TeleTrusT
Pioneers in IT security.

Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 23.05.2012

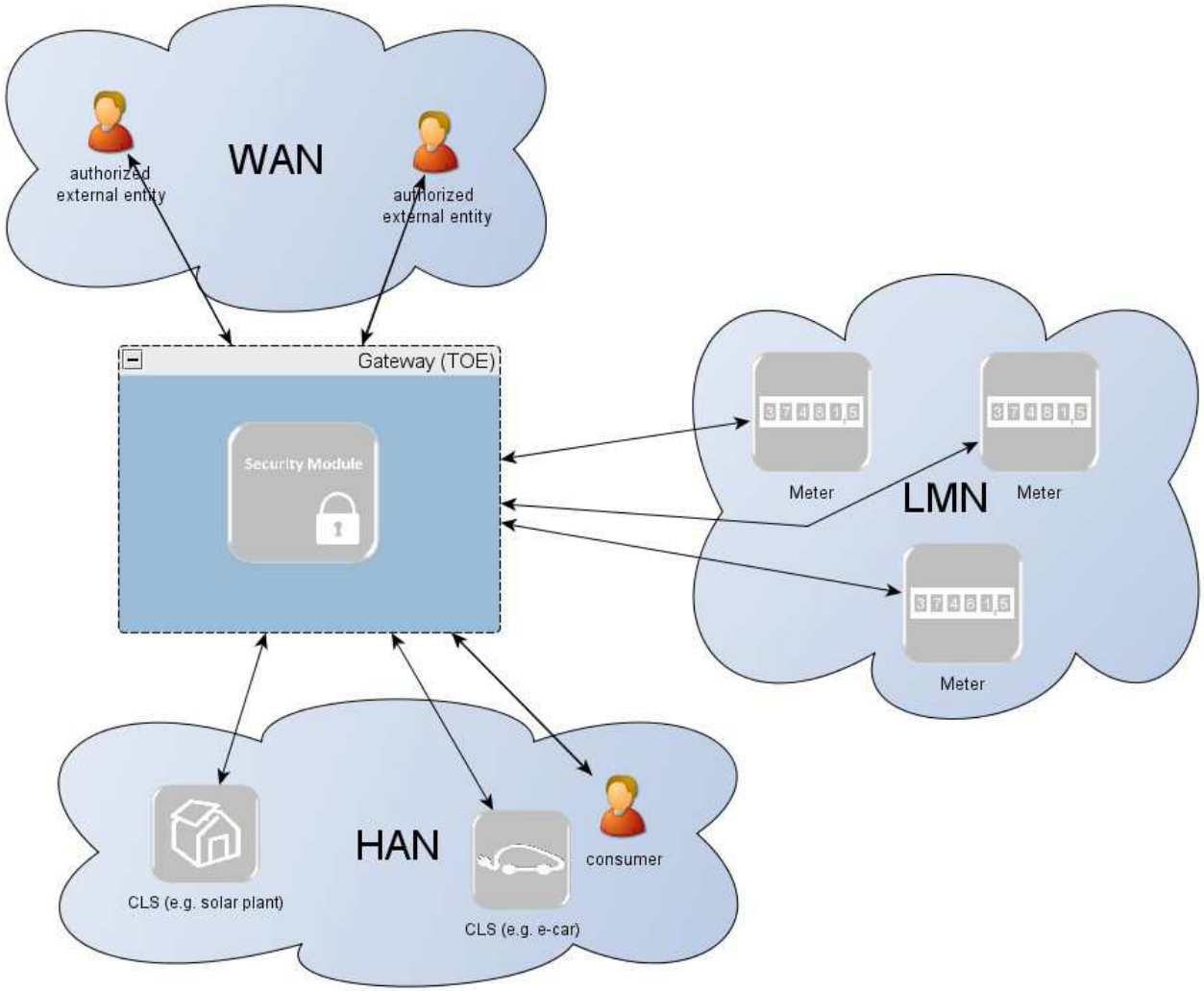
Sichere Identitäten in Smart Grids

Dr. Thomas Störtkuhl, TÜV SÜD AG

Agenda

1. **Beispiele für Kommunikationen**
2. **Digitale Zertifikate: Basis für Authentifizierung**
3. **Automatisiertes Ausrollen von digitalen Zertifikaten**

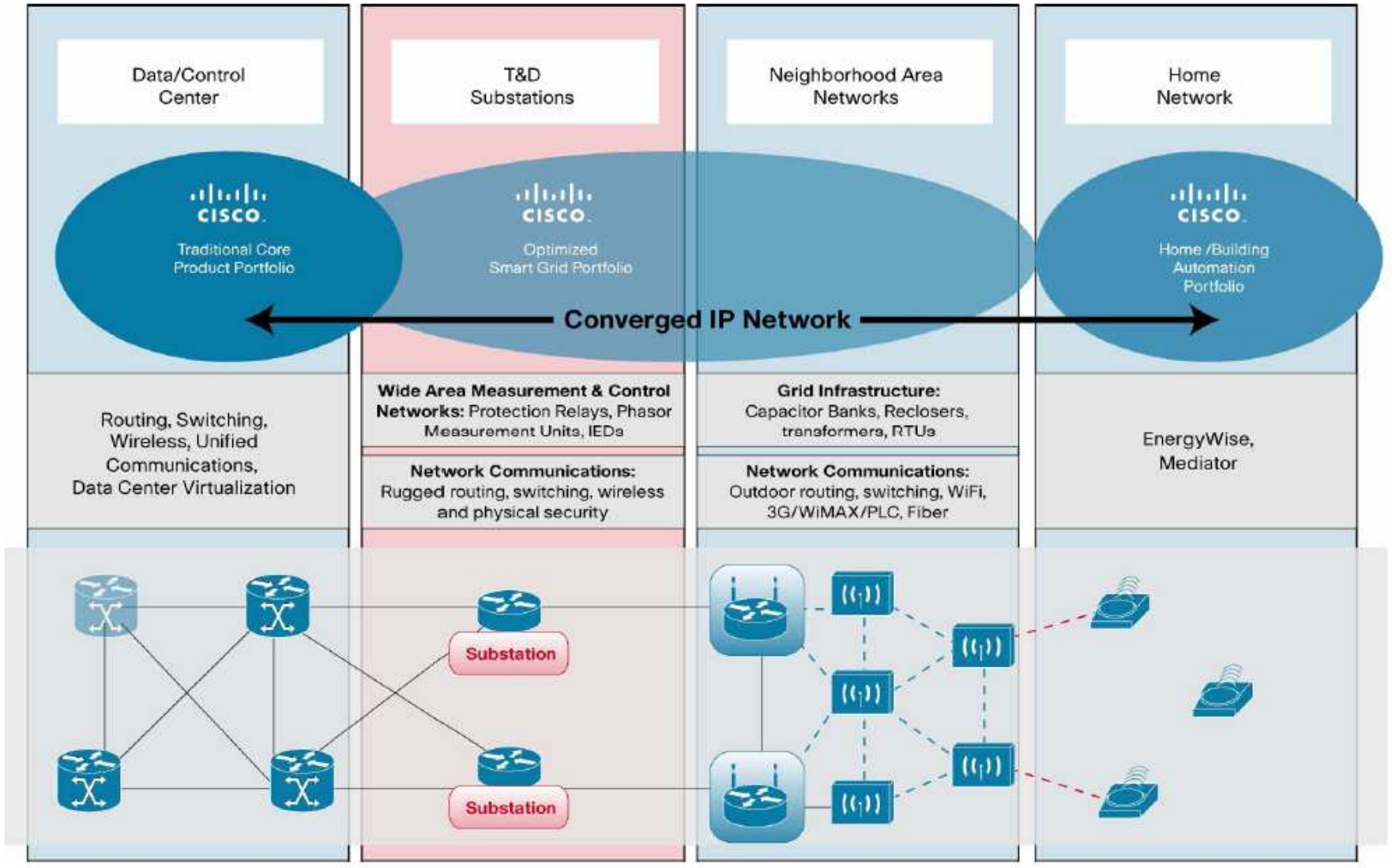
Smart Meter Gateway



WAN Wide Area Network
LMN Local Metrological Network
HAN Home Area Network
CLS Controllable Local Systems

Quelle: Protection Profile for the Gateway of a Smart Metering System, Federal Office for Information Security, v01.01.01

Smart Grid Vision von Cisco



Quelle: Cisco Smart Grid: Substation Automation Solutions for Utility Operations, Cisco, White Paper, 2010
http://www.cisco.com/en/US/prod/collateral/routers/ps10967/ps10977/white_paper_c11_593673.pdf

Abgesicherte Device-to-Device Kommunikation

adressiert in

IEC/TR 62443-3-1, Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems

IEC 62443-3-3, Security for industrial automation and control systems – Network and system security – Part 3-3: System security requirements and security assurance levels

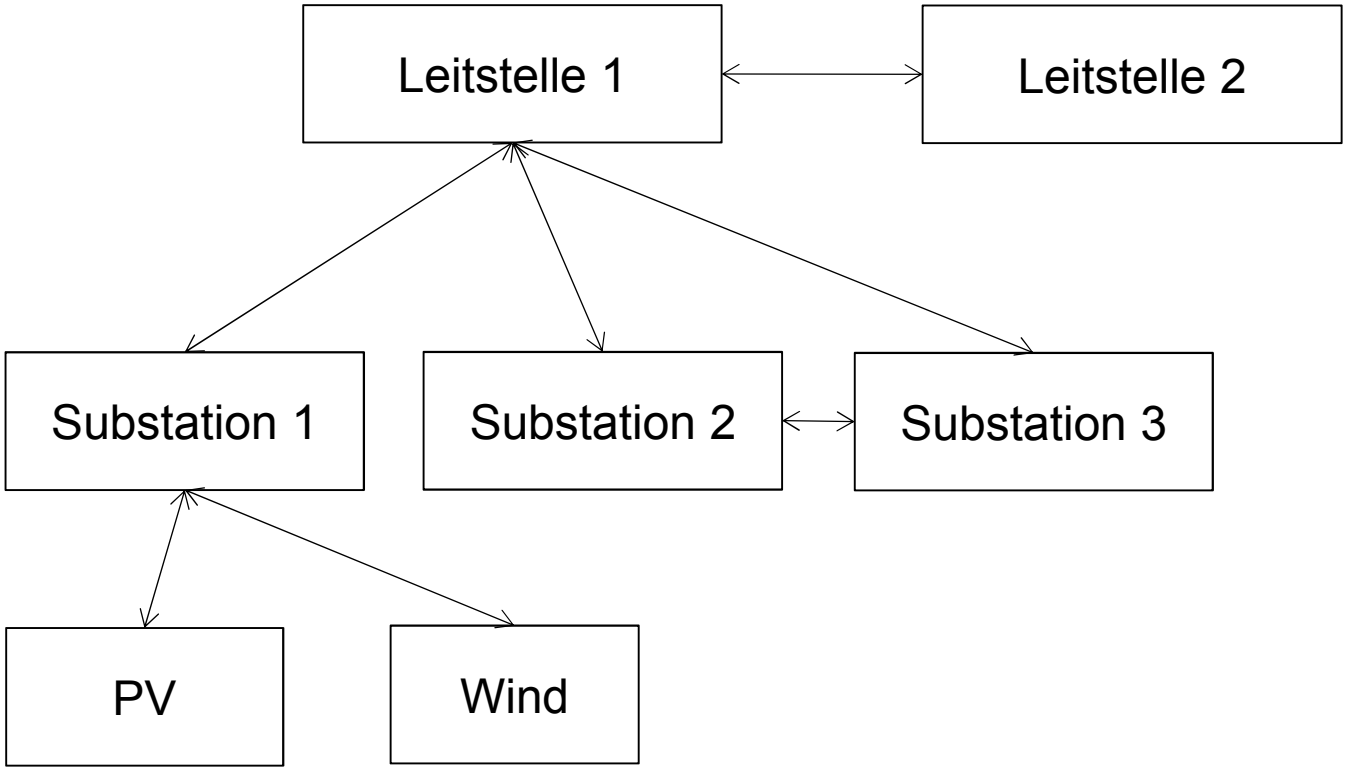
IEC TS 62351-3, Technical Specification, Power systems management and associated information exchange – Data and communication security- Part 3: Communication network and system security – Profiles including TCP/IP

IEC TS 62351-5, Technical Specification, Power systems management and associated information exchange – Data and communication security- Part 5: Security for IEC 60870-5 and derivatives

Protection Profile for the Gateway of a Smart Metering System, Federal Office for Information Security, v01.01.01

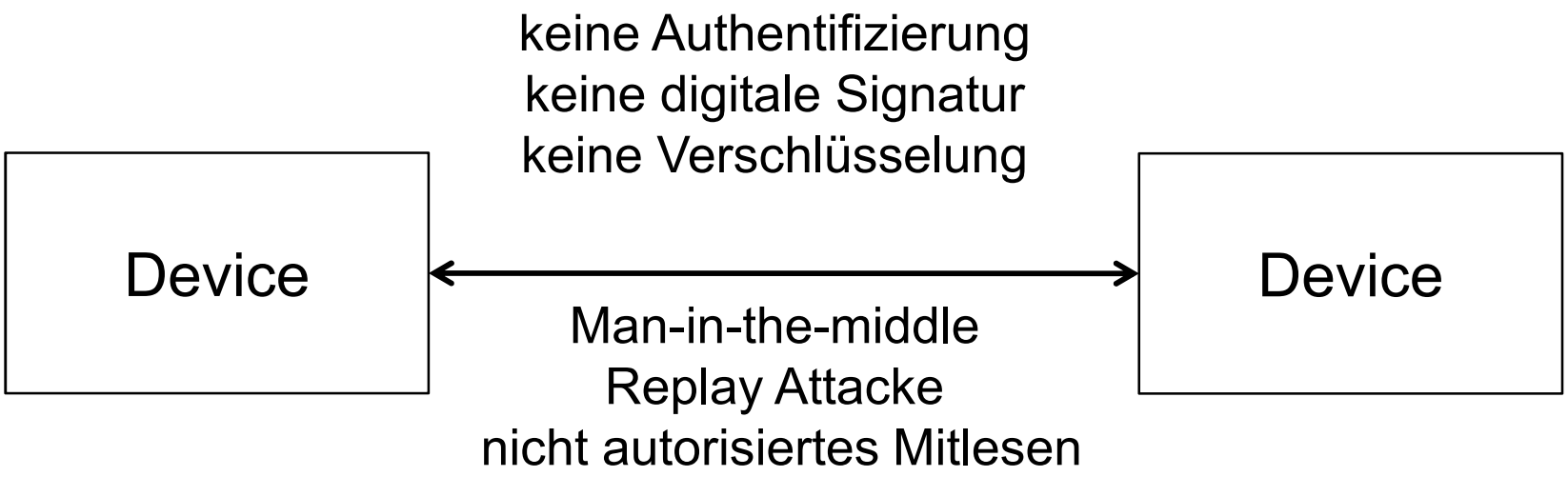
Device-to-Device Kommunikation in Smart Grids

einfaches Kommunikationsnetzwerk



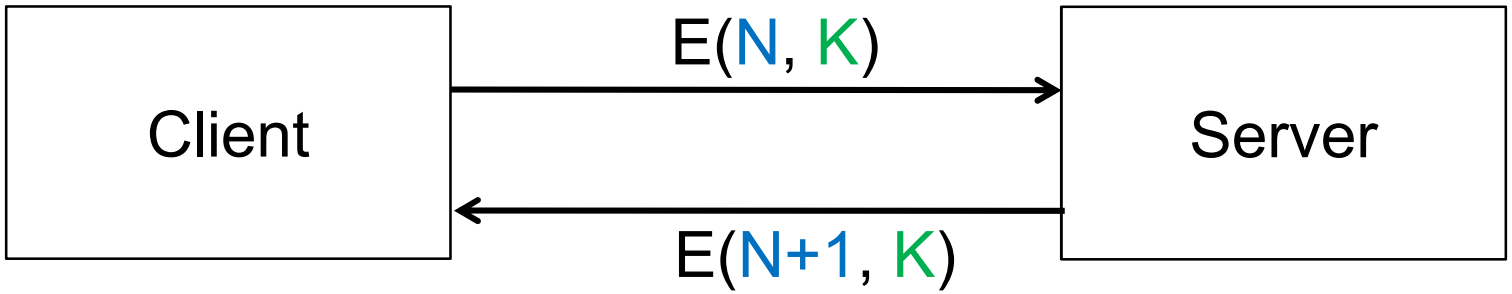
Ungesicherte Kommunikation

Bedrohungen bei ungesicherten Kommunikationsverbindungen



Authentifizierung mittels Challenge Response

Authentifizierung ist Grundlage einer sicheren Kommunikation



Einfaches Beispiel:

- sicherer Austausch des symmetrischen Schlüssels K via Asymmetrischem Algorithmus
- Client sendet eine zufällig gewählte Zahl *N* zum Server
- Cleint erwartet als Anwort des Servers die verschlüsselte Zahl *N + 1*
- two factors: PIN and smart card

Digitale Identität

gemäß RFC 5280

basic fields:
version
serial number
signature
issuer
validity
subject
subjectPublicKeyInfo
.....
extensions

digital signature of CA

CA: Certificate Authority

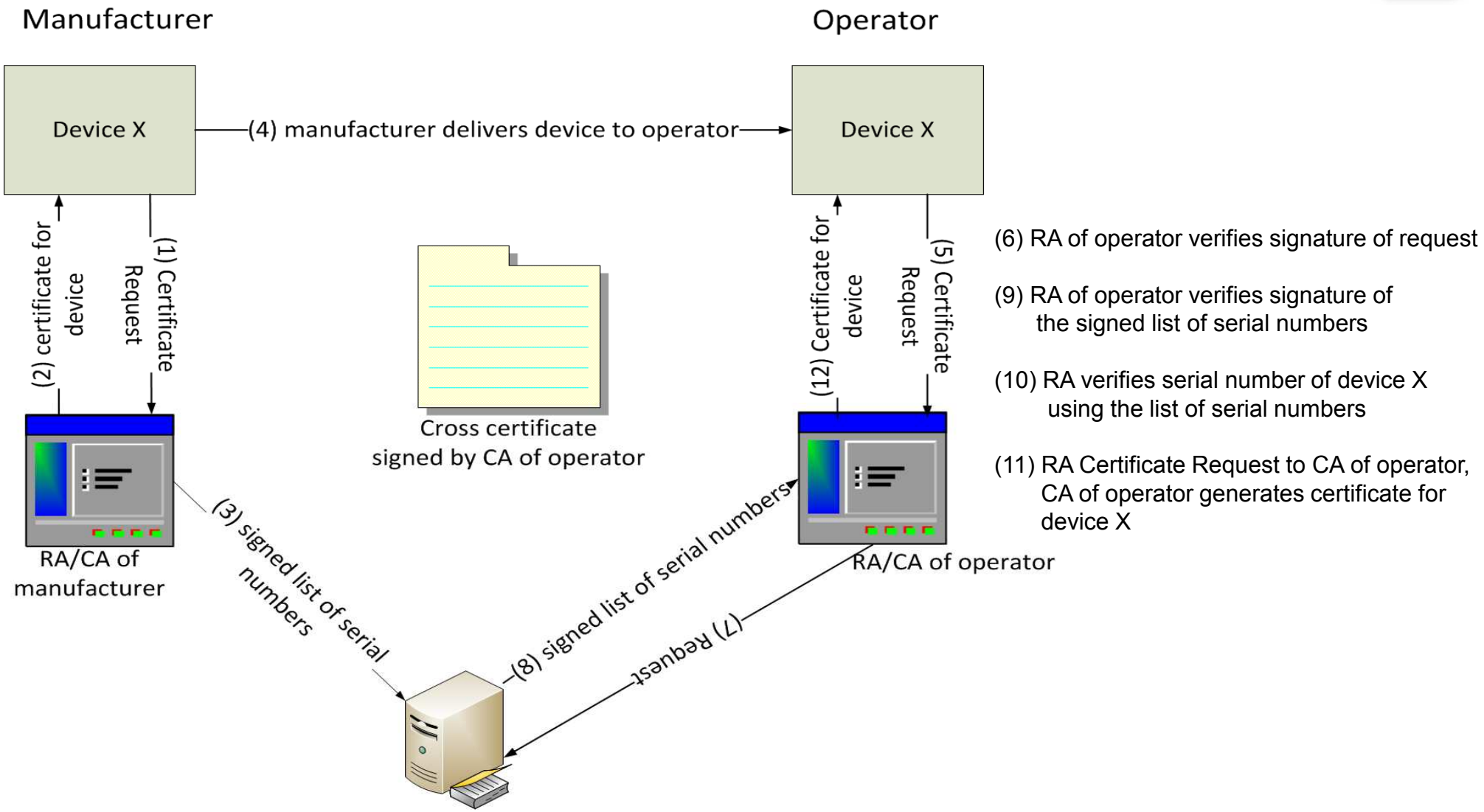
Eindeutige Identifier für Devices

Teil des subject field

- MAC (Media Access Control) Adresse
- Seriennummern
- Physical Unclonable Function (PUF)

werden Bestandteil des DN (distinguished name) des subject field

Automatisches Ausrollen von Zertifikaten



(6) RA of operator verifies signature of request

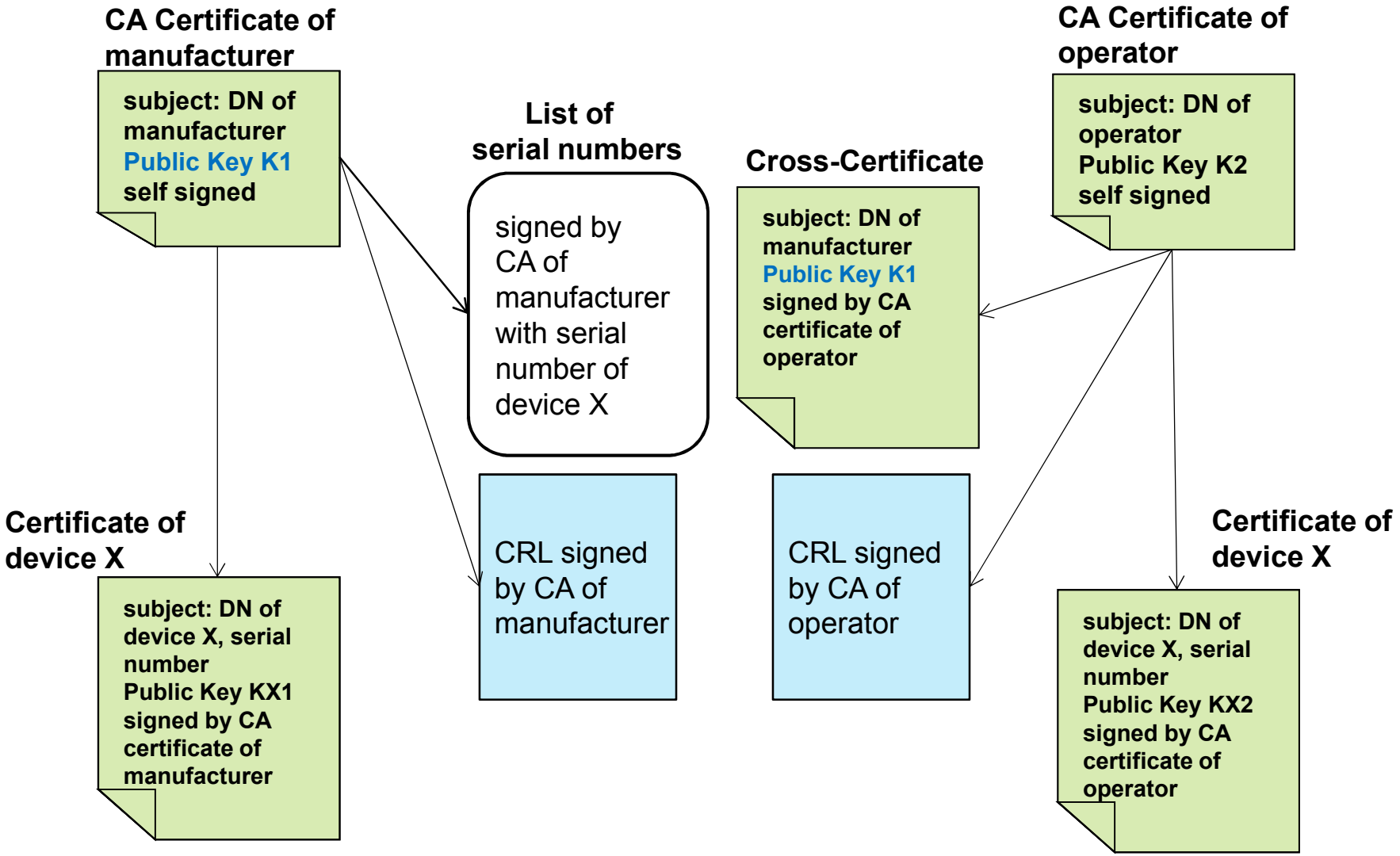
(9) RA of operator verifies signature of the signed list of serial numbers

(10) RA verifies serial number of device X using the list of serial numbers

(11) RA Certificate Request to CA of operator, CA of operator generates certificate for device X

Automatisches Ausrollen von Zertifikaten

Authentifikation und Verifikation



zu lösende Probleme

Standards sind notwendig

- Device kann CRL nicht laden: wie sieht die Fallback-Lösung aus?
- Lifetime von Zertifikaten und CRLs?
- Prozesse für
  - Renewal von Zertifikaten
  - Rezertifizierung
  - Certificate revocation
- Wie sollen die Protokolle SCVP oder OCSP?
- Wo müssen Directories redundant ausgelegt werden?
- Volumen: Management von Millionen von Zertifikaten und Schlüsseln
- Outsourcing aller CA und RA Dienste möglich/erwünscht/machbar?

Fazit

- Sichere Device-to-Device Kommunikation wird ein MUSS in der Zukunft werden (zumindest für kritische Kommunikationsverbindungen)
- Digitale Zertifikate für Devices sind notwendig
- Automatisiertes Ausrollen von Zertifikaten ist ein MUSS
- Das Certificate Management Protocol (CMP, RFC 4210) muss hier beachtet werden
- Ganzheitliche Sicht auf das Smart Grid ermöglicht die Absicherung der kritischen Device-to-Device Kommunikationen
- Vielleicht: IT Netzwerk nur dort verwenden/aufbauen, wo diese unbedingt erforderlich ist.

Standards

Standards für die Themen Zertifikate, PKI, TLS/SSL

- RFC 5246, The Transport Layer Security (TLS) Protocol, Version 1.2, http://tools.ietf.org/html/rfc5246
- ETSI, European Telecommunications Standards Institute, http://www.etsi.org/WebSite/homepage.aspx
- RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008, http://tools.ietf.org/html/rfc5280
- RFC 5055, Server-Based Certificate Validation Protocol (SCVP), http://www.rfc-editor.org/rfc/rfc5055.txt
- RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, http://www.ietf.org/rfc/rfc2560.txt
- RFC 4210, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), http://tools.ietf.org/html/rfc4210
- RFC 5273, Certificate Management over CMS (CMC): Transport Protocols, http://tools.ietf.org/html/rfc5273

Literatur, links

- Security Technology for Smart Grid Networks, Anthony R. Metke and Randy L. Ekl, IEEE TRANSACTIONS ON SMART GRID, VOL. 1, NO. 1, JUNE 2010, p. 99-107
- Cisco Smart Grid: Substation Automation Solutions for Utility Operations, Cisco, White Paper, 2010 http://www.cisco.com/en/US/prod/collateral/routers/ps10967/ps10977/white_paper_c11_593673.pdf
- Protection Profile for the Gateway of a Smart Metering System, Federal Office for Information Security, v01.01.01

Contact

Embedded Systems Team:

embedded@tuev-sued.de
www.tuev-sued.com/embedded

Dr. Thomas Störtkuhl

thomas.stoertkuhl@tuev-sued.de

Phone: +49 89 5791-1930

Fax: +49 89 5791-3437

Mobil: +49 151 2764 5644

TÜV SÜD AG
Embedded Systems V-INM
Barthstr. 16
80339 Munich
Germany