Fachhochschule Dortmund

ruhr valley

if(is) internet-sicherheit.

Concept of a Life-Cycle Management with Tamper Resistant Distributed Cyber-Physical Systems

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
FORSCHUNG AN FACHHOCHSCHULEN

CONCEPT OF A LIFE-CYCLE MANAGEMENT WITH TAMPER RESISTANT DISTRIBUTED CYBER-PHYSICAL SYSTEMS

KONZEPT EINES LIFE-CYCLE-MANAGEMENTS MIT MANIPULATIONSSICHEREN VERTEILTEN CYBER-PHYSISCHEN SYSTEMEN

VORTRAG: DAVID BOTHE

ANDREAS PUESCHE, PROF. DR. SABINE SACHWEH, PROF. DR. (TU NN) NORBERT POHLMANN

INHALT

- CYBER-PHYSISCHE SYSTEME UND DAS INTERNET DER DINGE
- SICHERHEITSMERKMALE
- LIFE-CYCLE ÜBERSICHT
- (KRITISCHE) PHASEN DES LIFE-CYCLE
- FAZIT

Fachhochschule
Dortmund

ruhr valley

if(is)
internet-sicherheit.

CYBER-PHYSISCHE SYSTEME UND DAS INTERNET DER DINGE

CYBER-PHYSISCHE SYSTEME UND DAS INTERNET DER DINGE

Cyber-physische Systeme (CPS) = Internet of Things (IoT)
?

CYBER-PHYSISCHE SYSTEME UND DAS INTERNET DER DINGE

Cyber-physische Systeme (CPS):

- **Cyber-physisch** – Kombination aus rechnerischen und physischen Elementen
- **Cyber** – Software, Betriebssystem, „Rechnersystem“
- **Physisch** – Aktoren und Sensoren
- **Auswirkung** – Reale Welt (Motor, Hebearm, Pumpe, …)
- **Lokal** – CPS die lokal vernetzt sind
- **Vernetzt (IoT)** – CPS, die über unsichere Netzwerke (Internet) kommunizieren

  - Können also IoT-Komponenten besitzen!

CYBER-PHYSISCHE SYSTEME UND DAS INTERNET DER DINGE

Dependability (Zuverlässigkeit) eines verteilten CPS hängt ab von:

- **Availability (Verfügbarkeit)** – Fähigkeit, mit dem CPS zu kommunizieren.
- **Reliabilty (Ausfallsicherheit)** – Stabil laufendes CPS, ohne Unterbrechungen
- **Safety (Arbeitssicherheit)** – Keine Konsequenzen für Nutzer und Umgebung (Realwelt-Auswirkung CPS)

(Internet-) Sicherheit eines verteilten CPS hängt ab von:

- **Integrity (Integrität)** – Keine Manipulation der Hard- oder Software des CPS
- **Confidentiality (Vertraulichkeit)** – Schutz der (Anwender-) Daten vor Enthüllung
- **Authenticity (Authentizität)** – Glaubwürdigkeit bei Kommunikation mit CPS (Manipulierte Sensordaten?)

Quelle: A. Hoeller and R. Toegl, “Trusted Platform Modules in Cyber-Physical Systems: On the Interference Between Security and Dependability, “ 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, 2018, pp. 136-144. Concept of a Life-Cycle Management with Tamper Resistant Distributed Cyber-physical Systems |

Fachhochschule Dortmund

ruhr valley

if(is)
internet-sicherheit.

SICHERHEITS-MERKMALE

SICHERHEITSMERKMALE

Trusted Platform Module (TPM):

- **Hardware** – passiver, fest verbauter Chip, physisch getrennt vom Rest des Systems
- **Schlüssel** – Erzeugen von Schlüsseln
- **Ablage** – sicheres Ablegen von Schlüsselmaterial (Storage Root Key)
- **Crypto** – Enthält kleinen kryptografischen Co-Prozessor zum Ver- und Entschlüsseln
- **Zufallszahlen** – Eigener *True Random Number Generator* (Random nicht vom System abhängig)
- **Integrität** – Messen der Manipulationsfreiheit durch Referenzwerte (z.B. Bootprozess „aufzeichnen“)

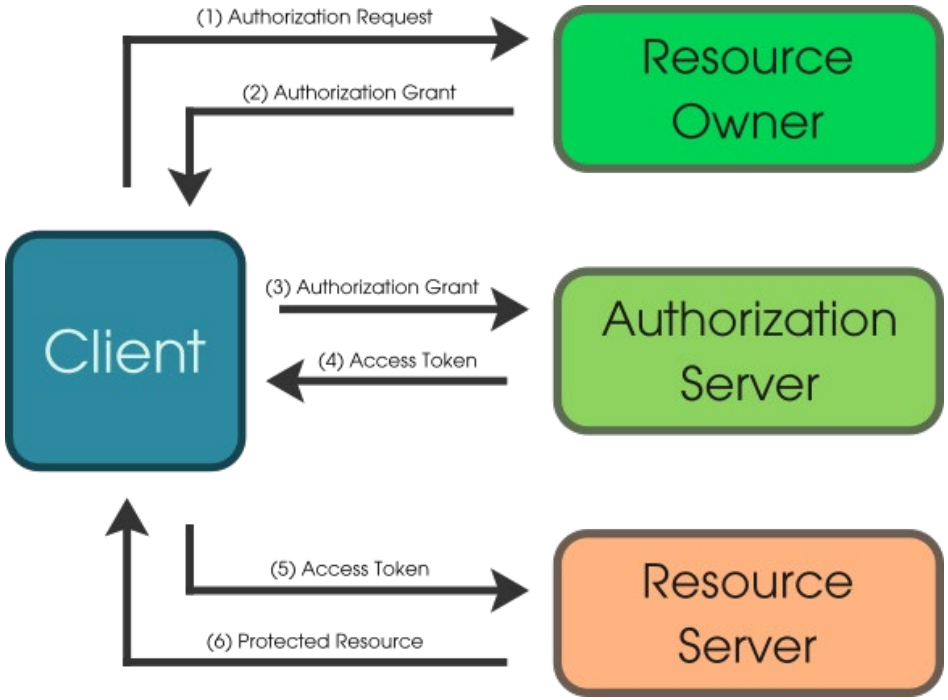
SICHERHEITSMERKMALE

Transport Layer Security (TLS):

- **HTTPS** – Ermöglicht sichere Kommunikation über unsichere Netzwerke (Internet)
- **Client/Server Authentication** – Server authentifiziert sich gegenüber Client und umgekehrt

Open Authentication (OAuth2.0):

- **Framework** – Zugriff auf Ressourcen durch Anwendungen anhand rollenbasierter Zugriffsrechte

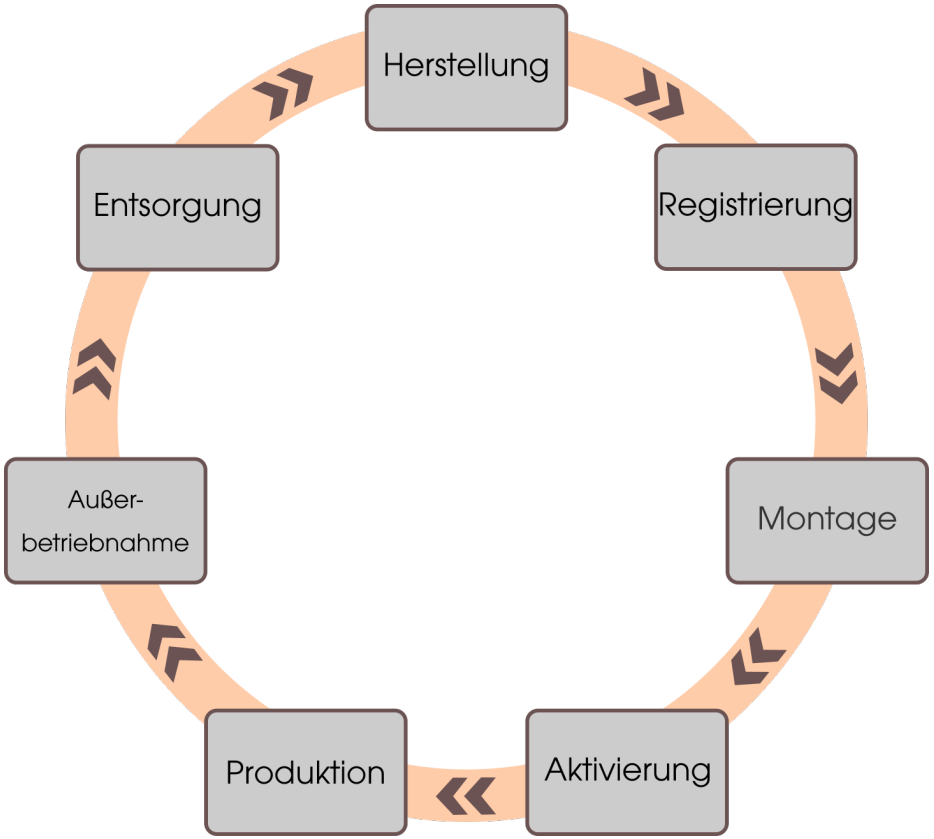


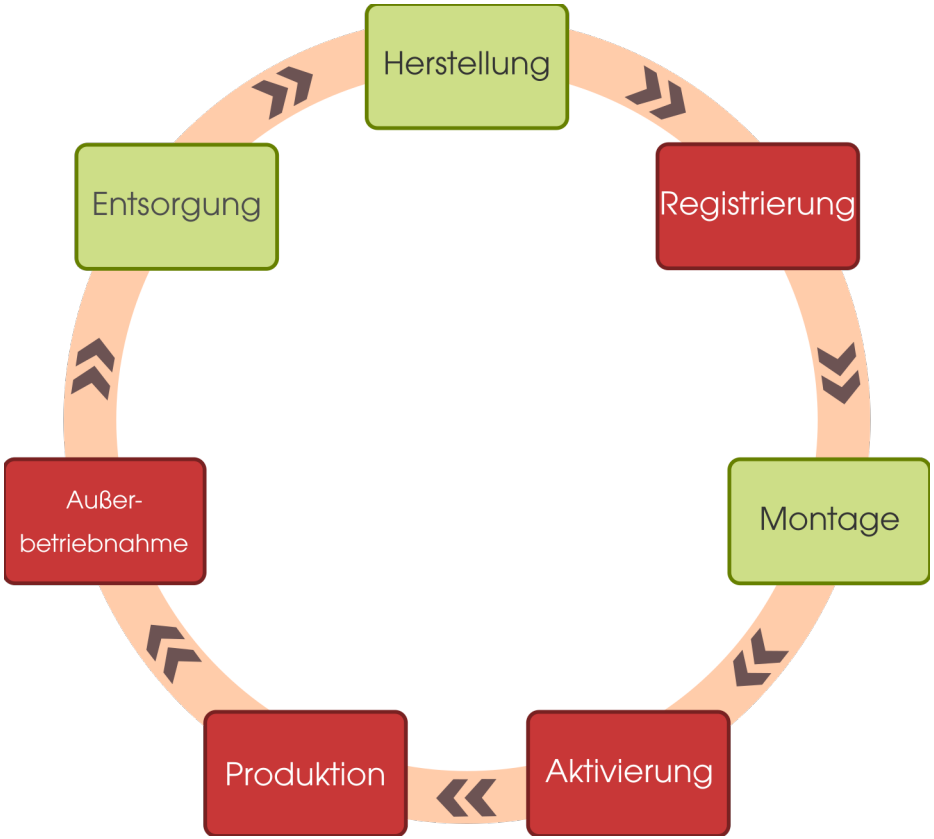
Fachhochschule
Dortmund

ruhr valley

if(is)
internet-sicherheit.

LIFE-CYCLE ÜBERSICHT


Herstellung
Registrierung
Montage
Aktivierung
Produktion
Außer-
betriebnahme
Entsorgung


Herstellung
Registrierung
Montage
Aktivierung
Produktion
Außer-
betriebnahme
Entsorgung

Fachhochschule
Dortmund

ruhr valley

if(is)
internet-sicherheit.

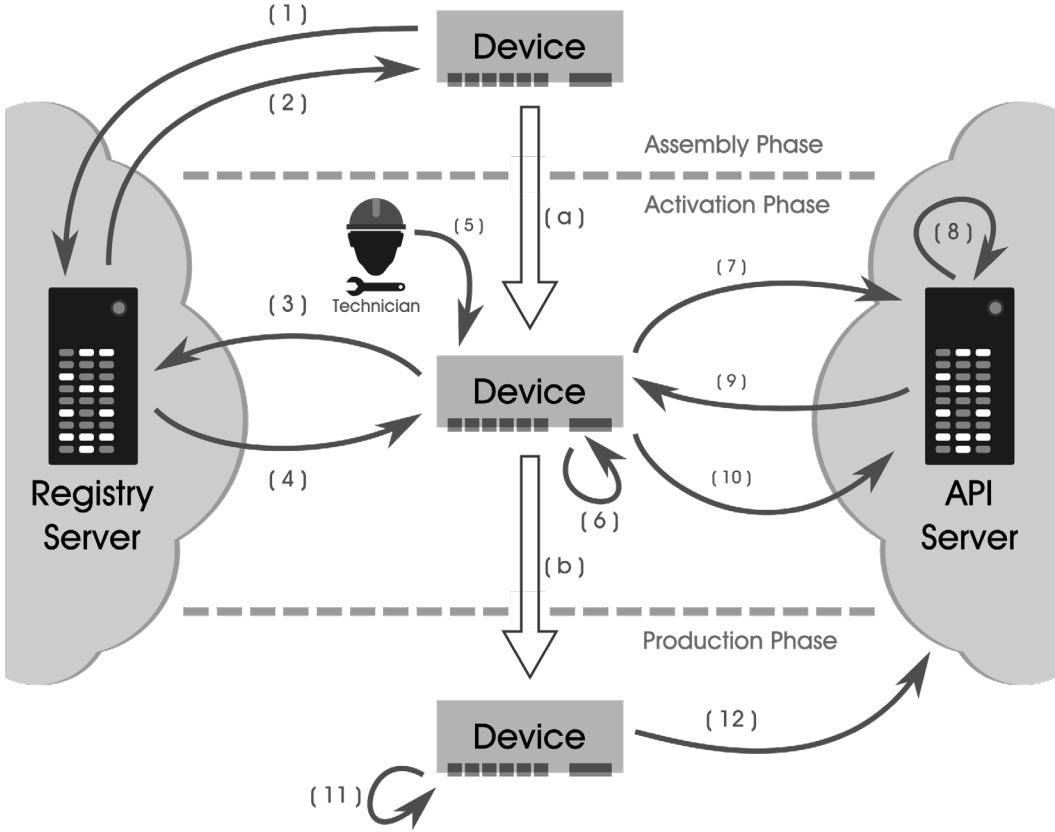
(KRITISCHE) PHASEN DES LIFE-CYCLE

HERSTELLUNG

- **Firmware** – Frei von unbekannter und unerwünschter Software
- **Identifier** – Eindeutige ID erzeugen und sicher abspeichern (Seriennummer)
- **Trusted Platform Module (TPM)** – Storage Root Key (SRK) für TPM erzeugen (Ownership) Schlüssel erzeugen um ID zu verschlüsseln.

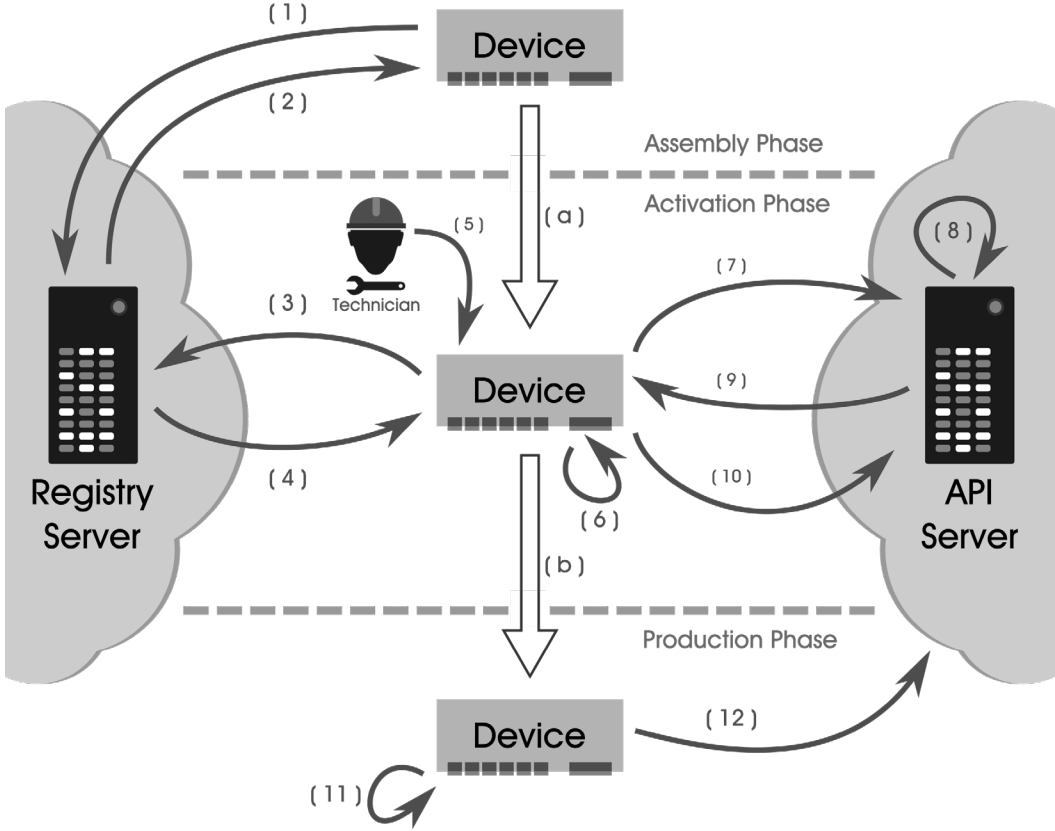
SRK:

- hierarchische Schlüsselstruktur
- verlässt TPM nicht



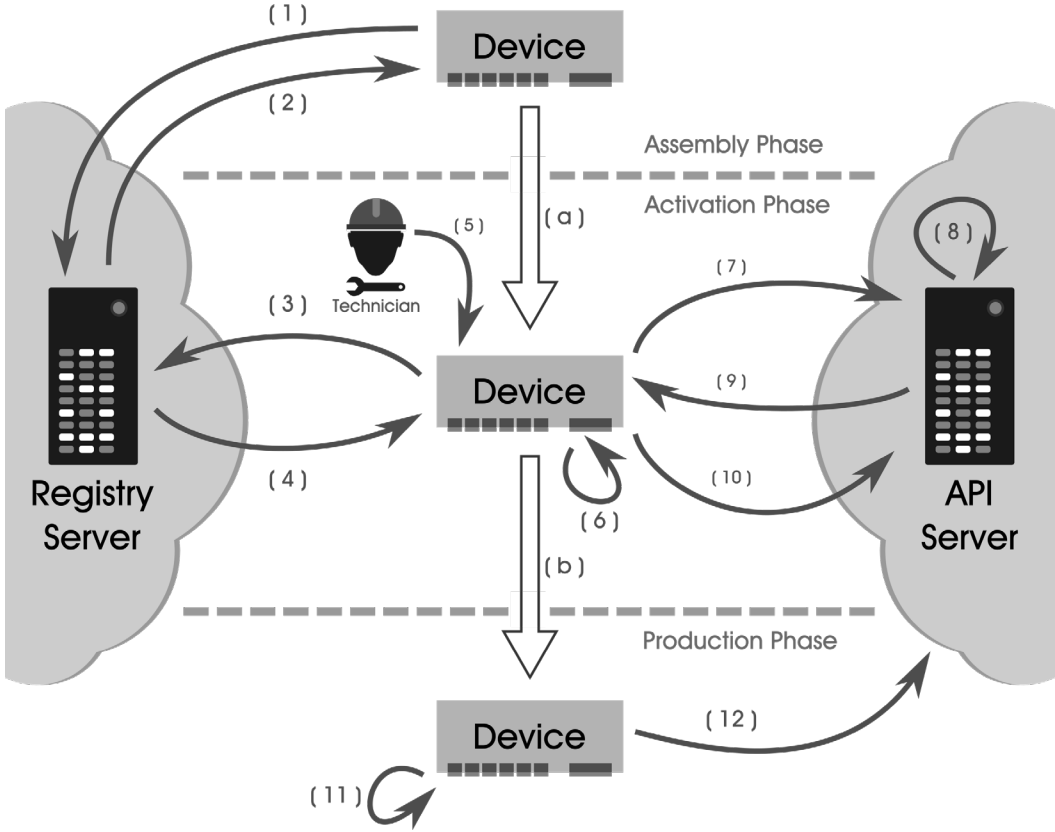
REGISTRIERUNG (KRITISCH)

- **Backend** – Manuelle Registrierung der Seriennummer in Cloud (1) (Whitelist)
- **Vorbereitung** – One-Time Token, Zertifikat und Schlüsselpaar erzeugen und auf dem Gerät ablegen. (2)
- **Whitelisting** – Auslieferung durch Hersteller, Geräte bekannt. Keine unregistrierten Geräte in Umlauf.



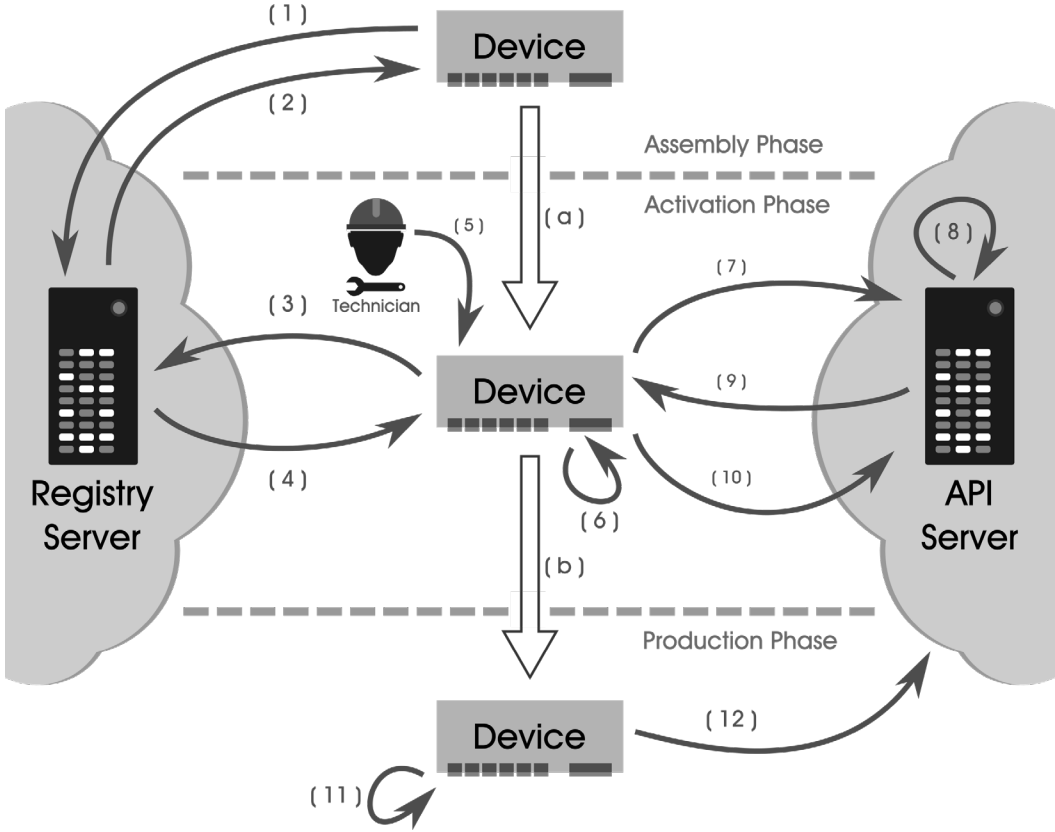
MONTAGE

- **Installation** – Techniker montiert das Gerät am Bestimmungsort. Das Gerät verlässt den Hersteller. Die Umgebung ist nicht mehr kontrolliert. (a)
- **Anschluss** – Externe Komponenten und Energieversorgung.
- **Verbindung** – Aufbau einer Internetverbindung zur Cloud.



AKTIVIERUNG (SEHR KRITISCH) 1/2

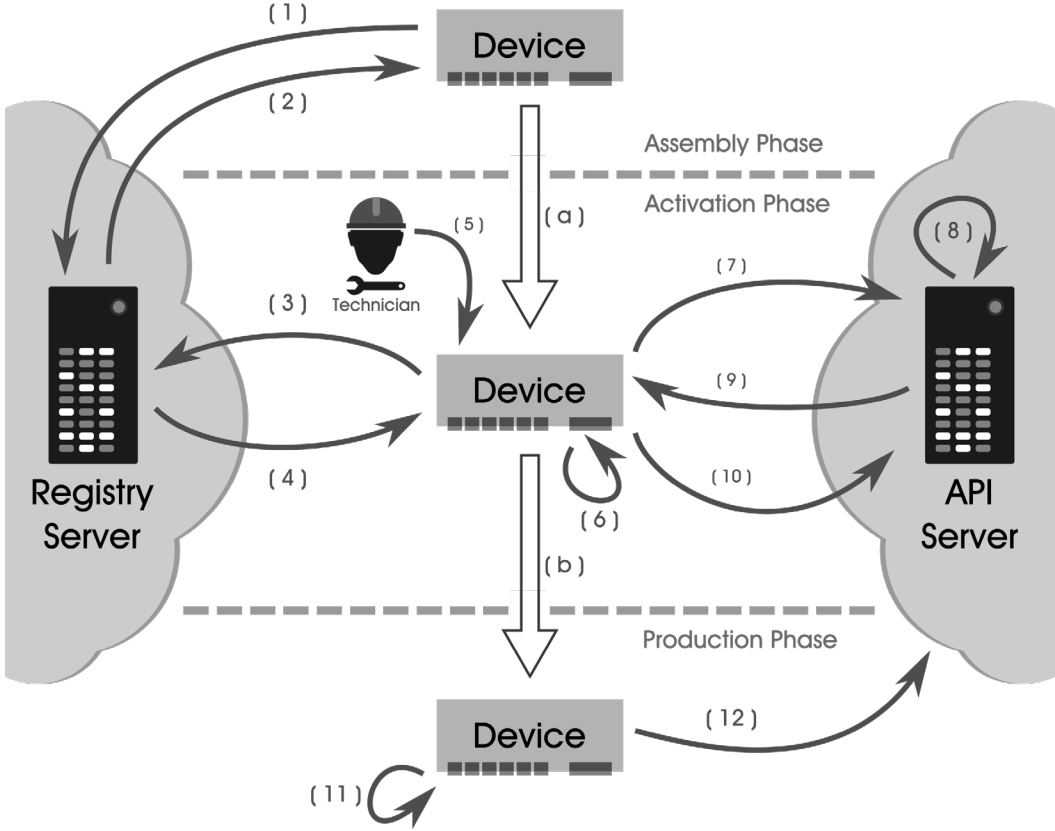
- **Startup** – Erstanmeldung des Geräts anhand Zertifikat + One-Time-Token. (3)
- **Setup** – Neues Setup Token durch Cloud für API Zugriff während Aktivierung.
- **Techniker** – Stellt eigene Authentifikation bereit (Smartcard, Token, ect.) (5)
- **Keys** - Gerät erzeugt Schlüsselpaar (6)
- **Cert** - Gerät stellt Zertifikat-Request an API Server mit Schlüssel + Techniker-Auth. (7)



AKTIVIERUNG (SEHR KRITISCH) 2/2

- **Sign** – Server signiert bei Erfolg Zertifikat-Request (8)
- **Final Cert** – Finales Zertifikat für den Client sowie ein Token für OAuth2.0 an Gerät ausstellen (9)
- **TPM** – Initialisierung aller Komponenten und sichere Ablage aus (9) mit SRK
- **Clear** – Alle ehemaligen Tokens werden ungültig (Cloud)
- **Connect** – erste erfolgreiche API Verbindung (10)

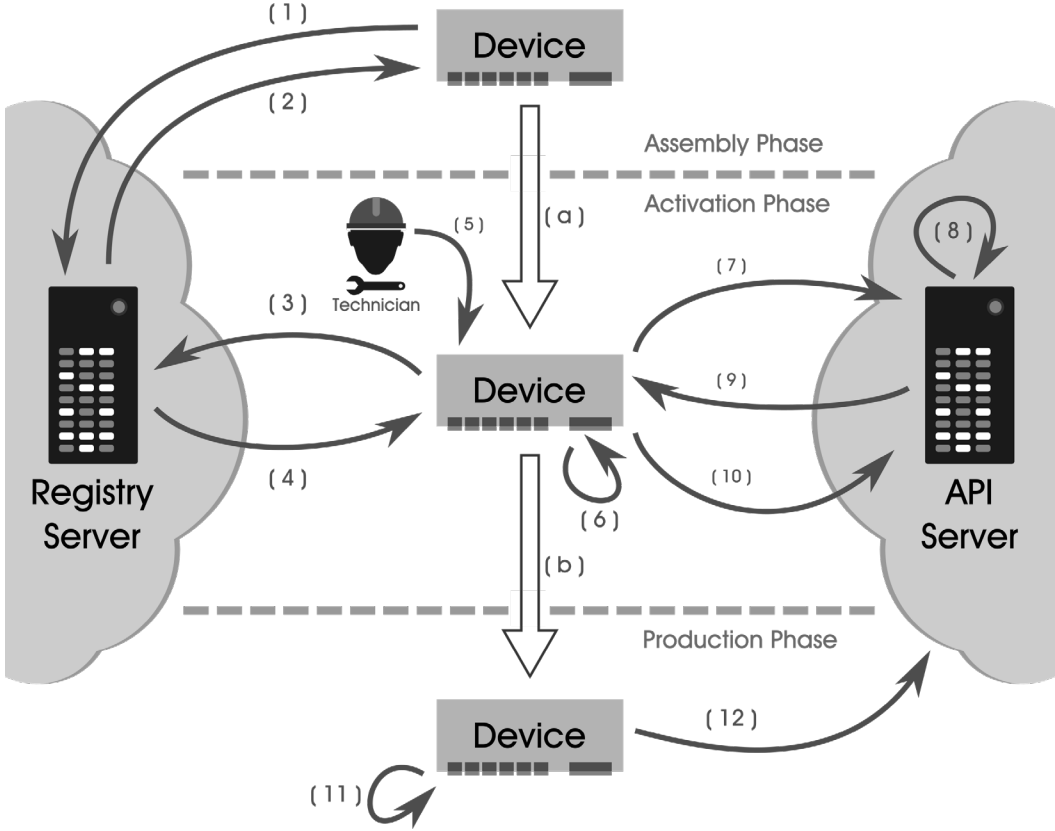
Sequenz als TRANSAKTION!



PRODUKTION (KRITISCH)

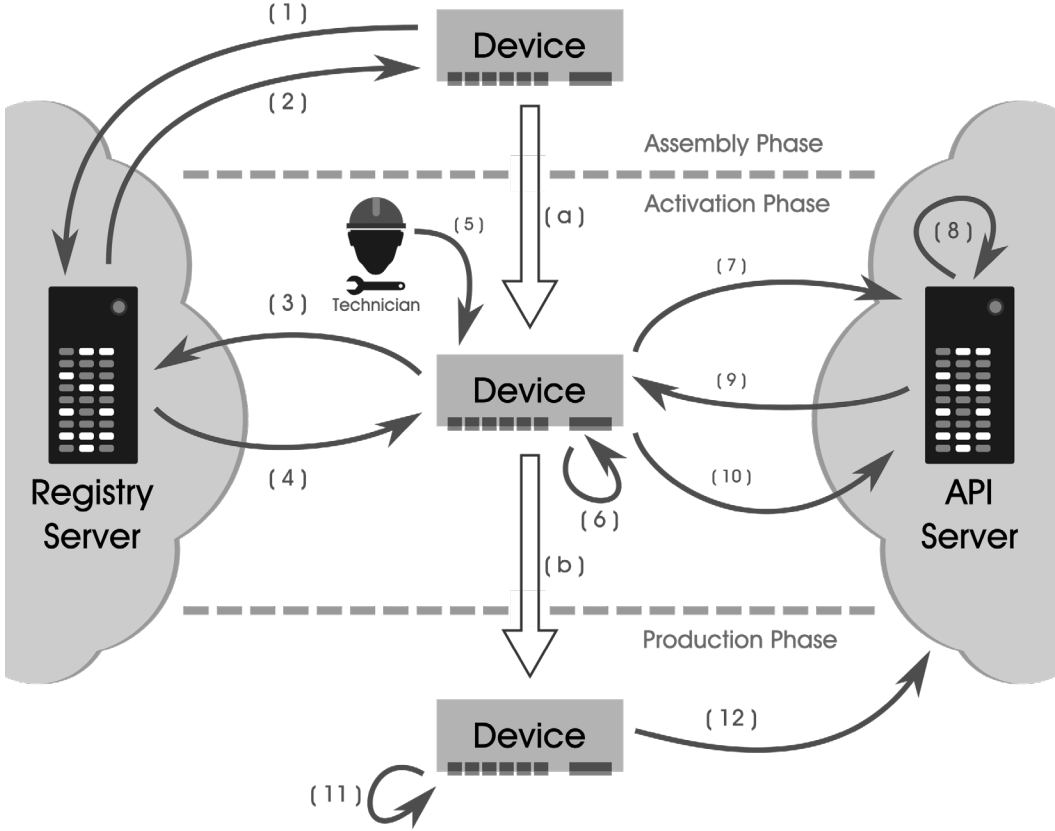
- **Restart** – Neustart des Geräts (11), Aufnahme der Betriebsphase (b) und erster Login (12)
- **Integrity**– Regelmäßiges Prüfen der Systemkonfiguration (Software-Komponenten) per TPM und Report an Cloud.
- **Cloud** – deckt manipulierte Geräte auf und entscheidet über Verarbeitung
- **Updates** – TPM Messungen ebenfalls!

Cloud kann verschiedene Maßnahmen unternehmen: Kommunikation verweigern, Quarantänedaten, ect.



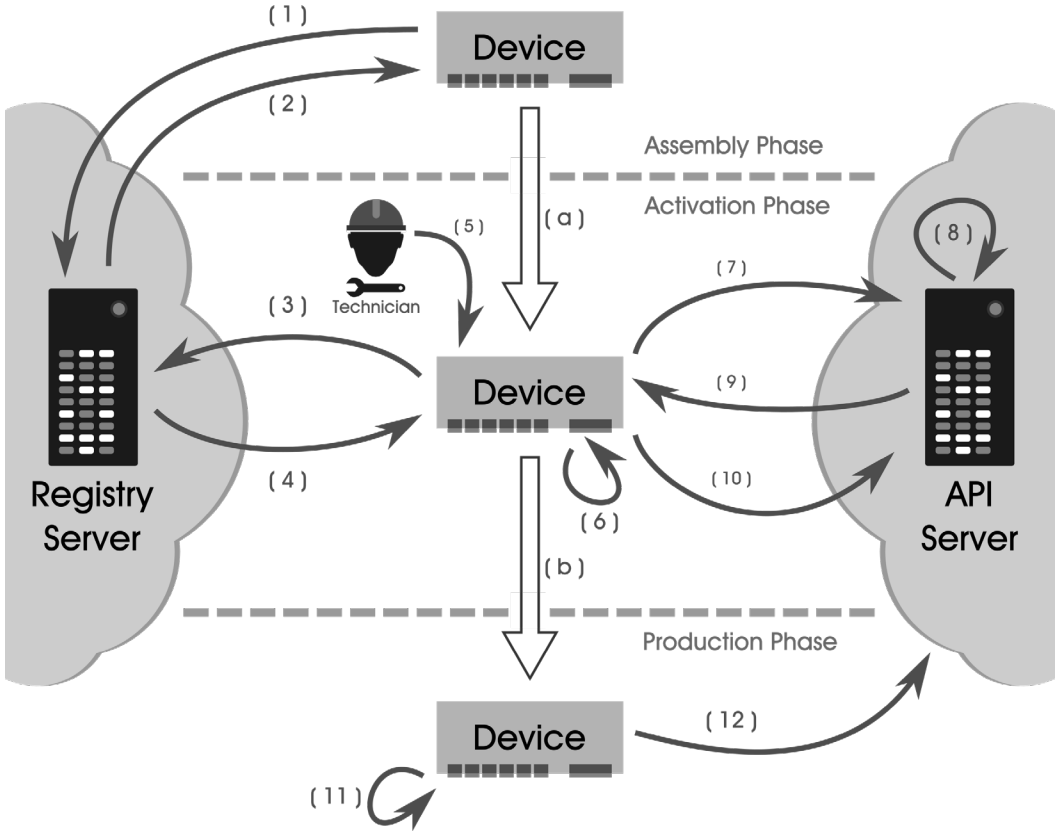
AUßERBETRIEBNAHME (KRITISCH)

- **Flag** – Markieren der Geräte durch Betreiber.
- **Techniker** – Spezifischer Techniker demontiert Gerät. Schlüsseltausch analog zu Aktivierungsphase.
- **Time** – Zeitdifferenz zwischen den Phasen, kritische Nutzerdaten müssen entfernt werden (DSGVO)
- **TPM** – Entleeren (Clear) aller Werte.
- **Memory** – Speicher sowie Arbeitsspeicher werden überschrieben/geleert.



ENTSORGUNG

- **Hardware** – Nur noch „nacktes“ Gerät übrig.
- **Recycle** – Gerät kann recycelt werden.



Fachhochschule
Dortmund

ruhr valley

if(is)
internet-sicherheit.

FAZIT

FAZIT

Einfluss der CPS auf reale Welt

Verteilte Systeme

Hohe Sicherheitsanforderungen

Verteilung erfordert sicheres und durchgeplantes Protokoll

Fachhochschule Dortmund

if(is) internet-sicherheit.

Kontakt

Institut für Internet-Sicherheit – if(is)
Neidenburger Str. 43
45897 Gelsenkirchen

David Bothe

Vertrauenswürdige IT-Systeme

bothe@internet-sicherheit.de

Paper:

pohlmann@internet-sicherheit.de

andreas.puesche@fh-dortmund.de

sabine.sachweh@fh-dortmund.de

ruhr valley

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
FORSCHUNG AN FACHHOCHSCHULEN