

PKI Diagnostiker: Bestandsaufnahme und Härtung für deine Windows-PKI

Deine Windows-PKI stellt seit Jahren Zertifikate aus, aber welche genau, für wen und wann sie ablaufen, weiß keiner so richtig. Der PKI Diagnostiker liest die ausgestellten Zertifikate deiner Active Directory Certificate Services aus, macht daraus ein Inventar mit Historie und Ablauf-Monitor und prüft die PKI auf bekannte Fehlkonfigurationen. Der Scan ist in Sekunden durch, die Express-Edition kostet nichts.

Die Zertifizierungsstelle, die einfach läuft

Jede gewachsene Windows-Umgebung hat sie: die interne Zertifizierungsstelle, die vor vielen Jahren in einem Projekt aufgesetzt wurde. Der Kollege, der sie eingerichtet hat, ist längst in einer anderen Abteilung. Seitdem läuft sie einfach. Sie stellt Zertifikate für Webserver, Domänencontroller, WLAN, VPN und alles Mögliche aus, und niemand schaut so genau hin. Bis an einem Dienstagmorgen der interne Webdienst mit einer Zertifikatswarnung aufschlägt und das halbe Haus beim Helpdesk anruft.

Die Fehlersuche läuft dann nach Schema F: Welches Zertifikat ist abgelaufen? Wer hat es beantragt? Gibt es ein Nachfolgezertifikat, das nur nicht eingebunden wurde? Und während man das herausfindet, fällt auf, dass die Konsole der Zertifizierungsstelle mehrere tausend ausgestellte Zertifikate auflistet, sortiert nach Anforderungs-ID. Eine Übersicht ist das nicht, eher ein Telefonbuch ohne Alphabet.

Kürzere Laufzeiten, mehr Gelegenheiten für Ausfälle

Die Laufzeiten öffentlicher TLS-Zertifikate werden schrittweise verkürzt: seit März 2026 auf höchstens 200 Tage, ab März 2027 auf 100 Tage und ab März 2029 auf 47 Tage. Das betrifft zunächst öffentliche Zertifikate, verändert aber den Rhythmus im ganzen Zertifikatsbetrieb. Mehr Wechsel bedeuten mehr Gelegenheiten, einen zu verpassen. Wer seinen Bestand nicht kennt, verliert hier schnell den Überblick.

Und dann gibt es noch die Seite, über die ungern geredet wird: Eine falsch konfigurierte Zertifikatvorlage kann einem Angreifer den Weg zum Domänenadministrator ebnen. Die bekannten Angriffsklassen rund um ADCS, unter dem Kürzel ESC durchnummeriert, sind keine Theorie, sondern ein Standardkapitel in jedem ernst gemeinten Angriff auf ein Active Directory.

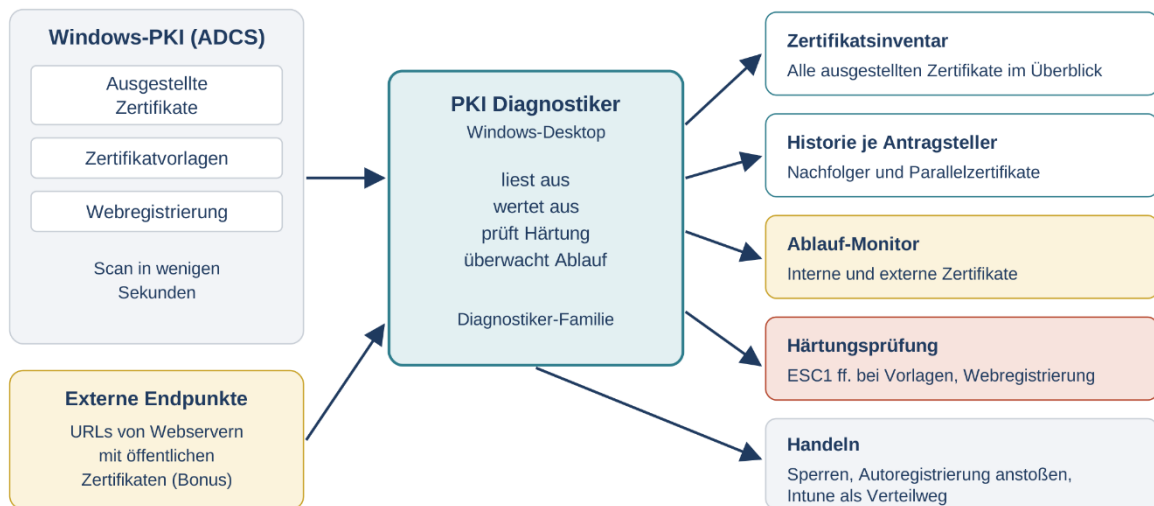
Kurz gesagt hat die interne PKI zwei Gesichter. Im Betrieb ist sie ein stiller Dienstleister, dessen Fehler sich als Ausfall bemerkbar machen. In der Sicherheit ist sie ein Schlüsselbund für das gesamte Active Directory, dessen Fehler sich überhaupt nicht bemerkbar machen, bis jemand sie ausnutzt. Beides lässt sich nur beurteilen, wenn du weißt, was die CA ausgestellt hat und wie sie eingerichtet ist. Genau an dieser Stelle setzt der PKI Diagnostiker an.

Was der PKI Diagnostiker macht

Der PKI Diagnostiker ist ein Windows-Desktop-Werkzeug aus der Diagnostiker-Familie, eine Eigenentwicklung von boddenberg.de. Er liest die ausgestellten Zertifikate deiner Windows-PKI, also der **Active Directory Certificate Services (ADCS)**, aus und wertet sie aus. Aus einer endlosen Liste von Anforderungen wird ein Inventar, das du filtern, sortieren und verstehen kannst.

Dazu kommt die Härtingsprüfung: Der Diagnostiker sucht nach bekannten Fehlkonfigurationen, etwa den ESC-Angriffsklassen (ESC1 und folgende) bei Zertifikatvorlagen und der Webregistrierung. Damit beantwortet er zwei Fragen auf einmal: Was hat meine CA eigentlich ausgestellt? Und ist sie so eingerichtet, dass sie mir nicht selbst gefährlich wird?

PKI Diagnostiker: Funktionsprinzip



Funktionsprinzip: Der PKI Diagnostiker liest ausgestellte Zertifikate, Vorlagen und Webregistrierung der ADCS-Zertifizierungsstelle aus und erzeugt daraus Inventar, Historie, Ablauf-Monitor und Härtingsbefunde. Externe Endpunkte kommen als Bonusfunktion hinzu.

Sekunden statt Stunden

Der Scan einer Zertifizierungsstelle ist nach Sekunden durch. Deshalb gibt es beim PKI Diagnostiker auch kein Modell, das nach Durchlaufen abrechnet: Du scannst, wann und so oft du willst.

Die Funktionen im Detail

Zertifikatsinventar

Das Fundament ist das Inventar: alle ausgestellten Zertifikate deiner CA in einer Übersicht. Damit weißt du endlich, wie viele Zertifikate tatsächlich im Umlauf sind, welche Vorlagen genutzt werden und wo sich Altlasten angesammelt haben. Das klingt banal, ist aber in vielen Umgebungen das erste Mal, dass jemand den Bestand wirklich vor sich sieht.

Historie je Antragsteller

Für jeden Antragsteller (Subject) zeigt der Diagnostiker die Zertifikats-Historie. Du siehst, welche Zertifikate für einen Server oder Dienst nacheinander ausgestellt wurden. Das ist Gold wert, wenn du herausfinden musst, ob ein Nachfolgezertifikat existiert, ob es mehrere parallele gültige Zertifikate gibt oder warum ein Dienst ein altes Zertifikat verwendet.

Ablauf-Monitor

Der Ablauf-Monitor zeigt dir, welche Zertifikate demnächst ablaufen. Damit wird aus der Dienstagmorgen-Überraschung ein Eintrag auf der Wochenplanung. Ein Zertifikat zu erneuern, bevor es abläuft, kostet ein paar Minuten. Hinterher kostet es einen Vormittag und einige Nerven. Gerade bei Zertifikaten, die nur alle paar Jahre fällig werden, hat das niemand im Kopf. Der Ablauf-Monitor hat es im Blick, auch wenn der Kollege, der das Zertifikat damals beantragt hat, längst nicht mehr im Haus ist und die Erinnerung im Kalender mit seinem Postfach verschwunden ist.

Härtungsprüfung

Die Härtingsprüfung untersucht die PKI auf bekannte Fehlkonfigurationen, insbesondere die ESC-Angriffsklassen bei Zertifikatvorlagen und der Webregistrierung. Gerade Vorlagen sind oft über Jahre kopiert, angepasst und wieder kopiert worden. Eine einzige zu großzügig eingestellte Vorlage reicht, und aus einem normalen Benutzerkonto wird mit etwas Geschick ein sehr privilegiertes.

Sperren, Autoregistrierung und Intune

Zum Funktionsumfang gehören außerdem das **Sperren von Zertifikaten** als eigenes Modul, das **Anstoßen der Autoregistrierung** und die Unterstützung von **Intune als Verteilweg**. Damit kannst du aus der Analyse heraus direkt handeln, statt in drei verschiedene Konsolen zu wechseln.

Bonusfunktion: externe Endpunkte

Nicht jedes kritische Zertifikat stammt aus deiner eigenen CA. Deshalb kannst du als Administrator zusätzlich die URLs von Webservern mit öffentlichen Zertifikaten eintragen. Der Diagnostiker behält diese Endpunkte im Blick und schickt dir Ablaufbenachrichtigungen. Bei immer kürzeren Laufzeiten öffentlicher Zertifikate ist das ein angenehmes Sicherheitsnetz.

Funktion	Was sie leistet
Zertifikatsinventar	Alle ausgestellten Zertifikate der CA in einer auswertbaren Übersicht
Historie je Antragsteller	Abfolge der Zertifikate pro Subject, Nachfolger und Parallelzertifikate erkennen
Ablauf-Monitor	Zertifikate, die demnächst ablaufen, rechtzeitig sehen
Härtungsprüfung	Bekannte Fehlkonfigurationen wie ESC1 ff. bei Vorlagen und Webregistrierung finden
Sperren	Zertifikate als eigenes Modul sperren

Funktion	Was sie leistet
Autoregistrierung	Autoregistrierung gezielt anstoßen
Intune als Verteilweg	Zertifikate über Intune verteilen
Externe Endpunkte	Ablaufbenachrichtigungen für Webserver mit öffentlichen Zertifikaten

PKI Diagnostiker auf einen Blick

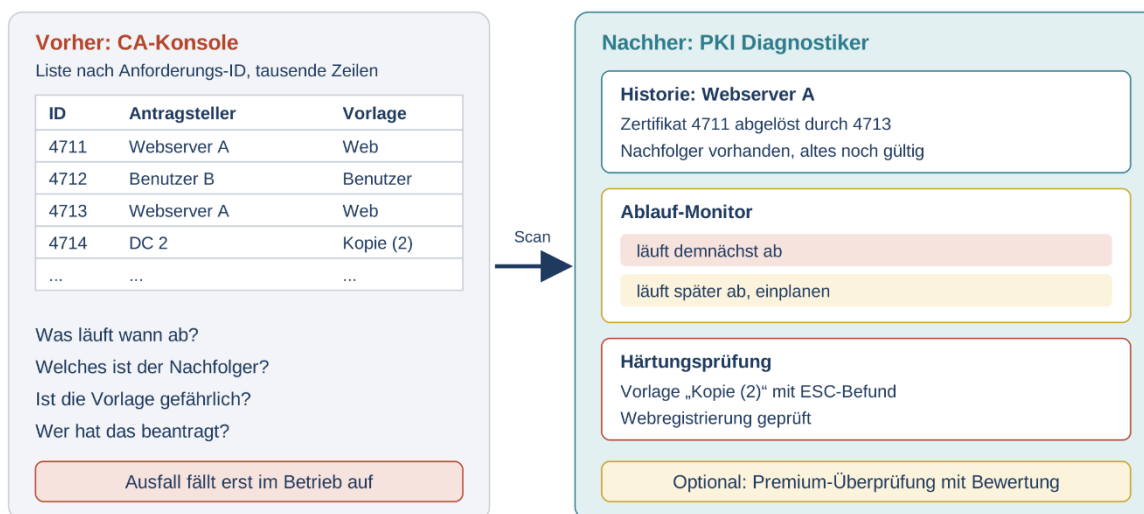
- **Produkttyp:** Bestandsaufnahme, Ablaufüberwachung und Härtingsprüfung für Windows-PKI (ADCS), Diagnostiker-Familie
- **Plattform:** Windows-Desktop-Anwendung
- **Datenquelle:** ausgestellte Zertifikate, Zertifikatvorlagen und Webregistrierung der ADCS-Zertifizierungsstelle; optional externe Webserver-Endpunkte
- **Scandauer:** wenige Sekunden, daher kein durchlaufbegrenztes Capture-Modell
- **Zielgruppe:** Betreiber einer Windows-PKI, Active-Directory- und Sicherheitsverantwortliche
- **Lizenzmodell:** Express kostenlos, Premium-Überprüfung durch boddenberg.de, weitere Ausbaustufen auf Anfrage
- **Hersteller:** Eigenentwicklung von boddenberg.de

Typischer Einsatz: vom Scan zur Bewertung

Der Einstieg ist absichtlich niederschwellig. Mit der kostenlosen Express-Edition scannst du deine Zertifizierungsstelle und bekommst eine Ausgabe zur Analyse. Schon das reicht in vielen Fällen, um zu sehen, ob die PKI aufgeräumt ist oder ob sich ein genauerer Blick lohnt.

Wenn du eine fachliche Bewertung möchtest, kommt die Premium-Überprüfung ins Spiel: Die Scan-Ausgabe wird bei boddenberg.de ausgewertet und bewertet. Du erfährst dann nicht nur, was gefunden wurde, sondern auch, wie ernst es ist und was zu tun ist. Gerade bei den Härtingsbefunden ist diese Einordnung wichtig, denn nicht jede Abweichung ist gleich ein Notfall, und manche unscheinbare Einstellung ist es eben doch.

Vorher und nachher



Vorher und nachher: Aus einer unübersichtlichen Anforderungsliste in der CA-Konsole werden mit dem PKI Diagnostiker ein Inventar mit Historie, ein Ablauf-Monitor und eine priorisierte Härtungsbewertung.

Erst scannen, dann diskutieren

Bevor du in einer Runde über den Zustand eurer PKI spekulierst, lass den Express-Scan laufen. Er kostet nichts, dauert Sekunden, und die Diskussion danach ist deutlich kürzer, weil alle auf dieselben Zahlen schauen.

Abgrenzung zu CertBinder und SMimeManager

Rund um Zertifikate gibt es bei boddenberg.de mehrere Werkzeuge, und jedes hat seine eigene Aufgabe. Der PKI Diagnostiker ist die **Bestandsaufnahme der eigenen CA**: Was wurde ausgestellt, was läuft ab, wo ist die PKI angreifbar?

- [CertBinder](#) kümmert sich um das Erneuern von TLS-Zertifikaten und das Einbinden des neuen Zertifikats in die Dienste, in denen das alte lief.
- [SMimeManager](#) verwaltet S/MIME-Zertifikate für die Signatur und Verschlüsselung von E-Mails.
- Der PKI Diagnostiker liefert den Überblick, auf dessen Basis du entscheidest, wo du aufräumen, härten oder automatisieren musst.

Für wen der PKI Diagnostiker gedacht ist

Der PKI Diagnostiker ist für alle gedacht, die eine Windows-PKI betreiben oder verantworten: Administratoren, die den Zertifikatsbestand endlich im Griff haben wollen, Active-Directory-Verantwortliche, die wissen möchten, ob ihre Vorlagen ein Einfallstor sind, und Sicherheitsverantwortliche, die eine belastbare Aussage zum Zustand der PKI brauchen.

Systemhäuser und Partner, die den Diagnostiker bei ihren Kunden einsetzen möchten, bekommen eigene Konditionen auf Anfrage.

Typische Anlässe für einen Scan sind schnell aufgezählt: Eine PKI wird von einem neuen Team übernommen und niemand weiß genau, was sie alles tut. Ein Sicherheitsaudit steht an und die Frage nach den Zertifikatvorlagen ist absehbar. Ein Zertifikatsausfall hat gerade für Ärger gesorgt und soll sich nicht wiederholen. Oder die Umstellung auf kürzere Laufzeiten wirft die Frage auf, wie viele Zertifikate überhaupt regelmäßig gewechselt werden müssen. In allen Fällen ist der erste Schritt derselbe: Bestand aufnehmen, bevor man irgendetwas verändert.

Hintergrundwissen zu Aufbau, Betrieb und Härtung von ADCS findest du im Kompetenzbereich [PKI mit ADCS](#). Wie die PKI in die Gesamtabsicherung passt, beschreibt der Kompetenzbereich [Microsoft 365 Security](#).

Editionen und Lizenzierung

Weil der Scan nur Sekunden dauert, folgt der PKI Diagnostiker einem anderen Modell als seine Geschwister in der Diagnostiker-Familie.

Edition	Leistungsumfang	Preis (netto)
Express	Scan der Zertifizierungsstelle und Ausgabe zur Analyse	kostenlos
Premium-Überprüfung	Auswertung und Bewertung der Scan-Ergebnisse durch boddenberg.de	1.000 €
Weitere Ausbaustufen	Auf Anfrage	auf Anfrage

Preise und Lizenzbedingungen für weitere Ausbaustufen nennt dir Uli auf Anfrage. Der Preis für die Premium-Überprüfung ist netto zuzüglich Mehrwertsteuer.

Beratung, Einführung und Schulung

Wenn der Scan Handlungsbedarf zeigt, musst du ihn nicht allein abarbeiten. Ich unterstütze dich bei der Härtung von Zertifikatvorlagen und Webregistrierung, beim Aufräumen des Bestands, bei der Planung einer neuen PKI-Struktur und bei der Vorbereitung auf kürzere Zertifikatslaufzeiten. Auch Schulungen für Administratoren, die eine Windows-PKI übernehmen und verstehen wollen, gehören dazu. ADCS ist ein Thema, bei dem sich ein Tag gründliches Verständnis über Jahre auszahlt.

Häufige Fragen

Was kostet der Einstieg?

Nichts. Die Express-Edition mit Scan und Ausgabe zur Analyse ist kostenlos. Erst wenn du eine fachliche Auswertung und Bewertung durch boddenberg.de möchtest, fällt für die Premium-Überprüfung ein Betrag von 1.000 € netto an.

Wie lange dauert ein Scan?

Wenige Sekunden. Genau deshalb gibt es kein Modell, das nach Durchläufen abrechnet. Du kannst so oft scannen, wie es für dich sinnvoll ist.

Was sind die ESC-Angriffsklassen?

Unter dem Kürzel ESC (ESC1 und folgende) sind bekannte Fehlkonfigurationen in ADCS zusammengefasst, etwa bei Zertifikatvorlagen und der Webregistrierung, über die Angreifer ihre Rechte ausweiten können. Die Härtingsprüfung des PKI Diagnostikers sucht gezielt nach solchen Schwachstellen.

Kann ich auch öffentliche Zertifikate überwachen?

Ja, über die Bonusfunktion „externe Endpunkte“. Du trägst die URLs deiner Webserver mit öffentlichen Zertifikaten ein und bekommst Ablaufbenachrichtigungen.

Ersetzt der PKI Diagnostiker den CertBinder?

Nein. Der PKI Diagnostiker ist die Bestandsaufnahme deiner eigenen CA. Der CertBinder erneuert TLS-Zertifikate und bindet sie in die Dienste ein. Beide ergänzen sich: Der eine zeigt, wo es brennt, der andere sorgt dafür, dass beim Zertifikatswechsel nichts ausfällt.

Kann ich aus dem Diagnostiker heraus auch handeln?

Ja. Neben der Analyse gehören das Sperren von Zertifikaten als Modul, das Anstoßen der Autoregistrierung und Intune als Verteilweg zum Funktionsumfang.

Weiter geht's

- [Kompetenzbereich PKI mit ADCS](#): Aufbau, Betrieb und Härtung der Windows-PKI
- [Kompetenzbereich Microsoft 365 Security](#): die PKI im Gesamtbild der Absicherung
- [CertBinder](#): TLS-Zertifikate erneuern und überall einbinden
- [SMimeManager](#): S/MIME-Zertifikate zentral verwalten
- [Entra Diagnostiker](#): Sicherheitsanalyse für Microsoft Entra ID