TeleTrusT
Pioneers in IT security.

it-sa 2012

Nürnberg, 16.10.2012

Smart Meter Gateway: Informationsflusskontrolle und Datenschutz mittels Security Kernel Framework

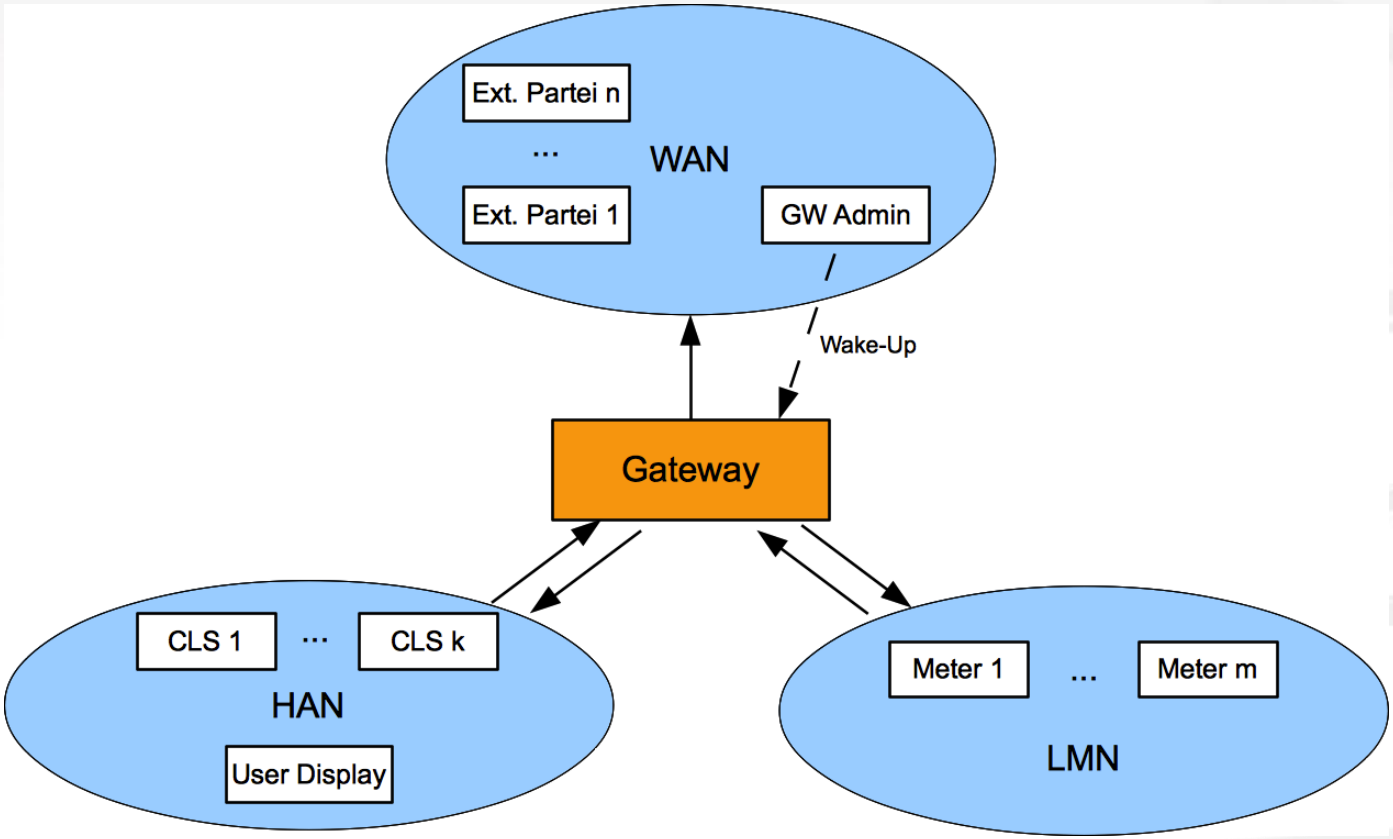
Michael Gröne
Sirrix AG security technologies

Agenda

- Sicherheitsanforderungen für Smart Meter Gateways
- Das TURAYA™ High-Assurance Security Kernel Framework
- Anwendung des Security Kernel Framework auf Smart Meter Gateways
- Fazit

Sicherheitsanforderungen für Smart Meter Gateways

Smart Meter Gateways



Notwendige Sicherheitsfunktionen

- Bereitstellung von sicheren Kommunikationskanälen zwischen Netzwerken
- Schutz der Privatsphäre / Datenschutz:
  - Pseudonymisierung von Verbraucherdaten
  - Gatewayadministratoren dürfen keine Verbraucherdaten einsehen können
- Vertraulichkeits- und Integritätsschutz von Inhaltsdaten
  - Auf dem Gerät
  - Beim Transfer zu externen Parteien
- Benutzerauthentifizierung für Verbraucher
- Sichere Ausführungsumgebung für die Verarbeitung auf dem Gerät
- Sicheres Remote-Update (Firmware, Policies)
- Logging
- Selbsttests

Problemstellung

- Smart Meter / Smart Meter Gateway Hersteller sind i.d.R. keine IT-Sicherheitsexperten
  - Nicht vertraut mit Common Criteria Evaluierungsprozess
  - Notwendigkeit zur Entwicklung neuer oder Anpassung bestehender System-Software zur Erfüllung der Anforderungen
  - Notwendigkeit einer Demo, dass Produkte Daten gem. PP schützen
- Alleinige Verwendung von Embedded Linux OS + Firewall-Funktionalität ist nicht ausreichend
  - Schutz der Daten auf dem Gerät
  - Kontrolle des Informationsflusses
  - Remote Administratoren dürfen keine Daten der Verbraucher einsehen können

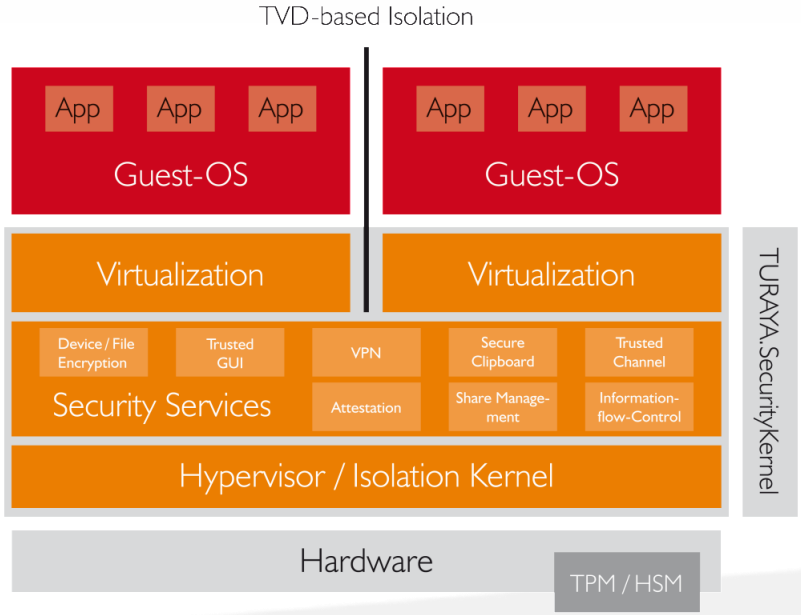
Das TURAYA™ High-Assurance Security Kernel Framework

SecurITy made in Germany

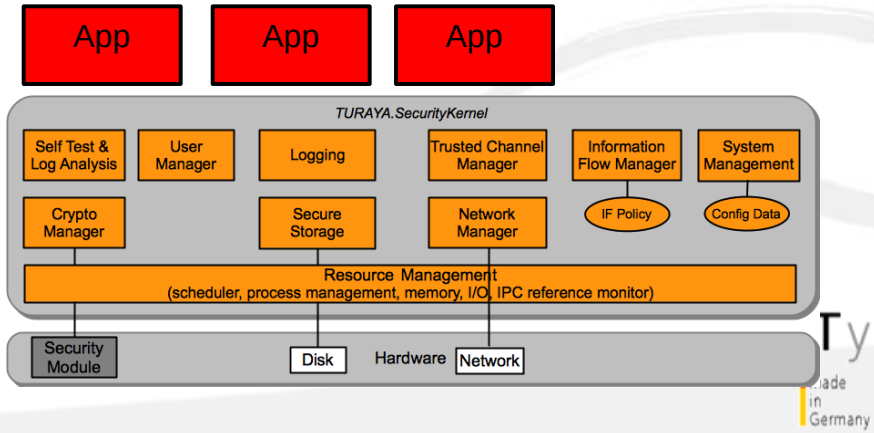
TURAYA™ High-Assurance Security Kernel Framework

- Sicherheitsarchitektur basierend auf den funktionalen Anforderungen der Common Criteria
- Plattformunabhängigkeit:

Server-Systeme (Virtualisierung, Cloud)



Endnutzer / Embedded Devices



Erfahrungen

- Forschungs- und Entwicklungsprojekte:
  - EMSCB: Individuelle PCs, Laptops
  - OpenTC: Trusted Infrastructures (PCs, Server, Virtual Data Center)
  - TClouds: Trusted Cloud Infrastructures
  - Emergent: Informationsflusskontrolle in digitalen Unternehmen
  - RUBTrust/MediTrust: Evaluierung bestimmter Einsatzfelder
  - TrustedMobile/BizzTrust: Smartphones
- HASK-PP: Common Criteria Protection Profile für den Security Kernel (EAL 5)
  - Hauptkonzept: Isolierte Domänen für Daten/Ausführung, Trusted Computing
  - Ansatz: Einfachheit (nur wenige Main Security Requirements, Implementierungsunabhängigkeit)

TURAYA

SecurITy made in Germany

HASK-PP Zertifikat

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-CC-PP-0039-2008

Common Criteria Protection Profile

Protection Profile for a High Assurance Security Kernel
Version 1.14

developed by Sirrix AG

Assurance Package claimed in the Protection Profile:
Common Criteria Part 3 conformant
EAL 5

Common Criteria

The Protection Profile identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the Protection Profile and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 14 November 2008
For the Federal Office for Information Security

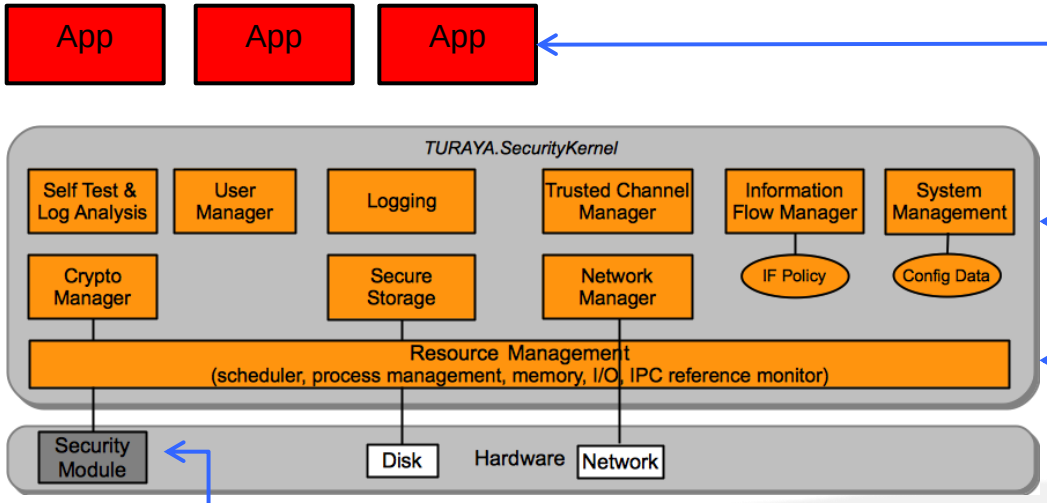
Bundesamt für Sicherheit in der Informationstechnik - 9 -

Bernd Kowalski
Head of Department

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Framework-Ansatz: Reduzierte Komplexität

- Ziel: Reduzierung der Größe der Trusted Computing Base
  - Einfacher in der Wartung und Evaluierung (z.B. Common Criteria)
  - Reduzierung der Angriffsfläche
- Ansätze: Microkernel, Virtualisierung, Code Optimization (z.B. Entfernung nicht benötigter Libraries)



Komplexe Applikationslogik
(kann auch Gerätetreiber beinhalten)

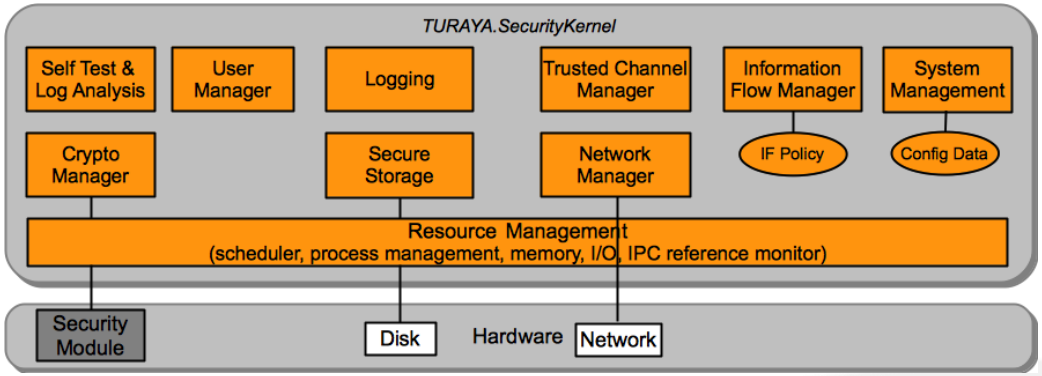
Basissicherheitsdienste

Basisressourcenmanagement

Hardwaresicherheitsmodul
(z.B. TPM)

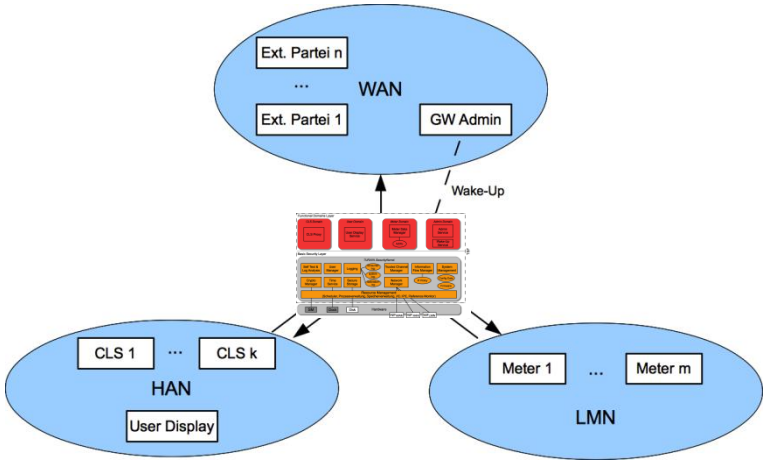
Framework-Ansatz: Modularität

- Ziel: Nutzbarmachung des Security Kernel für versch. Anwendungsszenarien
  - Komponenten hinzufüg- oder entfernbar (bedarfsabhängig)
  - Komponenten können durch alternative Implementierungen ersetzt werden (abhängig von Hardware- oder notw. Sicherheitseigenschaften)
- Beispiele:
  - Resource Management: L4 Microkernel, Xen hypervisor, SELinux, etc.
  - Hardware Security Module: HSM, TPM, Smartcard, etc.



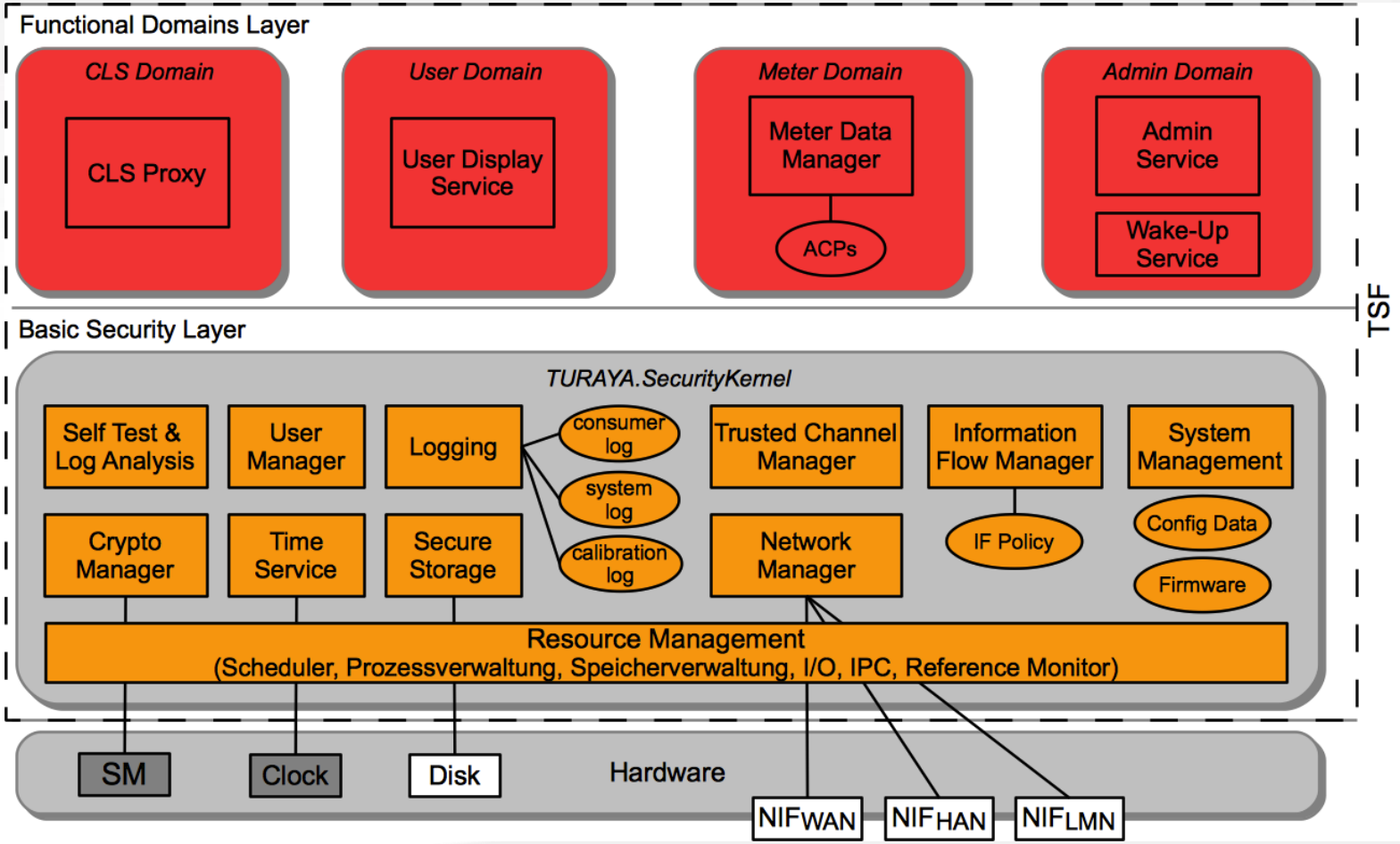
SecurITy made in Germany

Anwendung des Security Kernel Framework auf Smart Meter Gateways

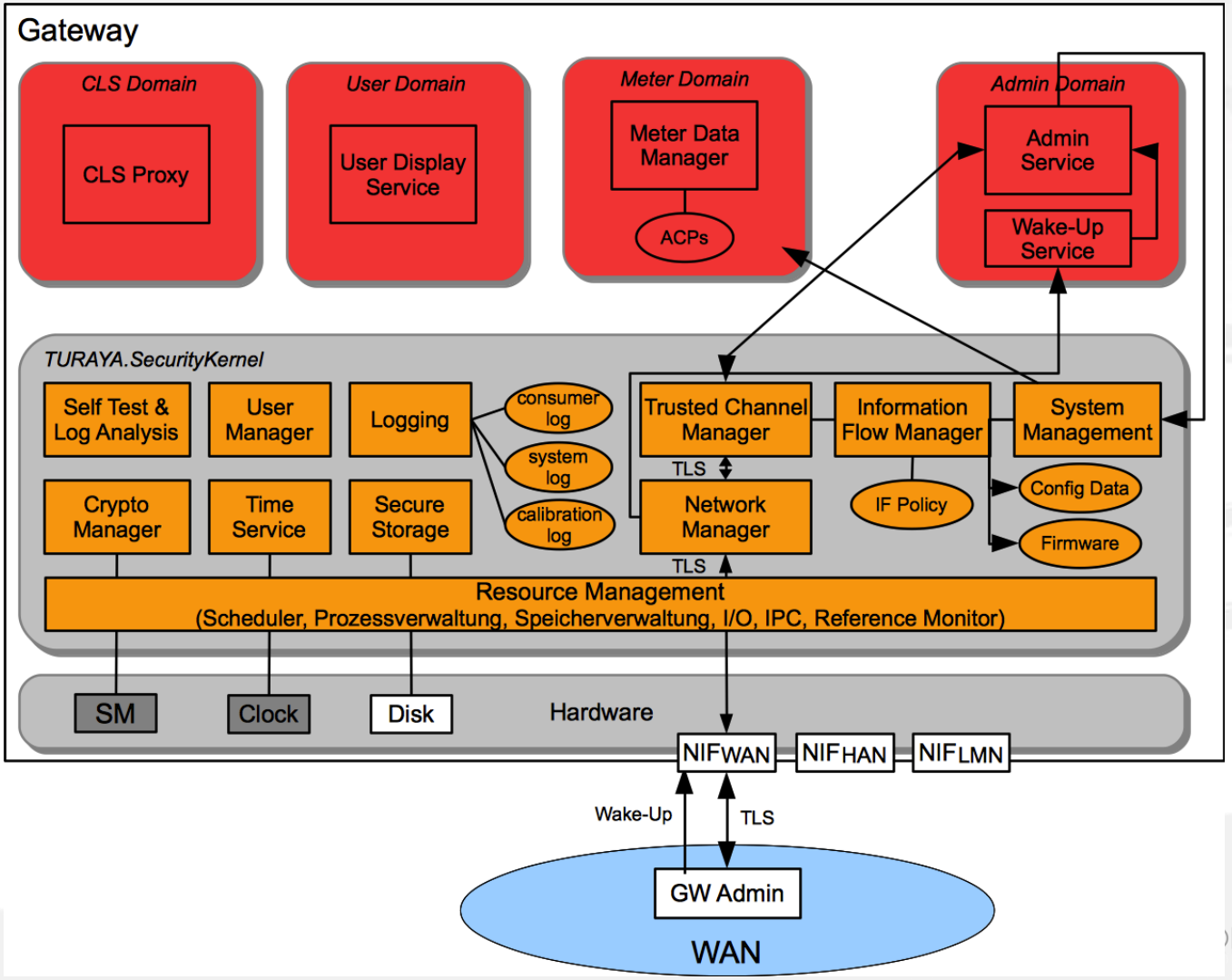


SecurITy made in Germany

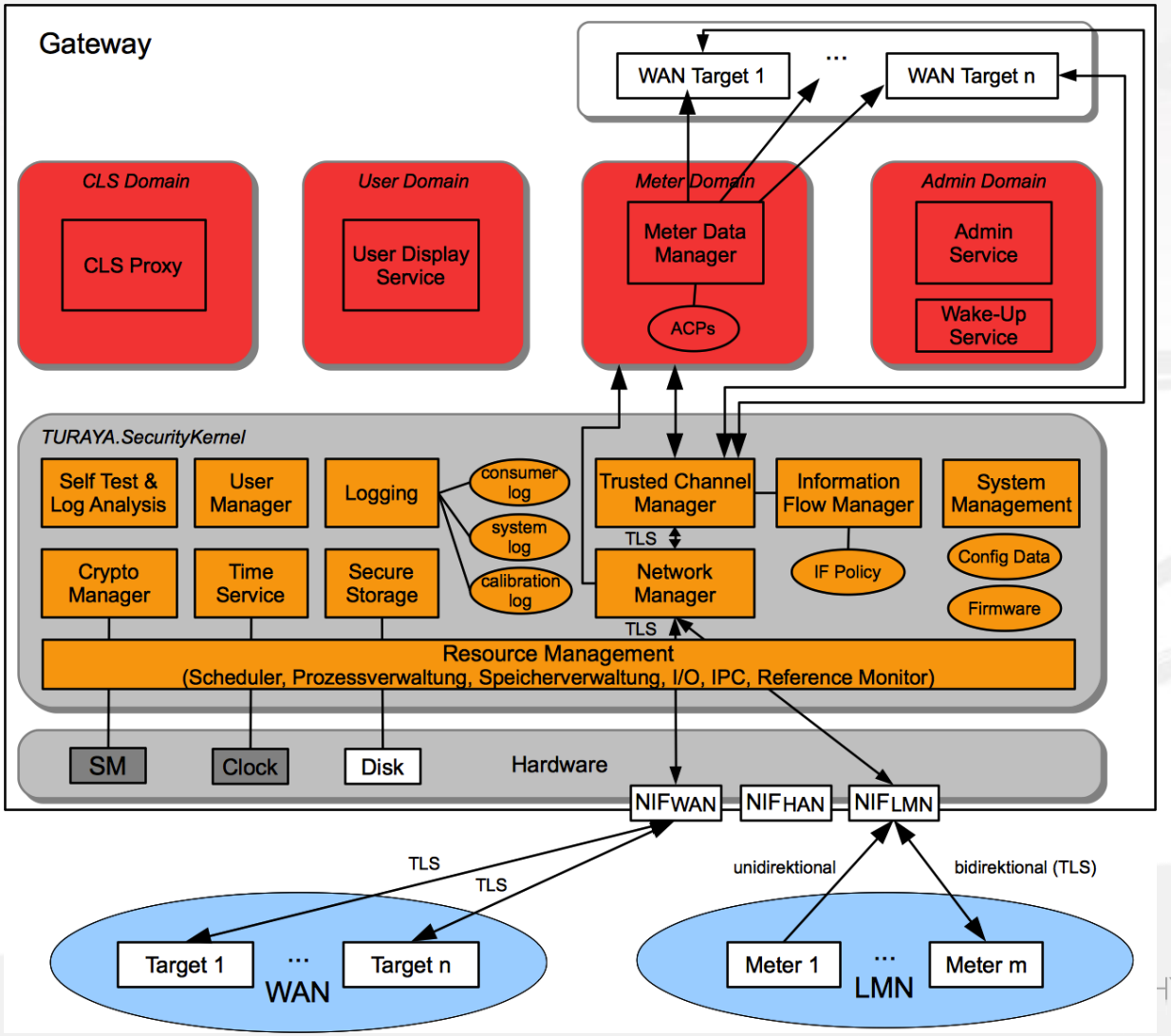
High Level Sicherheitsarchitektur (Gateway)



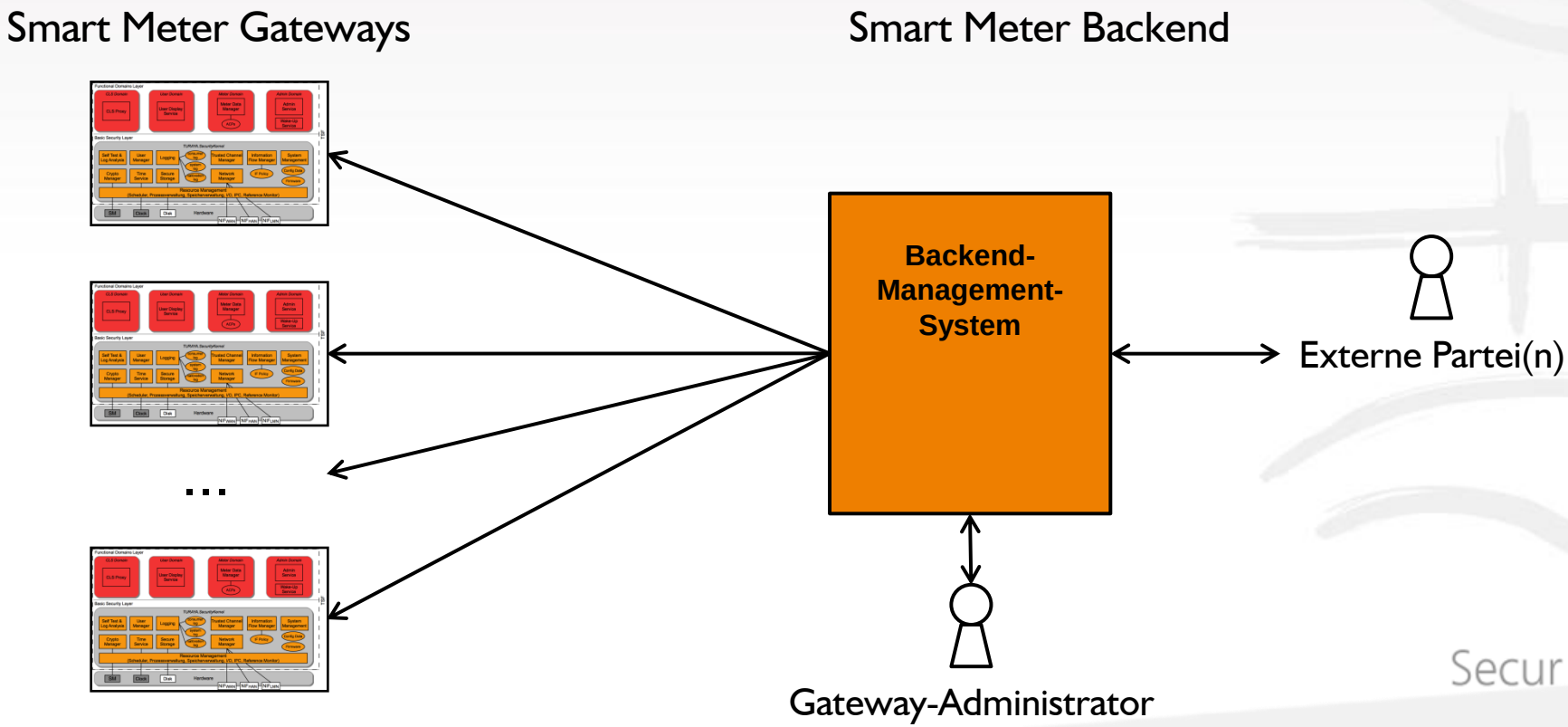
Administrierung des Gateway



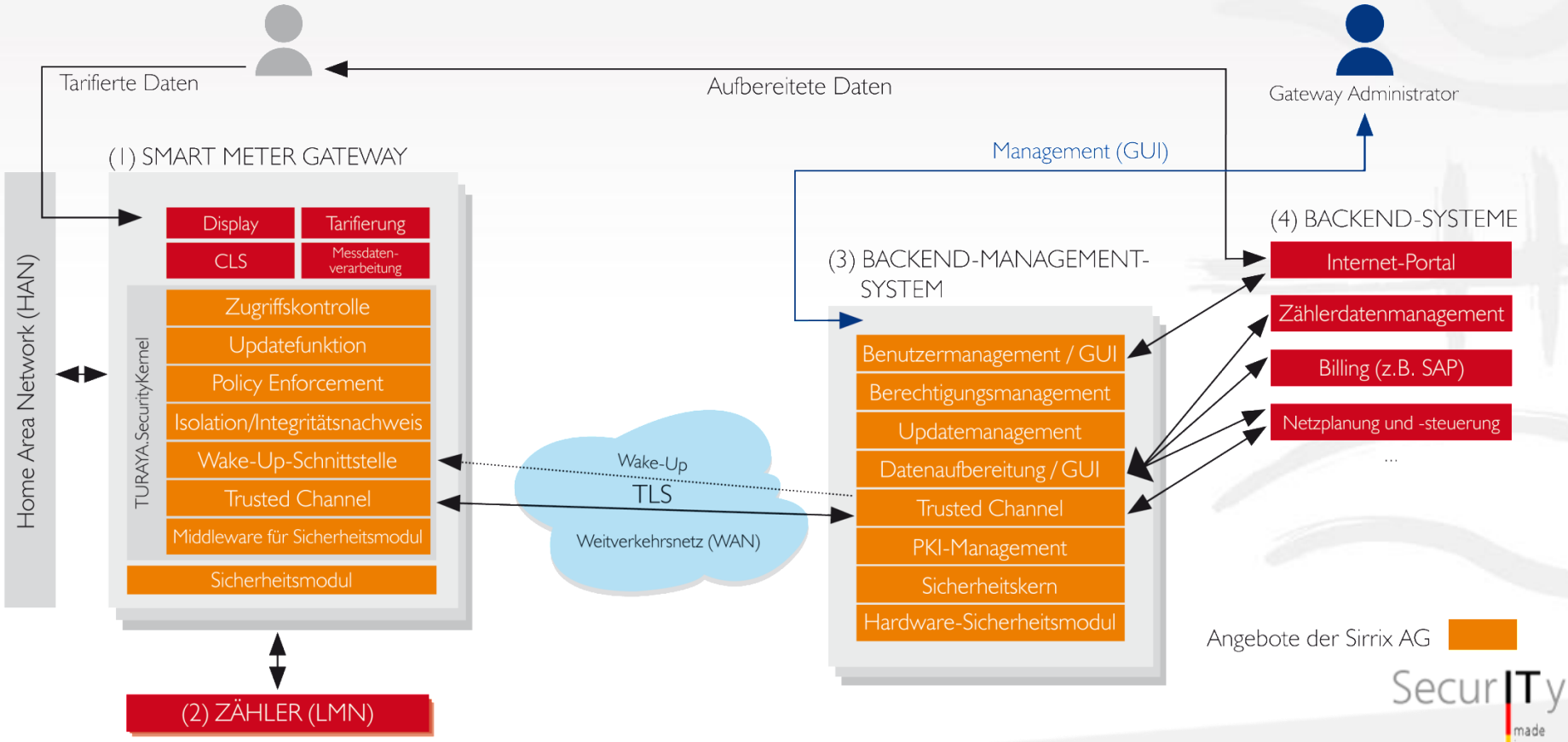
Messwerte-Verarbeitung und -Weiterleitung



Smart Meter Backend



Ausblick: Trusted Smart Metering Architektur



SecurITy made in Germany

Fazit

- Smart Meter Gateway Komponenten müssen hohe Sicherheits- und Datenschutzanforderungen adressieren
  - Regulatorische Anforderung einer Common Criteria Evaluierung
  - Durch das BSI entwickeltes Schutzprofil EAL 4+ und TR
- TURAYA™ High-Assurance Security Kernel Framework & HASK PP
  - Sicherheitsarchitektur basierend auf Erfahrungen aus vielen Projekten
  - Kann auf individuelle Bedürfnisse zugeschnitten werden (Ansatz der minimalen Komplexität)
  - Stellt Basissicherheitsmodule für viele Anwendungsfälle bereit
- Security Kernel Framework als Basis für Smart Meter Gateways
  - Hilfreich bei Implementierung der geforderten Sicherheitsfunktionalität
  - Reduziert Aufwand für Entwicklung (modularer Ansatz)

TURAYA

SecurITy made in Germany

Vielen Dank!

Fragen?

Sirrix AG
Lise-Meitner-Allee 4
44801 Bochum

Tel +49 234 / 61 00 71-0
Fax +49 234 / 61 00 71-500

Email info@sirrix.com
Web www.sirrix.de

Michael Gröne

Email: m.groene@sirrix.com