T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2013
Berlin, 04. - 05.11.2013

Integritätsschutz durch ‚Security by design‘

Dr. Peer Wichmann
WIBU-SYSTEMS AG

Übersicht

- Vorstellung
- Voraussetzungen
- Bedrohungsszenarien
- Code-und Daten-Integrität
- Vorwärtstest
- Rückwärtstest
- Authentifizierungskette

Peer Wichmann

- Über 20 Jahre im Gebiet Kryptographie und Systemsicherheit
- Promotion zum Thema ‚systematische Analyse‘
- Leiter einer Forschungsgruppe am Forschungszentrum Informatik in Karlsruhe
- Professorenvertreter in Karlsruhe
- Lehrbeauftragter am HPI in Potsdam
- Seit 2004 Kryptograph bei einem Anbieter für ‚Dongles‘

Voraussetzungen

- Symmetrische Kryptographie
  - Verschlüsselung von Massendaten (AES)
- Asymmetrische Kryptographie
  - Schlüsselpaar, Signatur (RSA, ECDSA)
- Kryptographische Hashfunktionen
  - ‚Fingerabdruck' von Daten (SHAx)
- Zertifikate
  - Authentisierung öffentlicher Schlüssel
  - Zertifikatsketten

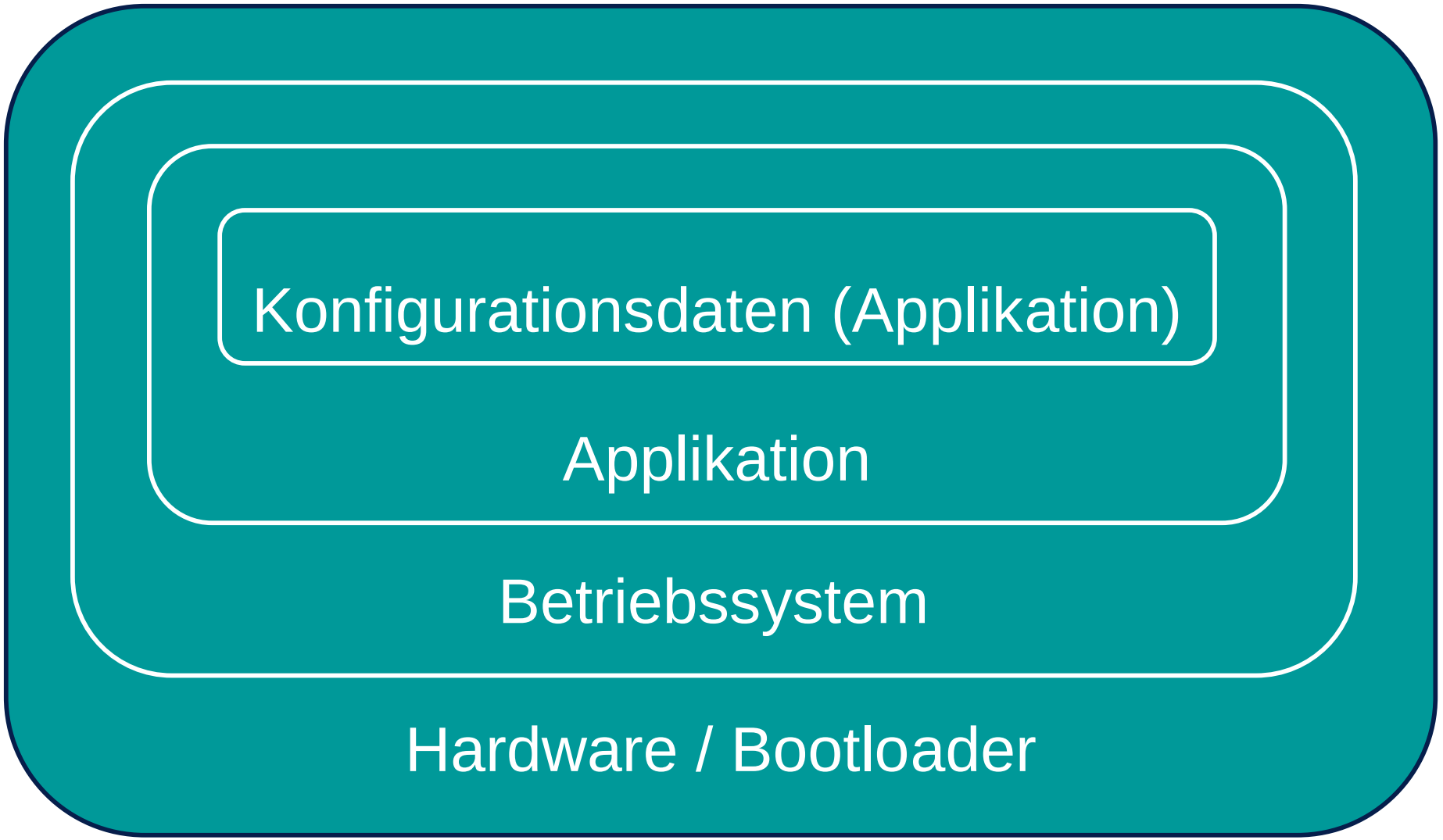
Bedrohungen

- Der Angreifer dupliziert ein Gerät in Aussehen und Funktionalität. Er tauscht die Gräte aus.
- Der Angreifer erstellt neue Software und tausche den Datenträger aus.
- Der Angreifer modifiziert Software oder Daten auf dem Datenträger.
- Der Angreifer verändert Software oder Daten aus der Ferne.
- Hardware wird gestohlen und analysiert.

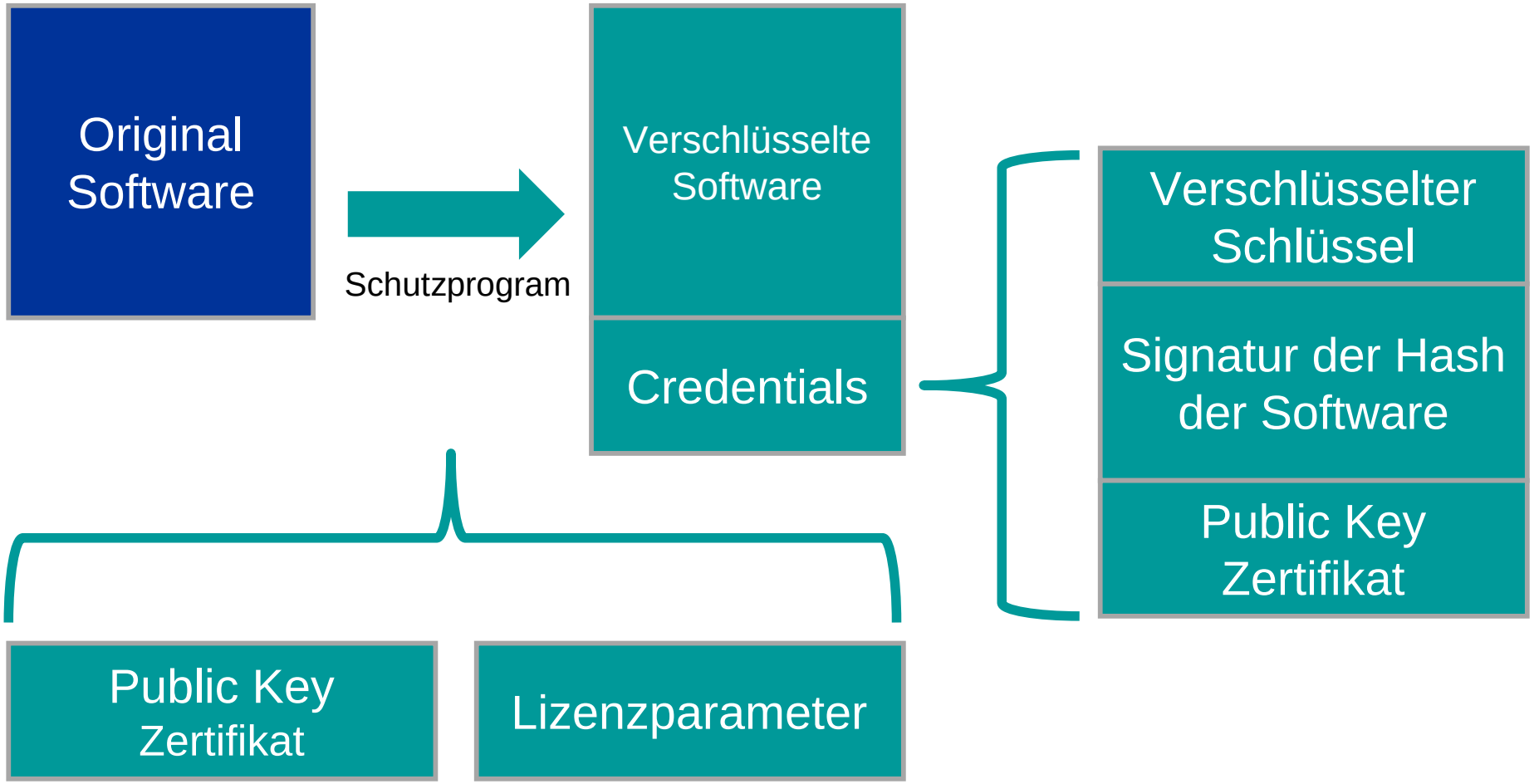
Code- und Daten-Integrität

- ‚Alle Komponenten überprüfen sich gegenseitig‘
  - Bootloader
  - Betriebssystem
  - Applikation
  - Konfiguration

Systemstruktur



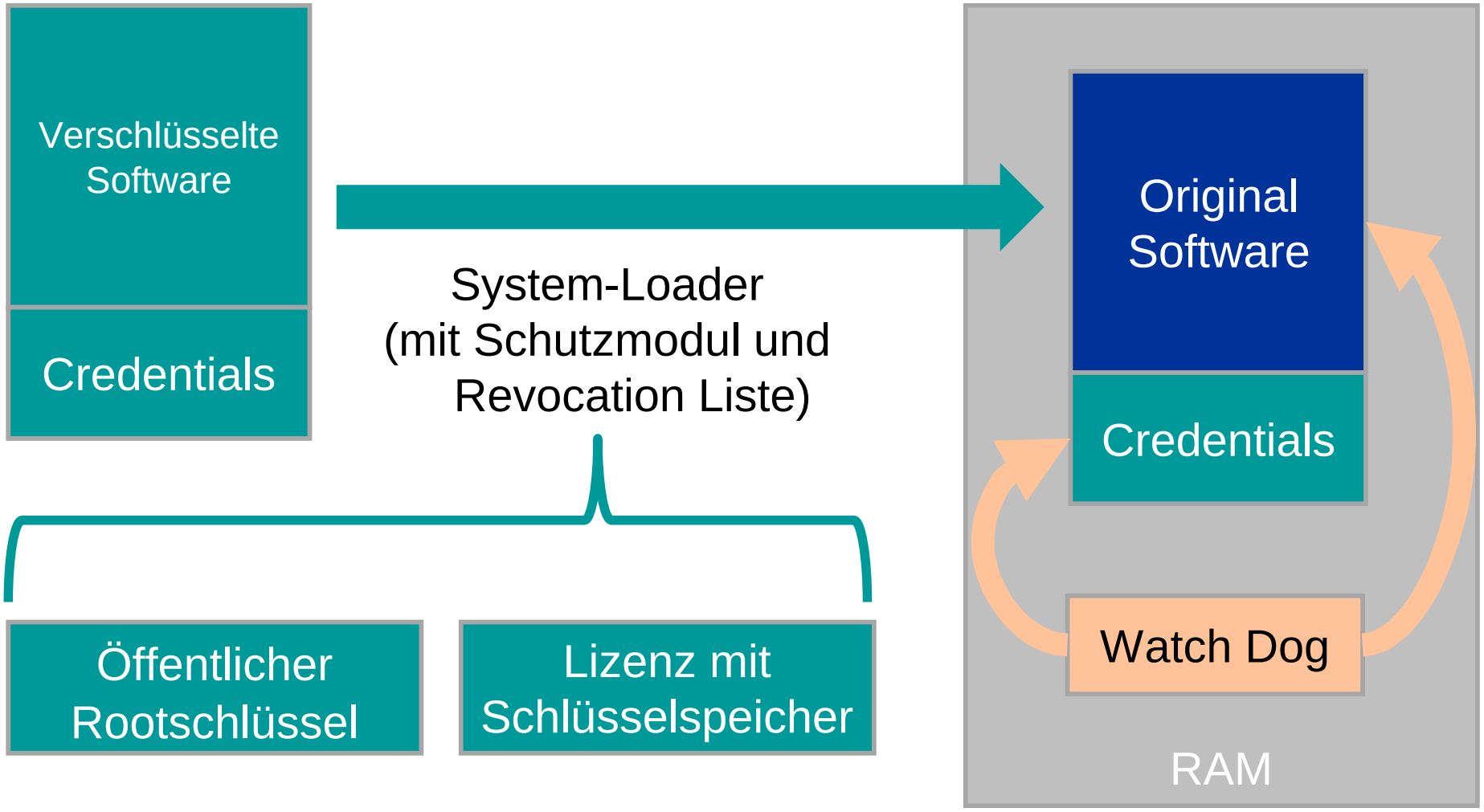
Integritätsprüfung (Schutzprozess)



Schutzprozess

- Generieren des Hashes der Originalsoftware
- Signieren des Hashes mit dem privaten Schlüssel
- Verschlüsseln der Originalsoftware
  - Schlüssel wird aus Originalsoftware abgeleitet
  - Schlüssel wird verschlüsselt abgelegt
  - Schlüssel in Sicherheitshardware sichern
- Den öffentlichen Schlüssel mit Zertifikatskette hinzufügen

Integritätsprüfung (Laufzeit)



Überprüfung zur Laufzeit

- System loader (mit Schutzmodul) prüft aktuelle Lizenzen
  - Entschlüsselung des Schlüssels
  - Entschlüsselung der Originalsoftware
- Schutzmodul prüft gesamte Zertifikatskette gegen den öffentlichen Rootschlüssel
- Schutzmodul berechnet Hash der Originalsoftware
- Schutzmodul überprüft das Zertifikat der Software

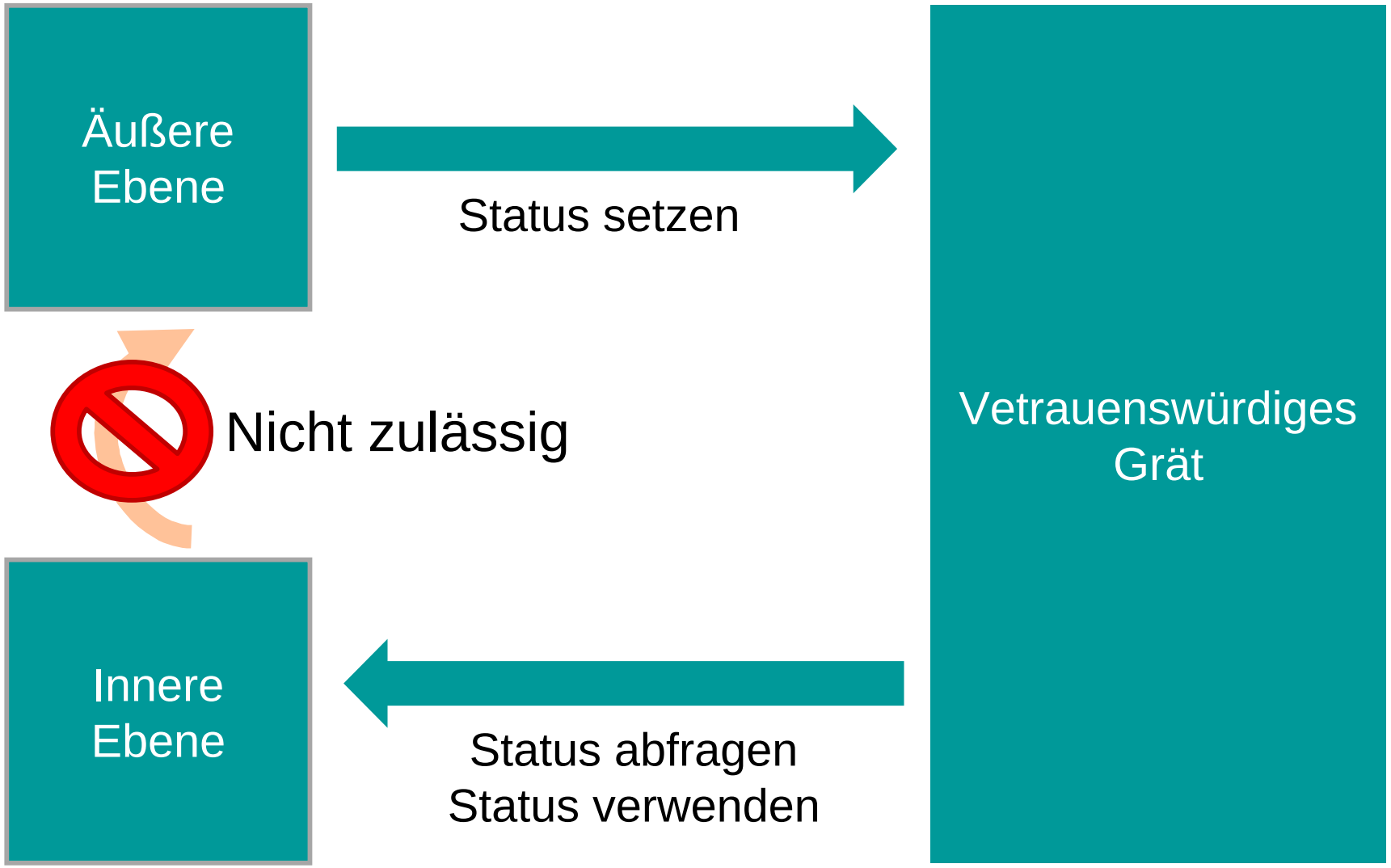
Überprüfung zur Laufzeit II

- Schutzmodul überprüft Zertifikatsattribute
  - Zulässige Hardware
  - Ablauf von Zertifikaten
  - Zertifikatsrückruf
- Watch Dog (optional) überprüft die Software im Speicher

Probleme

- Muss für jede Ebene gemacht werden
- Zertifikatskette
  - Schlüssel und Zertifikate müssen erzeugt werden
- Zulässige Controllers
  - Wie erhält man eine eindeutige Identifizierung der Hardware?
- Performance der Lösung
  - Anzahl der Zertifikate
  - Asymmetrische Kryptographie
- Integration in Bootloader

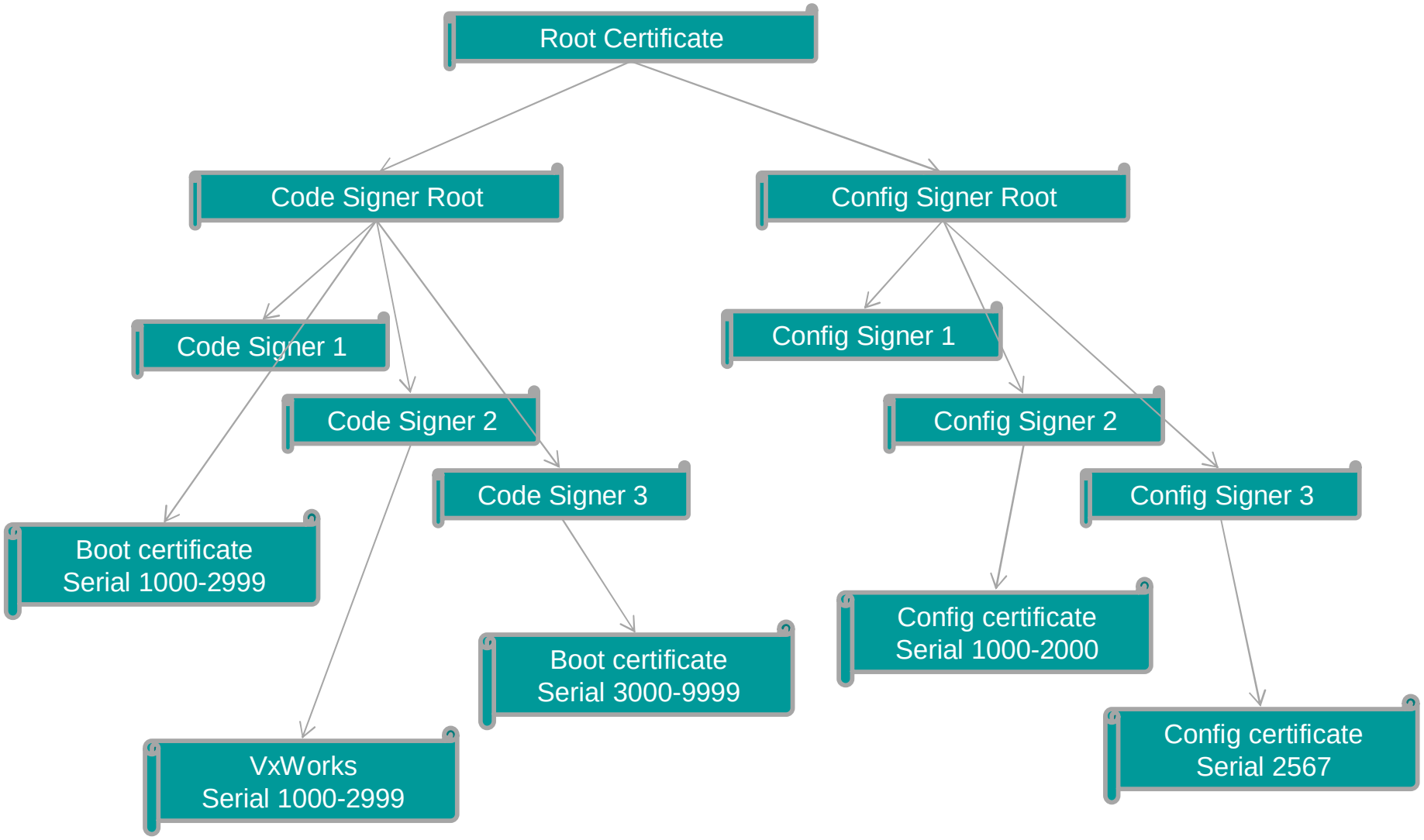
Rückwärtstest



Rückwärtstest

- Typischerweise kann die innere Ebene die äußere Ebene nicht zugreifen
- Lösung: Zustandsbehaftete Maschine
  - Die äußere Ebene setzt einen Zustand
  - Die innere Ebene prüft und verwendet den Zustand
- Voraussetzungen:
  - Vetrauensanker (CmDongle oder TPM)
  - Vetrauensanker für den ersten Schritt (secure boot)

Zertifikatskette



Dr. Peer Wichmann
peer.wichmann@wibu.de