Integration von TNC in ein deutsches Smart Meter Gateway

Carl-Heinz Genzel, Olav Hoffmann, Richard Sethmann
Hochschule Bremen, Flughafenallee 10, 28199 Bremen

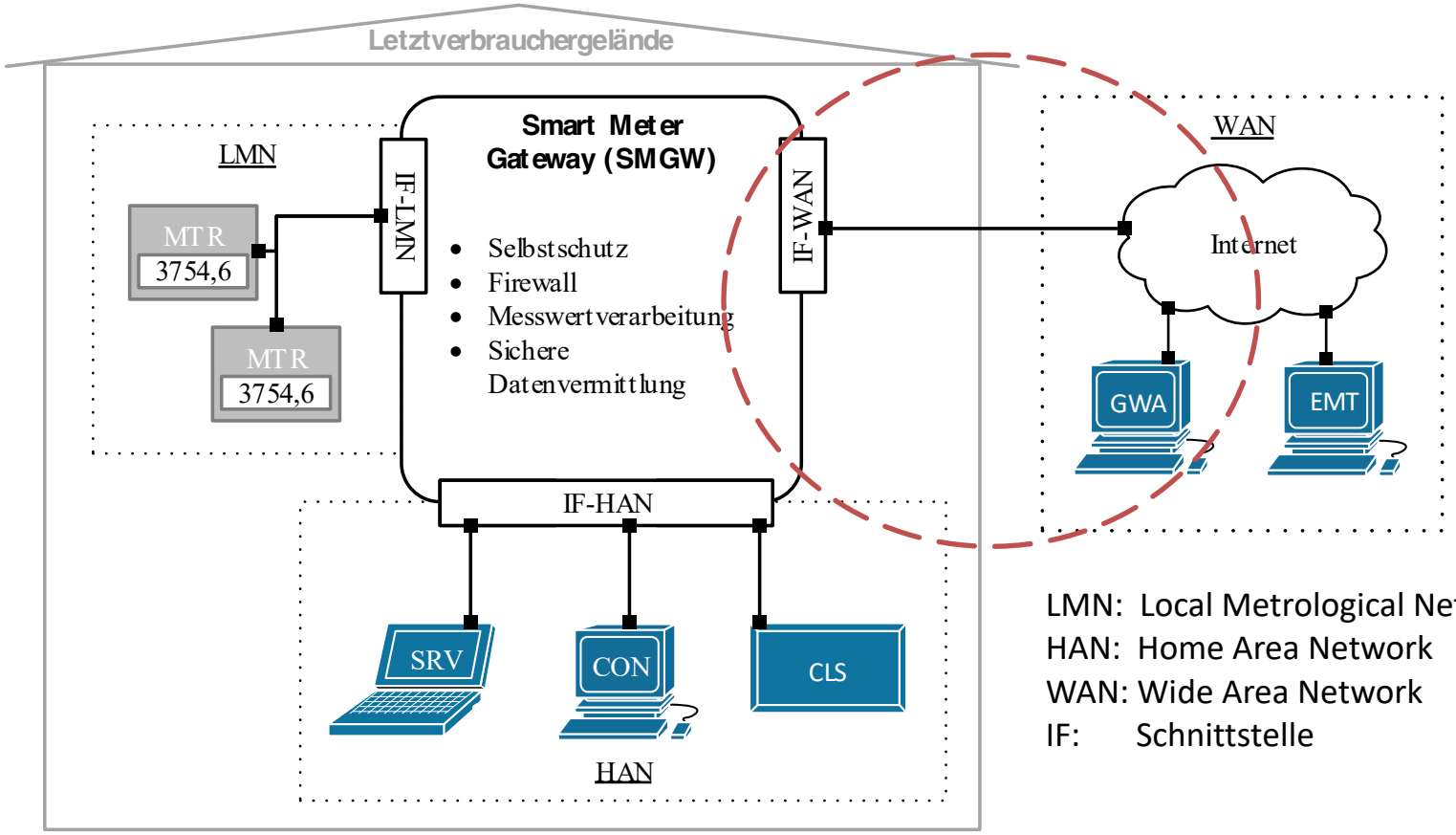
Inhalt

1. Motivation
2. Smart Metering System
3. Integritätskonzept
4. TNC Integration
5. Java basierte TNC-Bibliothek
6. Fazit & Ausblick

Motivation

- Gesetzliche Einführung intelligenter Messsystem
- Sicherheitsarchitektur des Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Forschungsprojekt Sichere Powerline-Datenkommunikation im intelligenten Energienetz (SPIDER)
  - Problem: Analyse der Sicherheitsarchitektur zeigt Gefährdung der Integrität einer zentralen Komponente
  - Lösung: Trusted Network Connect (TNC) der Trusted Computing Group (TCG) zum Schutz der Integrität

Smart Metering System



LMN: Local Metrological Network
HAN: Home Area Network
WAN: Wide Area Network
IF: Schnittstelle

MTR: Smart Meter
SRV: Service Techniker

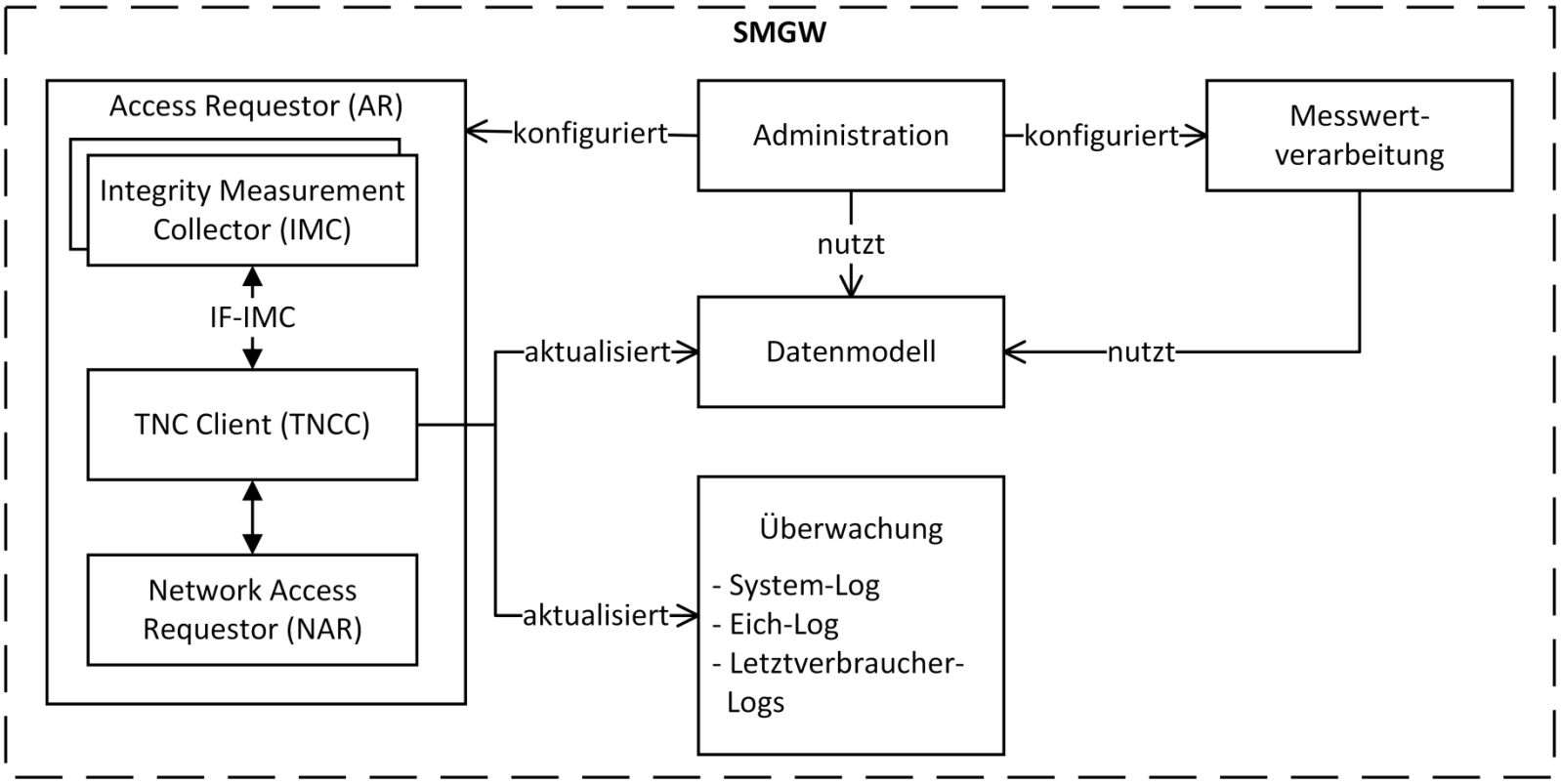
CON: Konsument
CLS: Controllable Local System

GWA: Gateway Administrator
EMT: Externer Marktteilnehmer

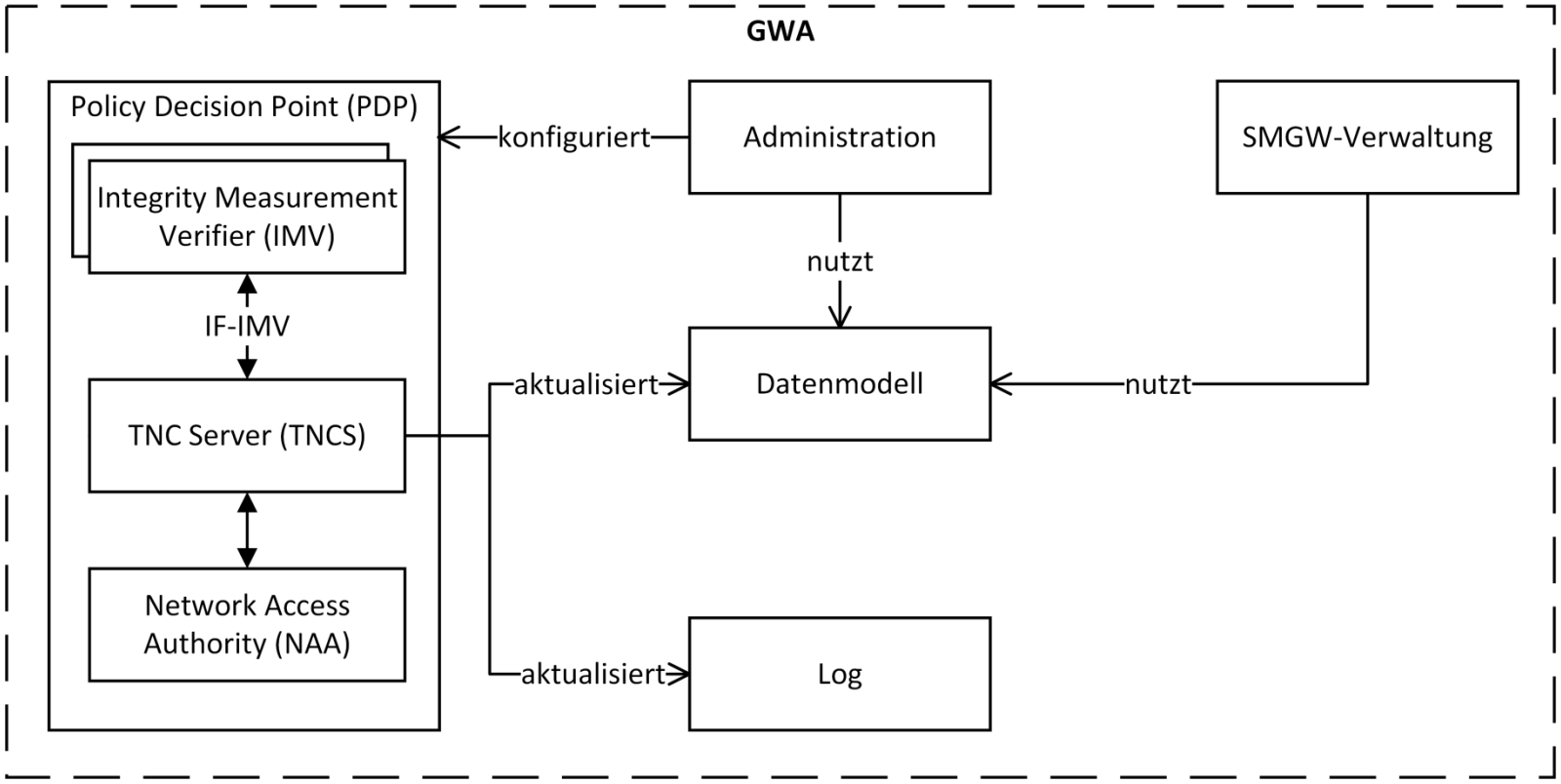
Integritätskonzept

- Physische Integritätskontrolle
  - Hardwareschutz (z.B. Plombe)
- Integritätskontrolle zur Startzeit
  - Secure Boot-Verfahren
- Integritätskontrolle zur Laufzeit
  - Remote Attestation mit TNC
    - Regelmäßige Messung des Systemzustands
    - Attestierung der Integrität anhand der Messwerte durch eine entfernte Instanz

Software Integration von TNC: SMGW



Software Integration von TNC: GWA



Data Transport: TNC IF-T vs. BSI IF-WAN

- SMGW muss immer erreichbar sein → TNC IF-T: Binding to TLS
- Empfehlungen des TNC IF-T: Binding to TLS ...
  - entsprechen teilweise den Vorgaben des BSI
  - widersprechen teilweise den Vorgaben des BSI
- Mindestens eine Vorgabe der TCG widerspricht den Vorgaben des BSI vollständig:
  - Cipher Suite TLS_RSA_WITH_AES_128_CBC_SHA

Data Transport: TNC IF-T (BSI)

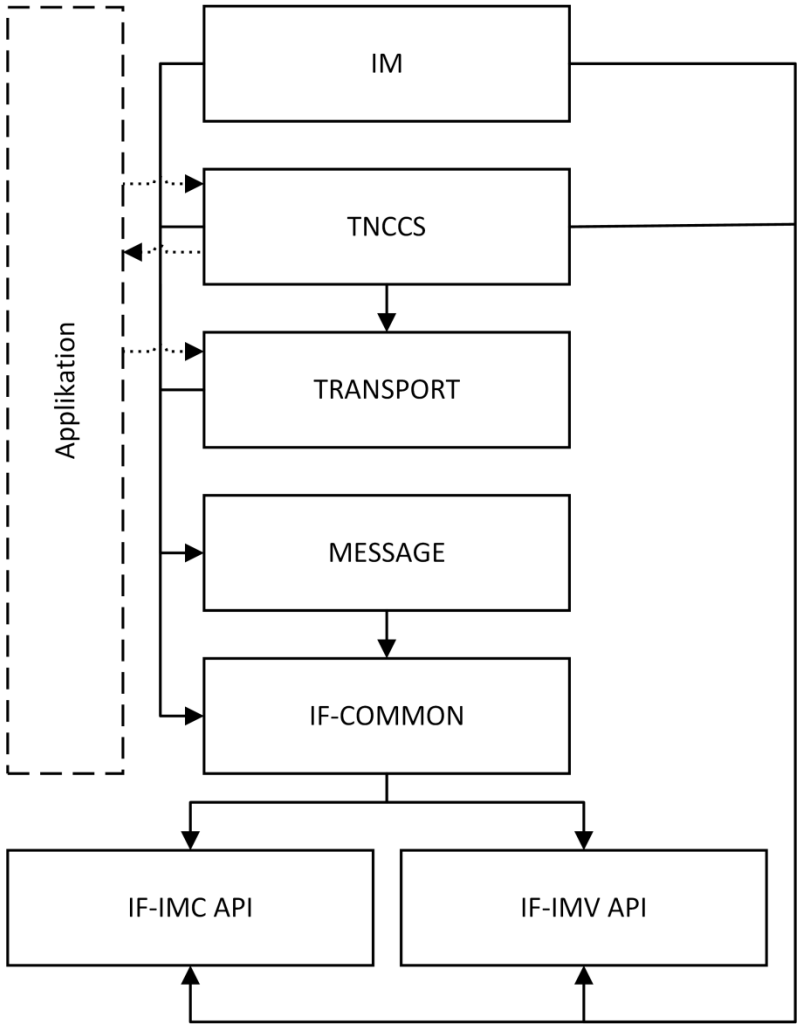
- Angepasstes IF-T Binding to TLS
  - SMGW ist immer Initiator einer Verbindung und einer Integritätsprüfung
  - Immer bidirektionale Authentifizierung mit Zertifikaten
  - Eine Integritätsprüfung pro Verbindung
  - Integritätsprüfung in zwei Übertragungszyklen abgeschlossen
  - TLS-Parameter im Rahmen der obligatorischen Vorgaben an das BSI angepasst
  - Vorgabe der TCG zur Cipher Suite nicht anwendbar

Java basierte TNC-Bibliothek

- Open Source Projekt an der Hochschule Bremen
- BSD 3-Clause Lizenz
- Unterstützte TCG-Spezifikationen
  - IF-T-TLS 2.0 (TLS-Parameter implementierungsabhängig)
  - IF-TNCCS 2.0
  - IF-IMC 1.3
  - IF-IMV 1.3
  - IF-M 1.0
- ≈ 35 000 Codezeilen, vollständig dokumentiert
- Download: https://github.com/trusthsbremen/jtnc

Java basierte TNC-Bibliothek

- Module
  - IM, TNCCS, TRANSPORT zur Entwicklung von IMC/V, TNCC/S and NAA/R
    - inkl. Schnittstellen zur ext. Anwendung
  - MESSAGE für objekt-orientierte IF-M-, IF-TNCCS- und IF-T-Nachrichten
  - IF-COMMON mit gemeinsamen Datenstrukturen und standardisierten TCG-APIs



SMGW with ID EHSB0100000001 started.
Listening for Wake-Up on 0.0.0.0:30090.

Connect to DestinationPair [host=192.168.100.1, port=30271] for integrity handshake.

Connection state has changed to TNC_CONNECTION_STATE_CREATE

Version negotiation and authentication completed successfully. Transport phase started.

Connection state has changed to: TNC_CONNECTION_STATE_HANDSHAKE

[Measurement and validation exchange …]

New integrity status for SMGW : **TNC_INTEGRITY_STATE_POSITIVE**

Connection state has changed to TNC_CONNECTION_STATE_ACCESS_ALLOWED.

Round trip limit exceeded. Closing connection...

Connection state has changed to TNC_CONNECTION_STATE_DELETE

GWA started. Listening for incoming MANAGEMENT connections on port 30443 and TNC connections on port 30271.

#>push(EHSB0100000001,sensor_setup_ON_60.xml)

Open transport connection.

Connection state has changed to TNC_CONNECTION_STATE_CREATE

Version negotiation and authentication completed successfully. Transport phase started.

Connection state has changed to: TNC_CONNECTION_STATE_HANDSHAKE

Checksum Test:

Property	Expected	Actual
Value	PhkxhHjnWdMI/[…]=	PhkxhHjnWdMI/[…]

Rating: 1 of 1

[Further measurement and validation exchange …]

New integrity status for SMGW EHSB0100000001 : **TNC_INTEGRITY_STATE_POSITIVE**

Connection state has changed to TNC_CONNECTION_STATE_ACCESS_ALLOWED.

Underlying transport was closed.

Connection state has changed to TNC_CONNECTION_STATE_DELETE

Fazit

- Demonstrative Implementierung von TNC im Smart Metering System
  - Integration eines AR beim SMGW
  - Integration eines PDP beim GWA
  - Konfiguration von TNC am SMGW durch die spezifizierte Managementschnittstelle des BSI
- Open Source Projekt für eine TNC-Bibliothek in Java (jTNC): https://github.com/trusthsbremen/jtnc
- Ergebnisse wurden im Rahmen des TCG Members Meeting vorgestellt (Wien, 06/2016)

Ausblick

- Integration von TNC in weitere Komponenten des Smart Grid
- Integration weiterer Elemente zur Überwachung eines Smart Metering Systems und dem Smart Grid
- Implementierung einer Java Test Suite für TNC Test Cases und Überarbeitung der Java API der TCG
- Weiterentwicklung des SMGW vom Prototypen zum Produkt durch die devolo AG und die DECOIT GmbH

Vielen Dank

Fragen?