn noch direkter: weniger Feuerwehreinsätze, weniger Suchen in alten Tabellen und eine Historie, die jede Frage nach dem Wer und Wann beantwortet.

Editionen und Lizenzierung

SMimeManager wird pro Benutzer lizenziert. Der Richtpreis liegt bei **50 € pro verwaltetem Benutzer** als Einmallizenz, netto zuzüglich Mehrwertsteuer. Kein Abo, keine monatliche Rechnung, die still mitläuft. Für größere Vorhaben sind **Projekt- und Enterprise-Lizenzen** möglich. Systemhäuser, Partner und Multiplikatoren bekommen eigene Konditionen, bitte anfragen.

Lizenzform	Grundlage	Hinweis
Benutzerlizenz	Richtpreis 50 € netto pro verwaltetem Benutzer	Einmallizenz, kein Abo
Projektlizenz	auf Anfrage	für abgegrenzte Vorhaben
Enterprise-Lizenz	auf Anfrage	für größere Organisationen

Lizenzform	Grundlage	Hinweis
Partner und Systemhäuser	eigene Konditionen	bitte anfragen

Alle weiteren Details zu Lizenzbedingungen nennt dir Uli auf Anfrage.

Beratung, Einführung und Schulung

Ein Werkzeug ersetzt kein Konzept. Bei S/MIME stellen sich vorab Fragen, die mit der Software wenig zu tun haben: Welche Zertifikate brauchst du für externe Partner, welche reichen intern? Wie ist die eigene PKI aufgestellt, und ist die Schlüsselarchivierung überhaupt eingerichtet? Wer darf Schlüssel wiederherstellen, und wie wird das dokumentiert? Hier hilft die Erfahrung aus rund 30 Jahren Microsoft-Enterprise-Projekten, unter anderem mit Active Directory Certificate Services und Exchange. Auf Wunsch begleitet Uli die Einführung von der Bestandsaufnahme über die Einrichtung bis zur Schulung der Administratoren, damit SMimeManager nicht nur installiert, sondern im Alltag auch gelebt wird. Hintergrundwissen rund um Mailsicherheit findest du außerdem im Kompetenzbereich [Microsoft 365 Security](#).

Häufige Fragen

Brauche ich eine eigene Windows-PKI, um SMimeManager zu nutzen?

Nein. SMimeManager bezieht Zertifikate auch per ACME bei öffentlichen Zertifizierungsstellen. Wenn du eine eigene PKI mit Active Directory Certificate Services betreibst, kannst du sie zusätzlich oder stattdessen nutzen. Beide Quellen laufen in derselben Verwaltung zusammen.

Funktioniert SMimeManager mit Exchange Online?

Ja. SMimeManager unterstützt Microsoft-Technologien on-premises und in der Cloud, also Exchange und Exchange Online beziehungsweise Microsoft 365 sowie Active Directory und Entra ID. Gerade hybride Umgebungen sind ein typisches Einsatzfeld.

Wo liegen meine Zertifikatsdaten?

In einer lokalen Datenbank bei dir. SMimeManager ist eine Windows-Anwendung und kein Cloud-Dienst. Die Daten bleiben beim Kunden, das ist eine bewusste Grundentscheidung bei allen Produkten von boddenberg.de.

Was passiert, wenn ein Mitarbeiter seinen privaten Schlüssel verliert?

Dann kommt die Schlüsselsicherung ins Spiel. SMimeManager bietet ein Frontend für die Key Archival von ADCS und auf Wunsch einen eigenen, CA-unabhängigen Escrow. Voraussetzung ist, dass der Schlüssel vorher gesichert wurde. Deshalb gehört die Schlüsselsicherung an den Anfang jeder S/MIME-Einführung.

Kann ich Zertifikate über Intune verteilen?

Die Intune-Integration für die Verteilung ist auf der Roadmap. Wenn das für dich ein wichtiges Kriterium ist, sprich es im Vorgespräch an.

Für wie viele Postfächer ist SMimeManager ausgelegt?

Die Zielgröße liegt bei 20 bis 1.000 Postfächern. Für größere Organisationen sind Projekt- und Enterprise-Lizenzen möglich.

Wie unterscheidet sich SMimeManager von CertBinder?

SMimeManager kümmert sich um S/MIME-Zertifikate für Personen und deren E-Mail.

[CertBinder](#) ist für TLS-Zertifikate auf Servern zuständig, also das Erneuern und Einbinden in Dienste wie IIS, Exchange oder ADFS. Wer eine Bestandsaufnahme der eigenen Zertifizierungsstelle braucht, schaut sich den [PKI Diagnostiker](#) an.

Weiter geht's

- Kompetenzbereich [PKI mit ADCS](#): Grundlagen und Praxis der Windows-PKI
- Kompetenzbereich [Microsoft 365 Security](#): Mailsicherheit im Gesamtbild
- [CertBinder](#): TLS-Zertifikate erneuern und in alle Dienste einbinden
- [PKI Diagnostiker](#): Bestandsaufnahme und Härtingsprüfung der eigenen CA
- Kompetenzbereich [Microsoft 365 in der öffentlichen Verwaltung](#)