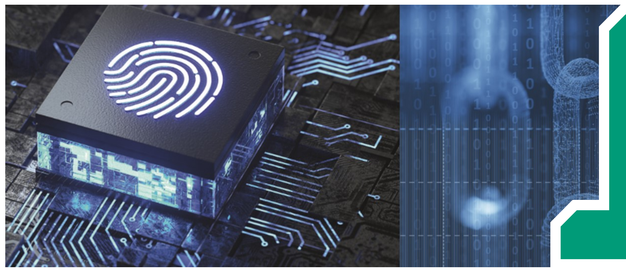


VE-ASCOT Vertrauenswürdige Elektronikkomponenten mit einer Chain of Trust

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
FKZ:16ME0270K

Velektronik

Ziele & Chain of Trust (CoT)

In verteilten Produktionsprozessen elektronischer Baugruppen spielt das Vertrauen in alle beteiligten Hersteller eine zentrale Rolle um qualitativ hochwertige Komponenten produzieren zu können. Hier ist das Vertrauen in eine hohe Fertigungsqualität von Bauelementen gefragt, aber auch das Vertrauen in die korrekte Funktionsweise und Integrität der gesamten elektronischen Komponente. Das hier gewählte Mittel zur Herstellung von Vertrauen innerhalb eines Produzenten- und Herstellerverbands ist die Einführung eines Abbilds des Produktions- und Inbetriebnahmeprozesses in Form einer kryptografisch gesicherten Chain of Trust (CoT). Produktionsschritte sowie insbesondere auch spezifische Merkmale der Hardware Komponente werden in Form eines geschützten Datensatz zentral auf der elektronischen Baugruppe sicher abgespeichert und können dann jederzeit auch während der Betriebsphase für eine Überprüfung ausgelesen und kryptografisch geprüft werden.

Industrial Use Case

Die Zustandsüberwachung von industriellen Anlagen wie Energie- oder Transportinfrastruktur mit IoT Geräten verfolgt u.a. das Ziel, Wartungsarbeiten vorauszusagen und die Ersatzteilbeschaffung zu optimieren. Neben einer sicheren Datenübertragung zwischen IoT Geräten und Cloud, muss das Vertrauen in Hardware und Software sicher gestellt sein. In ASCOT wird dies anhand von Traktionstransformatoren für Bahnanwendungen demonstriert.

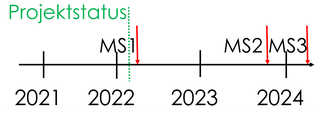
Medical Use Case

SCHÖLLY ist ein international führender Hersteller von medizinischer Gerätetechnik im bildgebenden Anwendungsbereich der Endoskopie. Mit der Erfahrung in der Herstellung von zertifizierter Elektronik wirkt Schölly bei der Bereitstellung eines Demonstrators zur Bildverarbeitung in der Medizintechnik mit.

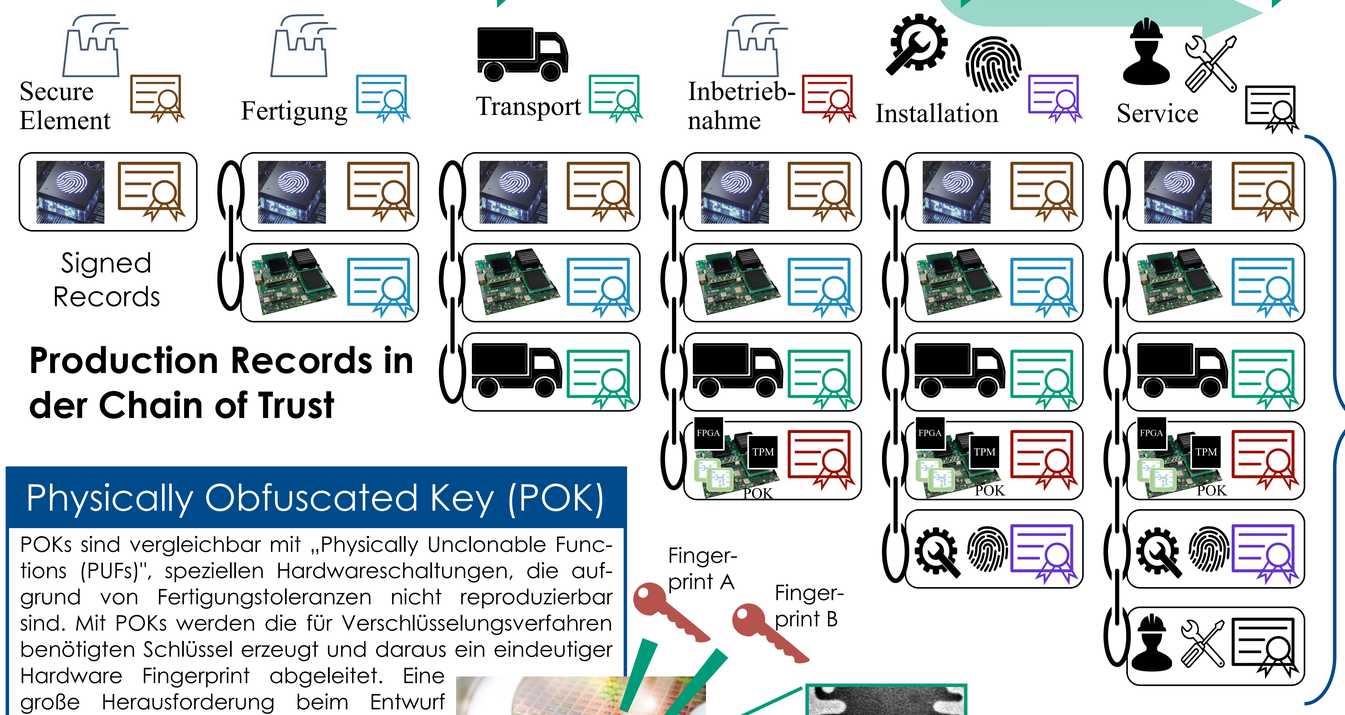
VE-ASCOT at a Glance

Koordinator:	WIBU-SYSTEMS AG
Ansprechpartner:	Ralf Fust
Projektvolumen:	4,71 Mio. €
Projektlaufzeit:	01.03.2021 - 29.02.2024
Projektpartner:	Gemäß Firmenlogos unten
Techology Readiness Level (TRL):	
Verified Boot	3 -> 5,
Demonstratoren	2 -> 5
POK	3 -> 4
COT	2 -> 4
TPM	4 -> 5
KI	2 -> 4

Projektstatus



Fertigung – Fingerprinting – Betrieb



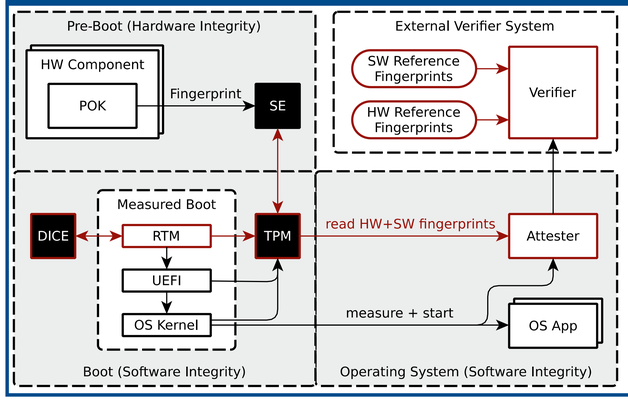
Production Records in der Chain of Trust

Physically Obfuscated Key (POK)

POKs sind vergleichbar mit „Physically Unclonable Functions (PUFs)", speziellen Hardwareschaltungen, die aufgrund von Fertigungstoleranzen nicht reproduzierbar sind. Mit POKs werden die für Verschlüsselungsverfahren benötigten Schlüssel erzeugt und daraus ein eindeutiger Hardware Fingerprint abgeleitet. Eine große Herausforderung beim Entwurf stellt die Absicherung gegen Hardware-Backdoors dar, weshalb POKs bislang nicht in hochintegrierten Schaltungen eingesetzt wurden.

Ausnutzung von Fertigungstoleranzen (Infineon)

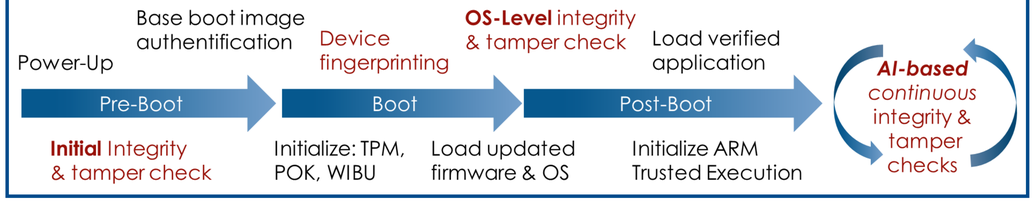
Trusted Computing & Integrity Verification



Die Verzahnung von Hardware- und Softwareintegrität erfolgt mithilfe des Trusted Platform Modules (TPM) 2.0 unter Verwendung des TPM-Ökosystems (Trusted Boot, TPM 2.0 Software Stack (TSS2) und Remote Attestation). Die Device Identifier Composition Engine (DICE) soll für die Absicherung der Integrität von Peripherie-Komponenten auf dem Board erfolgen. Verfahren, Protokolle und Datenstrukturen sollen in der Trusted Computing Group (TCG) und der IETF standardisiert werden.

Secure Boot & Fingerprinting

Die Verfahren zum Secure Boot auf FPGA-Basis stellen sicher, dass ausschließlich authentifizierte Hard- und Software genutzt wird. Aus den charakteristischen Merkmalen der Hardwarekomponenten sowie der Umgebungs- und Betriebsparameter wird ein eindeutiger Fingerabdruck des Gesamtsystems erstellt. Durch eine kontinuierliche Prüfung der Merkmale zur Laufzeit werden mit Hilfe von KI-Methoden Veränderungen durch Dritte sicher erkannt.



Kontakt
Ralf Fust
ralf.fust@wibu.com
www.ascot-trust.info

WIBU SYSTEMS · UNIVERSITÄT BIELEFELD · SIEMENS Ingenuity for life · Fraunhofer SIT · Infineon · KIT Karlsruher Institut für Technologie · Schölly EXCELLENCE INSIDE (Assoziierter Partner) · ReVisionOne Engineering GmbH (Unterauftragnehmer)