



Datenschutz im intelligenten Stromnetz

Ronald Petrlc

18. DFN Workshop

„Sicherheit in vernetzten Systemen“

15.02.2011



Agenda

- Problemstellung
- Anforderungen an das intelligente Stromnetz
 - Funktionalität
 - Sicherheit
 - Datenschutz
- Konzept: datenschutzfreundliches intelligentes Stromnetz
 - Architektur
 - Funktionsweise
- Fazit und Ausblick



Problemstellung

Wie intelligent ist das zukünftige
Stromnetz?



Smart Grid: Ziele

- Was soll das intelligente Stromnetz („Smart Grid“) bieten?
- Einsparungen für Energieversorgungsunternehmen (EVU)
 - Automatisches (entferntes) Auslesen der Zählerstände
 - Bessere Planung des Stromzukaufs an der Stromhandelsbörse
 - Bessere Nutzung grüner Energie
 - Monetärer Anreiz für den Endverbraucher Strom in Zeiten „erhöhter“ Verfügbarkeit zu nutzen
 - Transparenz für den Endverbraucher
 - Senkung des Stromverbrauchs



Smart Grid: Umsetzung

- Wie kann dies gelingen?
 - Intelligenter Stromzähler („Smart Meter“)
- Smart Meter
 - Eingebettetes System mit integrierter Kommunikationstechnologie
 - Ausgehende Kommunikation
 - ¼-stündliche Übermittlung des Stromverbrauchs an EVU
 - „Live“-Einsicht in aktuellen Stromverbrauch für Kunden
 - Eingehende Kommunikation
 - „Befehle“ vom EVU
 - Aktueller Strompreis





Smart Grid: Rechtliches

Liberalisierung des Strommarkts

- EG-Richtlinie 1996
 - Ziel: Trennung EVU und Netzbetreiber
- Umsetzung in nationales Recht (EnWG)
 - 2005: Bundesnetzagentur als staatl. Regulierungsbehörde
 - 2008: Liberalisierung Messstellenbetrieb/Messung
 - ab Jan. 2010: Einbau von Messeinrichtungen „die dem jeweiligen Anschlussnutzer den **tatsächlichen Energieverbrauch** und die **tatsächliche Nutzungszeit** widerspiegeln.“ (§ 21b Abs. 3a)
 - Letztverbraucher kann monatliche, vierteljährliche oder halbjährliche Abrechnung fordern (§ 40 Abs. 2)
 - ab Dez. 2010: EVU muss Tarif anbieten „der einen Anreiz zu Energieeinsparung oder Steuerung des Energieverbrauchs setzt“ ... „insbesondere lastvariable oder tageszeitabhängige Tarife“ (§ 40 Abs. 3)



Smart Grid: Situation heute

Wo ist das Stromnetz heute schon „intelligent“?



Quelle: [2]



Smart Grid: „Schutzziel“ Sicherheit

- Ist das intelligente Stromnetz auch sicherer?
 - Analoge elektro-mechanische Zähler → digitale eingebettete Systeme
 - ...auf diesen Systemen läuft Software!

- Welche Angreifer kommen in Frage?
 - Terroristen
 - Kunden
 - Spekulanten
 - ...

- Mehr dazu: Vortrag von Klaus J. Müller



Smart Grid: „Schutzziel“ Datenschutz

Datenschutz im Smart Grid?

- ULD Schleswig Holstein: Smart Meter erheben *personenbezogene Daten* und erlauben eine *Ausforschung der Lebensgewohnheiten der Betroffenen* [3]

Warum?

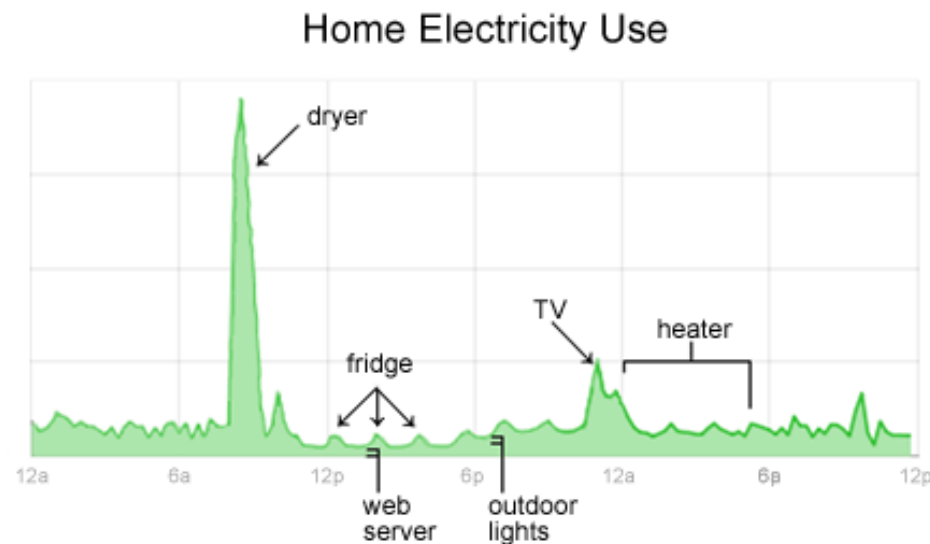


Smart Grid: „Schutzziel“ Datenschutz

Datenschutz im Smart Grid?

- ULD Schleswig Holstein: Smart Meter erheben *personenbezogene Daten* und erlauben eine *Ausforschung der Lebensgewohnheiten der Betroffenen* [3]

Warum?



Quelle: <http://dvice.com/archives/2009/02/googles-powerme.php>

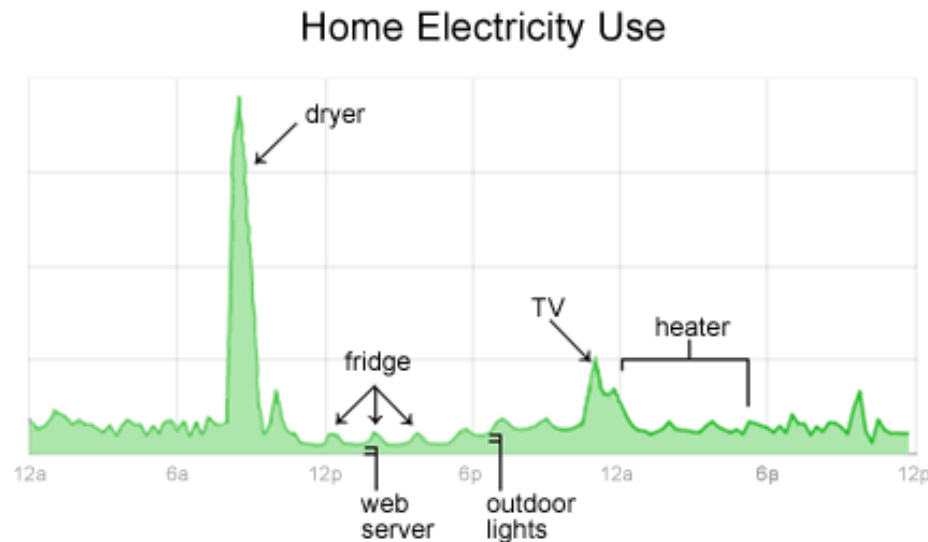


Smart Grid: „Schutzziel“ Datenschutz

Datenschutz im Smart Grid?

- ULD Schleswig Holstein: Smart Meter erheben *personenbezogene Daten* und erlauben eine *Ausforschung der Lebensgewohnheiten der Betroffenen* [3]

Warum?



Quelle: <http://dvice.com/archives/2009/02/google-powerme.php>



Smart Grid: Dilemma Nutzen vs. Datenschutz

- Erste Ansätze: Seltenerere regelmäßige Übermittlung
 - Auslastungsplanung für EVU möglich?

- Unser Ansatz
 - Potential von Smart Metering beibehalten
 - Gleichzeitig Datenschutz gewährleisten!

➤ Technischer Datenschutz



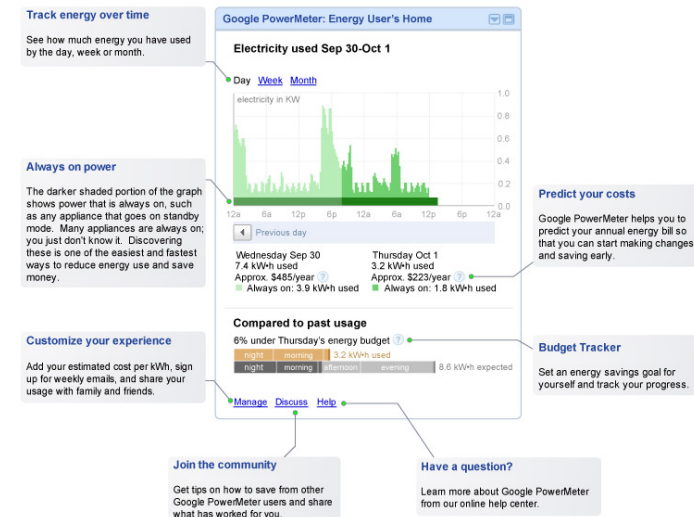
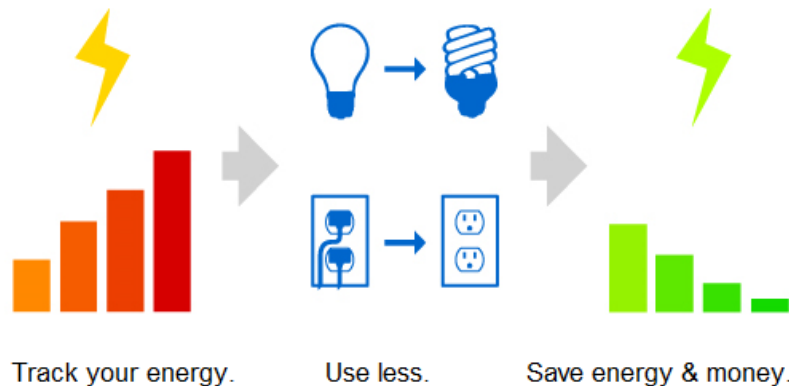
Anforderungen an das intelligente Stromnetz

Wie kann das Stromnetz „intelligent“
und datenschutzfreundlich sein?



Anforderung: Funktionalität

- Verbesserte Auslastungsplanung für EVU
- Energiesparmaßnahme für Endverbraucher



– Ja, aber geht das auch ohne Google?



Anforderung: Sicherheit

Schutzziele

- Vertraulichkeit
 - Personenbezogenes Datum Stromverbrauch muss geheim bleiben
- Authentizität
 - Beteiligte Instanzen müssen einander „kennen“
 - Falsche Daten an Smart Meter/EVU → schwerwiegende Auswirkungen
- Integrität der Smart Meter
 - Smart Meter außerhalb der „vertrauenswürdigen Zone“ des EVU



Anforderung: Datenschutz

Anonymität der Verbraucher gegenüber EVU

	Periode 1	Periode n	Σ
Kunde 1	$e_{1,1}$			$e_{1,n}$	
...					
...					
Kunde m	$e_{m,1}$			$e_{m,n}$	
Σ					



Anforderung: Datenschutz

Anonymität der Verbraucher gegenüber EVU

	Periode 1	Periode n	Σ
Kunde 1	$e_{1,1}$			$e_{1,n}$	
...	Private Information der Kunden				
...					
Kunde m					
	$e_{m,1}$			$e_{m,n}$	
Σ					

Legitime Kenntnis des EVUs



Angreifer

Potentielle Angreifer:

- Verbraucher (aus Sicht des EVU)
 - Kompromittieren Smart Meter Software → bezahlen weniger
- EVU (aus Sicht der Verbraucher)
 - Erstellt Verbraucher-Profil
- Terroristen
 - Verursachen Zusammenbruch der Energieversorgung

Konkurrierende Parteien

- Netzbetreiber vs. Energieversorger
 - Abwerben von Kunden
 - Bereitstellung/Bezahlung der Infrastruktur



Anforderungen zusammengefasst

- EVU erhält weiterhin ¼-stündlich Verbrauchswerte
 - EVU kann Verbrauchswerte keinem Kunden zuordnen
- EVU geschützt vor manipulierten Daten
- Infrastruktur geschützt vor Zusammenbruch



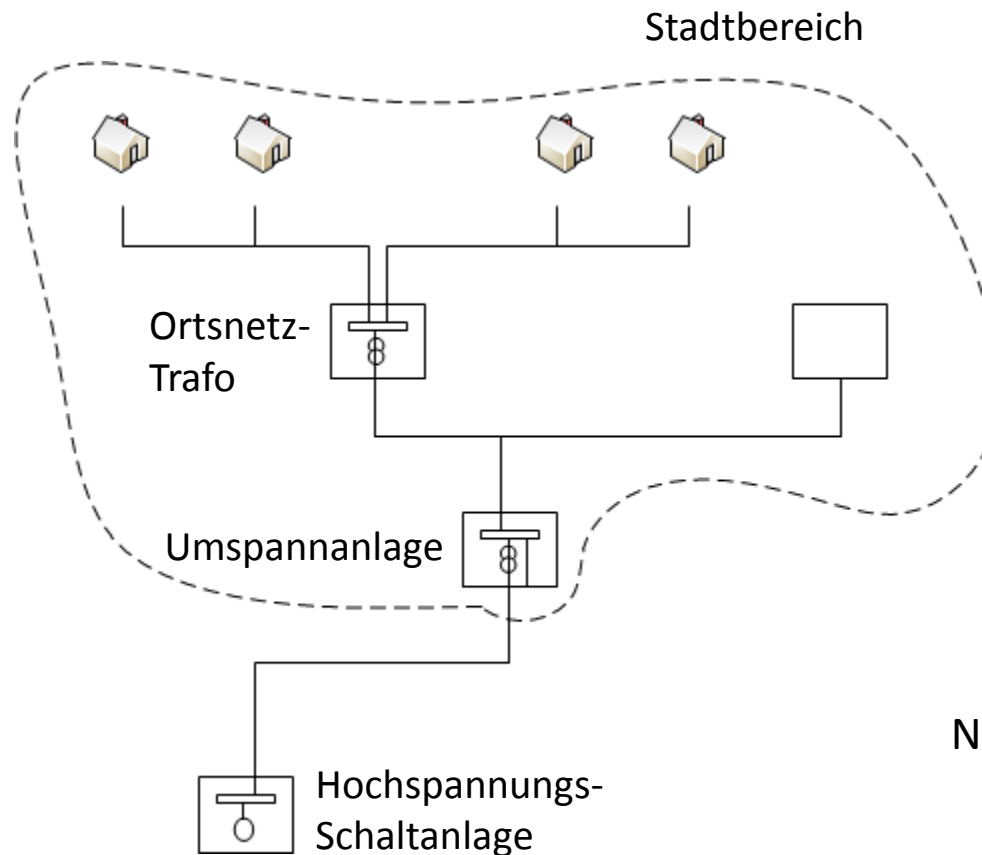
Konzept: datenschutzfreundliches intelligentes Stromnetz

Das „Smart Grid“ aus unserer Sicht



Architektur

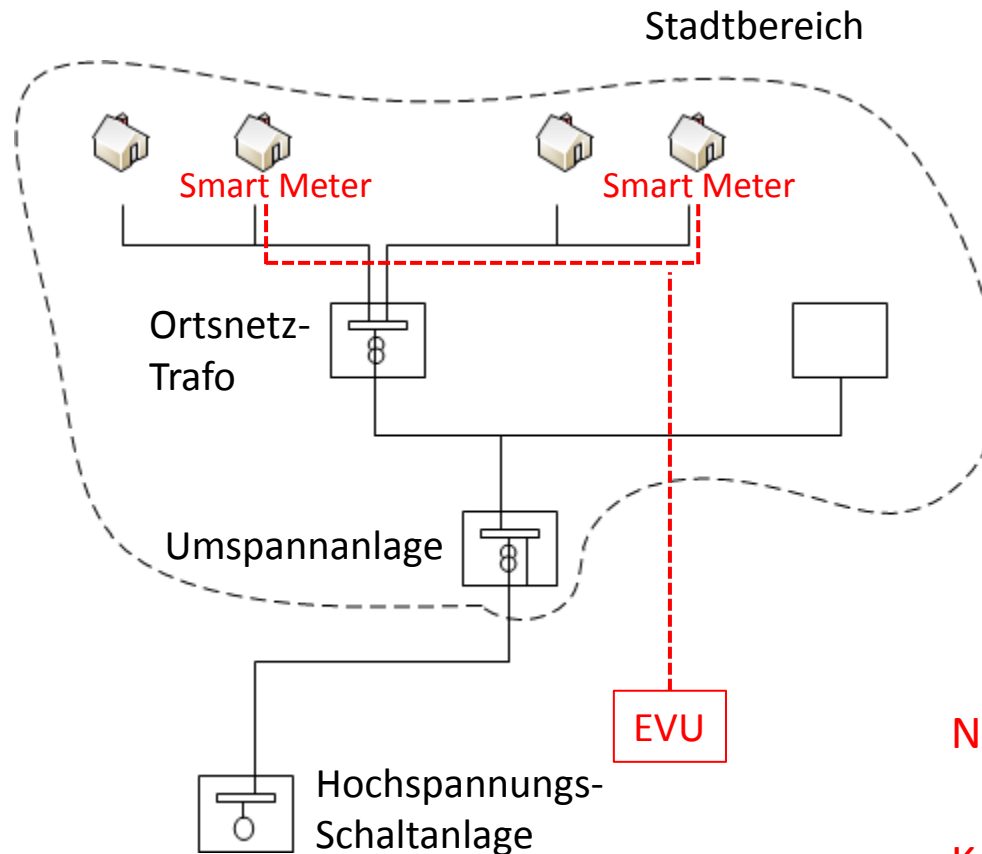
Stromnetz gestern





Architektur

(Intelligentes) Stromnetz heute



Netzbetreiber \neq EVU

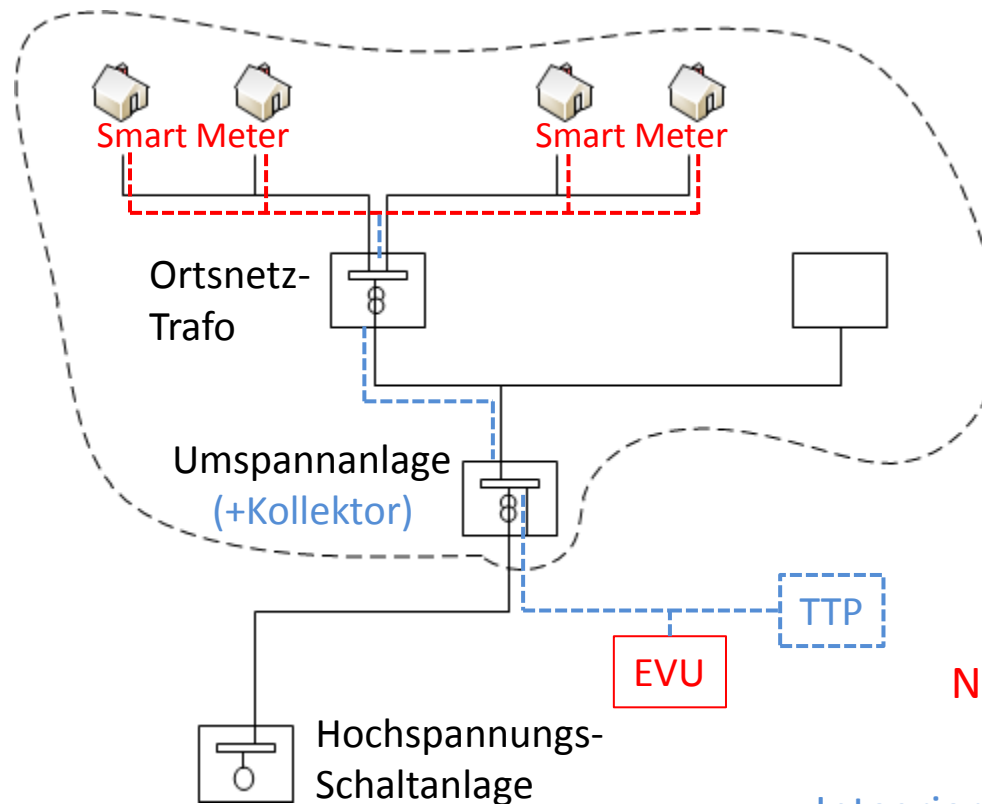
Kommunikationskanal



Architektur

Intelligentes Stromnetz morgen (unsere Sicht!)

Stadtbereich



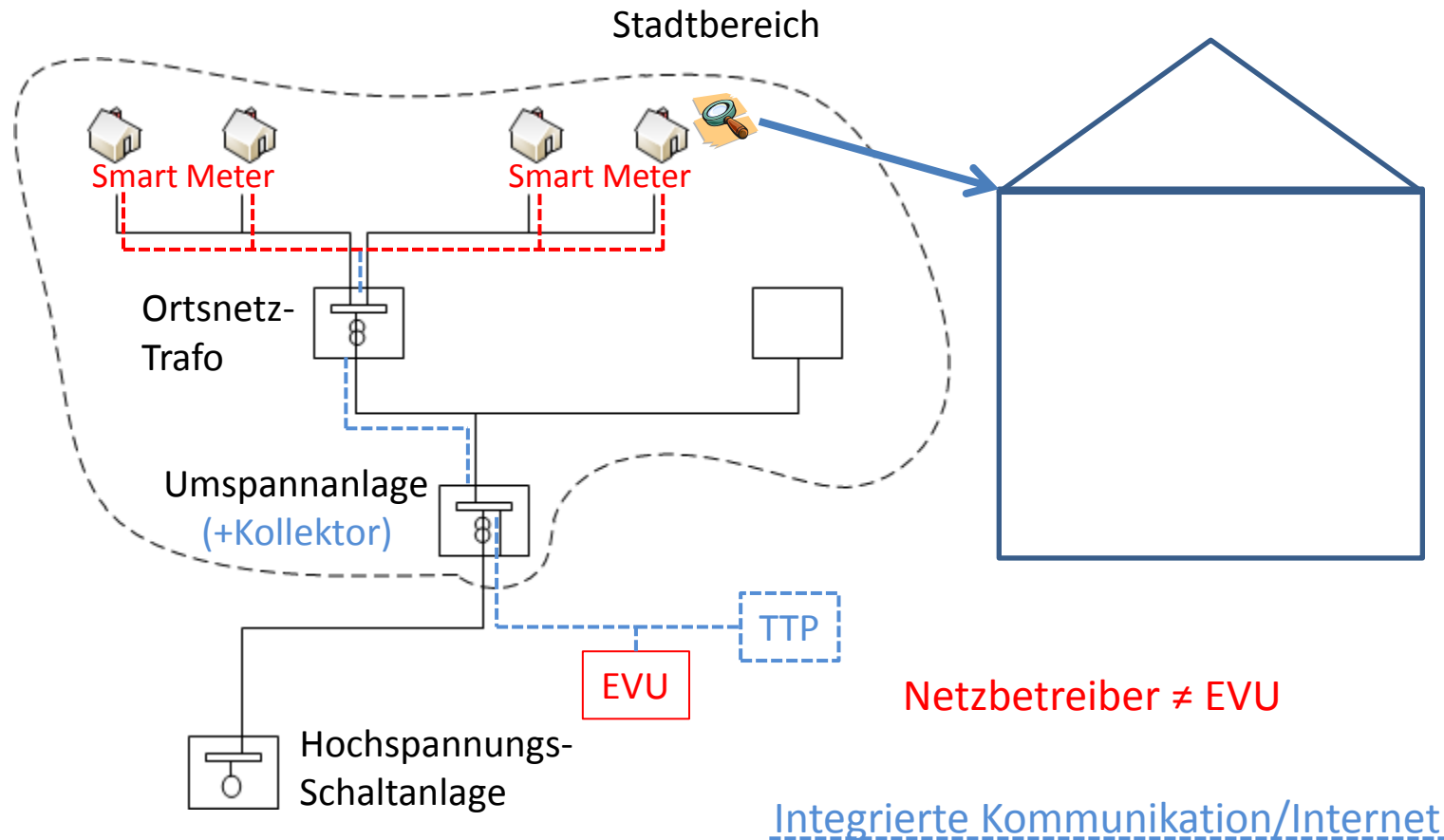
Netzbetreiber \neq EVU

Integrierte Kommunikation/Internet



Architektur

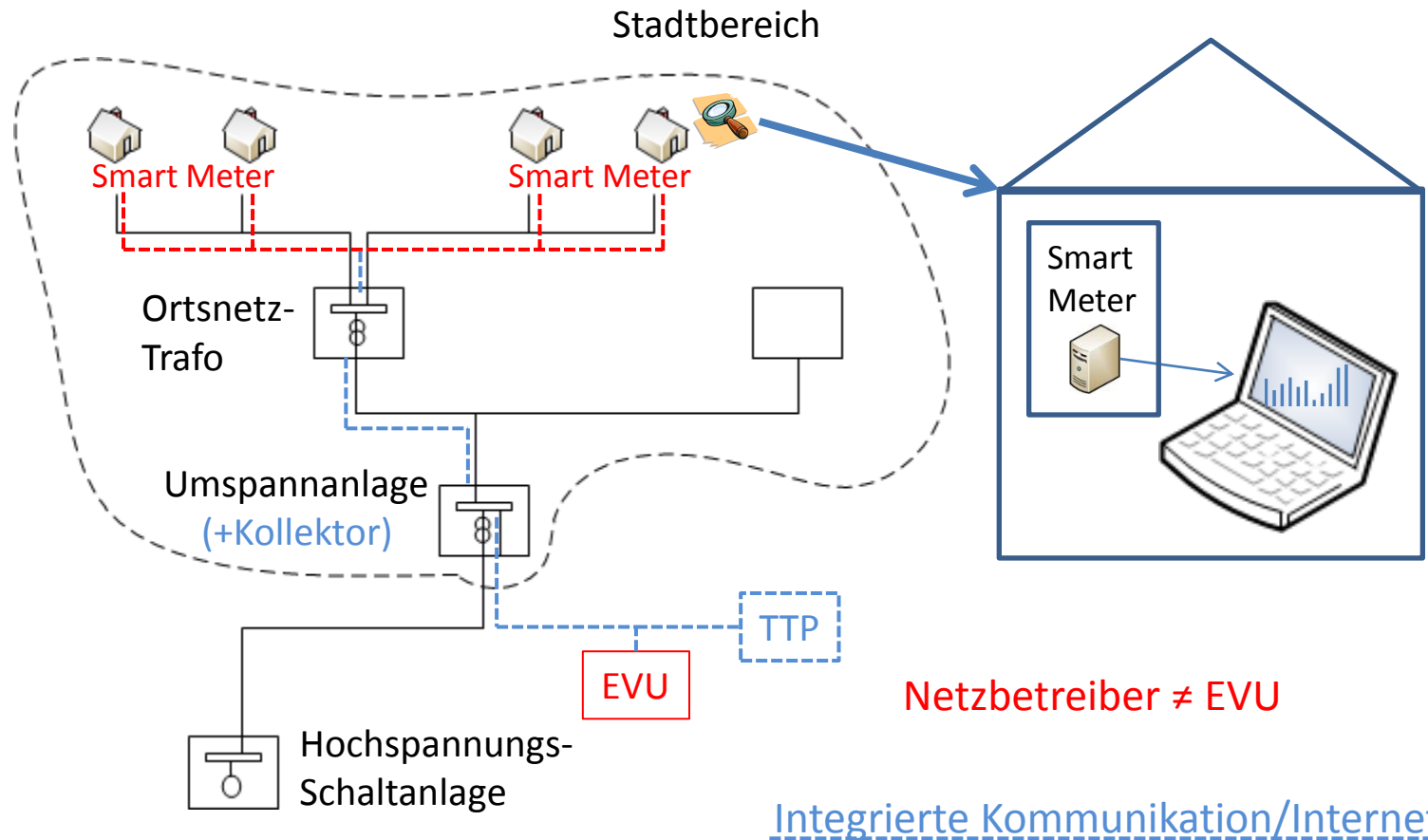
Intelligentes Stromnetz morgen (unsere Sicht!)





Architektur

Intelligentes Stromnetz morgen (unsere Sicht!)





Voraussetzungen

Smart Meter mit *Trusted Platform Module* (TPM)

- Eindeutige Identifizierung (über *Endorsement Key* (EK))
- Nötig auch für Integritäts-Prüfung

Netzbetreiber arbeitet korrekt

- „Proxy“ zwischen Smart Meter und EVU
 - Authentifizierung der Verbrauchsdaten für EVU
 - Anonymisierung des Kunden gegenüber EVU

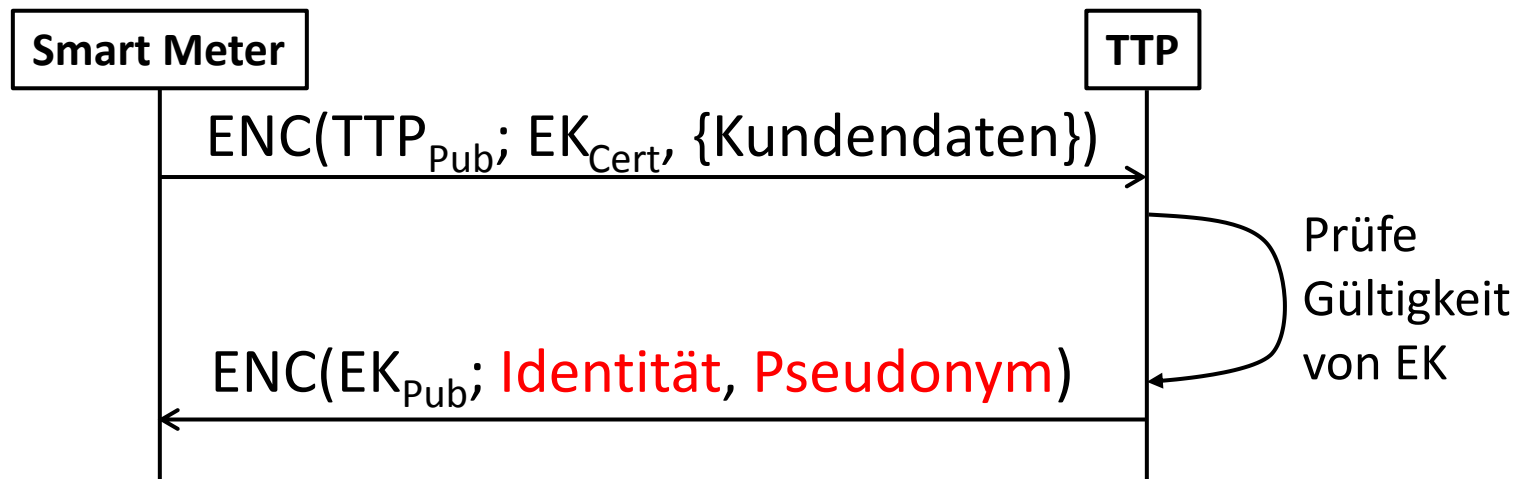
Trusted Third Party

- Darf nicht zum „Flaschenhals“ werden



Funktionsweise: Initialisierungsphase

- Übernahme von Smart Meter durch Kunden
 - TTP stellt Smart Meter eine Identität und ein Pseudonym aus

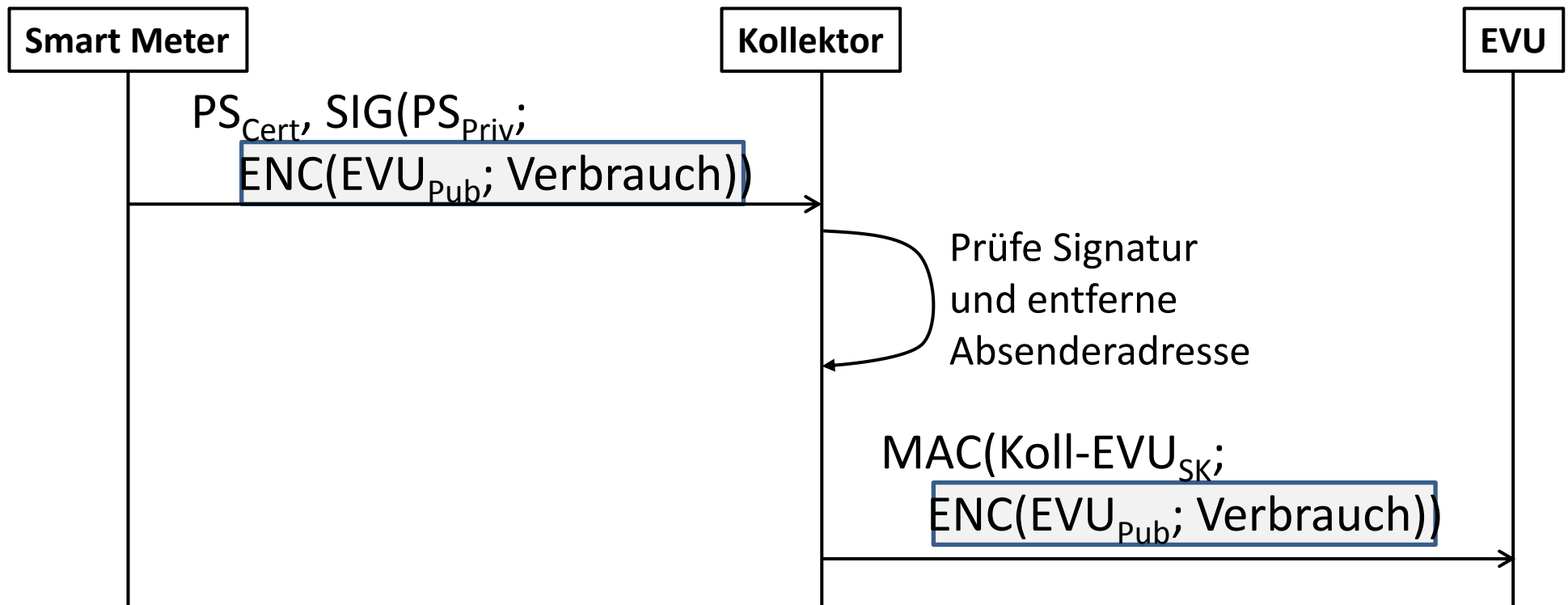


Identität = $(ID_{Priv}, \text{SIG}(TTP_{Priv}; ID_{Cert}))$
Pseudonym = $(PS_{Priv}, \text{SIG}(TTP_{Priv}; PS_{Cert}))$



Funktionsweise: Datenübermittlung

¼-stündliche Datenübermittlung zum EVU





Funktionsweise: Integritätsschutz

Smart Meter muss Authentizität von Updates prüfen

- TTP signiert Software-Updates
 - Zertifikatsmanagement im Smart Meter einfacher
 - Zertifizierung von Software durch TTP besser kontrollierbar/durchsetzbar

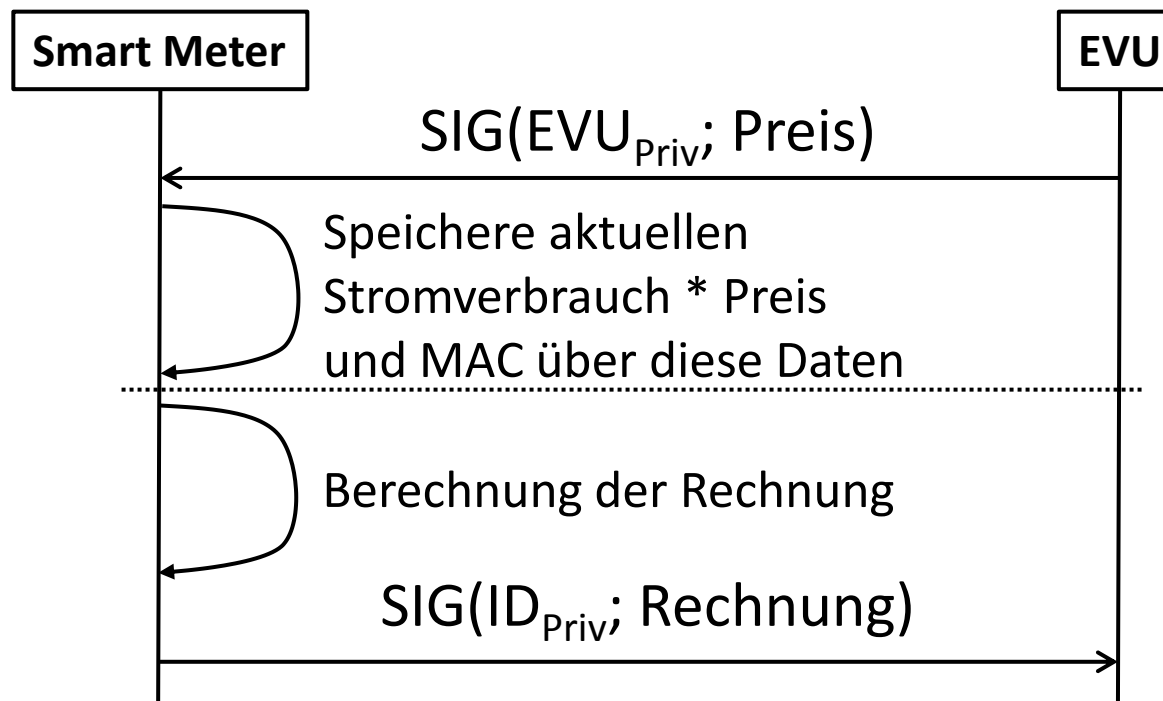
Regelmäßiges Prüfen der Smart Meter-Integrität

- Über *Remote Attestation* zu Netzbetreiber
- Soll u.a. sicherstellen, dass Update tatsächlich installiert wurde



Funktionsweise: Abrechnung

- Abrechnung erfolgt im Smart Meter → Übermittlung der Rechnung an EVU
 - Setzt Integrität der Software auf Smart Meter voraus!





Fazit und Ausblick

Erreichen wir unser Ziel?



Analyse

Schutz vor „bösem“ EVU?

- Kann ¼-stündliche Verbrauchsdaten nur einer Stadt zuordnen
- Erhält monatlich Rechnungen von seinen Kunden in einer Stadt
- Beziehung zwischen Verbrauchsdaten und Rechnung kann nicht hergestellt werden

➤ **Verbraucher-Anonymität gegenüber EVU gewahrt**



Analyse

Schutz vor „bösem“ Netzbetreiber?

- Netzbetreiber sieht Verbrauchsdaten nicht im Klartext
- Bekommt nur Verbrauchswert pro Jahr übermittelt

➤ **Profilbildung unter Pseudonym für Netzbetreiber nicht möglich**



Analyse

Schutz vor kooperierendem EVU und Netzbetreiber?

- Netzbetreiber erhält Verbrauchswert von Kunde pro Jahr
- EVU erhält in einem Jahr $\frac{1}{4}$ -stündlich Verbrauchswerte von all seinen Kunden in einer Stadt

➤ „Matching“ praktisch nicht möglich

- Sofern genügend Verbraucher/Stadt Kunden vom selben EVU
- Korrekte Arbeitsweise des Kollektor-Knoten vorausgesetzt
 - Zertifizierung und Prüfung durch unabhängige Instanz nötig!
- Je geringer das Übermittlungsintervall, desto mehr Daten fallen an
→ Matching wird schwieriger!



Analyse

Schutz vor „bösem“ Kunden?

- Integrität der Smart Meter-Software wird überprüft
- Falsche Kundenangaben können nachvollzogen werden
- Daten werden manipulationssicher gespeichert/übertragen

➤ **Sicherheit im Smart Grid gegeben**



Analyse

Schutz vor Dritten?

- Kein Einblick in personenbezogene Daten
 - Verschlüsselung von Daten
- Kein Einspielen von falschen Daten
 - Authentifizierung der Daten



Fazit

Ältere Vorschläge: Seltener regelmäßige Datenübermittlung

- Widerspricht Auslastungsplanung von EVU

Unser Konzept

- Weiterhin regelmäßige Datenübermittlung an EVU
- Datenschutz und Sicherheit gewährleistet



Herausforderungen

- Kollektor muss korrekt arbeiten
- TPM für eingebettete Systeme sinnvoll?
- Wer trägt Mehrkosten für Sicherheit/Datenschutz?



Ausblick

- Implementierung unseres Konzepts
- Verwendung von Smartcard statt TPM?
 - Integritätsschutz nach wie vor möglich?



Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:
Ronald Petrlic
Universität Paderborn
AG Sicherheit in Netzwerken
ronald.petrlic@uni-paderborn.de



Quellenangaben

- [1] „Das Stromnetz beginnt zu denken“, FAZ, Sep. 2009,
<http://www.faz.net/s/RubD16E1F55D21144C4AE3F9DDF52B6E1D9/Doc~EDEB58114DD5F401DB20DDA0F94CDAF9E~ATpl~Ecommon~Scontent.html>
- [2] „Smart Metering Projects Map“,
<http://maps.google.com/maps/ms?ie=UTF8&oe=UTF8&msa=0&msid=115519311058367534348.0000011362ac6d7d21187>, Feb. 2011
- [3] „Datenschutzrechtliche Bewertung des Einsatzes von ‚intelligenten‘ Messeinrichtungen für die Messung von gelieferter Energie (Smart Meter)“, Unabhängiges Zentrum für Datenschutz Schleswig Holstein, Sep. 2009,
<https://www.datenschutzzentrum.de/smartmeter/20090925-smartmeter.html>
- [4] „Google powermeter“, <http://www.google.com/powermeter>
- [5] „Vision and Strategy for Europe’s Electricity Networks of the Future“, European SmartGrids Technology Platform, <http://www.smartgrids.eu/documents/vision.pdf>