SwissSign

essendi it
IT-Beratung und -Entwicklung

CHECKLISTE FÜR AUTOMATISIERTES ZERTIFIKATSMANAGEMENT

Sarah Zügel, essendi it | Marco Flükiger, SwissSign | Nürnberg | 26.10.2022

#1 Fakten & Trends

#2 Herausforderungen bei der Automatisierung

#3 Checkliste für automatisiertes Zertifikatsmanagement

#4 Vorteile des automatisierten Zertifikatsmanagements

SARAH ZÜGEL

Seit 2011 bei essendi it

Geschäftsführerin

Schwerpunktthemen essendi GmbH

- Zertifikatsmanagement, PKI & Key Management
- IT-Consulting und IT- Security Consulting
- Individuelle Softwareentwicklung, Wartung und Support
- Anwendungsintegrationen

MARCO FLÜKIGER

Seit 2021 bei SwissSign

Sales & Partner Manager

Schwerpunktthemen SwissSign AG

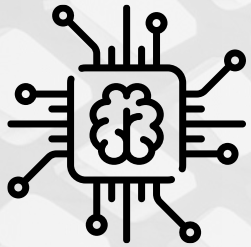
- Dank elektronischen Zertifikaten können
  - Daten verschlüsselt und damit vor ungewolltem Zugriff geschützt ausgetauscht werden,
  - Dokumente rechtsgültig signiert werden,
  - Personen, Server etc. sich sicher authentisieren.

Fakten und Trends im Zertifikatsmarkt

Erfahrungswerte bei SwissSign:

- Im Jahr 2021 hat SwissSign **64%** mehr Zertifikate im Vergleich zum Vorjahr verkauft.
- Durchschnittlich bezieht ein Kunde **450** anerkannte Zertifikate (SSL und/oder S/MIME) bei SwissSign
- Vor allem wurden im Jahr 2021 mehr S/MIME Zertifikate verkauft als im Jahr zuvor – Grund: **neue Datenschutz-Grundverordnung** – (viele dieser S/MIME Zertifikate werden bereits durch eine automatisierte Lösung bezogen.)
- Über die **Private MPKI** (eigene gehostete Root und ICA) hat SwissSign ein Wachstum von **30%** verzeichnet**.**
- Manueller Zertifikatstausch dauert laut Kundenfeedback **ca. 2 Stunden** pro Zertifikat
- Gartner rechnet mit bis zu **5 Stunden** pro Zertifikat

Herausforderungen bei der Prozessautomatisierung



Komplexität des Themas

Unklarheit über den Status Quo

Zeitaufwand für die Einführung von Automatisierungslösungen inkl. Produkt-Suche

Viele Stakeholder mit unterschiedlichem Wissensstand

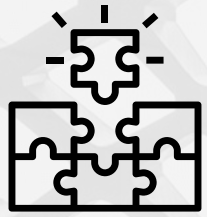
Kosten / Budget für eine Lösung

Checkliste für automatisiertes Zertifikatsmanagement

Schritt 1: Wie ist der Status Quo?

- ✓ Anzahl der Zertifikate
- ✓ Welche CAs/PKIs werden genutzt (trusted / nontrusted Certificates)
- ✓ Wichtigste Use Cases – Priorisierung aufgrund:
  - ✓ der Anzahl Zertifikate
  - ✓ Folgen eines unbemerkten Zertifikatsablaufes
  - ✓ Laufzeit der Zertifikate
- ✓ Wohin müssen Zertifikate verteilt werden
- ✓ Welche Automatisierungsmechanismen sind im Einsatz? Funktionieren sie?
- ✓ …

Checkliste für automatisiertes Zertifikatsmanagement



Schritt 2: Anforderungen sammeln

- ✓ Wer soll Zertifikate beantragen können?
- ✓ Wo soll das Schlüsselmaterial generiert / gespeichert werden? Und Verantwortlichkeit
- ✓ Wer gibt den initialen Impuls zur Zertifikatsbeantragung? Und welcher Weg soll genutzt werden?
- ✓ Was passt in den Workflow der Admins?
- ✓ Müssen interne Compliance-Themen beachtet werden?
- ✓ Dürfen Agenten im RZ eingesetzt werden?
- ✓ Zukünftige Use Cases berücksichtigen
- ✓ …

- ✓ 1 bis 3 Use Cases aussuchen, Reihenfolge festlegen (iteratives Vorgehen)
- ✓ Vorhandene Automatisierungswege prüfen (was kann/soll weiter genutzt werden?)
- ✓ Automatisierungstool wählen

Checkliste für automatisiertes Zertifikatsmanagement

Schritt 3: Erste Use Cases implementieren

- ✓ Mit ausgewählten Use Cases starten, Erfahrungen sammeln
- ✓ **Zielprozess aufzeigen:** Schnittstellen / Rollen / beteiligte Programme und Kommunikationswege identifizieren? In welche vorhandene Prozesse kann / sollte die Zertifikatsbeantragung integriert werden, z.B. Prozessmanagement-Tool?
- ✓ Projektplan: Wer sind die Stakeholder? Welche Freigaben müssen dafür eingeholt werden? Welche Berechtigungen werden benötigt?
- ✓ Architektur und Implementierung der Lösung: Bereitstellung der Infrastruktur, Integration in den vorhandenen Netzplan, Kommunikationswege öffnen & sichern

Schritt 4: Prozess ausrollen

- ✓ Architektur-Fragen: Weitere / künftige Use Cases für Zertifikate identifizieren, auch mit den Stakeholdern
- ✓ Vor dem Breiteneinsatz: interne Kommunikation, über den Changeprozess informieren
- ✓ Welche weiteren Fragen haben sich ergeben und müssen zukünftig beachtet werden?

Installation > Konfiguration > Testphase > Pilotierung > Breiteneinsatz

Checkliste für automatisiertes Zertifikatsmanagement

SwissSign essendi it IT-Beratung und -Entwicklung

Tipps zur Toolauswahl

- Tool passend zur Zertifikatsanzahl und den Anforderungen dimensionieren.
- Ausgangssituation und (zukünftige) Anforderungen (Muss / Soll / Kann) genau definieren, denn nicht alle Tools decken alles ab oder lassen sich später erweitern:
  - Anzahl an Zertifikaten, Zertifikatsarten, Usecases und die vorhandene Infrastruktur beachten
  - Sind nur interne Prozesse oder auch externe (mit Partnern oder Services) beteiligt
  - Wie kommen Zertifikate auf die Zieldevices? Wo werden die Schlüssel generiert?
  - Open Source j/n?
  - Möglichkeit, auf individuelle Kundenanforderungen einzugehen / individuelle Produktweiterentwicklung
  - Usability / Einfachheit des Tools = Zufriedene Mitarbeiter
  - Dynamische Prozesse, Flexibilität, Nachhaltigkeit bei der Toolauswahl
  - Anbieterland relevant ? (Wartungs- und Supportleistungen)
  - Kann eine automatisierte Aktivierung etc. durchgeführt werden?
  - Können verschiedene User / Gruppen / Berechtigungen abgebildet werden?
  - Müssen Netzwerkgrenzen überwunden werden?
  - Wer ist verantwortlich?
  - Von wem kommt der Impuls für eine Erneuerung?
  - Welche Systeme sind beteiligt?
  - Wohin müssen ggf. Informationen verteilt werden?

Mehrwerte durch Automatisierung

- **Sicherheit** — **Erhöhte Sicherheit im IT-Betrieb durch Automation** sowie selbsttätiger Erneuerung von Zertifikaten, Alert und Monitoring verhindern ungeplanten Ablauf von Zertifikaten.
- **Prozesse** — **Einmal einrichten, dann laufen die Prozesse automatisiert.** Einfaches Onboarding, in wenigen Schritten ready-to-go. Zertifikate können selbsttätig und rund um die Uhr ausgestellt und verteilt werden
- **Usability** — **Einfacher Umgang und Handling der Anwendung** standardisiert und automatisiert, wenig Detailkenntnisse über Zertifikate nötig
- **Krypto-Agility** — **Schnelle Handlungsfähigkeit z.B. bei Datenänderungen an Zertifikaten** oder Kompromittierung von Schlüsseln (wichtig hinsichtlich ISO27001)
- **Kostenersparnisse** — Deutliche Ersparnis von Prozesskosten, Nutzung out of the Box, **Mitarbeiter-Kapazitäten für das Zertifikatshandling PKI/-Infrastruktur werden für andere Aufgaben frei** oder müssen nicht aufgebaut werden.

Vielen Dank für Ihre Aufmerksamkeit

Wir freuen uns auf Ihren Besuch in Halle 7A Stand 419

Kontaktdaten

SwissSign AG

SwissSign AG

Sägereistrasse 25

CH-8152 Glattbrugg

+ 41 848 77 66 55

https://www.swisssign.com/

info@swisssign.com

essendi it GmbH

essendi it GmbH

Dolanallee 19

D-74523 Schwäbisch Hall

+49 89 944 697-71

https://xc.essendi.de

xc@essendi.de