200 Tage
SSL-Zertifikate

- Was ändert sich? -

PSW GROUP

ISO 27001 CERTIFIED

25 JAHRE PSW GROUP

- SSL-Zertifikate
- Code Signing
- S/MIME
- eSigning
- IoT
- VMC/CMC

Niklas Fritscher
Head of Support & Validation, PSW GROUP

PSW GROUP

ISO 27001 CERTIFIED

Einleitung/ Agenda

- Ausblick 2026
- 200 Tage SSL-Zertifikate und die Hintergründe
- SSL-Zertifikate: Was ändert sich?
- Die wichtigsten Daten der CAs in der Übersicht
- Lösungsansätze: Was ist möglich?
- Unsere Empfehlung
- Q&A

Ausblick 2026

SSL-Zertifikate (öffentliche Zertifikate)

- Erste große Laufzeitverkürzung am 15. März 2026
  - Maximale Gültigkeit: 200 Tage (zuvor 398 Tage)
- Entfernung Client-Authentifizierung
  (ab Mai 26 – März 27)

S/MIME-Zertifikate

- Neue Laufzeit seit Juli 2025
  - Maximale Gültigkeit: 2 Jahre (zuvor 3 Jahre)

Code Signing Zertifikate

- Neue Laufzeit seit März 2026
  - Maximale Gültigkeit: 460 Tage (zuvor 39 Monate)

Warum werden Laufzeiten kürzer?

Treiber der Entwicklung

- Zentrales Ziel: Erhöhung der Sicherheit
  - Schnellere Reaktion auf Sicherheitsprobleme
  - Reduzierung kompromittierter Schlüssel
  - Schnellere Umsetzung neuer Kryptografie
  - Automatisierung wird zum Standard

Wer entscheidet über die Änderungen?

- CA/Browser Forum
  - Zusammenschluss von Zertifizierungsstellen & Browserhersteller

Auszug der einflussreichsten CAs und Browser aus dem CA/Browser Forum:

digicert® SECTIGO GlobalSign Google Mozilla

PSW GROUP

200 Tage SSL-Zertifikate

Der Beschluss zur Verkürzung von Zertifikatslaufzeiten

- **Bisher:** maximale Zertifikatslaufzeit von 398 Tagen
- **Abstimmung (Ballot) im April 2025:** Schrittweise Laufzeitkürzung bis 2029
  - März 2026: 200 Tage
  - März 2027: 100 Tage
  - März 2029: **47 Tage**

Die Zukunft der Laufzeiten von SSL-Zertifikaten

- Die Einführung der 200-Tage-Gültigkeitsdauer ist nur der erste Schritt.
- **Die Richtung ist klar:** Die Laufzeiten von SSL-Zertifikaten werden in den kommenden Jahren weiter sinken.

CA/B CA/BROWSER FORUM

PSW GROUP

SSL-Zertifikate: Was ändert sich?

Angekündigte Änderungen der CAs

- Gelten für alle neu ausgestellten und erneuerten SSL-Zertifikate
- Datum der Umstellung abhängig von der jeweiligen CA
- **In unserem Portfolio:** Einführung von 198 bzw. 199-Tage-Zertifikaten

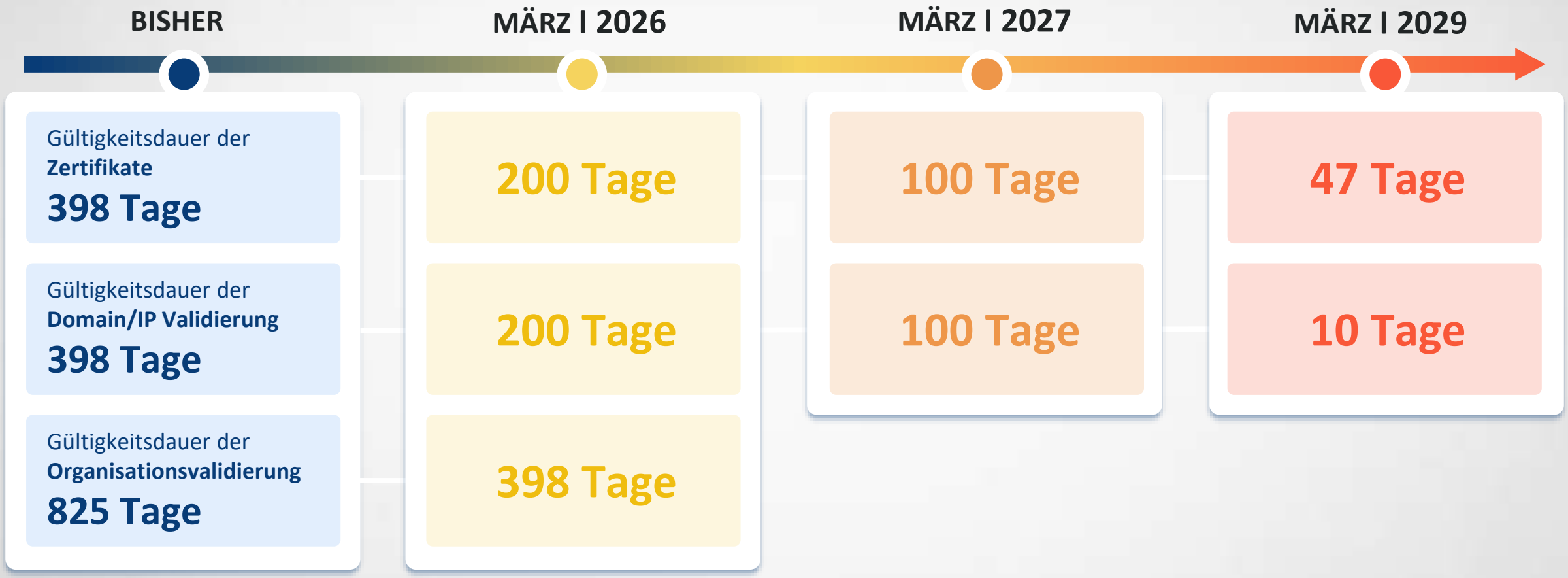
Bestehende SSL-Zertifikate

- Bereits ausgestellte Zertifikate bleiben bis zum Ablaufdatum gültig
- Keine nachträgliche Verkürzung der bestehenden Laufzeit

Neue und erneuerte SSL-Zertifikate

- Nach den Stichtagen werden Zertifikate mit maximal 198 bzw. 199 Tagen ausgestellt
- Betrifft alle neu ausgestellten und erneuerten Zertifikate der jeweiligen CA und bestehende Zertifikats-Pakete

200 Tage SSL-Zertifikate: Was ändert sich?



PSW GROUP

PSW GROUP

Auswirkungen für Unternehmen

Häufigere Zertifikatserneuerungen

- Zertifikate müssen deutlich öfter erneuert werden
- Stark steigende Anzahl an Zertifikaten

Steigendes Risiko von Zertifikatsausfällen

- Menschliche Fehler durch verpasste Renewal-Termine
- Abgelaufene Zertifikate führen zu nicht erreichbaren Websites

Mehr Aufwand für IT-Teams

- Höherer Verwaltungsaufwand
- Zertifikatsmanagement nimmt mehr Zeit in Anspruch

Die wichtigsten Daten der CAs in der Übersicht

Zertifizierungsstelle (CA)	Laufzeit	Ausführung	Datum
digicert®	199 Tage	single/multi	24.02.2026
SwissSign	198 Tage	single	09.03.2026
D-Trust	199 Tage	single	11.03.2026
SECTIGO®	199 Tage	multi	12.03.2026
Certum	199 Tage	**single**/multi	13.03.2026
GlobalSign.	199 Tage	multi	15.03.2026

PSW GROUP

Lösungsansätze

Zertifikatspakete

PSW API

ACME

CLM

PSW GROUP

Lösungsansatz: Zertifikatspakete

Zertifikatspakete: Einfacher Umgang mit kürzeren Laufzeiten

- Laufzeitunabhängige Bereitstellung von Zertifikaten
- Planbarer Zertifikats-Workflow
- Zertifikatspakete ermöglichen Produktlaufzeiten von einem bis drei Jahre

Ihre Vorteile:

- ✓ Kalkulierbare Laufzeiten und Kosten
- ✓ Fester Preis über die gesamte Paketlaufzeit
- ✓ Preisvorteil gegenüber dem Einzelkauf
- ✓ Bestellaufwand wird reduziert

Lösungsansatz: PSW API

API-Schnittstelle

- Programmierschnittstelle zur Anbindung externer Systeme
- Ermöglicht den automatisierten Austausch von Daten zwischen Anwendungen
- Zugriff auf definierte Funktionen und Daten über standardisierte Endpunkte
- Kommunikation erfolgt über strukturierte Anfragen und Antworten

Ihre Vorteile:

- ✓ Automatisierung von Prozessen
- ✓ Nahtlose Integration in bestehende Systeme
- ✓ Zeit- und Kostenersparnis
- ✓ Flexibel und erweiterbar

Hinweis an unsere API Kunden:

Umsetzung prüfen: Zertifikatspakete auch per API möglich

Lösungsansatz: ACME

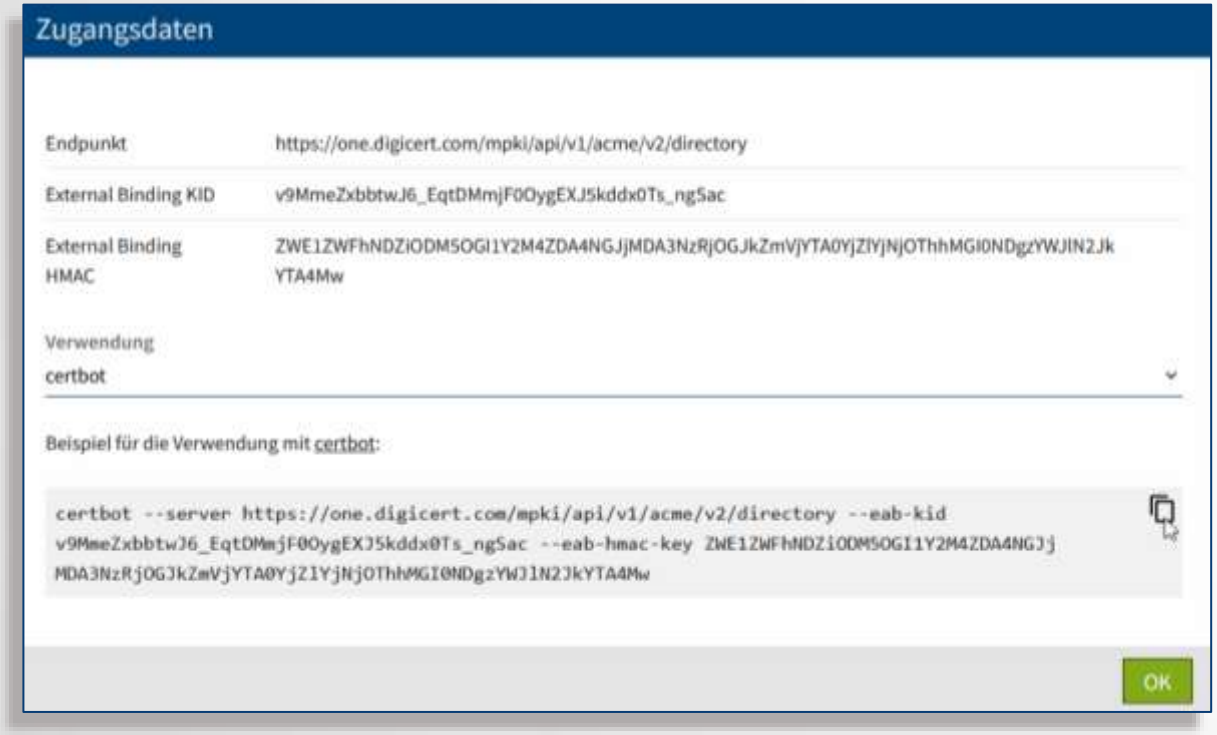
Was ist ACME?

- Protokoll zur automatisierten Verwaltung von SSL-Zertifikaten
- Offener Standard für viele Webserver-Umgebungen
- Kommunikation zwischen Client und Zertifizierungsstelle über definierte Endpunkte

Ihre Vorteile

- ✓ Kompletter Lebenszyklus eines Zertifikates wird abgebildet
- ✓ Reduzierung manueller Verwaltungsaufwände
- ✓ Skalierbare Verwaltung vieler Zertifikate
- ✓ Volumenunabhängig
- ✓ Reseller-/Mandantenfähig
- ✓ Kostengünstig und schnell implementiert

Lösungsansatz: ACME



Endpunkt:

Der Endpunkt gibt an, wo das Zertifikat erstellt und abgerufen wird.

External Binding KID (Key Identifier)

Der Key Identifier identifiziert das PSW/DigiCert-Konto und das Automatisierungsprofil für die Zertifikatsausstellung.

External Binding HMAC

Der Key Identifier identifiziert das PSW/DigiCert-Konto und das Automatisierungsprofil für die Zertifikatsausstellung.

PSW GROUP

Lösungsansatz: CLM

Certificate Lifecycle Management (CLM)

- Softwarelösung zur Verwaltung digitaler Zertifikate und Schlüssel
- Unterstützt Public- und Private-PKI-Umgebungen
- Besonders geeignet bei hoher Zertifikatsanzahl

Ihre Vorteile

- ✓ Zentrale Übersicht aller Zertifikate (SSL, S/MIME, Code Signing, IoT etc.)
- ✓ Modularer Aufbau für individuelle Kundenwünsche
- ✓ Zertifikatserfassung mittels Certificate Discovery
- ✓ Unterstützung bei der Einhaltung von Sicherheits- und
- ✓ Compliance-Anforderungen

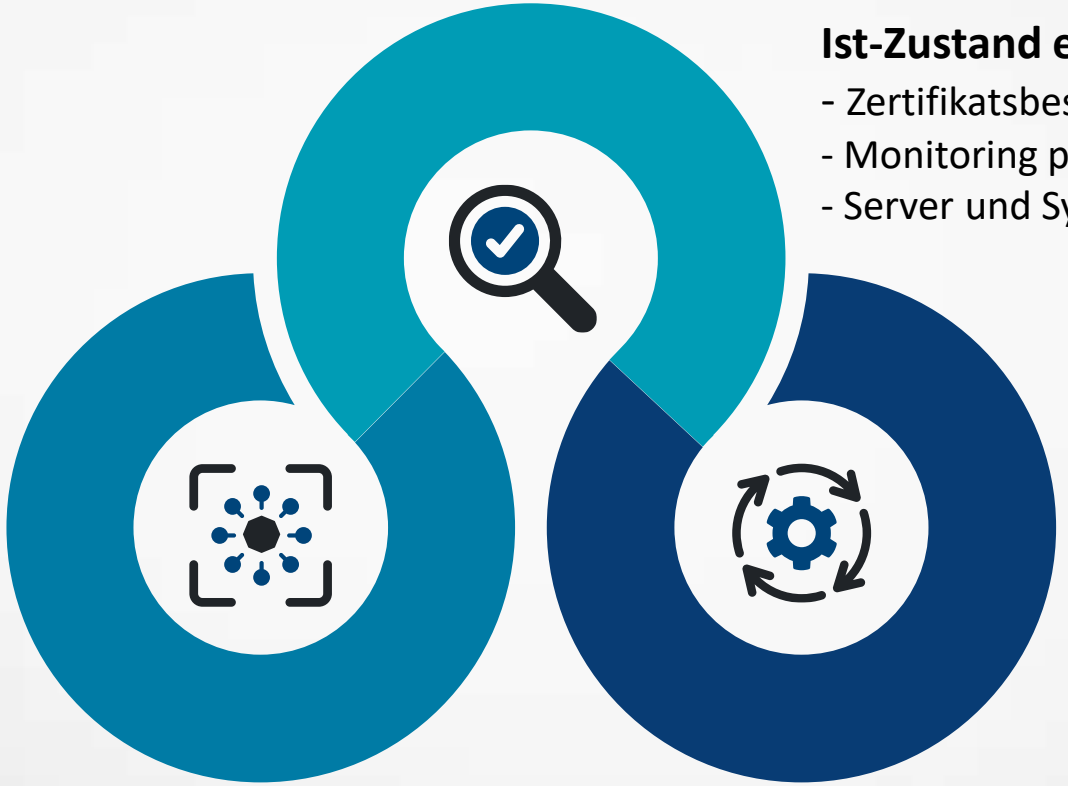
Lösungsansatz: CLM

Quelle: Gartner

PSW GROUP

Unsere Empfehlung: Grundstein legen

Ist-Zustand ermitteln
- Zertifikatsbestand überprüfen
- Monitoring prüfen & aktualisieren
- Server und Systemlandschaft prüfen (ACME-fähig?)



Rahmen definieren
Was soll automatisiert werden?
SSL, S/MIME, IoT, etc?

Umsetzung
- Automatisierungslösung einführen
- Zentrale Verwaltung aller Zertifikate

PSW GROUP

Sprechen Sie direkt mit uns!

secIT by heise

18. & 19. März 2026
Hannover

Aussteller:
Glashalle, Stand 10

CLOUDFEST

24. bis 26. März 2026
Europa-Park Rust

Besucher:
Termine vor Ort möglich

it sa
Die IT-Security Messe und Kongress

27. bis 29. Oktober 2026
Nürnberg

Aussteller:
Hallo 9, Stand 210

Terminanfragen unter: marketing@psw.de

Unsere neue Broschüre finden Sie unter:
www.psw-group.de/downloads

PSW GROUP **Newsletter** abonnieren
und immer auf dem Laufenden bleiben bei allen Themen rund um digitale Zertifikate

www.psw-group.de/newsletter-abonnieren/

Bewerten Sie uns auf Google

GEPRÜFTER ONLINE-SHOP EHI

Excellent Shop
10 Jahre zertifiziert

Q&A

Wir beraten Sie umfassend zu Ihrer Zertifikats- und Automatisierungsstrategie

www.psw-group.de/zt-automation

PSW GROUP

ISO 27001 CERTIFIED