smartservice
thüga solutions+

Zeulenroda-Triebes, 18.09.2023
Václav Vacek

Zertifikate und Zertifizierungen im Bereich Smart Metering.

Wie Sie souverän den Überblick behalten.

Kontakt.

Václav Vacek
Team Lead Advanced Metering Infrastructure (GWA)

Thüga SmartService GmbH

+49 9282 9999 218
vaclav.vacek@smartservice.de

Fakten über uns.
Kompetenz auf einen Blick.

Naila
München
Freiburg

> 35
Jahre
Erfahrung

% 100
Thüga
Anteilseigner

60 ca.
SAP-
Systeme

> 300
Mitarbeiter
:innen

35.000
Messstellen
Zählerfernauslesung RLM

Kunden
> 300

> 7000
System-User

> 100
GWA Kunden

Pro Jahr
160
Mio.
EDIFACT-
Nachrichten

Eigene SubCA

Umsatz
52
Mio.

Wie viele Zertifikate gibt es in diesem SMGW?

+ Root-CA	Signaturzertifikat x3
+ Sub-CA	Signaturzertifikate
+ GWA	ENC, SIG, TLS
+ SMGW-Gütesiegelzertifikat	ENC, SIG, TLS
+ SMGW-Wirkzertifikat	ENC, SIG, TLS
+ EMT	ENC, SIG, TLS
+ GWH	SIG
+ HAN	TLS: GW, CON, SRV, CLS
+ LMN	TLS
+ Zähler-Signaturschlüssel	SIG
+ LMN-Zähler	Symmetrisch
+ wM-Bus-Zähler-Schlüssel	Symmetrisch

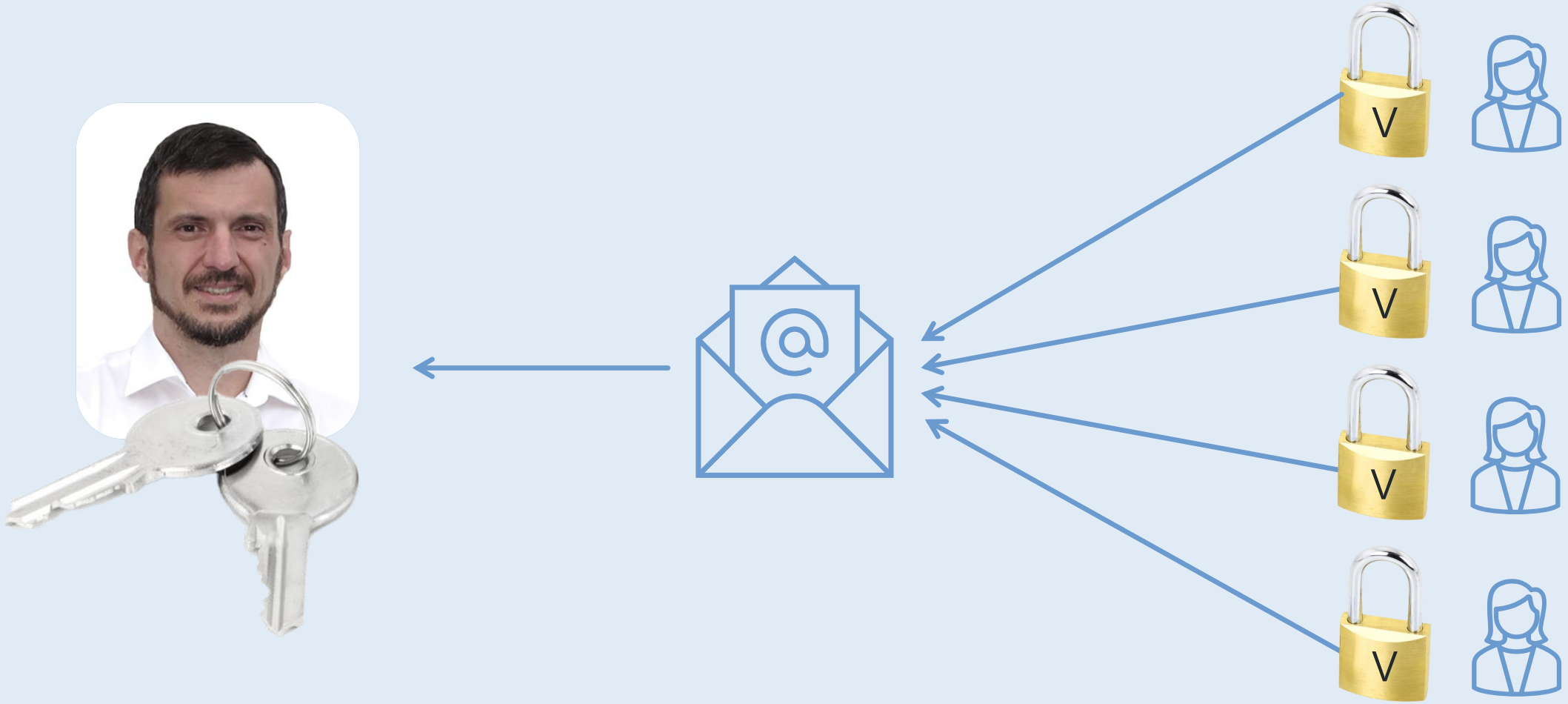
> 25 Zertifikate/ Schlüssel

Was ist ein Zertifikat überhaupt?

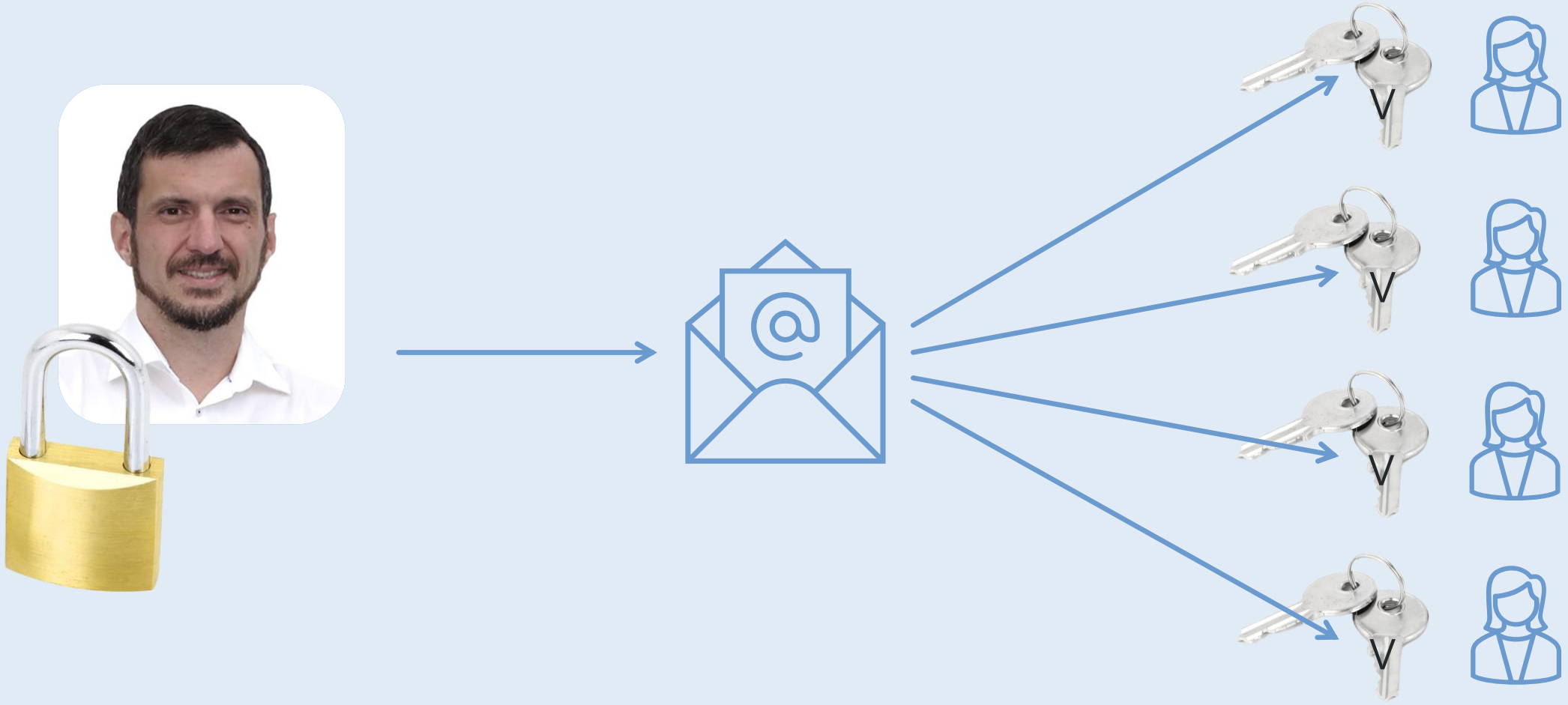
Was ist ein Zertifikat überhaupt?

- Ein digitales Zertifikat ermöglicht eine vertrauenswürdige Zuordnung von Entitäten zu ihren öffentlichen Schlüsseln.
- Mit einem Schlüsselpaar (geheim+öffentlich) kann man:
  - Verschlüsseln
  - Signieren
- Asymmetrische Verschlüsselung: Schloss + Schlüssel
- Knacken?

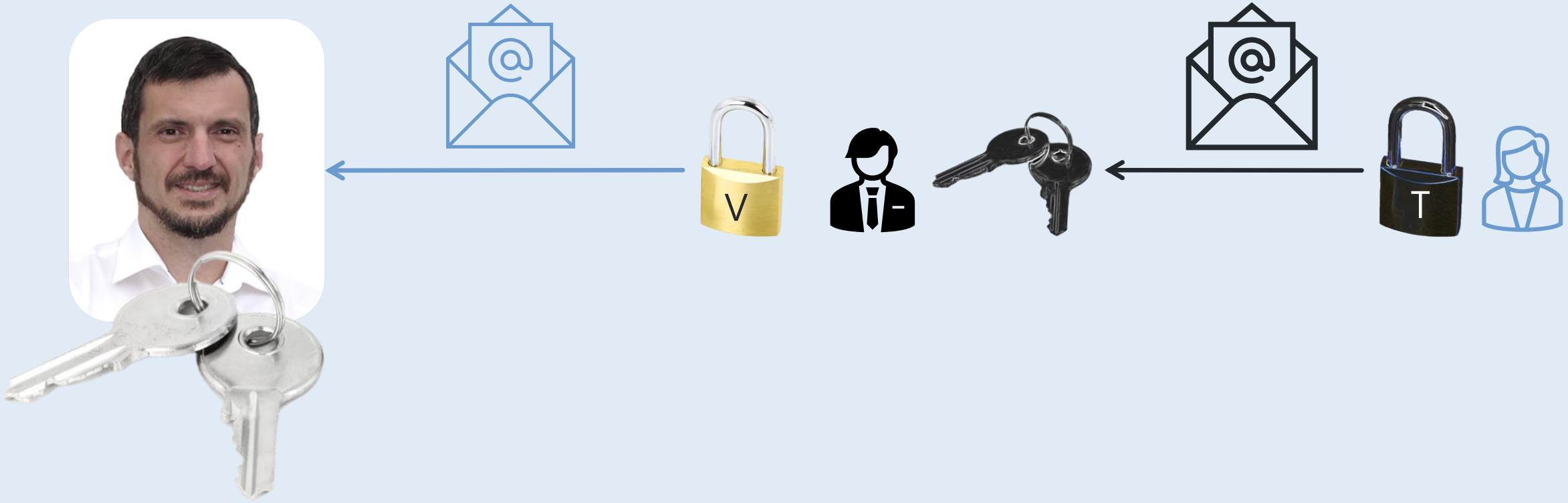
Verschlüsselung.



Signierung.



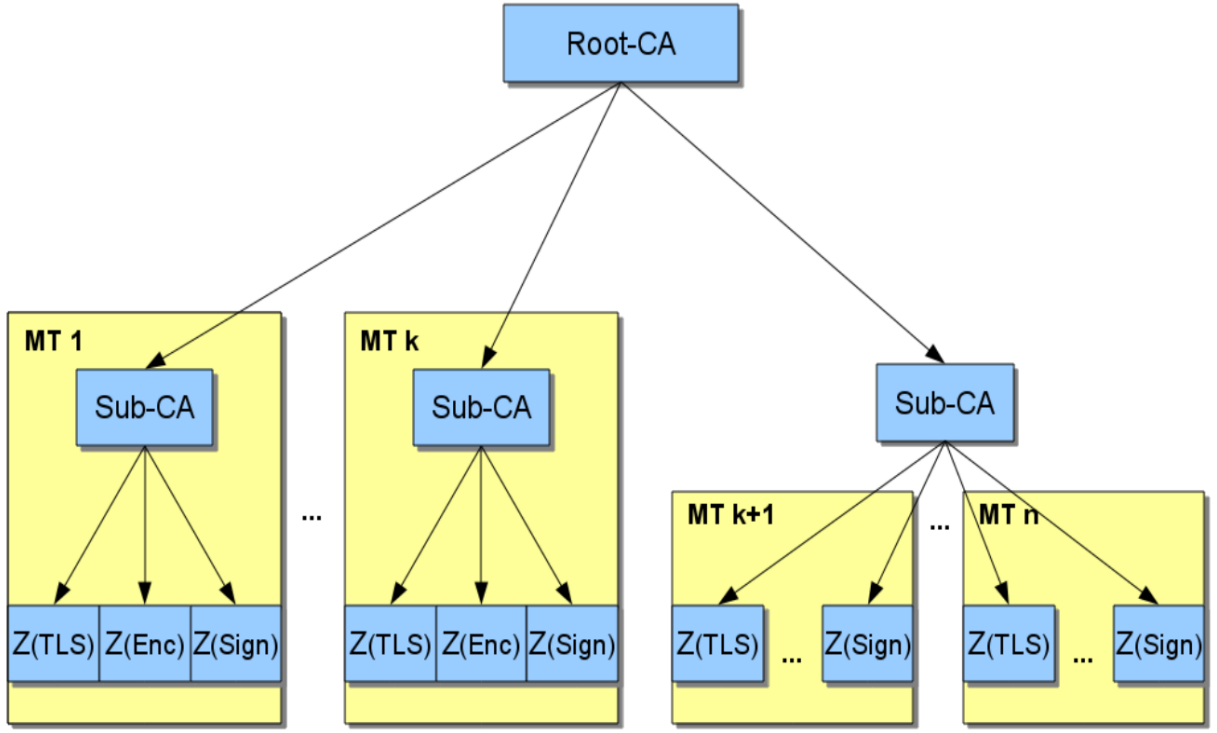
MITM.



Public Key Infrastruktur (PKI).

Vertrauenshierarchie für die Sicherstellung der Authentizität der öffentlichen Schlüsseln.

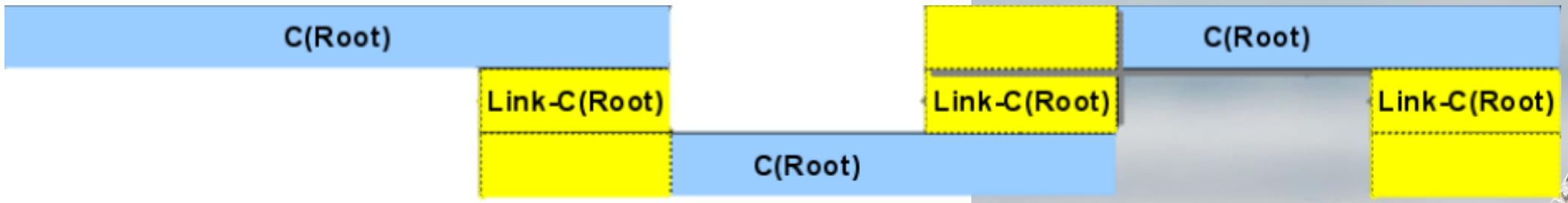
- + Hoheitlicher Vertrauensanker (Root-CA)
- + Endnutzerzertifizierung (Sub-CA)
- + Endnutzer: EMT, GWA, GWH, SMGW



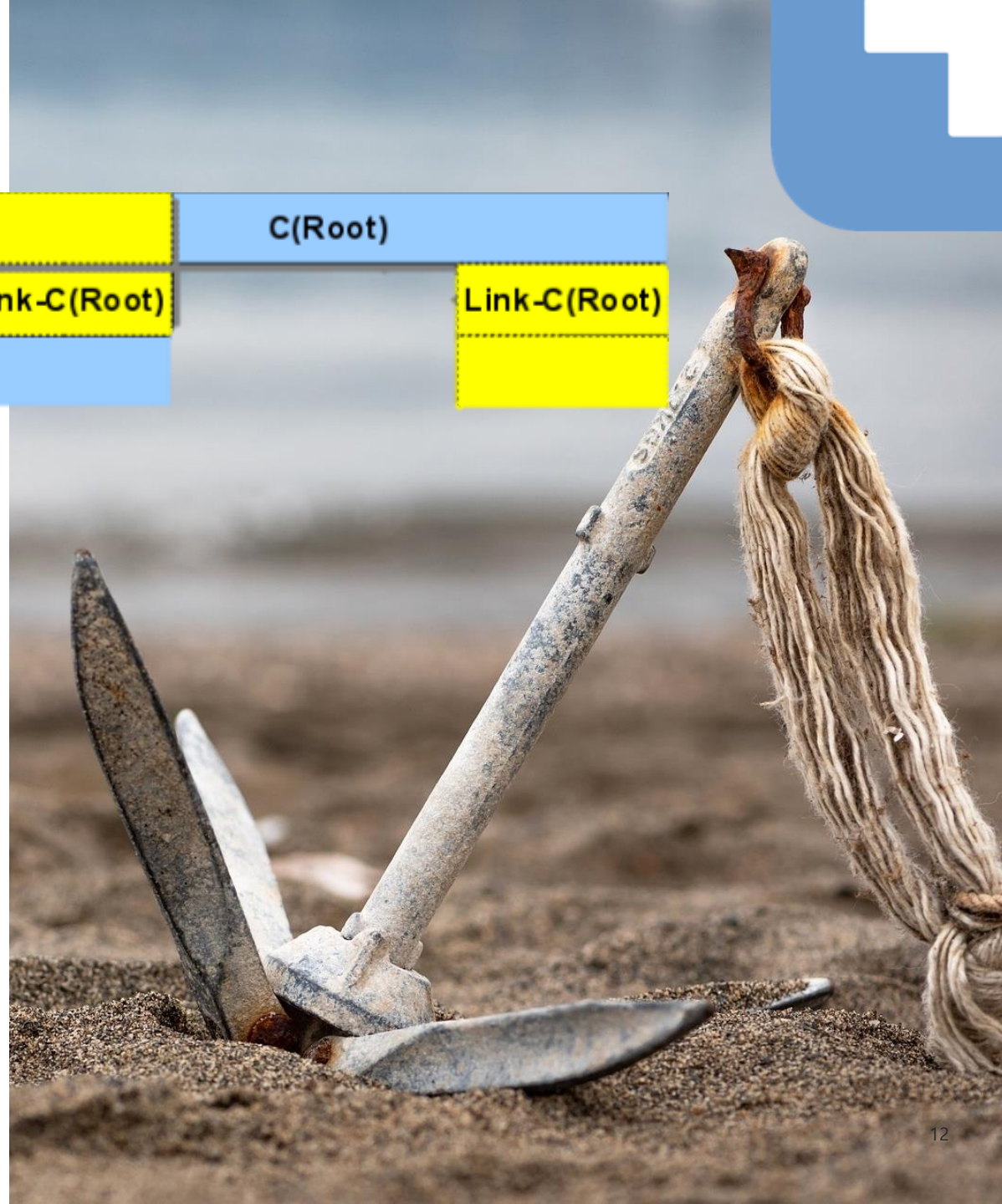
Umgang mit Zertifikaten.

Gültigkeit		Generierung	Stärke
Lang (8 Jahre)	+ Root	Schwierig (vier Augen)	Sehr stark
	+ Sub-CA		
	+ GWA, GWH, aEMT		
Kurz (2 Jahre)	+ SMGW, pEMT	Einfach (automatisch)	Stark

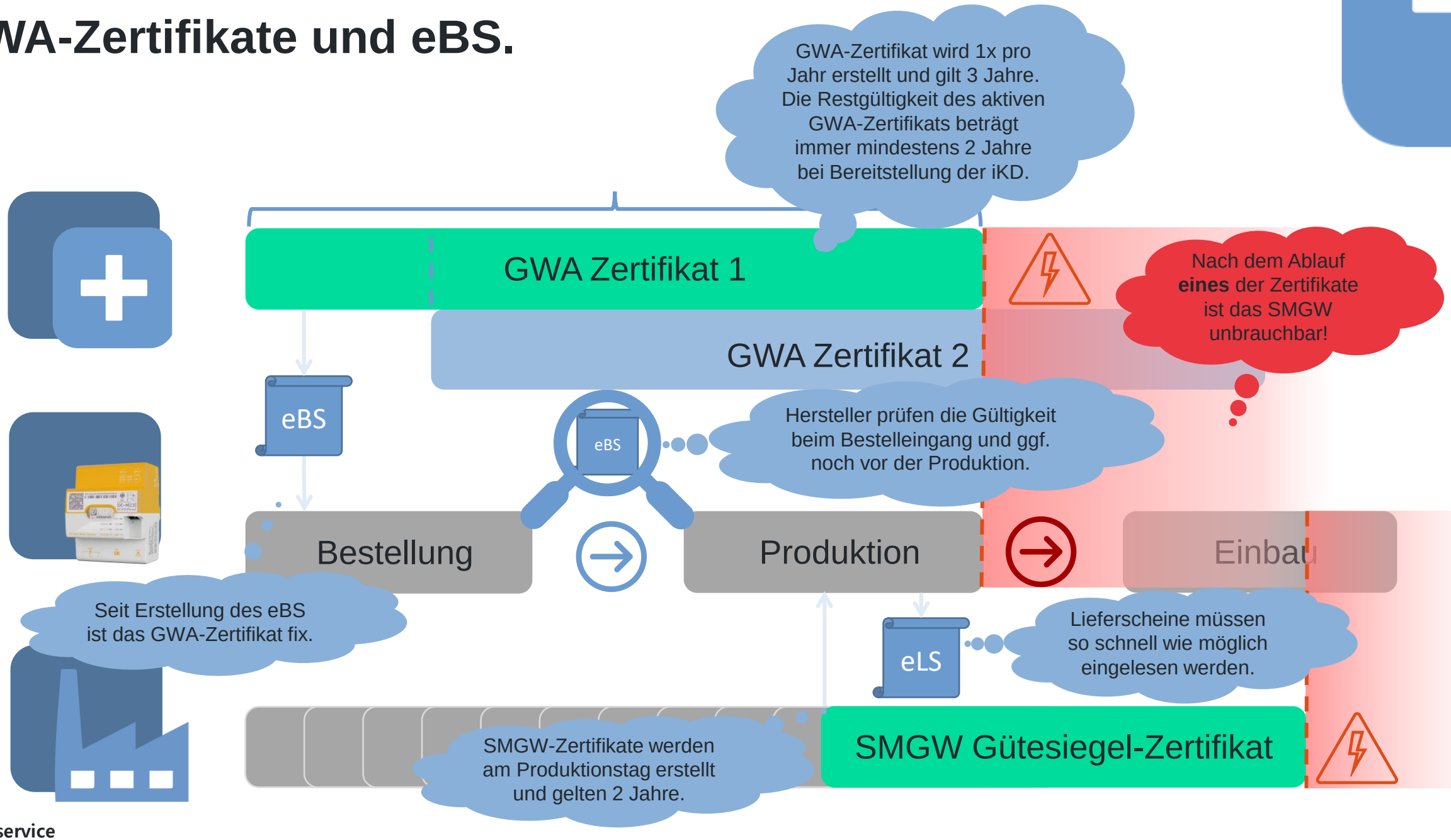
Root-Zertifikat



- Vertrauensanker!
- Schöne Theorie, aber: momentan 3 Root-Zertifikate gleichzeitig gültig
- Verschiedene Auslieferungsstatus der SMGWs
- Mit extremer Vorsicht zu genießen!



GWA-Zertifikate und eBS.



Entsorgung und Zertifikate.

+ Invalidierung der SMGW-Zertifikate notwendig
+ Lösung: Sperrlisten in der PKI
+ Nach Inbetriebnahme – Aufgabe des GWA
+ Vor Inbetriebnahme – **Aufgabe des MSB / GWH**

Zertifizierungen.

- Root-CA: ISO/IEC27001 + TR-03145-1
- Sub-CA: ISO/IEC270011 + TR-03145-1; Nachweis gegenüber Root-CA
- GWH: PTB BMPB + Modul D; BSI-CC-PP-0073 für das SMGW
- GWA: TR-03109-6; Nachweis gegenüber Sub-CA
- SMGW: BSI-CC-PP-0073 + TR-03109-1
- aEMT: ISO/IEC27001 (durch Dritten möglich)
- pEMT: Sicherheitskonzept

BSI-CC-PP-0073.

- + Common-Criteria-zertifikat
- + Prüfung auf Schwachstellen durch BSI
- + Separat für jede Firmware-Version
- + Gültigkeit 2 Jahre, kann (muss aber nicht) verlängert werden.

Nicht zertifizierte SMGWs dürfen nicht im Produktivsystem eingebunden werden.

Wie Sie *souverän* den Überblick behalten?

+ Nicht möglich
+ Es gibt aber Dienstleister und Strukturen, die Sie in der Problematik unterstützen.

Falsch?

Product Consultant Gateway-Administration Energiewirtschaft (m/w/d)

Vielen Dank.

smartservice