VE-ASCOT: Sichere Elektronikkomponenten mit einer CHAIN OF TRUST

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Pitch zur Digitalen Fachkonferenz Vertrauenswürdige Elektronik 2022

Referent: Ralf Fust, **WIBU-SYSTEMS AG**, Karlsruhe

FKZ: 16ME0270K, Verb.Nr. ME2ZEUS001

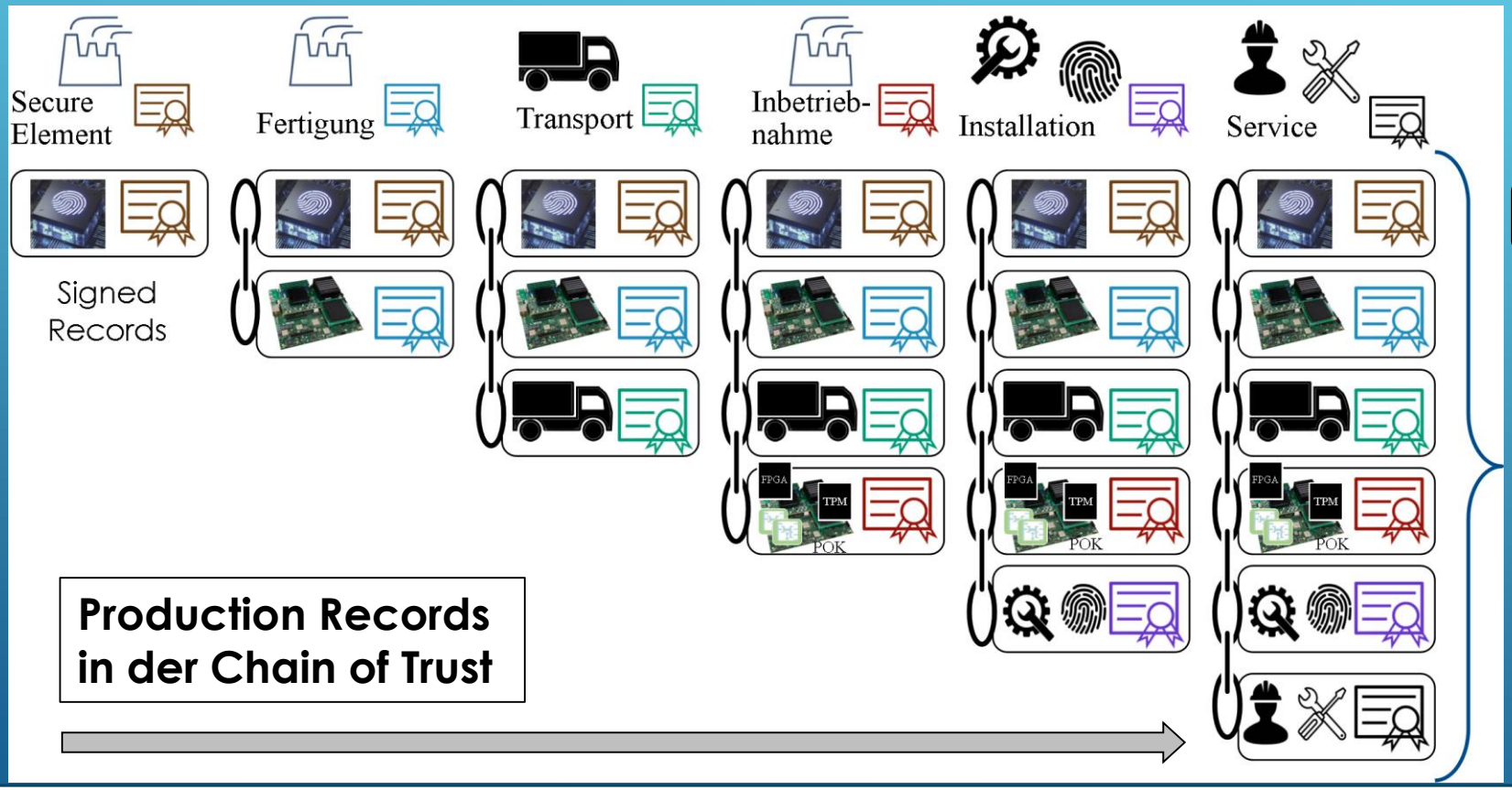
PRODUCT LIFE CYCLE MANAGEMENT MIT EINER COT

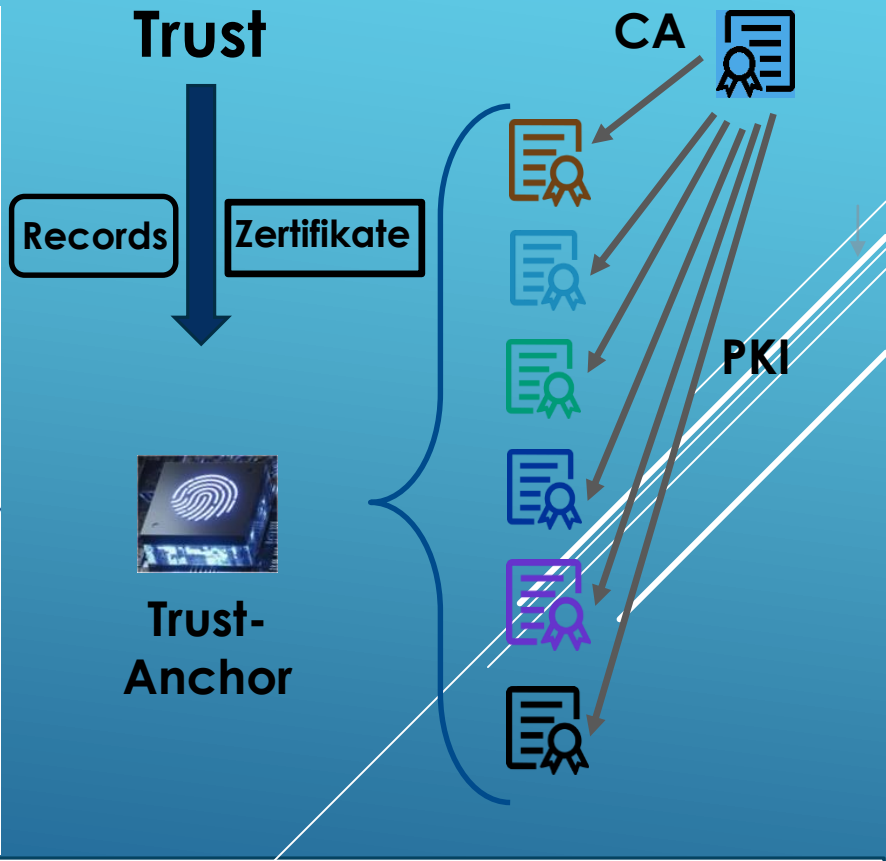
Trusted Split-Manufacturing
Komponenten Integration
Erstellung DID

Fingerprinting,
HW Merkmale,
TPM, Erstellung DID

Echtheitsnachweis,
HW/SW-Attestation
DID, Multiple Stage
Secure Boot

Vertrauensinfrastruktur
Herstellerverband, CA





HARDWARE FINGERPRINTING

Klassifizierung Merkmale

deterministisch
statisch

stochastisch
dynamisch

Klassifizierung Elektronische Komponente

gleich

einzigartig

Merkmals-Baukasten

TPM

Chip Power

Temp. Verlauf

POK /PUF

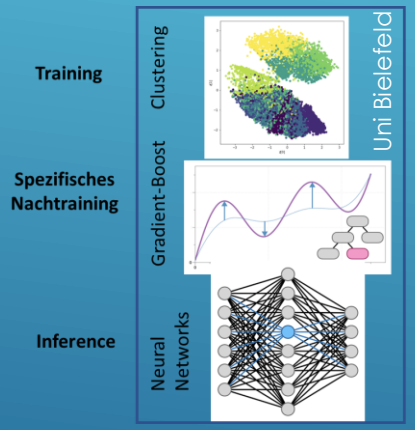
Chip Serial

Speicher-auslastung

Infineon

Überprüfung

Challenge Response
Vergleich/Verlauf
Systemantworten
KI-Methoden
Attestation



Trusted Boot

Pre-Boot

Check

Post-Boot

OK

OK

OK

Fail

activate

Trust-Anchor

stop/restart…

DEMONSTRATOR UND ANALYSE

Medical Use Case

- High Resources
- High Security Requirements

FPGA Xilinx UltraScale – Research Platform

HW-Plattform Identifier (statisch)
- PL-PUF
- Device DNA
- Device IDs

Verified Boot Manager

FW-Update

Dyn. partielle Rekonfiguration

Betriebssystem
1. Zephyr/FreeRTOS @Cortex R5
2. Linux (Cortex @Cortex A53, RISC-V

Secure FPGA Subsystem

HW-Fingerprints (zur Laufzeit: Merkmale intern & extern)

KI-basierte Klassifikation der Integrität (pre/post-boot)

Applikation

TPM

WIBU Secure Element

Infineon POK

Measurement Environment

Industrial Use Case - Siemens

- Low (Battery) Power
- Low Ressources
- High Safety and Security Level
- Wireless Sensor Connection
- Firmware- Update OTA

Siemens AG

Analyse und Prüfmethoden

- Bewertung unterschiedlicher Verfahren zur Merkmalsauswertung – KI-basiert vs. konventioneller Logik
- Integration von Open Source Architektur – Risc-V
- Vergleich TPM 2.0 vs. Secure Element – Synergieeffekte

Sichere
Elektronikkomponenten
mit einer **Chain of Trust**

Vielen Dank

VE-ASCOT