

Die Zukunft digitaler Zertifikate

Automatisierung als Schlüssel zum Erfolg

essendi it GmbH

- IT-Security, Management digitaler Zertifikate, digitale Identitäten, Krypto, PKI; Produktfamilie **essendi xc**
- Individuelle Software-Lösungen und Beratung für versch. Branchen
- 70 Mitarbeiter an 2 Standorten
 - Business-Analysten (IREB®)
 - Wirtschaftsinformatiker
 - Software-Ingenieure / -Entwickler (ISAQB®)
 - Testmanager (ISTQB®)
 - IT Security Experten
 - Projektmanager – auch agil (PMI®, IPMA)
 - DHBW-Studenten, Auszubildende (IHK)
- Gründung im Jahr 2000, familiengeführt, EU-company
- Tochterunternehmen: essendi it AG, Schweiz  
- Webseiten: <https://xc.essendi.de> und <https://essendi.de>





WO ZERTIFIKATE BENÖTIGT WERDEN

- Webserver (TLS/SSL)
- SSL-Server im Intranet
- Loadbalancer, Appliance
- VPN (Homeoffice, Vertragspartner)
- Mailserver, Mailgateway
- Cloud-Instanzen (AWS, Azure, GCP)

WO ZERTIFIKATE BENÖTIGT WERDEN

- Überwachungskameras
- Switches
- Steuerungen
- Zugangskontrollen



WARUM ÜBERHAUPT AUTOMATISIEREN?

LAUFZEITVERRINGERUNG

- Vervierfachung der manuellen Aufwände

POST QUANTEN KRYPTOGRAPHIE

- Möglichkeiten schaffen um einfach den Wechsel durchzuführen

ANZAHL DER ZERTIFIKATE

- Anzahl der Zertifikate steigt stetig

NEUE VORGEHEN

- ZeroTrust
- Cloud First

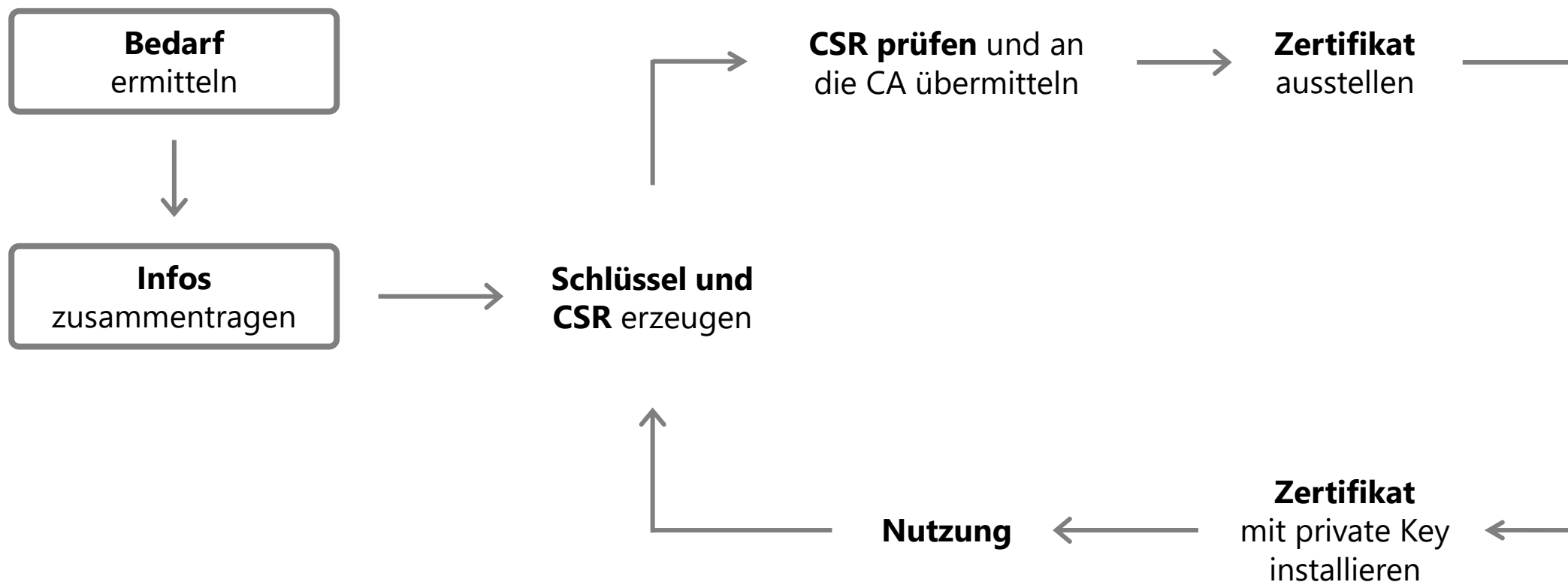
STABILITÄT / STANDARDISIERUNG

- Stabilität durch Automatisierung der Prozesse
- Standards für Prozesse

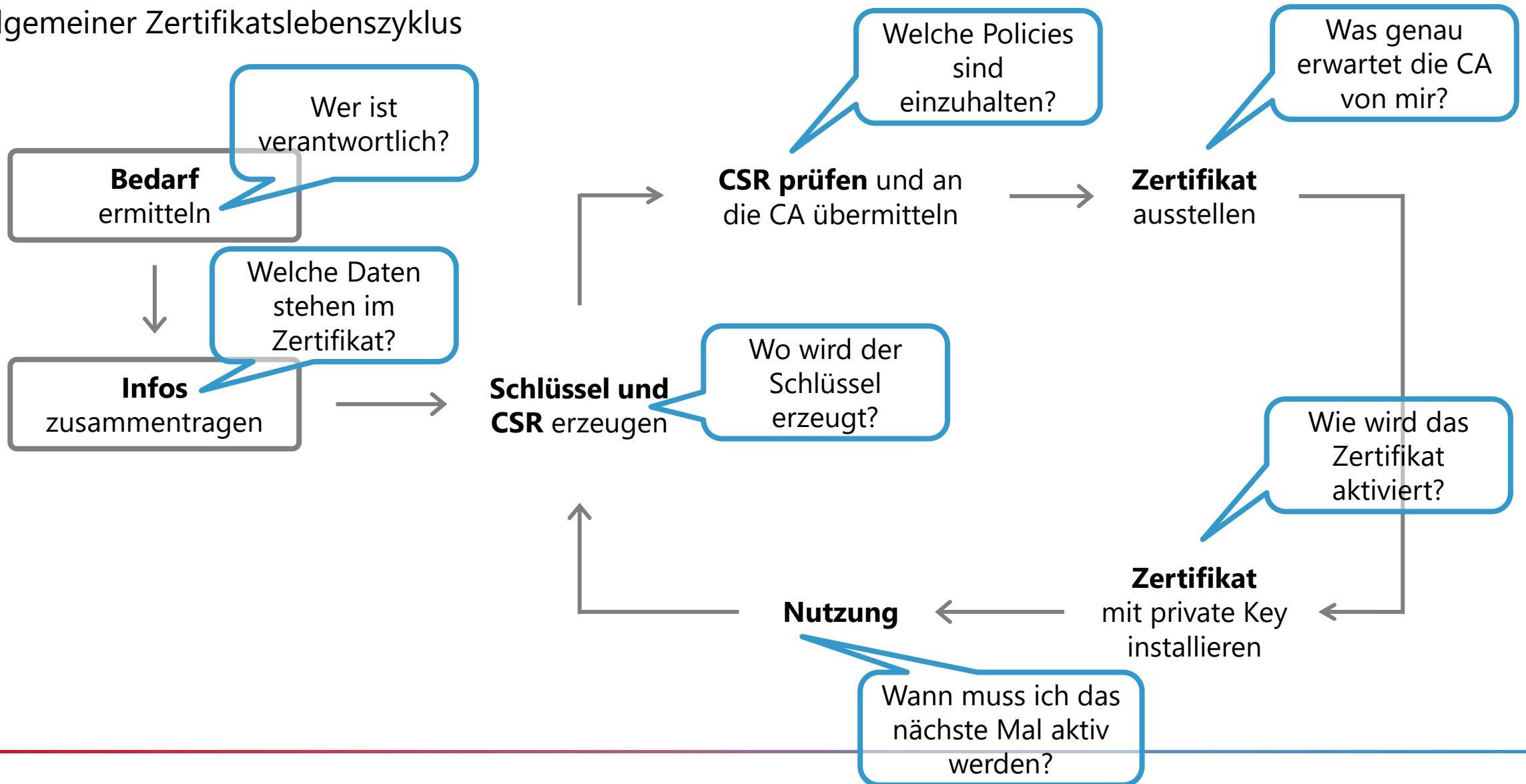
MINIMIERUNG VON KOSTEN

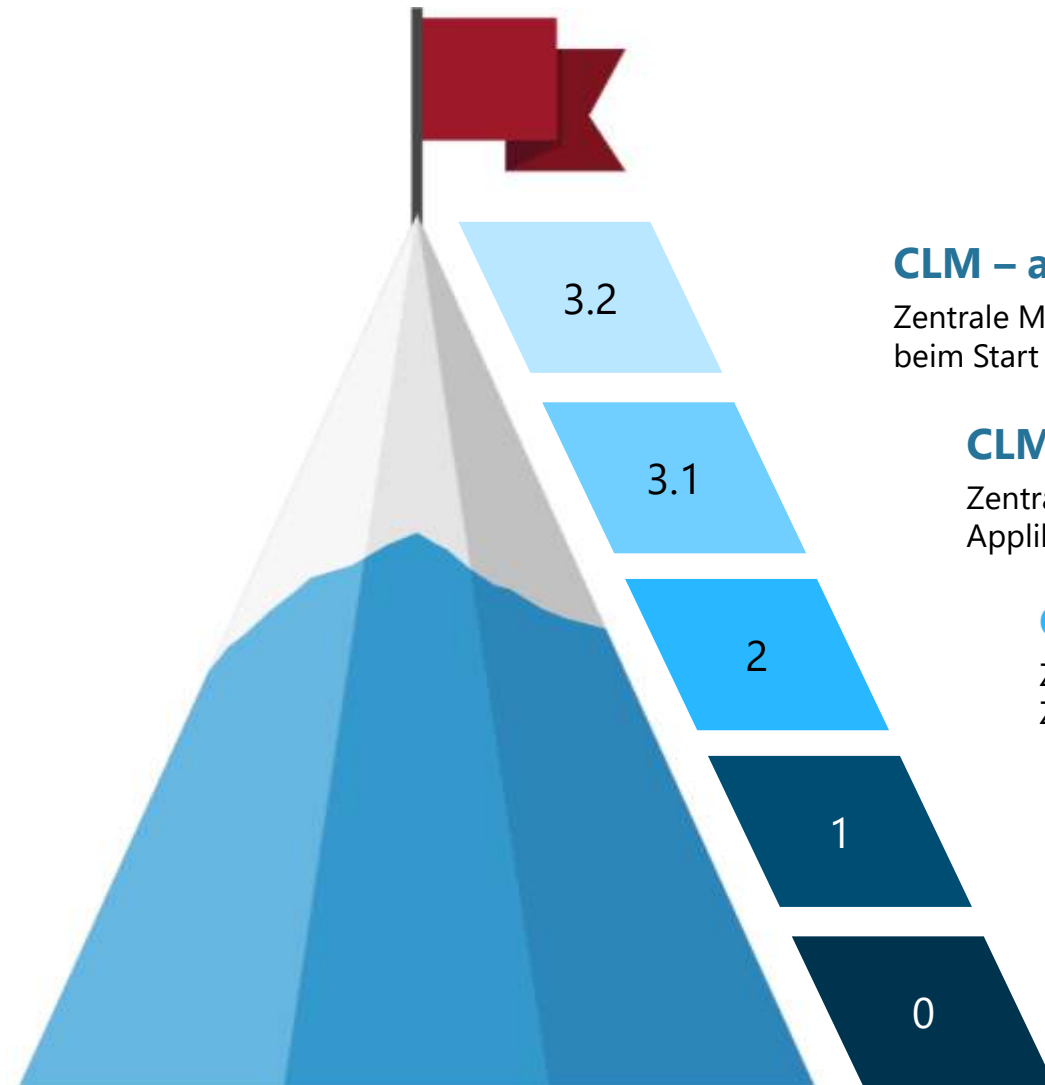
- Freiwerden von Kapazitäten und Ressourcen

Allgemeiner Zertifikatslebenszyklus



Allgemeiner Zertifikatslebenszyklus





CLM – auto enrolled (client based)

Zentrale Management Lösung in Kombination mit Enrollment Prozessen, die automatisch beim Start Zertifikate beziehen

CLM – pull automation (client based)

Zentrale Management Lösung in Kombination mit Schnittstellen, die von Applikationen und Services angesprochen werden können

CLM – push automation

Zentrale Management Lösung in Kombination mit Verteileinheiten, die die Zertifikate auf Zieldevices bringen

Certificate Lifecycle Management (CLM)

Zentrale Management Lösung mit Prozessautomatisierung z.B. über ein SelfService-Portal optional mit zentraler Erstellung der private Keys

Management by Excel / Sharepoint / Outlook

Sämtliche Zertifikatsinformationen sind innerhalb einer zentralen Excel-Tabelle gespeichert und gepflegt

Vorteile:

- Schnell aufgesetzt
- Einfach in der Handhabung
- Einfache Erweiterbarkeit

Nachteile:

- Wird schnell unübersichtlich
- Keine automatische Überwachung der Gültigkeit
- Keine inhaltliche Prüfung der Zertifikate

Einsatzgebiete:

- 10 - ~50 Zertifikate (bei Unterstützung durch Kalender etc.)



Beschreibung:

- **Zentrales** Tool zur Verwaltung der Zertifikate
- Automatisches Überwachen von **Laufzeit** und **Qualitätsattributen**
- Verwendung von Templates für die Beantragung von Zertifikaten:
 - Einhaltung von **Policies** und **Normen** (NIST, ISO, CPS)
 - **Vereinfachung** der Prozesse für die Antragssteller
- **Berechtigungssteuerung**



Vorteile:

- **Einfach in der Handhabung** für Antragssteller
- **Zentrales Management** für die Zertifikate und Keys (optional)

Nachteile:

- Keine komplette Automatisierung
 - **Ausbringung** erfolgt weiterhin **manuell**

Einsatzgebiete:

- 50 ++ Zertifikate
- Backup-Lösung oder Lösung für Sonderanwendungen



Beschreibung:

- Verwendung von **Standardprotokollen** wie SCP / Powershell Remoting
- Anbindungen von **Cloudanwendungen**
- Zertifikate werden über ein Portal **zentral** beantragt und **im Anschluss** auf die Zielgeräte **ausgebracht**



Vorteile:

- Einfach in der Handhabung
 - SelfService für Antragssteller
 - **Standardprotokolle** im Einsatz
- Zentrales (Key-)Management möglich

Nachteile:

- Eine Anwendung hat Zugriff auf sämtliche Zielsysteme
- **Manueller Konfigurationsaufwand** vorhanden für Antragssteller

Einsatzgebiete:

- 100 - ~250 Zertifikate



CLM – PULL AUTOMATION (CLIENT BASED)

Beschreibung:

- Zertifikatsbeantragung über
 - **WebService-Schnittstelle** durch Services
 - Beantragung über **Clients** (ACME etc.)
- **Zertifikat** wird nach Ausstellung **automatisch** gepullt und **ausgebracht**



Vorteile:

- **Vollständige Automatisierung** möglich
- **Lokale Schlüsselerstellung** möglich
- Bekannte Schnittstellen (REST, ACME, ...)

Nachteile:

- **Keine zentrale Steuerung** (jeder Client ist für sich selbst verantwortlich)

Einsatzgebiete:

- 150 ++ Zertifikate
- > 500 Zertifikate, in Kombination mit anderen Schnittstellen sinnvoll



Beschreibung:

- Direkt **beim Aufsetzen / Starten** des Devices wird dieses mit Zertifikaten versorgt
- Versorgung läuft über **Enrollment-Protokolle** oder über Clients
- Der Endanwender bekommt im besten Fall gar nichts davon mit



CLM – AUTO ENROLLED (CLIENT BASED)

Vorteile:

- **Zentrale Steuerung** möglich
- Anwender muss **keine manuellen Schritte** unternehmen

Nachteile:

- hoher **Konfigurationsaufwand**

Einsatzgebiete:

- 150 ++ Zertifikate
- > 500 Zertifikate, in Kombination mit anderen Schnittstellen sinnvoll



- **Überblick** verschaffen, wie viele Zertifikate und wie viele Anwendungsfälle?
- Bewerten Sie Ihre Situation, **wie viel Zeit** benötigen Sie **aktuell** für Zertifikate,
 - in Zukunft wird sich diese vervierfachen.
- Welche **Policies / Regelungen** müssen Sie einhalten?
 - Netzwerkgrenzen, Einschätzungen zu Protokollen etc.
- Welche UseCases / Anwendungen unterstützen welche Art von **Schnittstellen**? Ist hier eine **Gruppierung** möglich?

System	Anbieter	Netzwerk- zone	Verantwortlicher	Anzahl	Schnittstellen / Systemgrenzen	Zertifikatstyp	Inbetriebnahme automatisierbar
IIS	Microsoft	1	Zentral IT	5	Höchste Sicherheitsstufe, nur durch Admins erreichbar	TLS / SSL	Ja (Zeitpunkt beachten)
Überwachungs- kamera	Axis	3	Facility	20	Subnetz je Gebäude zu beachten	TLS / SSL	Ja

Treffen Sie uns!

essendi it auf der it-sa



Besuchen Sie uns!

Das essendi Team freut sich auf den gemeinsamen Austausch mit Ihnen.



Herzlichen Dank!

Julian Weeber

essendi it GmbH

www.essendi.it