
PrimeKey

PrimeKey®

Vertrauenswürdige Ausstellung von digitalen Geräte-Identitäten innerhalb der Fertigungsprozessen

Andreas Philipp
andreas.philipp@primekey.com

PrimeKey. Creating Trust for the Connected Society

Founded
2002

Employees
115+

Ownership
Privately-held

30 bil
certs issued

We develop software and hardware **for PKI and signing**

Offices in:
Stockholm, Sweden
San Mateo, USA
Aachen, Germany
Melbourne, Australia

Home of:
EJBCA.ORG
SignServer.ORG
BOUNCY CASTLE

We believe in **Open Source** – Transparency brings trust

Geräte Identitäten / Geräte Zertifikate

- Basisanforderungen an die Cybersicherheit gemäß IEC 62443-3-3

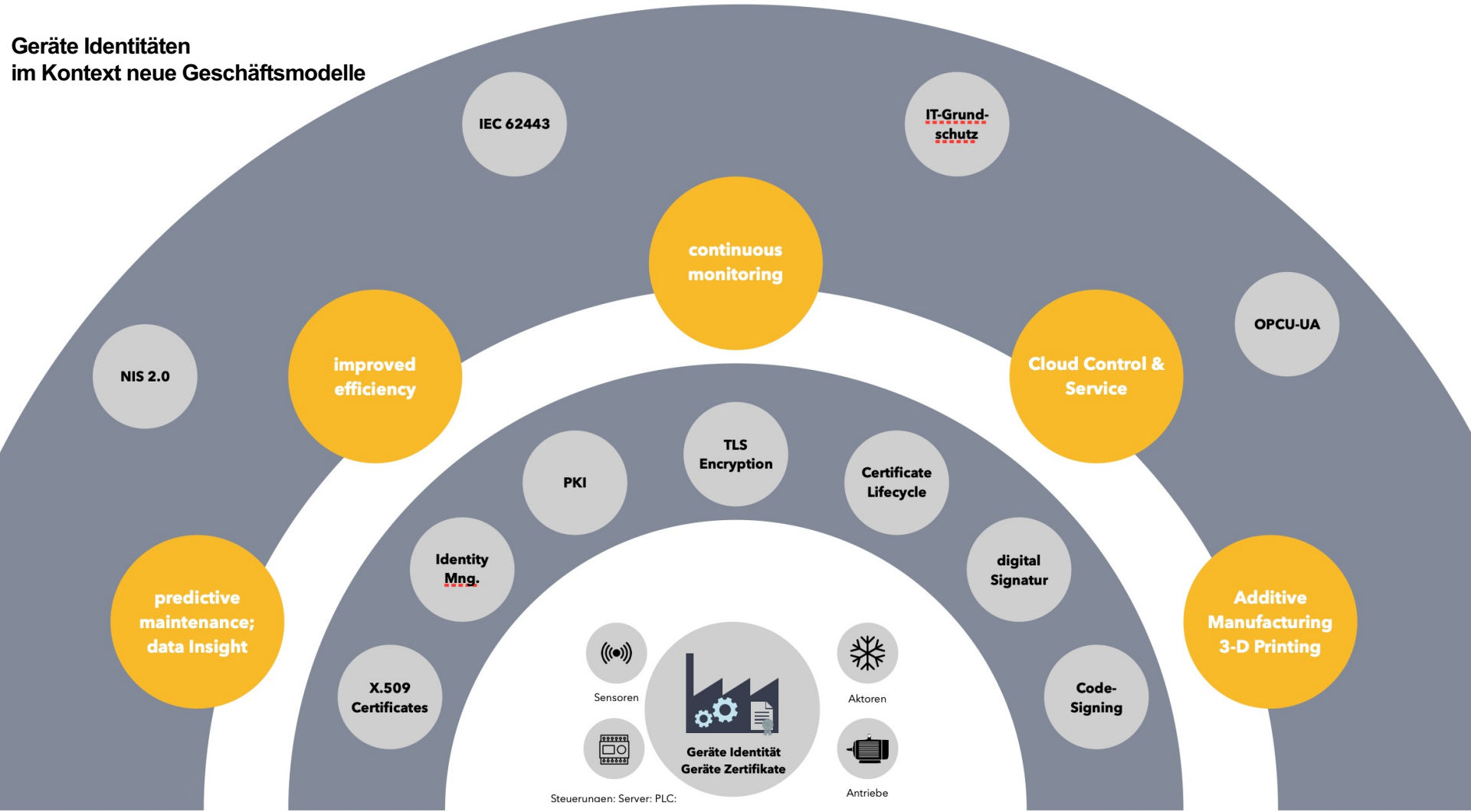
- Grundlage dafür: Geräte Zertifikate
  - Definition: Ein Geräte Zertifikate schafft eine Identität für jede kommunizierende Element in einem IoT-Ökosystem und stellt sicher, dass jedes Gerät bei der Verbindung authentifiziert und die Kommunikation zwischen den Geräten geschützt ist.

Basisanforderungen (Foundational Requirements – FR)

Nr.	Kürzel	Titel	Titel deutsch
1	IAC	Identification and Access Control	Identifizierung und Authentifizierung
2	UC	Use Control	Nutzungskontrolle
3	SI	System Integrity	Systemintegrität
4	DC	Data Confidentiality	Vertraulichkeit der Daten
5	RDF	Restricted Data Flow	Eingeschränkter Datenfluss
6	TRE	Timely Response to Events	Rechtzeitige Reaktion auf Ereignisse
7	RA	Resource Availability	Verfügbarkeit der Ressourcen

Quelle: IEC 62443-3-3

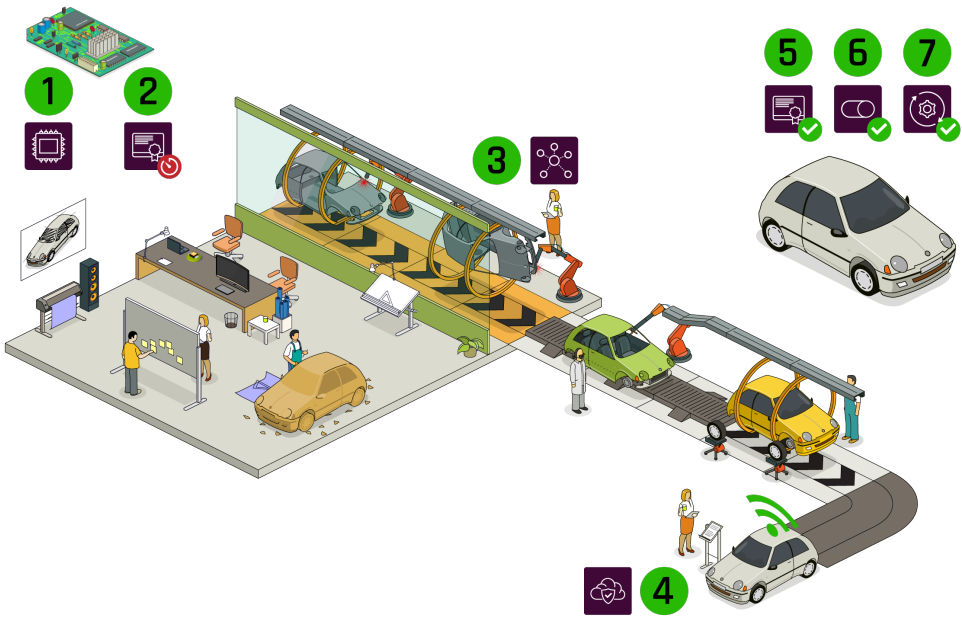
Geräte Identitäten
im Kontext neue Geschäftsmodelle



Der erste Schritt ist entscheidend

- Das „Geburtszertifikat“ ist die Grundlage des Vertrauen!
- Nachweis der Herkunft
- Die Basis aller nachgelagerten Abläufe und Verfahren

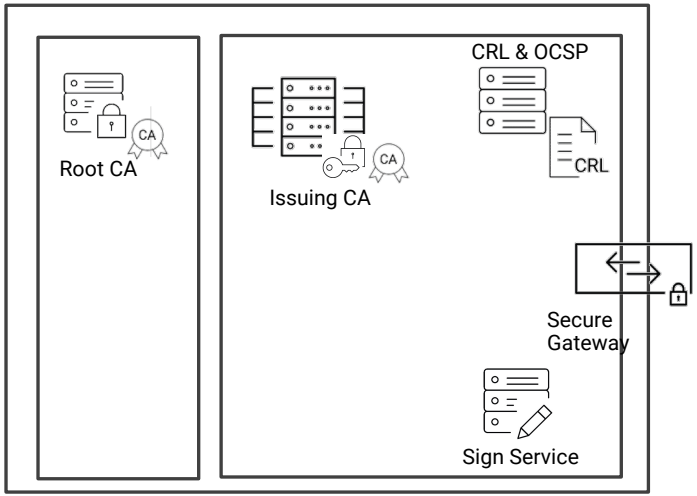
Ausstellung und Verwaltung von Geräte Zertifikaten ist wesentlich!



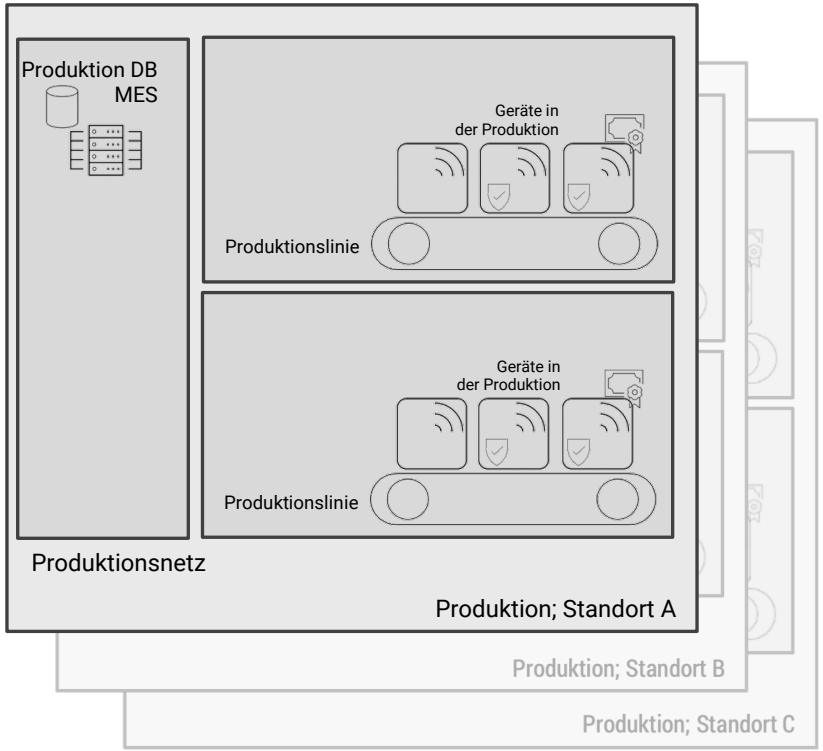
Umsetzung

- Voraussetzung:
  - Zentraler PKI Dienst
  - Ausstellung der Geräte Zertifikate in der Fertigung (weltweit)
  - Überprüfung der Identität im Rahmen der Fertigungsprozesse
  - Einhaltung von Normen und Standards

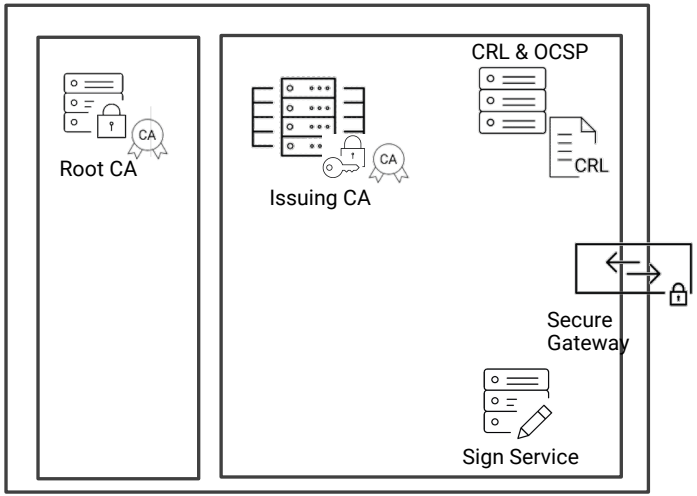
Projektübersicht



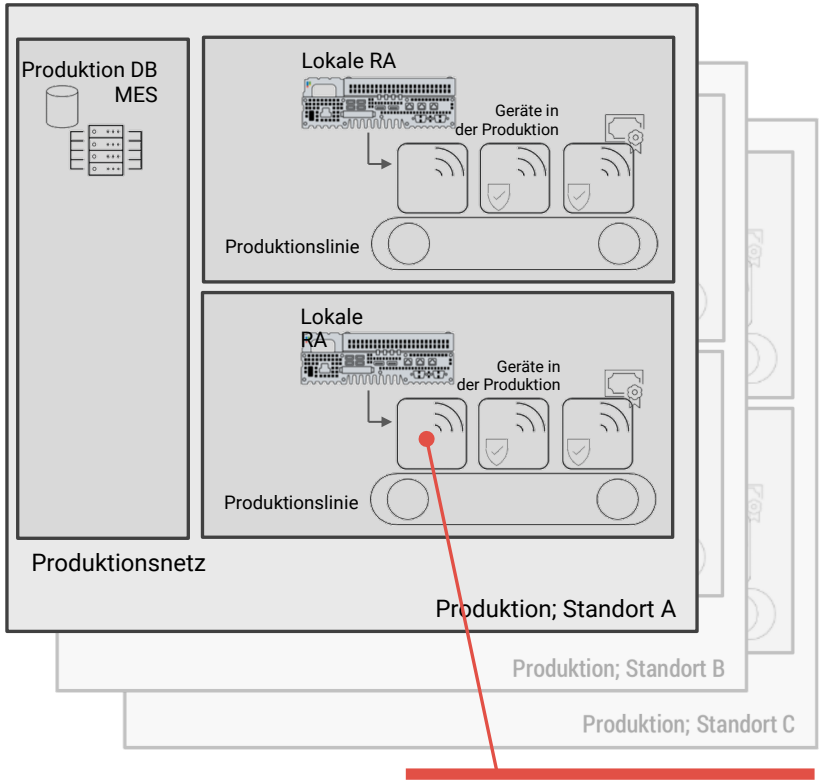
Zentraler PKI-Dienst



Projektübersicht

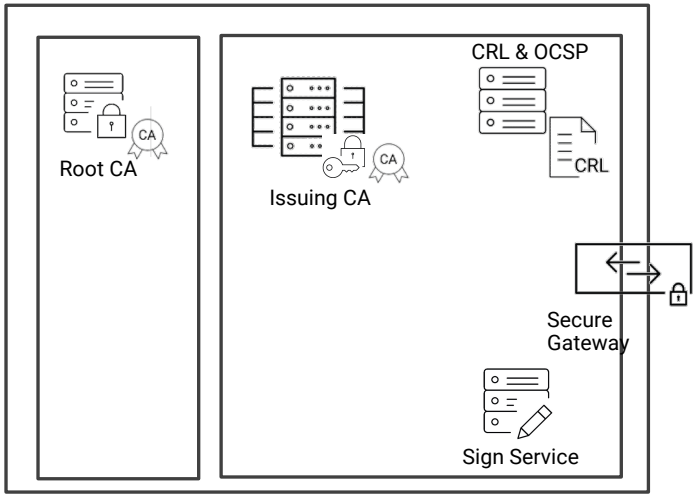


Zentraler PKI-Dienst

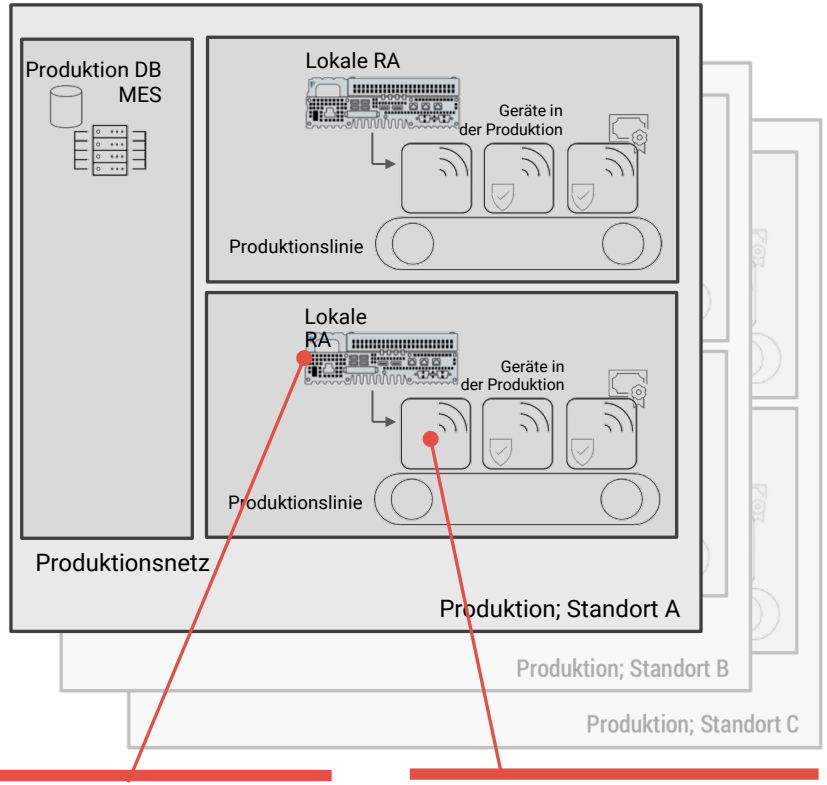


Das **Gerät** in der Produktion erhält seine “Parameter" (Seriennummer, MAC-Adressen, ...). Es hat keine technischen Mittel, um dies zu beweisen, wenn es ein Hersteller-Geräte-Zertifikat anfordert.

Projektübersicht



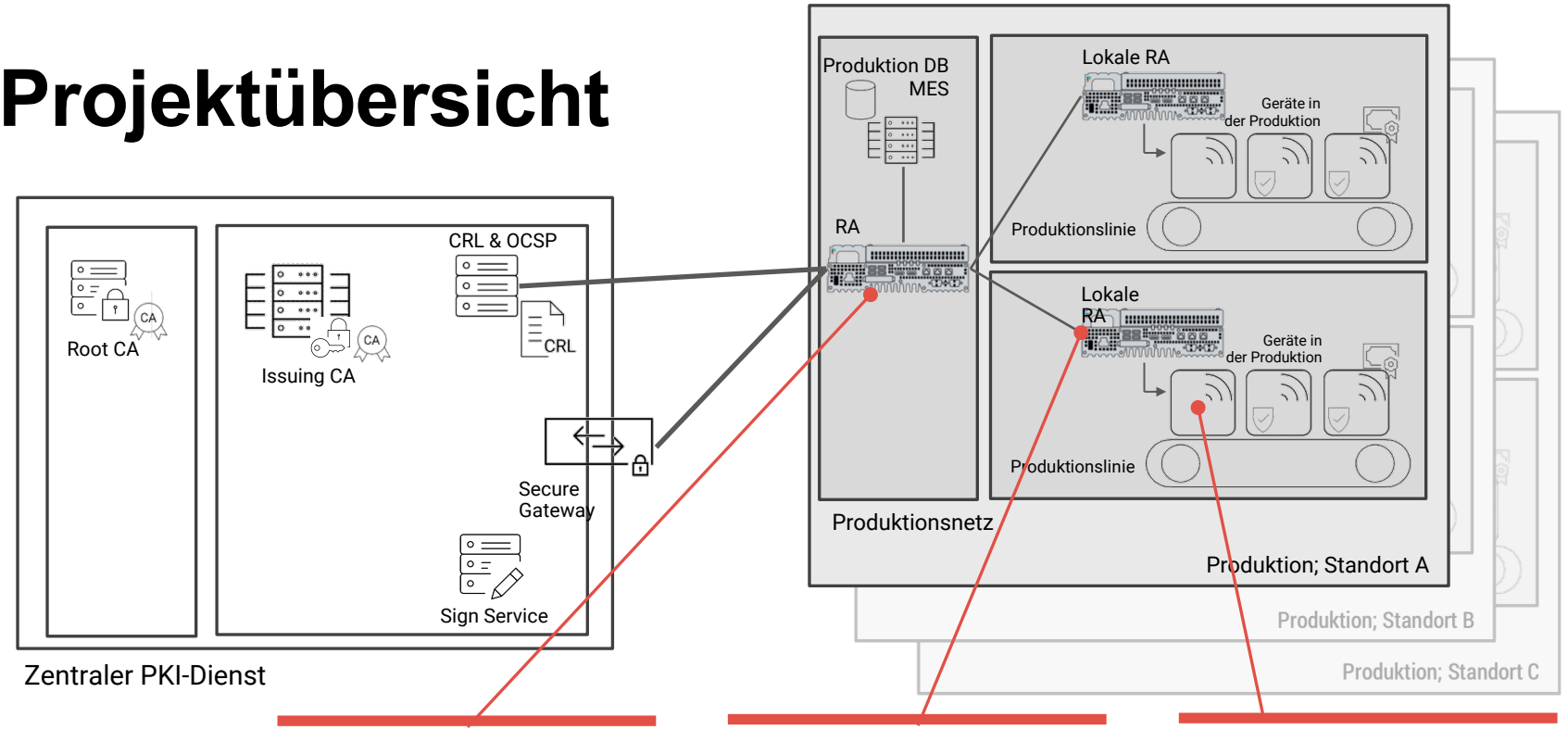
Zentraler PKI-Dienst



Die lokale Registrierungsstelle LRA, befindet sich an der Produktionslinie. Die LRA muss im Namen des Geräts handeln. Sie erstellt oder leitet die Zertifikatsanforderung an den PKI Dienst oder eine zwischengeschaltete Registrierungsstelle (RA) weiter.

Das **Gerät** in der Produktion erhält seine “Parameter" (Seriennummer, MAC-Adressen, ...). Es hat keine technischen Mittel, um dies zu beweisen, wenn es ein Hersteller-Geräte-Zertifikat anfordert.

Projektübersicht

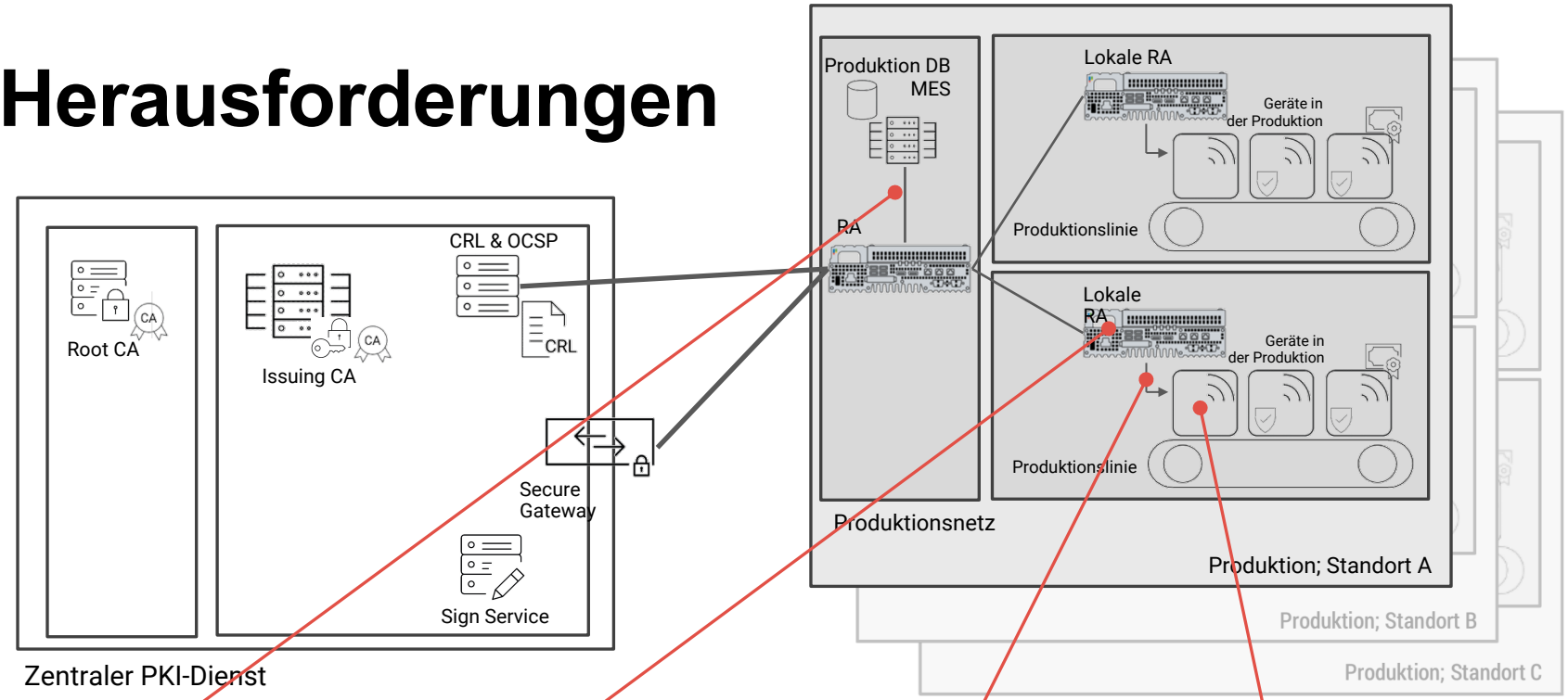


Die Registration Authority (RA) wird zwischen der LRA und dem PKI-Dienst angesiedelt sein. Die Aufgabe der RA besteht darin, die Anfragen zu bündeln und Validierungen, auf Grundlage der Informationen aus Produktions-DB's oder MES durchzuführen.

Die lokale Registrierungsstelle LRA, befindet sich an der Produktionslinie. Die LRA muss im Namen des Geräts handeln. Sie erstellt oder leitet die Zertifikatsanforderung an den PKI Dienst oder eine zwischengeschaltete Registrierungsstelle (RA) weiter.

Das **Gerät** in der Produktion erhält seine "Parameter" (Seriennummer, MAC-Adressen, ...). Es hat keine technischen Mittel, um dies zu beweisen, wenn es ein Hersteller-Geräte-Zertifikat anfordert.

Herausforderungen



Produktionsprozesse
Die LRA / RA muss sich den vor Ort definierten Produktionsabläufen anpassen.

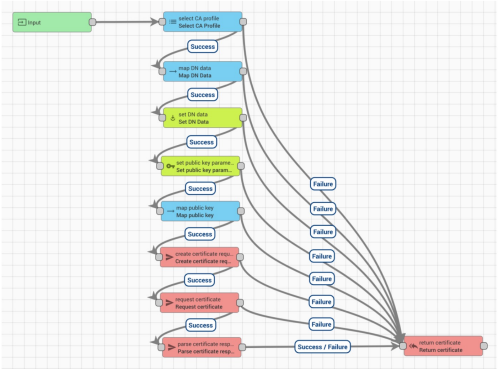
Sicherheit
Die LRA/RA unterliegen eingeschränkter Kontrolle. Hoher Schutz der kryptographischen Mittel.

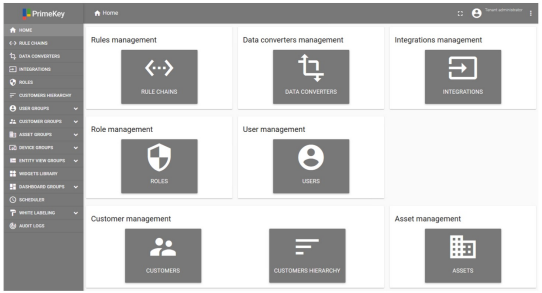
Kommunikation Gerät <-> LRA
Je nach Leistungsfähigkeit des Geräts kann eine Vielzahl von Protokollen verwendet werden, z.B. proprietäres TCP, OPC UA, CMP, REST, ...

Schlüsselgenerierung
Das Gerät generiert sein Schlüsselpaar entweder selbst oder die LRA übernimmt dies im Auftrag des Geräts (z. B. wegen fehlender Entropie oder Rechenleistung).

Lösung

- IPC basierte LRA Lösung
- Netzwerktrennung Geräte Seite / PKI Anbindung und Administration
- Graphische Workflow Modellierung
- Adapterkonzept zu Adaptierung von proprietären Kommunikationsschnittstellen





Ausblicke

- automatische Aktualisierung der LRA-Zertifikate
- Protokollierung und Überwachung
- Informations-Dashboard
- Unterstützung des Lightweight CMP Profile und EST
- Unterstützung von Anforderungen für digitale Signaturen
- SDK für “self-defined“ Enrollment Funktionen

First industrial grade PKI Registration Authority

Digital Identities for Industry 4.0

With a combination of trusted digital certificate issuing mechanisms and standards, a powerful hardware platform, as well as an integrated solid security concept, the Identity Authority Manager enables a secure issuing process in complex environments, such as manufacturing.

Birth certificates — the enabler for trusted supply chains

A trusted and secure birth certificate can enable automated deployment, operation and revocation or discontinuation processes for the device or unit during the lifecycle and thus remove complexity and save costs.

Flexible device registration

Flexibility and adaptivity are key for a successful smart factory solution. Following these principles, the Identity Authority Manager provides a comprehensive toolbox for implementation in any manufacturing environment.

Andreas Philipp
andreas.philipp@primekey.com