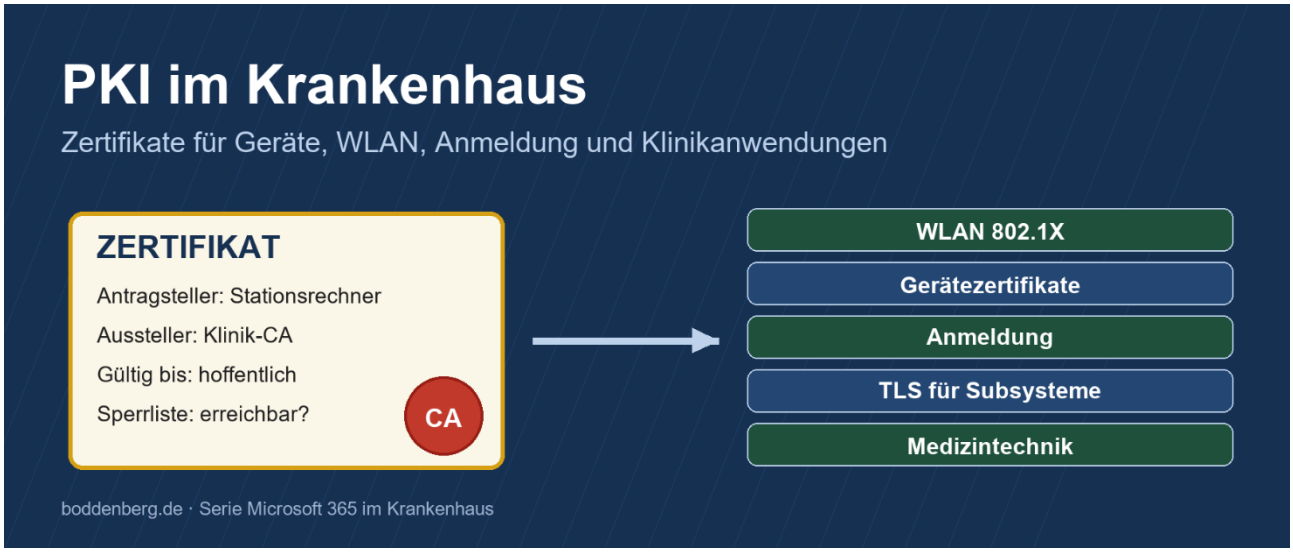
PKI im Krankenhaus: Zertifikate für Geräte, WLAN, Anmeldung und Klinikanwendungen



Wissen

Alle Beiträge der Serie rund um Kliniken, Klinikverbünde und Microsoft 365:

Microsoft 365 im Krankenhaus

Beratung

PKI-Bestandsaufnahme, Härtung und Neuaufbau mit erfahrener Begleitung:

Microsoft-365-Beratung für Krankenhäuser

Schulung

Wissen für IT-Team und Medizintechnik, damit die CA nicht zur Blackbox wird:

Microsoft-365-Schulung für Krankenhäuser

Fragen Sie in einer Klinik-IT, welche Systeme kritisch sind, hören Sie: KIS, Laborsystem, PACS, Netzwerk, Telefonie. Die Zertifizierungsstelle nennt kaum jemand. Sie steht irgendwo als virtuelle Maschine im Rechenzentrum, wurde vor Jahren für ein konkretes Projekt aufgesetzt, und seitdem läuft sie einfach. Bis eines Nachts die Stationsrechner kein WLAN mehr bekommen, die Visitenwagen offline sind und die Rufbereitschaft nach einer halben Stunde Fehlersuche bei einer Sperrliste landet, deren Gültigkeit am Vortag um 23:59 Uhr abgelaufen ist.

Die **PKI im Krankenhaus** ist das beste Beispiel für kritische Infrastruktur, die niemand als solche bestellt hat. Erst kam das WLAN mit 802.1X, dann die Gerätezertifikate für die Stationsrechner, dann die Zertifikatsanmeldung, dann TLS für die Schnittstellen zwischen KIS und Subsystemen, dann die Medizingeräte mit ihren ganz eigenen Vorstellungen von Schlüssellängen und Laufzeiten. Jede einzelne Entscheidung war vernünftig. In der Summe hängt heute an einem einzigen Dienst die Frage, ob auf Station gearbeitet werden kann.

Dieser Beitrag ordnet ein, wofür ein Krankenhaus Zertifikate braucht, wo die Grenze zur Telematikinfrastruktur verläuft und wie Sie eine über Jahre gewachsene Zertifizierungsstelle härten: Vorlagen und Berechtigungen, Sperrlisten und ihre Verfügbarkeit, Schlüsselschutz, Protokollierung und die heikle Frage, ob eine CA Zertifikate für die Domänen anderer Häuser im Verbund ausstellen darf. Er gehört zur Serie Microsoft 365 im Krankenhaus. Dass eine lokale PKI in einer Microsoft-365-Serie auftaucht, hat einen einfachen Grund: Gerätezertifikate kommen heute oft über Intune, die Anmeldung läuft hybrid über Active Directory und Entra ID, und wer Ihre CA kontrolliert, kontrolliert über kurz oder lang auch Ihre Identitäten.

Fakten: Das Wichtigste in Kürze

- Die interne CA trägt im Krankenhaus WLAN, Geräteidentität, Anmeldung und verschlüsselte Schnittstellen. Fällt sie aus oder werden ihre Sperrlisten ungültig, steht der Betrieb.
- Eine falsch berechtigte Zertifikatsvorlage kann jedes Benutzerkonto zum Domänen-Admin machen. Die CA gehört deshalb in die höchste Schutzstufe (Tier 0).
- Seit dem Windows-Update vom 9. September 2025 akzeptieren Domänencontroller für die Zertifikatsanmeldung nur noch stark zugeordnete Zertifikate; der Rückweg in den Kompatibilitätsmodus ist entfallen.
- Die Telematikinfrastruktur mit SMC-B und eHBA ist eine eigene Zertifikatswelt und nicht Teil der internen PKI.
- Zertifikate für andere Domänen im Verbund sind technisch schnell eingerichtet und organisatorisch eine Vertrauensentscheidung, die Geschäftsführung und Träger kennen müssen.

Wie die CA schleichend zur kritischen Infrastruktur wird

Eine Public-Key-Infrastruktur besteht aus Zertifizierungsstellen, Regeln, Vorlagen, Sperrlisten und Menschen, die wissen, was sie tun. In Windows-Umgebungen ist das in aller Regel Active Directory Certificate Services (ADCS): eine Root-CA, idealerweise offline, und eine oder mehrere ausstellende Unternehmens-CAs, die in Active Directory integriert sind und Zertifikate automatisch an Benutzer, Rechner und Dienste verteilen. Die Grundlagen, Architekturvarianten und typischen Fehler beschreibt der Kompetenzbereich PKI mit ADCS. Hier geht es darum, was im Krankenhaus alles darauf aufbaut.

WLAN mit 802.1X für Stationsgeräte

Der häufigste Einstieg: Stationsrechner, Visitenwagen, Tablets und Scanner sollen ins WLAN, aber nicht mit einem gemeinsamen Kennwort, das spätestens nach der zweiten Schulung auf einem Post-it am Medikamentenschrank klebt. Die Lösung ist 802.1X mit EAP-TLS: Jedes Gerät weist sich mit einem eigenen Zertifikat aus, der RADIUS-Server (oft der Netzwerkrichtlinienserver von Windows) prüft das Zertifikat und dessen Sperrstatus und weist das passende Netz zu. Das ist sicher, komfortabel und skaliert. Es macht aber auch die Erreichbarkeit der Sperrlisten zur Voraussetzung für jede WLAN-Anmeldung. Ist die Liste abgelaufen oder nicht abrufbar, lehnt der RADIUS-Server die Anmeldung in der Standardkonfiguration ab – völlig zu Recht, denn er kann nicht mehr ausschließen, dass das Zertifikat gesperrt ist.

Gerätezertifikate über Gruppenrichtlinie und Intune

Domänenmitglieder holen sich ihre Rechnerzertifikate per automatischer Registrierung aus der Unternehmens-CA. Für Geräte, die über Intune verwaltet werden – gemeinsam genutzte Tablets auf Station, Diensthandys, zunehmend auch Windows-Geräte ohne klassischen Domänenbeitritt – kommen die Zertifikate über SCEP- oder PKCS-Profile und den Intune-Zertifikatconnector, der wiederum bei der lokalen CA anfragt. Damit hängt die Geräteverwaltung aus der Cloud an einem Dienst im eigenen Rechenzentrum. Wie gemeinsam genutzte Geräte auf Station sonst organisiert werden, beschreibt der Beitrag Frontline in der Pflege: Gemeinsam genutzte Geräte, Schichtwechsel und Stationsrechner.

Eine Alternative für Intune-Geräte ist Microsoft Cloud PKI: Root- und ausstellende CA laufen als Dienst in Intune, die Sperrlisten hostet Microsoft, eine eigene ausstellende CA kann auch an eine bestehende ADCS-Root angehängt werden. Laut Microsoft-Dokumentation lassen sich pro

Mandant bis zu drei CAs anlegen, und eine Option zur Datenresidenz steht für Cloud PKI derzeit nicht zur Verfügung – ein Punkt, den Sie mit Informationssicherheit und Datenschutz vorab besprechen sollten. Cloud PKI ersetzt die lokale CA nicht für Domänencontroller, Server-TLS oder Medizintechnik; sie entlastet sie für verwaltete Endgeräte. Die Einzelheiten finden Sie in der Übersicht von Microsoft zu Microsoft Cloud PKI für Intune. Ob und wie sie lizenziert ist, prüfen Sie für Ihren Mandanten aktuell nach.

Zertifikatsbasierte Anmeldung

Smartcard oder Mitarbeiterausweis am Stationsarbeitsplatz, Windows Hello for Business mit Zertifikatsvertrauen, Anmeldung an virtuellen Desktops über einen Verbunddienst: Überall dort meldet sich ein Mensch nicht mit Kennwort, sondern mit einem Zertifikat an, das die interne CA ausgestellt hat. Der Domänencontroller prüft dabei, ob die ausstellende CA im NTAuth-Speicher der Gesamtstruktur steht, ob das Zertifikat gültig und nicht gesperrt ist und ob es eindeutig einem Konto zugeordnet werden kann.

Genau an der letzten Stelle hat Microsoft nachgeschärft. Seit dem Update vom 11. Februar 2025 laufen Domänencontroller standardmäßig im Erzwingungsmodus und verlangen eine starke Zuordnung, etwa über die SID-Erweiterung im Zertifikat (OID 1.3.6.1.4.1.311.25.2), die Unternehmens-CAs automatisch eintragen, oder über einen expliziten Eintrag im Attribut altSecurityIdentities. Mit dem Update vom 9. September 2025 ist der Registrierungsschlüssel, mit dem man in den Kompatibilitätsmodus zurückschalten konnte, entfallen. Wer Zertifikate über Offline-Vorlagen ausstellt, bei denen der Antragsteller den Namen selbst mitliefert, oder sie an einer anderen CA vorbei erzeugt, bekommt seitdem keine Anmeldung mehr. Das betrifft gern genau die Sonderfälle, die niemand dokumentiert hat. Wie die Anmeldung am Stationsarbeitsplatz insgesamt aussehen kann – Citrix, Karte, schneller Benutzerwechsel –, behandelt ein eigener Beitrag dieser Serie.

TLS für Klinikanwendungen und Subsysteme

KIS, Laborsystem (LIS), Radiologiesystem (RIS), PACS, Kommunikationsserver für die Schnittstellen, Dokumentenmanagement, Web-Oberflächen der Medizintechnik: Immer mehr Hersteller liefern ihre Systeme mit TLS aus oder verlangen es in neuen Versionen. Die Serverzertifikate dafür kommen sinnvollerweise aus der internen PKI, weil die Namen interne Namen sind und weil Sie Laufzeiten selbst bestimmen wollen. Öffentliche Zertifikate sind für interne Dienste ohnehin immer weniger geeignet: Die Höchstlaufzeit öffentlicher TLS-Zertifikate ist seit dem 15. März 2026 auf 200 Tage begrenzt, ab März 2027 auf 100 Tage und ab März 2029 auf 47 Tage, und große öffentliche Zertifizierungsstellen haben im Lauf des Jahres 2026 aufgehört, TLS-Zertifikate mit dem Verwendungszweck Client-Authentifizierung auszustellen. Für gegenseitige TLS-Authentifizierung zwischen Systemen führt damit kaum ein Weg an der eigenen PKI vorbei.

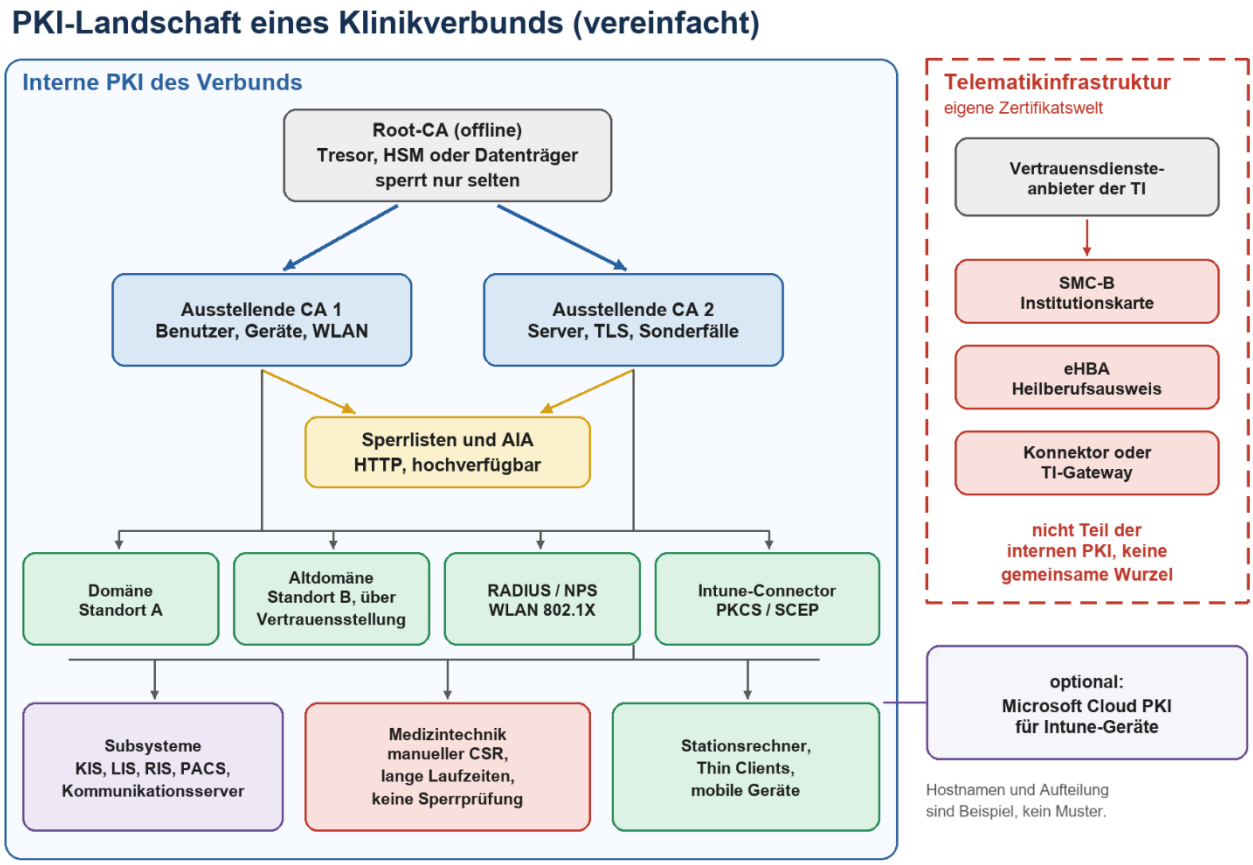
Dazu kommen die Infrastrukturdienste, die man leicht vergisst: LDAPS auf den Domänencontrollern, die Kerberos-Anmeldung per Zertifikat (PKINIT), RDP-Zertifikate, die Weboberflächen von Speichersystemen, Hypervisoren und Switches. Wer gerade NTLM zurückdrängt, landet zwangsläufig auch bei Kerberos und Zertifikaten; der Beitrag NTLM abschalten im Krankenhaus: Medizingeräte, Altanwendungen und Kerberos zeigt, warum diese Themen zusammen geplant werden sollten.

Medizingeräte mit eigenen Zertifikatsanforderungen

Und dann ist da die Medizintechnik. Ein Ultraschallgerät, das per DICOM mit TLS an das PACS senden soll, ein Infusionspumpen-Server mit Weboberfläche, ein Patientenmonitoring mit eigenem WLAN-Profil: Medizingeräte haben häufig Anforderungen, die sich mit einer modernen PKI schlecht vertragen. Der Zertifikatsantrag wird von Hand über die Gerätemenü-Oberfläche

erzeugt, die Schlüssellänge ist auf einen Wert festgelegt, der Hersteller empfiehlt zehn Jahre Laufzeit, eine Sperrprüfung findet nicht statt, und ein Zertifikatstausch erfordert einen Servicetechniker vor Ort. Änderungen an Medizinprodukten sind zudem nicht Sache der IT allein, sondern gehen über die Medizintechnik und den Hersteller.

Das ist keine Ausrede, diese Geräte aus der PKI herauszuhalten – im Gegenteil. Es ist ein Grund, für sie eigene, eng geschnittene Vorlagen zu bauen, die Laufzeiten bewusst festzulegen, die Geräte im Bestand zu dokumentieren und das Ablaufdatum jedes Zertifikats dort zu führen, wo auch Wartung und Einweisungen geführt werden. Wie Gerätenachweise zwischen CAFM und SharePoint organisiert werden können, beschreibt der Beitrag Medizinproduktebuch, Einweisungen, Gerätenachweise: MPBetreibV-Dokumentation zwischen CAFM und SharePoint.



PKI-Landschaft eines Klinikverbunds: zweistufige interne Hierarchie, hochverfügbare Sperrlisten, viele Abnehmer – und daneben die Telematikinfrastruktur als eigene Welt.

Einsatz, Vorlage, Risiko, Härtung im Überblick

Die folgende Tabelle fasst die typischen Einsatzzwecke zusammen. Sie ist bewusst knapp; in Ihrem Haus kommen wahrscheinlich ein paar Zeilen hinzu, von denen heute noch niemand weiß.

Einsatz	Typische Vorlage	Risiko	Härtung
WLAN 802.1X (Geräte)	Computer-Authentifizierung, automatische Registrierung	Sperrliste nicht erreichbar: kein WLAN auf Station	Hochverfügbare HTTP-Verteilpunkte, Überwachung der Gültigkeit, Registrierung nur für Computergruppen
Intune-Geräte	SCEP- oder PKCS-Vorlage für den Connector	Connector-Konto mit zu weiten Rechten, Namen frei wählbar	Eigene Vorlage je Profil, Connector als Tier-0-nahes System behandeln

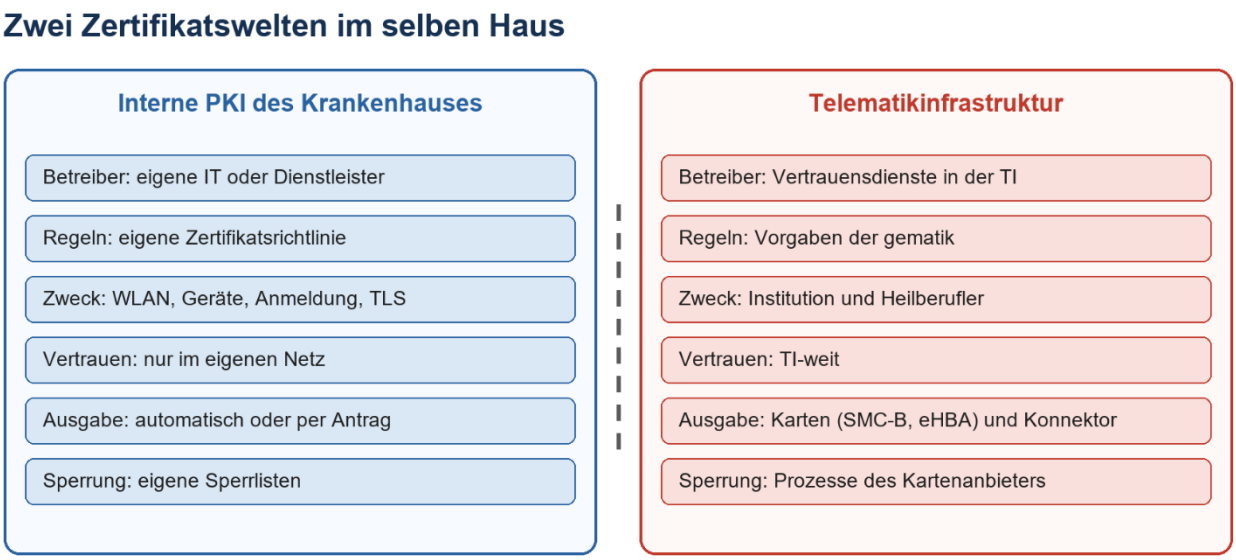
Zertifikatsanmeldung (Karte, Hello)	Smartcard-Anmeldung, Benutzer	Fremde Identität beantragbar, schwache Zuordnung	Namen aus dem AD, starke Zuordnung, Registrierungsagenten streng begrenzen
Domänencontroller	Kerberos-Authentifizierung	Fehlende oder abgelaufene DC-Zertifikate: LDAPS und PKINIT fallen aus	Automatische Registrierung, Ablaufüberwachung
TLS für KIS und Subsysteme	Webserver, eigene Kopie je Zweck	Antragsteller nennt Namen selbst, Client-Auth mit drin	Nur Serverauthentifizierung, Genehmigung durch Zertifikatverwaltung, kleine Berechtigungsgruppe
Gegenseitiges TLS zwischen Systemen	Eigene Vorlage mit Client- und Serverauth	Missbrauch als Anmeldezertifikat	Getrennte ausstellende CA oder nicht im NTAuth-Speicher, eng begrenzte Antragsteller
Medizintechnik	Offline-Vorlage, manueller Antrag	Lange Laufzeit, keine Sperrprüfung, Wildwuchs	Eigene Vorlage ohne Anmeldezweck, dokumentierte Laufzeit, Bestand mit Medizintechnik
Codesignatur und Skripte	Codesignatur	Signierte Schadsoftware	Wenige benannte Personen, Genehmigung, Schlüssel auf Token
S/MIME (falls genutzt)	Benutzer, Signatur und Verschlüsselung	Verlorene Schlüssel: verschlüsselte Mails unlesbar	Schlüsselarchivierung mit Wiederherstellungsagenten, Vier-Augen-Prinzip

Tipp: Fragen Sie zuerst: Wer hängt an der CA?

Bevor Sie irgendetwas härten, erstellen Sie eine Abhängigkeitsliste: welche Systeme Zertifikate der internen CA nutzen, wer dafür zuständig ist und was passiert, wenn das Zertifikat abläuft oder gesperrt wird. Diese Liste ist zugleich die Grundlage für den Notfallplan und für jedes Gespräch mit Medizintechnik und Herstellern.

Abgrenzung: Die Telematikinfrastruktur ist eine andere Welt

Im Krankenhaus gibt es noch eine zweite Zertifikatswelt, die mit der internen PKI regelmäßig verwechselt wird: die Telematikinfrastruktur (TI). Die Institutionskarte SMC-B weist das Krankenhaus als Einrichtung aus, der elektronische Heilberufsausweis (eHBA) die einzelne Ärztin oder den einzelnen Arzt; Konnektor oder TI-Gateway stellen die Verbindung her. Die Zertifikate dafür kommen von Vertrauensdiensteanbietern nach den Vorgaben der gematik, nicht aus Ihrer Zertifizierungsstelle.



Interne PKI und Telematikinfrastruktur: gleiche Technik, getrennte Zuständigkeiten, keine gemeinsame Wurzel.

Merkmal	Interne PKI	Telematikinfrastruktur
Zweck	WLAN, Geräte, Anmeldung, TLS im eigenen Netz	Identität von Einrichtung und Heilberuflern in der TI
Regeln	Eigene Zertifikatsrichtlinie des Hauses oder Verbunds	Vorgaben der gematik und der Kartenanbieter
Träger der Schlüssel	CA-Server, HSM, Geräte, Smartcards des Hauses	SMC-B, eHBA, Konnektor bzw. TI-Gateway
Zuständig im Haus	IT, Informationssicherheit	Meist IT gemeinsam mit TI-Verantwortlichen und Kartenverwaltung
Sperrung	Eigene Sperrlisten und Prozesse	Über die Prozesse des jeweiligen Kartenanbieters

Für die Praxis heißt das: Die TI-Zertifikate gehören nicht in den NTAuth-Speicher, die interne CA stellt keine Zertifikate aus, die eine TI-Identität vortäuschen könnten, und die Verwaltung von SMC-B und eHBA ist ein eigener Prozess mit eigenen Verantwortlichen. Berührungspunkte gibt es trotzdem: Der Konnektor oder das TI-Gateway steht in Ihrem Netz, die Kartenterminals auch, und die Ablaufdaten der Karten gehören genauso in eine Überwachung wie die Ihrer eigenen Zertifikate. Wer beides in einem Kalender pflegt, hat einen Kalender. Wer es nicht tut, hat zwei Überraschungen.

Warnung: Nicht vermischen

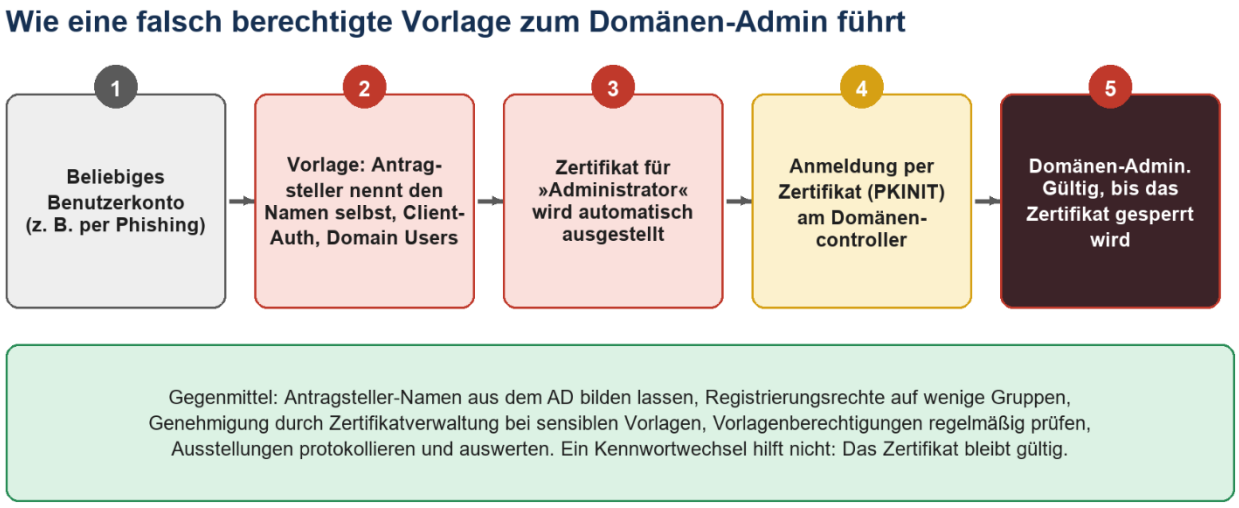
Die Idee, den eHBA oder einen anderen TI-Ausweis gleich auch für die Windows-Anmeldung zu nutzen, klingt elegant und ist ein eigenes Konzeptthema mit vielen offenen Fragen: wessen Vertrauensanker im NTAuth-Speicher landet, wie gesperrt wird und was passiert, wenn die Karte getauscht wird. Behandeln Sie das als separates Projekt, nicht als Nebeneffekt der PKI-Härtung.

Härtung: Was eine gewachsene Krankenhaus-CA braucht

Die gute Nachricht: Die Schwachstellen von ADCS sind gut erforscht und gut dokumentiert. Die schlechte: Sie sind auch bei Angreifern gut bekannt. In der Sicherheitsforschung sind Fehlkonfigurationen von Zertifikatsvorlagen und CAs seit Jahren als eigene Angriffsklasse katalogisiert, und Werkzeuge, die sie automatisch finden, sind frei verfügbar. In Ransomware-Fällen gehört die CA deshalb zu den Systemen, die zuerst angeschaut werden – von den Angreifern ebenso wie später von den Forensikern.

Vorlagen und Berechtigungen

Die gefährlichste Fehlkonfiguration ist schnell beschrieben: eine Vorlage, bei der der Antragsteller den Namen im Zertifikat selbst angeben darf, die den Verwendungszweck Client-Authentifizierung enthält, die ohne Genehmigung ausgestellt wird und für die eine breite Gruppe wie Domänenbenutzer die Registrierung erlaubt ist. Mit einer solchen Vorlage beantragt jedes beliebige Konto ein Zertifikat auf den Namen eines Administrators und meldet sich damit am Domänencontroller an. Eine solche Vorlage entsteht selten aus Absicht, sondern meist, weil ein Hersteller für sein Subsystem eine Kopie der Webserver-Vorlage braucht, der Name frei wählbar sein muss und die Berechtigung testweise großzügig gesetzt wurde. Testweise. Vor sechs Jahren.



Vom Benutzerkonto zum Domänen-Admin in fünf Schritten – und ein Kennwortwechsel hilft nicht.

Die Gegenmaßnahmen sind unspektakulär und wirksam:

- **Namen aus Active Directory bilden lassen.** Wo der Antragsteller den Namen selbst angeben muss (typisch bei Servern und Medizingeräten), enthält die Vorlage keine Client-Authentifizierung und wird erst nach Genehmigung durch die Zertifikatverwaltung ausgestellt.
- **Registrierungsrechte eng fassen.** Statt Domänenbenutzer oder Authentifizierte Benutzer eine benannte Gruppe je Zweck. Schreibrechte auf Vorlagen nur für die PKI-Administration.
- **Altvorlagen zurückziehen.** Vorlagen, die auf der CA veröffentlicht, aber nicht mehr gebraucht werden, nehmen Sie von der CA. Was nicht angeboten wird, kann nicht missbraucht werden.
- **CA-Schalter prüfen.** Die Einstellung, die den Antragstellern erlaubt, zusätzliche alternative Namen an jede Anfrage anzuhängen, hat auf einer Unternehmens-CA nichts verloren.
- **Webregistrierung absichern oder abschalten.** Die HTTP-Registrierungsschnittstellen der CA sind ein klassisches Ziel für NTLM-Relay. Wo sie nicht gebraucht werden, kommen sie weg; wo doch, gehören HTTPS und erweiterter Schutz für die Authentifizierung dazu.

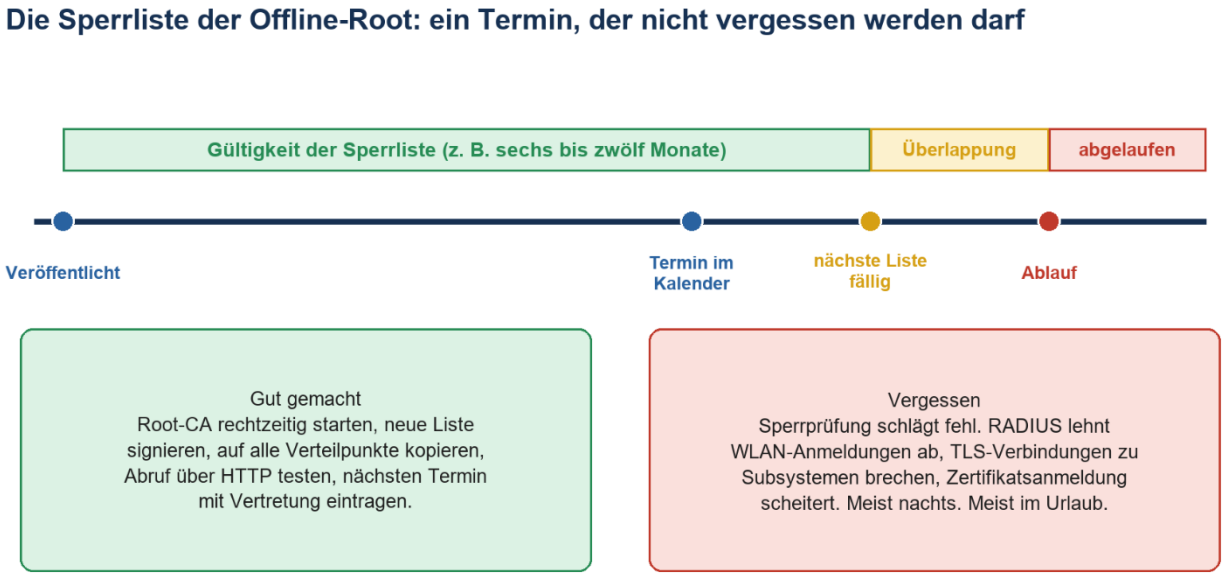
- **Rollen trennen.** CA-Administration, Zertifikatverwaltung und Sicherung sind unterschiedliche Rollen. Im kleinen Haus sind es vielleicht dieselben zwei Personen – dann wenigstens bewusst und dokumentiert.

Wenn Microsoft Defender for Identity im Einsatz ist, kann ein Sensor auf der CA Fehlkonfigurationen in Vorlagen und CA-Einstellungen als Sicherheitsbewertung anzeigen. Ein Ersatz für die eigene Prüfung ist das nicht, aber eine gute zweite Meinung. Mehr zu Erkennung und Absicherung im Zusammenspiel mit Microsoft 365 finden Sie im Kompetenzbereich Microsoft 365 Security.

Sperrlisten und ihre Verfügbarkeit

Sperrlisten sind das Bauteil, das im Alltag niemand sieht und im Ernstfall alle. Jedes Zertifikat enthält einen oder mehrere Verteilpunkte, an denen die prüfende Stelle die aktuelle Sperrliste abholen soll. Ist die Liste dort nicht abrufbar oder abgelaufen, schlagen strenge Prüfer fehl – und RADIUS für WLAN, Domänencontroller für die Zertifikatsanmeldung und viele TLS-Clients sind strenge Prüfer.

- **HTTP als Verteilpunkt.** LDAP-Pfade funktionieren nur für Domänenmitglieder und sind für Medizingeräte, Linux-Systeme und Intune-Geräte außerhalb des Netzes nutzlos. Ein HTTP-Verteilpunkt auf mindestens zwei Webservern, gern hinter einem internen Lastverteiler, ist Pflicht.
- **Laufzeiten und Überlappung.** Die Basis-Sperrliste der ausstellenden CA sollte länger gültig sein als ein langes Wochenende plus Reaktionszeit, mit ausreichender Überlappung. Delta-Sperrlisten verkürzen die Zeit bis zur Wirksamkeit einer Sperrung.
- **Die Root-CA nicht vergessen.** Die Sperrliste der Offline-Root läuft typischerweise nach einigen Monaten ab. Dann muss jemand die Root-CA starten, eine neue Liste signieren und verteilen. Dieser Termin gehört in einen Kalender mit Vertretung, nicht in das Gedächtnis eines einzelnen Administrators.
- **Überwachen.** Die Restlaufzeit jeder Sperrliste und die Erreichbarkeit jedes Verteilpunkts gehören in das Monitoring, mit Alarm deutlich vor dem Ablauf.
- **OCSP abwägen.** Ein Online-Responder beantwortet Statusanfragen einzeln und schneller. Er ist ein weiterer Dienst, der verfügbar sein muss; für viele Häuser reichen gut betriebene Sperrlisten.



Die Sperrliste der Offline-Root: Wer den Termin verpasst, legt WLAN, TLS und Zertifikatsanmeldung gleichzeitig still.

Warnung: Der Klassiker der Rufbereitschaft

Sperrlisten laufen nicht im Büroalltag ab, sondern genau dann, wenn sie ablaufen – also auch nachts, am Wochenende und am zweiten Weihnachtsfeiertag. Wenn die Notfallanweisung für diesen Fall nur aus dem Satz besteht, dass der Kollege Bescheid weiß, der gerade in Urlaub ist, haben Sie den Notfall bereits geplant. Schreiben Sie die Schritte zur Notverlängerung einer Sperrliste so auf, dass die Rufbereitschaft sie ausführen kann.

Schlüsselschutz

Der private Schlüssel der CA ist das Kronjuwel. Wer ihn besitzt, kann beliebige Zertifikate ausstellen, die Ihre gesamte Umgebung für echt hält – und zwar außerhalb jeder Protokollierung auf Ihrer CA. Ein solcher Schlüssel gehört deshalb in ein Hardware-Sicherheitsmodul (HSM) oder, wo das nicht wirtschaftlich ist, mindestens auf einen Server mit TPM-gestütztem Schlüsselspeicher, der wie ein Domänencontroller behandelt wird: Tier 0, kein Internetzugang, Anmeldung nur von privilegierten Administrationsarbeitsplätzen, keine fremden Agenten.

Für die Root-CA gilt das erst recht. Offline heißt offline: ausgeschaltet, nicht im Netz, die Sicherung des Schlüssels mit Vier-Augen-Prinzip an zwei getrennten Orten. Klingt selbstverständlich, ist es aber nicht, wenn die Root-CA als virtuelle Maschine auf demselben Hypervisor liegt wie alles andere und die Datensicherung sie jede Nacht brav mitsichert. Dann ist sie nicht offline, sondern nur ausgeschaltet – und ihr Schlüssel liegt in jedem Backup, auf das ein Angreifer mit Zugriff auf die Sicherung zugreifen kann.

Wichtig: Wiederherstellung ist Teil des Schlüsselschutzes

Eine CA, deren Wiederherstellung nie geübt wurde, ist eine Wette. Testen Sie die Rücksicherung von Datenbank und Schlüssel auf einem isolierten System, dokumentieren Sie die Schritte und hinterlegen Sie die Kennwörter und Token so, dass sie im Notfall verfügbar sind – aber nicht für jeden. Für die Notfallübung der Klinik-IT ist der Ausfall der CA ein lohnendes Szenario.

Protokollierung

Standardmäßig protokolliert eine Windows-CA deutlich weniger, als man im Ernstfall gern hätte. Damit Ausstellungen, Sperrungen, Vorlagenänderungen und Konfigurationsänderungen in der Ereignisanzeige landen, müssen Sie die Überwachung an der CA einschalten und zusätzlich die Objektzugriffsüberwachung im Betriebssystem aktivieren. Diese Ereignisse gehören an ein zentrales Protokollsystem und in eine regelmäßige Auswertung. Die interessanteste Frage dabei ist einfach: Wurden Zertifikate ausgestellt, deren Inhaber nicht zum Antragsteller passt, oder Anmeldezertifikate für privilegierte Konten, die niemand bewusst beantragt hat?

Protokolle über Zertifikatsanträge und Anmeldungen enthalten personenbezogene Daten. Zweck, Aufbewahrungsfrist und Zugriff sollten deshalb mit dem Datenschutzbeauftragten abgestimmt sein; wo Auswertungen Rückschlüsse auf Verhalten oder Leistung erlauben könnten, ist die Interessenvertretung früh einzubinden. Je nach Trägerschaft gelten das Betriebsverfassungsgesetz, das Personalvertretungsrecht des Bundes oder des jeweiligen Landes oder die kirchlichen Mitarbeitervertretungsordnungen, und die Regelungen unterscheiden sich im Detail. Mehr dazu im Beitrag Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft.

Zertifikate für andere Domänen im Verbund – darf die CA das?

In gewachsenen Klinikverbünden gibt es selten eine einzige Domäne. Häuser wurden übernommen, Gesellschaften gegründet, Altdomänen über Vertrauensstellungen angebunden. Und irgendwann kommt die Frage: Kann die CA des Verbunds nicht auch die Rechner und Benutzer des übernommenen Hauses versorgen? Technisch: ja, in mehreren Varianten. Die interessantere Frage ist, was man damit erlaubt.

- **Registrierung über Gesamtstrukturgrenzen.** Eine Unternehmens-CA kann über eine bidirektionale Gesamtstruktur-Vertrauensstellung auch Antragsteller aus einer anderen Gesamtstruktur bedienen, wenn Vorlagen und Konfiguration dorthin repliziert werden. Das ist praktisch und schafft eine dauerhafte Abhängigkeit.
- **NTAuth-Speicher der anderen Domäne.** Damit Zertifikate einer CA zur Anmeldung in einer anderen Gesamtstruktur taugen, muss diese CA dort im NTAuth-Speicher stehen. Damit vertraut die andere Gesamtstruktur jeder Anmeldung, die diese CA bescheinigt – für jedes zuordenbare Konto. Die CA wird damit für die andere Gesamtstruktur zu Tier 0.
- **Einschränkungen per Namensbeschränkung.** Über eine qualifizierte Unterordnung mit Namensbeschränkungen lässt sich festlegen, für welche Namensräume eine CA Zertifikate ausstellen darf, die in der anderen Umgebung akzeptiert werden. Das ist aufwendiger, begrenzt aber den Schaden.

Hinter der Technik stehen organisatorische Fragen, die nicht die IT allein beantworten kann: Sind die Häuser rechtlich eigenständige Gesellschaften mit eigener Geschäftsführung? Wer trägt die Verantwortung, wenn die CA des einen Hauses kompromittiert wird und damit die Domäne des anderen fällt? Ist das in den Verträgen zwischen den Gesellschaften und in der Zertifikatsrichtlinie geregelt? Und passt es zur Zielarchitektur – oder wird damit ein Übergangszustand zementiert, den man eigentlich mit der Konsolidierung der Domänen auflösen will? Wie Vertrauensstellungen und Altdomänen im Verbund sauber geordnet werden, beschreibt der Beitrag Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung; die Mandantenfrage auf der Microsoft-365-Seite behandelt Klinikverbund und Tenant-Strategie: Ein Mandant, mehrere Häuser, gewachsene Domänen.

> **Wichtig: Hinweis: keine Rechtsberatung**
>
> Ob und unter welchen Bedingungen eine Gesellschaft im Verbund für eine andere Zertifikate ausstellen und damit faktisch über deren Anmeldungen mitentscheiden darf, ist auch eine Frage der Verträge, der Auftragsverarbeitung und der Verantwortlichkeiten nach Datenschutzrecht. Die Antwort hängt von Trägerschaft, Gesellschaftsstruktur und Landesrecht ab. Klären Sie das mit Ihrer Rechtsabteilung oder externer Rechtsberatung, bevor die Technik Tatsachen schafft.

Die Rechtslage als Rahmen, nicht als Rezept

§ 391 SGB V verpflichtet Krankenhäuser, angemessene organisatorische und technische Vorkehrungen nach dem Stand der Technik zu treffen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme zu vermeiden. Die Vorschrift verweist auf die Möglichkeit, einen branchenspezifischen Sicherheitsstandard anzuwenden, dessen Eignung das BSI festgestellt hat. Für Häuser, die als Betreiber kritischer Anlagen den Pflichten des BSI-Gesetzes unterliegen, gelten stattdessen dessen Vorgaben. Der B3S „Medizinische Versorgung“ der Deutschen Krankenhausgesellschaft liegt in Version 1.3.1 vor, einer redaktionellen Überarbeitung vom 6. Januar 2026 der Version 1.3 mit Stand 10. Oktober 2025; die Eignung hat das BSI am 3. November 2025 für drei Jahre festgestellt.

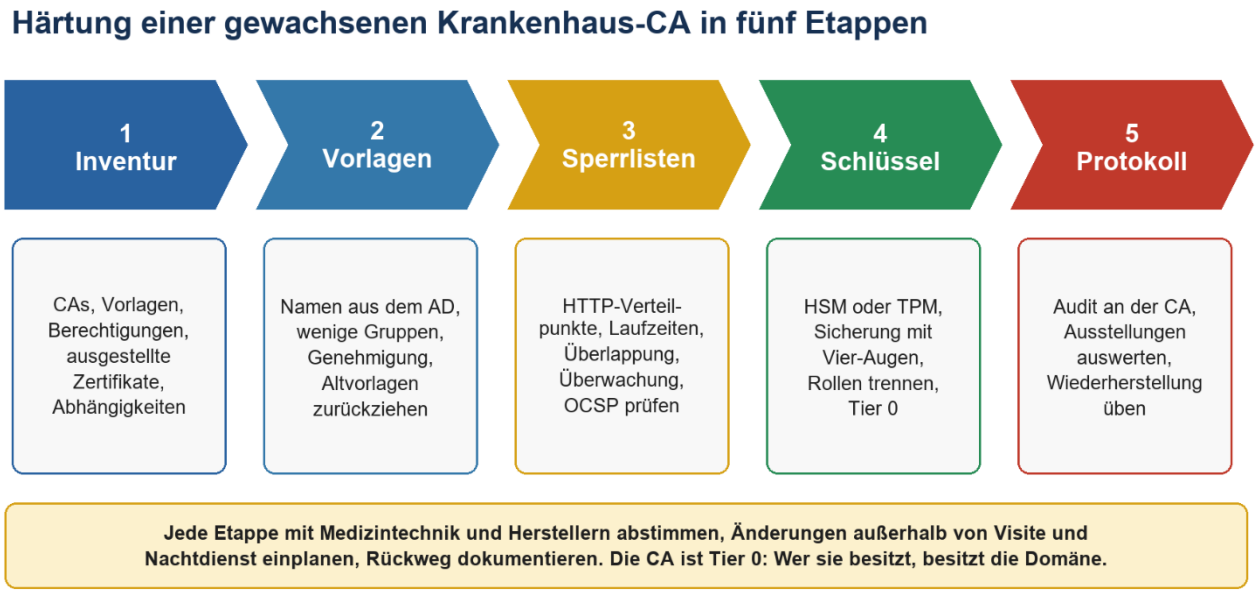
Eine Zertifikatsvorlage steht dort nicht. Aber eine PKI, deren Ausfall den Stationsbetrieb lahmlegt und deren Fehlkonfiguration die Übernahme der Domäne erlaubt, ist offensichtlich ein System, an dem sich der Stand der Technik messen lassen muss. Wie sich die Sicherheitspflichten insgesamt auf die Microsoft-365-Umgebung auswirken, steht im Beitrag NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten; die technische Umsetzung beschreibt NIS2 technisch umsetzen mit Microsoft 365.

Aus der Praxis: eine über Jahre gewachsene Krankenhaus-CA härten

Aus der Praxis: Begleitung eines Krankenhausverbunds mit mehreren Standorten

In einem Krankenhausverbund mit mehreren Standorten, den ich über viele Jahre begleitet habe, waren PKI-Aufbau und -Härtung kein Einzelprojekt, sondern ein Strang in einer größeren Aufräumarbeit, zu der auch Vertrauensstellungen zwischen den Domänen, die NTLM-Abschaltung und Kerberos gehörten. Die CA war über die Jahre mit den Anforderungen gewachsen, und mit jeder neuen Anforderung stieg auch das, was von ihr abhing.

Drei Erfahrungen tragen über diesen Einzelfall hinaus. Erstens: Härtung geht nur in Etappen. Wer Vorlagen und Berechtigungen auf einen Schlag bereinigt, ohne zu wissen, wer daran hängt, erfährt es über die Störungsmeldungen. Zweitens: Die Themen hängen zusammen. Wer NTLM zurückdrängt, braucht funktionierende Zertifikate und Kerberos; wer Vertrauensstellungen ordnet, muss klären, wessen CA wo vertraut wird. Drittens: Die wichtigste Härtungsmaßnahme ist organisatorisch – eine Zuständigkeit, die über einzelne Personen hinaus Bestand hat, und eine Dokumentation, mit der auch die Rufbereitschaft etwas anfangen kann.



Fünf Etappen für die Härtung einer gewachsenen CA – jede mit Abstimmung und dokumentiertem Rückweg.

Etappe für Etappe

Etappe	Was passiert	Wer muss mitreden
1 Inventur	CAs, veröffentlichte Vorlagen, Berechtigungen, ausgestellte und bald ablaufende Zertifikate,	IT, Medizintechnik, Systembetreuer der Subsysteme

	Verteilpunkte, Abhängigkeiten erheben	
2 Vorlagen	Gefährliche Kombinationen beseitigen, Gruppen einschränken, Genehmigung einführen, Altvorlagen zurückziehen	IT, Hersteller betroffener Systeme
3 Sperrlisten	HTTP-Verteilpunkte hochverfügbar machen, Laufzeiten festlegen, Root-Termine planen, Überwachung einrichten	IT, Netzwerk, Rufbereitschaft
4 Schlüssel	HSM oder TPM, Root wirklich offline, Sicherung mit Vier-Augen-Prinzip, CA als Tier 0 behandeln	IT-Leitung, Informationssicherheit, Geschäftsführung (Budget)
5 Protokoll und Notfall	CA-Überwachung einschalten, zentral auswerten, Wiederherstellung üben, Notfallanweisung schreiben	Informationssicherheit, Datenschutz, Interessenvertretung

Zertifikatsrichtlinie als Verfahrensanweisung

Die Regeln der PKI – wer welche Zertifikate bekommt, wer Anträge genehmigt, wie gesperrt wird, wer die Root-CA bedient – gehören aufgeschrieben. In der PKI-Welt heißen solche Dokumente Zertifikatsrichtlinie und Erklärung zum Zertifizierungsbetrieb. Im Krankenhaus heißen sie Verfahrensanweisung, und sie können dort leben, wo alle anderen Verfahrensanweisungen auch gelenkt werden: im QM-Handbuch mit Freigabe, Versionierung und Wiedervorlage. Das hat einen angenehmen Nebeneffekt: Im nächsten Zertifizierungsaudit nach KTQ oder ISO 9001 und bei der Prüfung nach § 391 SGB V oder BSIG liegt der Nachweis dort, wo der Auditor ihn erwartet. Wie das geht, zeigt der Beitrag QM-Handbuch mit SharePoint: Dokumentenlenkung im Krankenhaus, die im Audit hält.

Wer am Tisch sitzen muss

Rolle	Aufgabe rund um die PKI
Geschäftsführung	Auftrag, Budget für HSM und Redundanz, Entscheidung über Zertifikate für andere Gesellschaften im Verbund
IT-Leitung	Verantwortung für Betrieb und Härtung, Zuständigkeit über Personen hinaus sichern
IT-Administration	Vorlagen, Sperrlisten, Überwachung, Wiederherstellung, Notfallanweisung
Medizintechnik	Bestand zertifikatsabhängiger Medizingeräte, Abstimmung mit Herstellern, Laufzeiten
Informationssicherheitsbeauftragter	Risikobewertung, Einordnung in B3S oder BSIG-Pflichten, Auswertung der Protokolle
Datenschutzbeauftragter	Zweck und Aufbewahrung von Protokollen, Auftragsverarbeitung bei Cloud PKI oder Dienstleistern
Qualitätsmanagementbeauftragter	Zertifikatsrichtlinie als gelenkte Verfahrensanweisung
Betriebsrat, Personalrat oder MAV	Mitbestimmung bei Kartenanmeldung und Auswertung

	personenbezogener Protokolle

Wenn Sie die Bestandsaufnahme und die Härtung nicht allein stemmen wollen, unterstützt die Microsoft-365-Beratung für Krankenhäuser von der Inventur über die Vorlagenbereinigung bis zur Notfallanweisung. Damit das Wissen anschließend im Haus bleibt und nicht mit einer Person in Rente geht, gibt es die Microsoft-365-Schulung für Krankenhäuser.

Häufige Fragen zur PKI im Krankenhaus

Brauchen wir überhaupt eine eigene PKI?

Sobald Sie WLAN mit 802.1X, Zertifikatsanmeldung, TLS für interne Systeme oder gegenseitige Authentifizierung zwischen Systemen betreiben, ja. Öffentliche Zertifikate sind für interne Namen nicht vorgesehen, ihre Laufzeiten werden immer kürzer, und für Client-Authentifizierung werden sie praktisch nicht mehr ausgestellt. Die Frage ist also nicht, ob, sondern wie gut die eigene PKI betrieben wird.

Reicht Microsoft Cloud PKI statt ADCS?

Für Intune-verwaltete Endgeräte kann Cloud PKI die lokale CA deutlich entlasten. Für Domänencontroller, Server-TLS, Medizintechnik mit manuellen Anträgen und die klassische automatische Registrierung bleibt in der Regel eine lokale CA nötig. Prüfen Sie außerdem, ob die fehlende Datenresidenz-Option und die Begrenzung auf drei CAs pro Mandant für Ihr Haus tragbar sind.

Wie oft muss die Offline-Root eingeschaltet werden?

Mindestens so oft, wie es die Gültigkeit ihrer Sperrliste verlangt, und zusätzlich zur Verlängerung der ausstellenden CAs. Legen Sie den Rhythmus in der Zertifikatsrichtlinie fest und tragen Sie die Termine mit Vertretung ein. Ein Termin, den nur eine Person kennt, ist ein Ausfall mit Ansage.

Was tun mit Medizingeräten, die keine Sperrlisten prüfen können?

Dokumentieren, eng begrenzen, ausgleichen. Diese Geräte bekommen Zertifikate aus einer eigenen Vorlage ohne Anmeldezweck, mit bewusst gewählter Laufzeit und eingetragen im Gerätebestand. Kompensieren lässt sich das Risiko über Netzsegmentierung und begrenzte Kommunikationsbeziehungen. Bei der nächsten Beschaffung gehört die Zertifikatsfähigkeit in das Lastenheft.

Gehören SMC-B und eHBA in unsere PKI?

Nein. Sie gehören zur Telematikinfrastruktur mit eigenen Vertrauensdiensteanbietern und Regeln. Ihre interne CA stellt dafür nichts aus, und die TI-Zertifikate gehören nicht in Ihren NTAuth-Speicher. Die Ablaufdaten der Karten sollten Sie trotzdem überwachen – nur eben in einem eigenen Prozess.

Woran erkennen wir eine gefährliche Zertifikatsvorlage?

Am Zusammentreffen von vier Eigenschaften: Der Antragsteller darf den Namen selbst angeben, die Vorlage erlaubt Client-Authentifizierung, sie wird ohne Genehmigung ausgestellt, und eine breite Gruppe darf sich registrieren. Jede einzelne Eigenschaft kann berechtigt sein, die Kombination ist es nicht. Prüfen Sie außerdem, wer Schreibrechte auf Vorlagen und auf die CA selbst hat.

Was hat die PKI mit Microsoft 365 zu tun?

Mehr als man denkt. Gerätezertifikate für Intune-verwaltete Geräte, zertifikatsbasierte Anmeldung in hybriden Umgebungen und die Tatsache, dass Ihr lokales Active Directory meist die Quelle der synchronisierten Identitäten ist, verbinden beide Welten. Wer über eine falsch konfigurierte Vorlage Domänen-Admin wird, hat einen kurzen Weg zum Synchronisierungsserver und damit in den Tenant. Mehr dazu im Kompetenzbereich Microsoft Entra ID.

Fazit: Die CA ist Tier 0, auch wenn sie nie so bestellt wurde

Die PKI im Krankenhaus wächst mit jeder vernünftigen Einzelentscheidung: WLAN mit 802.1X, Gerätezertifikate, Zertifikatsanmeldung, TLS für Subsysteme, Medizintechnik. Irgendwann hängt an ihr der Stationsbetrieb, und eine falsch berechtigte Vorlage reicht für die Übernahme der Domäne. Das ist kein Grund zur Panik, sondern ein Grund, die CA so zu behandeln wie das, was sie geworden ist: ein System der höchsten Schutzstufe mit hochverfügbaren Sperrlisten, geschütztem Schlüssel, sauberen Vorlagen, Protokollierung und einer Zuständigkeit, die nicht an einer einzelnen Person hängt.

Die Telematikinfrastruktur bleibt dabei eine eigene Welt, und Zertifikate für andere Häuser im Verbund sind eine Vertrauensentscheidung, die nicht im Serverraum fallen sollte. Wer in Etappen härtet und jede Etappe mit Medizintechnik und Herstellern abstimmt, erreicht viel, ohne den Betrieb zu gefährden. Und wenn die Sperrliste der Root-CA das nächste Mal abläuft, steht der Termin längst im Kalender. Mit Vertretung.

Weiter im Thema

› Kompetenzbereich PKI mit ADCS

› NTLM abschalten im Krankenhaus: Medizingeräte, Altanwendungen und Kerberos

› Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung

› NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten

› Kompetenzbereich Kerberos

› Microsoft 365 im Krankenhaus: Warum die Klinik anders tickt als Verwaltung und Mittelstand