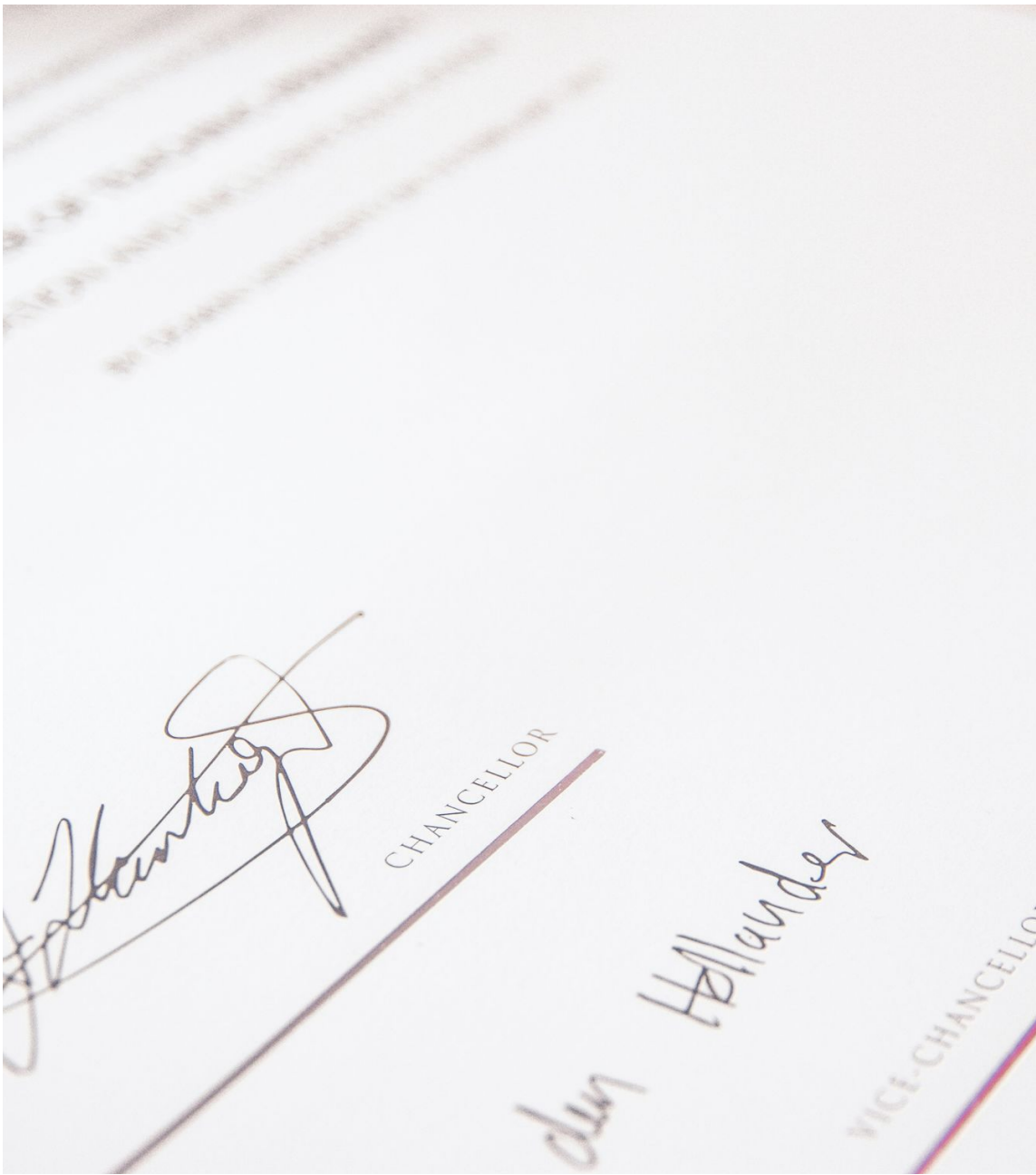
DIE UNSICHTBARE INFRASTRUKTUR DES VERTRAUENS

Wie verkürzte Laufzeiten, manuelle Prozesse und fehlende Transparenz das Zertifikatsmanage-ment zum kritischen Faktor im SAP-Betrieb machen

Ein automatics.ai Report über Stabilität, Automatisierung und die neue Verantwortung für digitale Vertrauensketten



automatics

EXECUTIVE SUMMARY

Zertifikate sind die unsichtbare Grundlage jeder sicheren SAP-Kommunikation.
Sie schützen Daten, authentifizieren Systeme und garantieren, dass jede Verbindung vertrauenswürdig bleibt. Doch was im Hintergrund abläuft, entscheidet über Stabilität, Verfügbarkeit und Compliance ganzer Unternehmensprozesse.

Viele SAP-Landschaften verwalten ihre Zertifikate noch immer manuell. Tabellen, verstreute Verantwortlichkeiten und fehlende Transparenz führen dazu, dass ablaufende oder fehlerhafte Zertifikate erst dann auffallen, wenn sie produktive Systeme blockieren. Schnittstellen brechen, Zahlungen stoppen, Portale fallen aus. Das sind keine Einzelfälle, sondern wiederkehrende Muster.

Mit den neuen Vorgaben der Zertifizierungsstellen und Browserhersteller, die Laufzeiten schrittweise immer weiter zu verkürzen, wird das Management dieser Zertifikate zu einem kontinuierlichen Prozess. Was früher einmal im Jahr erledigt wurde, muss nun mehrfach im Quartal geplant, geprüft und dokumentiert werden. Diese neue Taktung zwingt Unternehmen, ihre Prozesse zu überdenken – weg von manuellen Aufgaben, hin zu strukturierten, automatisierten Abläufen.

Ein modernes Zertifikatsmanagement basiert auf drei Grundprinzipien:

Sichtbarkeit: Jedes Zertifikat, jede Kette, jede Laufzeit ist zentral erfasst.
Automatisierung: Erneuerungen, Validierungen und Aktivierungen erfolgen planbar und dokumentiert.
Nachweisbarkeit: Jede Änderung ist nachvollziehbar, messbar und auditfähig.

So wird aus einem technischen Detail ein strategischer Bestandteil der IT-Governance.
Automatisierte Prozesse reduzieren Ausfälle, schaffen Compliance-Nachweise und entlasten Teams nachhaltig.
Zertifikate werden damit nicht mehr als Risiko betrachtet, sondern als zentraler Teil einer resilienten Infrastruktur.

Der Report zeigt, wie dieser Wandel gelingt – technisch, organisatorisch und kulturell.
Er beschreibt die Herausforderungen, die typischen Fehlerbilder und die Schritte hin zu einem transparenten, automatisierten Lebenszyklus.
Wer Zertifikate professionell managt, sichert nicht nur Systeme, sondern auch Vertrauen.

EDITOR'S NOTE

Zertifikate sind stille Akteure in jeder SAP-Landschaft.
Sie regeln Vertrauen, sichern Kommunikation und halten Systeme im Takt.
Und doch werden sie meist erst dann sichtbar, wenn sie versagen.

Dieser Report soll genau das ändern.
Er beleuchtet, wie aus kleinen Routinen betriebliche Risiken entstehen – und wie Automatisierung, Transparenz und Prozessdisziplin daraus Resilienz machen.
Ziel ist kein neues Tool und keine weitere Checkliste, sondern ein Bewusstsein dafür, dass Sicherheit planbar ist, wenn sie strukturiert gedacht wird.

Die Erkenntnis ist einfach:
Zertifikate sind keine Nebensache.
Sie sind ein Spiegel der operativen Reife.
Wer sie beherrscht, beherrscht Stabilität.

Happy reading!

Murat Bölükler
Vice President Sales and Customer Success
automatics.AI GmbH

Inhaltsverzeichnis

05 FALLSKIZZEN AUS DER PRAXIS

Reale Beispiele aus dem SAP-Betrieb zeigen, wie kleine Fehler im Zertifikatsmanagement zu großen Betriebsstörungen führen und welche Lehren Unternehmen daraus ziehen können

06 AUTOMATISIERUNG ALS RESILIENZPRINZIP

Ein standardisierter Lebenszyklus mit Inventar, Erneuerung, Validierung und geplanter Aktivierung macht Zertifikate vom Störfaktor zur planbaren Routine

07 COMPLIANCE, KONTROLLE, KONTINUITÄT

Zertifikatsmanagement liefert prüfbare Nachweise für Governance und Regulatorik, schafft klare Verantwortlichkeiten und sichert den Betrieb langfristig ab.

08 SCHLUSSWORT & AUSBLICK

Ein Fazit über die Rolle von Zertifikaten im modernen SAP-Betrieb, warum Sichtbarkeit und Routine zur Grundlage künftiger Stabilität werden und jetzt der richtige Zeitpunkt für Veränderung ist

01

EINLEITUNG

Zertifikate sind zum Taktgeber stabiler SAP-Landschaften geworden. Der aktuelle Auslöser ist eindeutig: Das CA/Browser Forum hat beschlossen, die maximale Laufzeit von TLS-Serverzertifikaten bis 2029 schrittweise auf 47 Tage zu verkürzen. Was heute noch als jährliche Routine gilt, wird zum Dauerbetrieb mit deutlich höherer Frequenz und geringeren Fehlertoleranzen. Heise und die Originalunterlagen des Forums ordnen diesen Schritt als notwendige Reaktion auf Sicherheitsrisiken und betriebliche Anforderungen ein. Das Ergebnis trifft den Alltag der Basis unmittelbar.

Der organisatorische Druck wächst, weil ablaufende oder falsch konfigurierte Zertifikate nachweislich Ausfälle verursachen. Branchenberichte dokumentieren Störungen durch abgelaufene Zertifikate quer über Branchen und Größenklassen. Diese Vorfälle entstehen selten durch fehlendes Wissen, sondern durch fehlende Sichtbarkeit, fehlende Routine und manuelle Arbeitsschritte, die unter Zeitdruck fehleranfällig werden.

SAP-Spezifika verstärken die Komplexität. ABAP verwaltet Zertifikate in PSE-Containern über STRUST, Java-basierte Komponenten sowie der Cloud Connector nutzen eigene Keystores und Trust Stores. Der Internet Communication Manager und der SAP Web Dispatcher prüfen Ketten, Vertrauensanker und Hostnamen jeweils an ihrem Prüfpunkt. Eine lokale Korrektur reicht deshalb oft nicht aus, wenn andere Vertrauensräume nicht synchron sind. Das ist in der SAP-Dokumentation detailliert beschrieben und erklärt, warum erfolgreiche Erneuerung mehr ist als ein Import.

Parallel reift der technische Weg zur Entlastung. Das IETF-Standardprotokoll ACME automatisiert Validierung und Ausstellung, senkt manuelle Schritte und schafft nachvollziehbare Abläufe. In Kombination mit planbaren Aktivierungen und Laufzeit-Monitoring entsteht ein Lebenszyklus, der Ausfälle verhindert und Nachweise liefert. Genau diesen Wandel zeichnet dieser Report nach, vom unsichtbaren Risiko hin zur sichtbaren Routine.

Die neue Normalität ab 2029:

47 Tage

Ab 2029 dürfen Zertifikate laut CA/Browser Forum nur noch 47 Tage gültig sein.

Das bedeutet:

Erneuerungen werden zum Dauerbetrieb.

Manuelle Verfahren verlieren Skalierbarkeit.

Automatisierung wird Pflicht, nicht Option.

01

02

DIE UNSICHTBARE ABHÄNGIGKEIT

Zertifikate sind die stille Infrastruktur einer SAP-Landschaft. Sie tragen Identität und Verschlüsselung, sie sichern Logins und Schnittstellen, sie halten Portale, Apps und Integrationen vertrauenswürdig. Wer im Alltag nur die Oberfläche sieht, übersieht schnell, dass im Hintergrund mehrere Vertrauensräume gleichzeitig wirken: der Internet Communication Manager auf den Applikationsservern, der SAP Web Dispatcher als Terminierungspunkt für HTTPS, ABAP mit seinen PSE-Containern, Java-basierte Komponenten mit eigenen Keystores sowie Cloud-Dienste mit separaten Truststores. Ein einziger Fehler in dieser Kette genügt und Anmeldungen scheitern, Services brechen ab, Integrationen stehen still.

Im ABAP-Stack ist STRUST der zentrale Anlaufpunkt. Hier werden PSEs erstellt, Zertifikate importiert und Vertrauensanker gepflegt. Die SAP-Dokumentation beschreibt den Ablauf, von der PSE-Erzeugung bis zum Kettenimport, und macht deutlich, dass Anzeige, Pflege und Vertrauenseinträge sauber voneinander zu trennen sind. Wer PSEs nur teilweise füllt oder den falschen Anker setzt, erzeugt scheinbar zufällige Fehler, die erst im Betrieb auffallen.

Zwischen Web Dispatcher und ICM entscheidet die SSL-Konfiguration über Stabilität. Kopfzeilen für Zertifikatsweitergabe, Profilparameter und die Zuordnung von Anmelde-Informationen müssen zueinander passen. Die relevanten Parameter und ihr Zusammenspiel sind in der SAP-Hilfe klar dokumentiert. Wird hier unvollständig konfiguriert, akzeptiert der Frontend-Proxy Anfragen, der Applikationsserver verwirft sie jedoch wegen fehlender oder nicht vertrauenswürdiger Zertifikate.

Hybride Szenarien erhöhen die Komplexität. Der Cloud Connector und BTP-Dienste prüfen eigene Truststores. Für ausgehende Verbindungen gelten gesonderte Regeln, zum Beispiel Client-Zertifikate oder zusätzliche Root-CAs im Keystore. SAP führt das in den Leitfäden zu Keystores, Outbound-Authentifizierung und Truststore-APIs aus. In der Praxis bedeutet das: Ein Erfolg im ABAP-PSE garantiert noch keine funktionierende Cloud-Integration, wenn der jeweilige Dienst sein eigenes Vertrauen separat verwaltet.

02

02

Zertifikate sind mehr als Gültigkeitsdaten. Sie enthalten Signaturen, vollständige Ketten und Namen, die zu Host und Dienst passen müssen. In STRUST, im Web Dispatcher und in Cloud-Keystores greifen diese Bausteine ineinander. Ein fehlender Intermediate, ein unpassender Subject Alternative Name oder ein vergessener Vertrauensanker erzeugt Fehlerbilder, die wie Netzwerk- oder Berechtigungsprobleme aussehen, tatsächlich aber reine Vertrauensfragen sind. SAPs technische Referenzen zu Zertifikatsweitergabe, Kettenprüfung und Parametrisierung zeigen, wie präzise diese Bausteine zusammenspielen.

Die Taktung verschärft sich. Das CA/Browser-Forum hat eine schrittweise Verkürzung der TLS-Lebensdauer beschlossen, bis auf 47 Tage im Zielbild. Heise und weitere Primärquellen ordnen ein, warum diese Entwicklung die betrieblichen Prozesse verändert. Was früher jährlich anstand, kommt künftig im Wochenrhythmus, mit allen Folgen für Planung, Genehmigung und Nachweis. Ohne strukturierte Erneuerung, saubere Validierung und dokumentierte Aktivierung steigt das Ausfallrisiko, selbst wenn Teams technisch alles richtig wissen.

Der Kern dieses Kapitels ist einfach. In SAP-Landschaften existiert kein einzelnes „das Zertifikat“, sondern ein Verbund aus Vertrauensspeichern, Konfigurationen und Rollen. Sichtbarkeit und saubere Mechanik entscheiden darüber, ob diese stille Infrastruktur zuverlässig trägt. Wer die beteiligten Stellen kennt und ihre Abhängigkeiten systematisch pflegt, verhindert Störungen, bevor sie entstehen. Aber schauen wir uns zunächst einmal an, warum manuelle Verfahren diesen Anspruch im Tagesgeschäft nicht einlösen und wie typische Brüche in Verantwortung und Transparenz entstehen.

02

03

DER MANUELLE BLINDFLUG

In vielen SAP-Landschaften fehlt der zentrale Blick auf Zertifikate. Zuständigkeiten verteilen sich über Basis, Netzwerk, Security und Schnittstellenverantwortliche. Jeder Bereich pflegt eigene Trust Stores und Verfahren. Im ABAP-Stack führt STRUST die Verwaltung der PSE-Container zusammen, hier werden Zertifikate erzeugt, importiert und Vertrauensanker gepflegt. Das ist korrekt und vom Hersteller so vorgesehen, dennoch bleibt es ohne Gesamtsicht ein lokaler Blick auf einen Teil der Landschaft.

Der operative Alltag zeigt, warum das problematisch ist. Tabellen altern schnell, Laufzeiten geraten aus dem Fokus, Änderungen nach Systemkopien werden nicht konsequent nachgezogen. Die technischen Bausteine verhalten sich dabei durchaus erwartbar: Web Dispatcher und ICM reagieren auf Zertifikatswechsel, Ketten und Weitergabeparameter müssen zusammenpassen, sonst akzeptiert der Frontend-Proxy eine Verbindung, die der Applikationsserver aufgrund fehlender oder nicht vertrauenswürdiger Informationen verwirft. SAP dokumentiert die Mechanik der Zertifikatsweitergabe und die relevanten Einstellungen eindeutig. Wer an einer Stelle unvollständig konfiguriert, erzeugt Fehlerbilder, die wie Netzwerk- oder Berechtigungsthemen wirken, tatsächlich aber reine Vertrauensprobleme sind.

Die vermeintliche Kleinigkeit eines Austauschs hat es ebenfalls in sich. Seit NetWeaver 7.10 kann ein geändertes SSL-PSE zur Laufzeit nachgeladen werden. Das verhindert harte Neustarts, leert jedoch den SSL-Session-Cache und zwingt neue Handshakes. Auf stark frequentierten Systemen kann das Lastspitzen erzeugen. Ohne Planung und Zeitfenster wird aus einem Routinewechsel schnell eine spürbare Beeinträchtigung. Diese Details sind in der Community mehrfach beschrieben und verweisen auf die einschlägigen SAP-Hinweise.

03

Hinzu kommt die Hybridität moderner Landschaften. Der Cloud Connector prüft seinen eigenen Trust Store und benötigt die passende Root-CA, um Client-Zertifikate korrekt zu validieren. Fehlt der Vertrauensanker, scheitern Verbindungen mit typischen Fehlern wie „unable to find valid certification path to requested target“. Das gleiche Muster zeigt sich in Integrationsplattformen, wenn Gegenstellen nicht in der Kette hinterlegt sind. Diese Phänomene sind in Praxisbeiträgen gut dokumentiert.

Frühwarnung ist verfügbar, wird aber oft nicht genutzt. Der Report SSF_ALERT_CERTEXPIRE prüft Laufzeiten und warnt rechtzeitig vor Ablauf. Er lässt sich über das Alert Framework einbinden und so in den Betriebsalltag integrieren. In vielen Umgebungen bleibt er unkonfiguriert oder deckt nur einen Teil der Zertifikate ab, etwa jene im ABAP-PSE, nicht aber externe Proxys oder Cloud-Keystores. Das ist kein technischer Mangel, sondern ein Prozessproblem: Ohne zentrale Sicht und definierte Verantwortung bleibt die Warnung im System hängen.

Die verkürzten Lebenszyklen verschärfen diese Lage. Laufzeiten bewegen sich in Richtung kurzer Intervalle, wodurch Erneuerungen häufiger und zeitkritischer werden. Was früher halbjährlich oder jährlich geplant wurde, fällt heute in engeren Takten an, inklusive Genehmigung, Aktivierung und Validierung. Wer weiterhin mit Tabellen, Einzelterminen und manuellen Importen arbeitet, erhöht die operative Unsicherheit, selbst wenn jedes Team seine Teilaufgabe fachlich korrekt erledigt. Die Folge sind unnötige Incidents und Ad-hoc-Maßnahmen, die vermeidbar wären, sobald Sichtbarkeit, Standard und Routine zusammenkommen.

Der Befund lässt sich in drei Beobachtungen bündeln. Erstens fehlen durchgängige Zuständigkeiten über Systemgrenzen hinweg. Zweitens werden Abhängigkeiten zwischen Trust Stores, Ketten und Parametern selten vollständig dokumentiert. Drittens existiert zwar eine technische Frühwarnung, sie erreicht jedoch nicht verlässlich die richtigen Empfänger. Wer diese Lücken schließt, reduziert Ausfälle und gewinnt Planungssicherheit zurück. Doch wie sehen typische Ausfälle in der Praxis aus und welche wiederkehrenden Muster sich daraus ableiten lassen?

03

03

1

- Zertifikat
- Ausfall
- Kette von Folgen

85 % aller Zertifikatsvorfälle entstehen durch einfache Ablauf- oder Kettenfehler.

Ein abgelaufenes Zertifikat kann:

Geschäftsportale blockieren.

Zahlungssysteme stoppen.

Integrationen zu Cloud-Diensten unterbrechen.

Quelle: Branchenweite Auswertungen von DigiCert und Venafi (2024).

03

04

WENN EIN ZERTIFIKAT AUSFÄLLT

Ausfälle durch Zertifikate beginnen selten laut. Meist zeigt sich das Problem als harmloser Verbindungsfehler, als Login, der nicht mehr greift, oder als Schnittstelle, die plötzlich keine Daten mehr annimmt. Dahinter stehen immer dieselben Mechanismen. Ein Zertifikat ist abgelaufen, eine Kette ist unvollständig, ein Vertrauensanker fehlt. In SAP-Landschaften wirken mehrere Vertrauensräume zugleich. Der Internet Communication Manager sichert HTTPS auf den Applikationsservern, der SAP Web Dispatcher terminiert Verbindungen und leitet Zertifikatsinformationen weiter, ABAP verwaltet PSEs, Java und Cloud-Komponenten arbeiten mit eigenen Keystores. Stimmen Ketten, Header und Vertrauensanker nicht überein, verweigert der Zielservice die Verbindung. Genau dieses Zusammenspiel ist in der SAP Hilfe beschrieben, inklusive der Parameter für die Zertifikatsweitergabe zwischen Web Dispatcher und ICM.

Typische Störungen folgen einem Muster. Beim Web Dispatcher genügt ein überfälliges Serverzertifikat und das Portal nimmt keine Verbindungen mehr an. In Finanzprozessen führt ein fehlender Intermediate im Client PSE zu abgewiesenen Zahlungen, weil der Gegenpart die Kette nicht validieren kann. Nach Systemkopien bleiben alte Hostnamen in Zertifikaten zurück und mTLS bricht, obwohl Netz und Berechtigungen korrekt sind. In hybriden Setups verliert der Cloud Connector das Vertrauen zum Gegenüber, wenn sein eigener Trust Store nicht aktualisiert wurde. SAP dokumentiert für diese Fälle die notwendigen Trust-Einstellungen sowie den Umgang mit Backend-Zertifikaten und den zugehörigen Truststores. Die Praxisempfehlung ist eindeutig. Vertrauen wird an der Kette gemessen und an der Stelle gepflegt, an der es technisch geprüft wird.

Auffällig ist, wie häufig Frühwarnungen fehlen oder zu spät kommen. Für ABAP existiert mit SSF_ALERT_CERTEXPIRE eine Bordfunktion, die Laufzeiten prüft und vor Ablaufen warnt. Diese Warnungen lassen sich in Benachrichtigungen und Dashboards integrieren. Auch Cloud-Dienste bieten Ereignisse für Zertifikatsabläufe. In vielen Landschaften bleiben diese Hinweise jedoch lokal und erreichen nicht die Rollen, die handeln müssen. Das ist kein technischer Mangel, sondern ein Prozessdefizit. Frühwarnung wirkt nur, wenn sie zentral sichtbar und eindeutig zugeordnet ist.

04

04

Die kurzfristige Entstörung ist meist klar. Kette prüfen, fehlende Intermediate hinzufügen, Vertrauensanker nachziehen, neues Zertifikat importieren, kontrolliert neu laden. In ABAP führt der Weg über STRUST und die saubere Pflege der PSEs. Die SAP Hilfe beschreibt die notwendigen Schritte, vom Import bis zum Speichern und der Zuordnung zum richtigen PSE. Wichtig ist die Nachprüfung nach dem Aktivieren. Eine Verbindung, die formal hergestellt wurde, ist erst dann belastbar, wenn Zertifikat, Kette und Hostnamen zusammenpassen und die Gegenseite dies bestätigt.

Langfristig reicht reaktive Entstörung nicht aus. Verkürzte Laufzeiten erhöhen die Frequenz von Erneuerungen und verschieben Zertifikate von der gelegentlichen Aufgabe in den Dauerbetrieb. Dieser Wandel macht Automatisierung zur betriebsnotwendigen Antwort. Das beginnt mit einem vollständigen Inventar aller Zertifikate und Vertrauensanker über alle Trust Stores hinweg. Es setzt sich fort mit definierten Vorläufen und standardisierten Erneuerungen. Wo möglich, werden Ausstellung und Erneuerung technisch angestoßen, etwa über standardisierte Schnittstellen wie ACME, das als IETF-Standard genau dafür entwickelt wurde. Entscheidend ist nicht das Werkzeug, sondern die Routine. Erneuern, bevor es kritisch wird. Validieren, bevor aktiviert wird. Dokumentieren, damit jede Änderung nachvollziehbar bleibt.

Am Ende zählt, ob der Betrieb stabil bleibt. Drei Kennzahlen genügen, um das sichtbar zu machen.

- Anteil automatisiert erneuerter Zertifikate.
- Anteil vollständig validierter Ketten nach der Aktivierung.
- Mean Time to Recover bei zertifikatsbedingten Incidents.

Diese Kennzahlen sind klar, prüfbar und anschlussfähig an bestehende Governance-Berichte. Sie zeigen, ob Zertifikate noch Anlass für Ad-hoc-Maßnahmen sind oder bereits Teil einer planbaren Routine.

04

FALLSKIZZEN AUS DER PRAXIS

Zertifikatsausfälle wirken unscheinbar, bis sie ganze Prozesse lahmlegen. In SAP-Systemen zeigen sie sich nicht als Sicherheitsvorfall, sondern als Betriebsstörung. Hinter Verbindungsabbrüchen, fehlgeschlagenen Authentifizierungen oder stillstehenden Schnittstellen steckt oft ein simples Ablaufdatum, eine unvollständige Kette oder ein fehlender Vertrauensanker. Die folgenden vier realen und fachlich belegten Beispiele zeigen, wie solche Fehler entstehen, welche technischen Mechanismen sie auslösen und welche Lehren sich daraus ziehen lassen.

Web Dispatcher - Portalzugriff blockiert

Ein globales Produktionsunternehmen betreibt mehrere Self-Service-Portale über den SAP Web Dispatcher. Das Zertifikat des zentralen Reverse Proxys war auf 398 Tage ausgestellt und sollte planmäßig erneuert werden. Der manuelle Import erfolgte, die Aktivierung blieb jedoch aus. Am folgenden Montagmorgen verweigerten alle HTTPS-Verbindungen den Zugriff mit dem Hinweis “SSL handshake failed”.

Technischer Hintergrund:
Der Web Dispatcher prüft die Gültigkeit des Serverzertifikats beim Handshake. Nach Ablauf wird der TLS-Handshake vom Client abgewiesen, weil keine gültige Identität vorliegt. Das Verhalten ist in der SAP-Hilfe für SSL-Parameter im ICM und Web Dispatcher dokumentiert.

Impact:
Zugriffe auf Lieferanten- und Serviceportale fielen weltweit aus, SLA-Verstöße und Incident-Reports folgten.

Lernpunkt:
Nach jeder Zertifikatsinstallation muss der ICM oder Web Dispatcher neu geladen werden, damit das neue Zertifikat aktiv wird. SAP beschreibt diese Laufzeitneuladeoption ab NetWeaver 7.10 explizit. Automatisierte Aktivierungen verhindern genau diese Lücke.

Multi-Bank Connectivity - Zahlungsläufe blockiert

Im Finanzsystem eines Konzerns läuft der gesamte Zahlungsverkehr über SAP Multi-Bank Connectivity (MBC). Nach der Aktualisierung der Zwischenzertifikate durch die Bank war das Client-PSE im ABAP-Stack nicht mehr vollständig. Die Intermediate-CA fehlte. Beim nächsten Lauf protokollierte das System “SSL peer certificate untrusted” und brach die Verbindung ab.

Technischer Hintergrund:
MBC nutzt mTLS (mutual TLS) zur beidseitigen Authentifizierung. Das Fehlen eines Intermediates unterbricht die Kette und führt dazu, dass die Gegenseite das Zertifikat des SAP-Clients nicht bis zur Root-CA validieren kann. SAP weist in seinen Leitfäden zu STRUST und Keystore-Pflege ausdrücklich auf den vollständigen Chain-Import hin.

Impact:
Zahlungsläufe stoppten, offene Lieferantenrechnungen konnten nicht abgewickelt werden, das Treasury aktivierte Notfallprozesse.

Lernpunkt:
Jede Zertifikatsänderung im Finanzumfeld erfordert eine vollständige Chain-Validierung und Testkommunikation vor Produktionsfreigabe. Automatisierte Prüfungen erkennen fehlende Intermediates, bevor Jobs starten.

Systemkopie - Vertrauensbruch durch falschen Hostnamen

Ein Sandbox-System wurde per Systemkopie aus der Produktion erstellt. Die Zertifikate im PSE enthielten noch die CN-Informationen des Ursprungssystems. Bei der Kommunikation über den SAP Cloud Connector trat der Fehler “CN mismatch – certificate not valid for host” auf.

Technischer Hintergrund:
In SAP ist der Common Name (CN) Teil der Identitätsprüfung bei mTLS. Wenn sich der Hostname ändert, aber das Zertifikat nicht erneuert wird, verweigert die Gegenseite den Handshake. SAP beschreibt diesen Zusammenhang in der Dokumentation zu SSL Hostname Verification und SNC-Zertifikaten.

Impact:
Integrationstests und Fiori-Zugriffe waren nicht mehr möglich, da Cloud-Dienste die Verbindung als potenziell manipuliert einstuften.

Lernpunkt:
Nach Systemkopien müssen Zertifikate neu generiert oder der Hostname im Zertifikat angepasst werden. Automatisierte Provisionierung stellt sicher, dass die CN-Daten der Zielumgebung entsprechen.

Cloud Connector - Vertrauensanker verloren

Nach einer Infrastrukturwartung wurde das Proxy-Zertifikat des Unternehmens erneuert. Der SAP Cloud Connector verwendete noch den alten Vertrauensanker. In den Logs erschien “unable to find valid certification path to requested target”, die Verbindung zur SAP BTP war unterbrochen.

Technischer Hintergrund:
Der Cloud Connector validiert Serverzertifikate des Proxy anhand seines Trust Stores. Fehlt der neue Root- oder Intermediate-Eintrag, scheitert die Authentifizierung. SAP erklärt dieses Verhalten in der Dokumentation zu „Trust Configuration in the Cloud Connector and BTP“.

Impact:
Datensynchronisation zwischen On-Premises-Systemen und der SAP BTP wurde für mehrere Stunden gestoppt.

Lernpunkt:
Nach Änderungen an Proxys oder CAs müssen Trust Stores im Cloud Connector synchronisiert werden. Regelmäßige Trust-Refreshes verhindern diese Art von Ausfall.

Diese vier Fälle zeigen unterschiedliche technische Ursachen, aber ein gemeinsames Muster. Zertifikate sind oft nicht das eigentliche Problem. Fehlende Transparenz, Routine und Überwachung sind es. Jeder Ausfall beginnt dort, wo Vertrauen stillschweigend vorausgesetzt wird. Der nächste Abschnitt zeigt, wie sich diese Risiken durch Automatisierung in planbare Abläufe verwandeln lassen.

AUTOMATISIERUNG ALS RESILIENZPRINZIP

Ein verlässlicher Betrieb entsteht, wenn Zertifikate nicht mehr als Einzelaufgabe gelten, sondern als standardisierter Lebenszyklus. Das beginnt mit vollständiger Sichtbarkeit. Jedes Zertifikat, jede Kette und jeder Vertrauensanker werden inventarisiert. Nur mit einem zentralen Bild lassen sich Ablaufdaten steuern und Verantwortlichkeiten eindeutig zuordnen. NIST empfiehlt hierfür ein formales Programm mit Rollen, Prozessen und technischer Validierung. Genau dieser Rahmen macht Zertifikatsmanagement messbar und auditfähig.

Erneuerungen verlassen den Kalender und folgen definierten Regeln. Trigger setzen vorlaufende Zeitfenster. Ausstellung und Verlängerung laufen, wo möglich, automatisiert. Das ACME-Protokoll ist dafür der IETF-Standard. Es beschreibt, wie eine Zertifizierungsstelle und ein Client die Validierung und Ausstellung sicher automatisieren. In der Praxis reduziert das manuelle Schritte, senkt Fehlerquoten und schafft klare Nachweise über alle Vorgänge.

Die Aktivierung neuer Zertifikate braucht kontrollierte Mechanik. In ABAP werden PSEs in STRUST gepflegt, anschließend wird serverseitig neu geladen. Seit NetWeaver 7.10 ist ein Laufzeit-Reload möglich, wodurch ein kompletter Neustart des ICM vermieden wird. Bestehende Verbindungen bleiben bestehen, neue Handshakes nutzen die aktualisierte Identität. Das minimiert Wartungsfenster und fügt sich in planbare Deployments ein.

Validierung ist der Kern der Qualitätssicherung. Vor der Aktivierung wird geprüft, ob Signatur, Kette und Hostnamen zueinander passen. Nach der Aktivierung bestätigt eine Gegenprobe, dass die Gegenseite die Kette akzeptiert. In hybriden Szenarien reicht eine lokale Prüfung nicht aus. Der Web Dispatcher leitet Zertifikatsinformationen weiter, der Applikationsserver prüft sie, Cloud-Dienste bewerten eigene Truststores. Nur wenn alle Prüfpunkte dieselbe Kette kennen, bleibt die Verbindung stabil. SAP dokumentiert die relevanten Parameter für SSL am ICM und die Pflege der Trust Stores in STRUST. Diese Hinweise bilden die Grundlage für reproduzierbare Rollouts.

Die Taktung wird enger. Das CA/Browser Forum hat die schrittweise Verkürzung der TLS-Lebensdauer beschlossen. Bis 2029 sinkt die maximale Gültigkeit auf 47 Tage. Fachberichte ordnen die Entscheidung ein und zeigen, warum Unternehmen ihre Abläufe beschleunigen müssen. Ohne Automatisierung wächst die Zahl der kritischen Wechsel und damit das Risiko von Ausfällen. Mit Automatisierung entsteht Routine, die kurze Lebenszyklen beherrschbar macht.

Automatisierung endet nicht beim Import. Monitoring und Nachweis gehören dazu. Ereignisse aus ABAP, Java und Cloud werden zusammengeführt. Ablaufwarnungen und Validierungsfehler sind zentral sichtbar. Jede Änderung wird protokolliert. Dadurch entsteht ein belastbarer Audit-Trail, der Technik und Governance verbindet. NIST beschreibt genau diese Kopplung aus Betriebsmechanik und Belegen als Best Practice für große Umgebungen.

Für den Betrieb reichen wenige Kennzahlen, um Fortschritt zu belegen und Engpässe früh zu erkennen.

- Anteil automatisiert erneuerter Zertifikate über alle Trust Stores.
- Anteil vollständig validierter Ketten nach Aktivierung.
- Mean Time to Recover bei zertifikatsbedingten Störungen.

Diese Kennzahlen sind eindeutig, technisch prüfbar und anschlussfähig an bestehende Reports. Sie zeigen, ob Erneuerungen noch reaktiv erfolgen oder bereits planbar sind. Sie machen sichtbar, ob Qualität vor dem Go-live gesichert ist oder erst im Incident auffällt.

Automatisierung ist damit kein Werkzeugthema, sondern eine Betriebsform. Sichtbarkeit schafft Kontrolle. Standardisierte Erneuerungen vermeiden Überraschungen. Validierte Aktivierungen schützen vor Folgeschäden. Und ein zentraler Nachweis verbindet Technik mit Verantwortung. So wird aus einem potenziellen Störfaktor eine planbare Routine, die den SAP-Betrieb stabilisiert und auf zukünftige Laufzeitverkürzungen vorbereitet.


COMPLIANCE,
KONTROLLE,
KONTINUITÄT

COMPLIANCE, KONTROLLE, KONTINUITÄT

Compliance ist im Betrieb nur dann wirksam, wenn sie sich belegen lässt. Zertifikate eignen sich dafür besonders, denn sie verbinden Technik, Verantwortung und Nachweis in einem Prozess. Sie sichern Kommunikationswege, sie spiegeln Identitäten, sie hinterlassen Spuren, die geprüft werden können. Wer Zertifikate strukturiert betreibt, kann jederzeit zeigen, dass Schutzmaßnahmen existieren, funktionieren und überwacht werden.

Regulatorische Rahmen wie NIS2 und DORA verlangen genau diese Art von Steuerung. Gefordert sind technische und organisatorische Maßnahmen, die Risiken senken, Vorfälle früh erkennen und fristgerecht melden. In der Praxis bedeutet das ein belastbares Zusammenspiel aus Inventar, Prozessen, Rollen und Belegen. Ein aktuelles Verzeichnis aller Zertifikate schafft Sichtbarkeit. Standardisierte Abläufe für Erneuerung und Aktivierung erzeugen Wiederholbarkeit. Zuständigkeiten sorgen dafür, dass Warnungen nicht im System hängen bleiben, sondern bei den Menschen landen, die handeln müssen.

Aus auditiver Sicht zählt nicht, dass ein Zertifikat vorhanden ist. Es zählt, dass der gesamte Lebenszyklus nachweisbar gesteuert wird. Prüfer fragen nach dem Inventar, nach Ablaufüberwachung, nach Genehmigungen und Protokollen. Sie wollen sehen, dass Änderungen nachvollziehbar sind und dass es definierte Reaktionen auf Abweichungen gibt. Ein gut geführter Zertifikatsprozess liefert diese Belege automatisch mit. Jedes Ereignis wird protokolliert, jede Aktivierung hinterlässt einen Nachweis, jede Eskalation ist nachvollziehbar.

Governance gibt dem Verfahren Halt. Richtlinien legen Laufzeiten, Algorithmen, Benennungen und Prüfintervalle fest. Ein Rollenmodell trennt Ausstellung, Aktivierung und Kontrolle. Regelmäßige Reviews prüfen, ob die Praxis zur Vorgabe passt, und ob Ausnahmen begründet und dokumentiert sind. So entsteht aus einem technischen Detail ein kontinuierlicher Kontrollpunkt, der in ISMS, Risiko- und Notfallmanagement anschlussfähig ist.

Kontinuität entsteht, wenn die Abläufe zur Routine werden. Warnfenster laufen täglich. Tests der Erneuerungsmechanik finden planmäßig statt. Stichproben in produktionsnahen Stufen bestätigen, dass Ketten vollständig sind und Hostnamen passen. Abweichungen werden nicht wegerklärt, sondern als Lernpunkte in die Richtlinien zurückgeführt. Aus Vorfällen werden Verbesserungen. Aus Verbesserungen wird Stabilität.

Damit Fortschritt sichtbar bleibt, helfen wenige Kennzahlen. Drei Größen genügen, um Governance und Betrieb zusammenzubringen.
- Anteil automatisiert erneuerter Zertifikate über die gesamte Landschaft.
- Anteil fehlerfreier Ketten nach Aktivierung, gemessen durch technische Validierungen.
- Mean Time to Recover bei zertifikatsbedingten Störungen, inklusive Ursache und Abhilfe.

Diese Werte sind mehr als Zahlen. Sie zeigen, ob Zertifikate noch Anlass für Ad-hoc-Maßnahmen sind oder bereits Teil eines reifen Betriebs. Sie verbinden Nachweis mit Wirkung und machen deutlich, dass Resilienz kein Zufall ist, sondern eine Konsequenz aus Sichtbarkeit, Prozessdisziplin und klaren Zuständigkeiten. Wer diesen Zustand erreicht, erfüllt nicht nur Anforderungen. Er schafft Vertrauen in den eigenen Betrieb.

SCHLUSSWORT & AUSBLICK

Zertifikate sind kein Randthema der IT-Sicherheit, sondern ihr stilles Fundament. Sie tragen die Vertrauenskette, die jede SAP-Kommunikation, jede Integration und jede Transaktion zusammenhält.
Die vergangenen Kapitel haben gezeigt, wie eng Technik, Organisation und Verantwortung dabei miteinander verwoben sind. Verkürzte Laufzeiten, wachsende Regulierungen und hybride Landschaften machen Zertifikatsmanagement zu einer Daueraufgabe.

Wer heute noch manuell verwaltet, reagiert - wer automatisiert, gestaltet.

Automatisierung bedeutet nicht den Verlust von Kontrolle, sondern ihren Gewinn. Ein vollständiges Inventar, klare Prozesse und ein dokumentierter Lebenszyklus verwandeln ein potenzielles Risiko in einen planbaren Standard. Wenn Zertifikate sichtbar, überprüfbar und nachvollziehbar werden, entsteht die Grundlage für Resilienz.

Das ist der eigentliche Wandel: Sicherheit wird zur Routine, nicht zur Reaktion.

Für SAP-Teams ist jetzt der Moment, diesen Schritt aktiv zu gehen. Nicht, weil eine neue Vorschrift es verlangt, sondern weil Stabilität planbar geworden ist. Die Werkzeuge, die Strukturen und das Wissen existieren - was fehlt, ist der Entschluss, Routinen zu schaffen, bevor der Druck steigt.

Die kommenden Monate werden zeigen, welche Organisationen Zertifikate als Teil ihres Sicherheitsrhythmus verstehen und welche sie weiterhin als gelegentliche Pflicht betrachten. Die einen werden Ausfälle vermeiden, die anderen daraus lernen.

Zertifikate werden bleiben aber die Art, wie wir sie managen, entscheidet, ob sie Last oder Stärke sind.

Wer Vertrauen sichtbar macht, gewinnt Kontrolle.
Und wer Kontrolle strukturiert, gewinnt Sicherheit.

ANHANG A

LITERATURVERZEICHNIS

Offizielle Standards und Richtlinien

NIST SP 1800-16: Securing Web Transactions: TLS Server Certificates. National Institute of Standards and Technology, 2023. https://www.nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management

CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Version 2.0. 2024. https://cabforum.org/baseline-requirements-documents/

IETF RFC 8555: Automatic Certificate Management Environment (ACME). Internet Engineering Task Force, 2019. https://datatracker.ietf.org/doc/html/rfc8555

Mozilla Foundation: Server Side TLS – Recommended Configuration. 2024. https://wiki.mozilla.org/Security/Server_Side_TLS

Fachartikel und Berichterstattung

Heise Online. „47 Tage: CAs und Browserhersteller beschließen kürzere Laufzeit für Zertifikate." Heise News, 13. August 2024. https://www.heise.de/news/47-Tage-CAs-und-Browserhersteller-beschliessen-kuerzere-Laufzeit-fuer-Zertifikate-10352867.html

DigiCert. Shorter Certificate Lifetimes: Impact and Guidance for Enterprises. DigiCert Blog, 2024. https://www.digicert.com/blog/shorter-certificate-lifetimes-impact-enterprises

Venafi. What 90-Day Certificate Lifetimes Mean for Enterprises. Venafi Blog, 2024. https://venafi.com/blog/what-90-day-certificate-lifetimes-mean-enterprises

SAP-Dokumentation und Community

SAP Help Portal: Maintaining PSE Files in Transaction STRUST (ABAP Systems). SAP SE, 2024. https://help.sap.com/docs/SAP_NETWEAVER_750/maintenance-of-pse-files-in-strust

SAP Help Portal: Internet Communication Manager (ICM): SSL Configuration and Certificate Handling. SAP SE, 2024. https://help.sap.com/docs/SAP_NETWEAVER_750/icm-ssl-configuration

SAP Help Portal: Configuring the SAP Web Dispatcher for SSL. SAP SE, 2024. https://help.sap.com/docs/SAP_NETWEAVER_750/web-dispatcher-ssl-configuration

SAP Help Portal: Trust Configuration in the Cloud Connector and BTP. SAP SE, 2024. https://help.sap.com/docs/SAP_CLOUD_CONNECTOR/operations-guide-trust

SAP Community Blog: Configuring Certificate Lifecycle Management in SAP Systems. SAP Community, 2023. https://community.sap.com/t5/technology-blogs-by-sap/configuring-certificate-lifecycle-management/bap/13389864

SAP Note 510007: ICM and SSL – Implementation and Configuration Guidelines. SAP Support Portal, 2023. https://me.sap.com/notes/510007

ANHANG A

ANHANG A

LITERATURVERZEICHNIS

Regulatorik und Compliance

Richtlinie (EU) 2022/2555: Network and Information Security Directive (NIS2). Amtsblatt der Europäischen Union, 2022.
https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Verordnung (EU) 2022/2554: Digital Operational Resilience Act (DORA). Amtsblatt der Europäischen Union, 2022.
https://eur-lex.europa.eu/eli/reg/2022/2554/oj

ISO/IEC 27001:2022: Information Security Management Systems – Requirements. International Organization for Standardization, 2022.
https://www.iso.org/standard/82875.html

Sicherheitsarchitektur und Best Practices

NIST SP 800-52 Rev. 2: Guidelines for the Selection, Configuration, and Use of TLS Implementations. NIST, 2019.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

ETSI TS 119 495: Electronic Signatures and Infrastructures – Certificate Management. ETSI, 2023.
https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.01.01_60/ts_119495v010101p.pdf

ANHANG A

ANHANG B

GLOSSAR

Begriff	Definition
ACME (Automatic Certificate Management Environment)	Ein offener IETF-Standard (RFC 8555), der die automatische Ausstellung und Erneuerung von Zertifikaten zwischen einem Client und einer Zertifizierungsstelle ermöglicht.
ABAP (Advanced Business Application Programming)	Die Programmiersprache und Laufzeitumgebung von SAP, in der Systemfunktionen wie STRUST für die Zertifikatsverwaltung implementiert sind.
BTP (Business Technology Platform)	SAP-Plattform für Cloud-Entwicklung und Integration. Zertifikate sichern dort API-Aufrufe, Trusts und Systemverbindungen.
CA (Certification Authority)	Eine vertrauenswürdige Stelle, die digitale Zertifikate ausstellt und deren Gültigkeit bestätigt. Grundlage jeder Public-Key-Infrastruktur.
Certificate Chain (Zertifikatskette)	Die hierarchische Abfolge von Zertifikaten, die von einem Endzertifikat bis zur Root-CA führt und das Vertrauen kryptografisch absichert.
Certificate Lifetime (Zertifikatslaufzeit)	Der Zeitraum, in dem ein Zertifikat gültig ist. Neue Vorgaben verkürzen TLS-Laufzeiten auf unter 90 Tage, um Sicherheit und Automatisierung zu fördern.
Cloud Connector	Komponente zur sicheren Verbindung von On-Premises-SAP-Systemen mit der SAP BTP. Verwaltet eigene Trust Stores und Zertifikatsketten.
DORA (Digital Operational Resilience Act)	EU-Verordnung, die Finanzinstitute verpflichtet, technische Kontrollen und Cyber-Resilienzmaßnahmen nachweisbar umzusetzen.
ICM (Internet Communication Manager)	SAP-Komponente für den Datenaustausch über HTTP(S). Verantwortlich für SSL-/TLS-Kommunikation und Zertifikatsnutzung auf Serverebene.
Intermediate Certificate	Ein von einer Root-CA ausgestelltes Zwischenzertifikat, das Endzertifikate signiert und die Vertrauenskette verlängert.
ISO/IEC 27001	Internationaler Standard für Informationssicherheitsmanagementsysteme. Definiert Anforderungen an Kontrollen, Nachweise und Risikobewertung.
Keystore / Trust Store	Datei oder Datenbank, in der Zertifikate, Schlüsselpaare und Vertrauensanker gespeichert sind. SAP-Systeme nutzen unterschiedliche Stores für ABAP, Java und Cloud.

ANHANG B

ANHANG B

GLOSSAR

Begriff	Definition
MTTR (Mean Time to Recover)	Durchschnittliche Zeit, die benötigt wird, um einen Systemausfall – hier verursacht durch Zertifikatsprobleme – vollständig zu beheben.
NIS2 (Network and Information Security Directive 2)	EU-Richtlinie zur Stärkung der Cybersicherheit kritischer Infrastrukturen. Verlangt dokumentierte technische Schutzmaßnahmen, auch im Zertifikatsmanagement.
OCSP (Online Certificate Status Protocol)	Echtzeitverfahren zur Überprüfung des Sperrstatus eines Zertifikats bei der ausstellenden CA. Ergänzt die klassische CRL-Prüfung.
PSE (Personal Security Environment)	SAP-eigenes Containerformat für Zertifikate und Schlüssel. In ABAP-Systemen über STRUST verwaltet.
RFC 8555	Internetstandard, der das ACME-Protokoll beschreibt. Grundlage der automatisierten Zertifikatsverwaltung in modernen IT-Systemen.
Root CA	Oberste Zertifizierungsstelle in einer Public-Key-Infrastruktur. Dient als Vertrauensanker für alle nachgeordneten Zertifikate.
SNC (Secure Network Communication)	SAP-Technologie für verschlüsselte und authentifizierte Verbindungen zwischen SAP-Komponenten, basierend auf Zertifikaten und Kryptobibliotheken.
STRUST	SAP-Transaktion zum Erstellen, Importieren und Verwalten von Zertifikaten im ABAP-Stack. Kernwerkzeug für SSL, SNC und Secure Login.
TLS (Transport Layer Security)	Sicherheitsprotokoll zur Verschlüsselung und Authentifizierung von Datenübertragungen. Nachfolger von SSL, Standard für Web- und SAP-Kommunikation.
Trust Anchor (Vertrauensanker)	Der oberste Punkt einer Zertifikatskette, meist die Root-CA, die das Vertrauen für alle nachgelagerten Zertifikate begründet.
Web Dispatcher	SAP-Komponente zur Lastverteilung und SSL-Terminierung. Leitet Anfragen an ABAP-/Java-Systeme weiter und verwaltet Zertifikate für eingehende HTTPS-Verbindungen.

ANHANG B