TeleTrusT
Pioneers in IT security.

Informationstag "Das Automobil als IT-Sicherheitsfall"

Berlin, 11.05.2012

Secure eMobility (SecMobil)

„Sichere IT für Elektromobilität – SmartCar, SmartGrid und SmartTraffic"

Dipl.-Ing. Antonio González Robles
Institut für Internet-Sicherheit-if(is)
Westfälische Hochschule, Gelsenkirchen

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

if(is) internet-sicherheit.

Agenda

I. Vorstellung des Projekts: Secure eMobility
„Sichere IKT für Elektromobilität – SmartCar, SmartGrid und SmartTraffic"

II. Beschreibung des „Betanken“ eines Elektroautos

- Authentifizierung an der Ladesäule
- Authentifizierung vom Auto aus

III. Domänen, Identitäten, IdMs

- Domänen-Vielfalt
- Identitäten-Typen
- Das Auto wird zum Sicherheitsfall

IV. Zusammenfassung / Ausblick

I. Secure eMobility

- Vorstellung des Projekts: Secure eMobility
  „Sichere IKT für Elektromobilität – SmartCar, SmartGrid und SmartTraffic"
- Projekt Konsortium:

  Große Partner aus Wissenschaft und Wirtschaft aus allen wichtigen Bereichen

escrypt Embedded Security

DAIMLER

smartlab

ELMOS

RUHR UNIVERSITÄT BOCHUM RUB

if(is) internet-sicherheit.

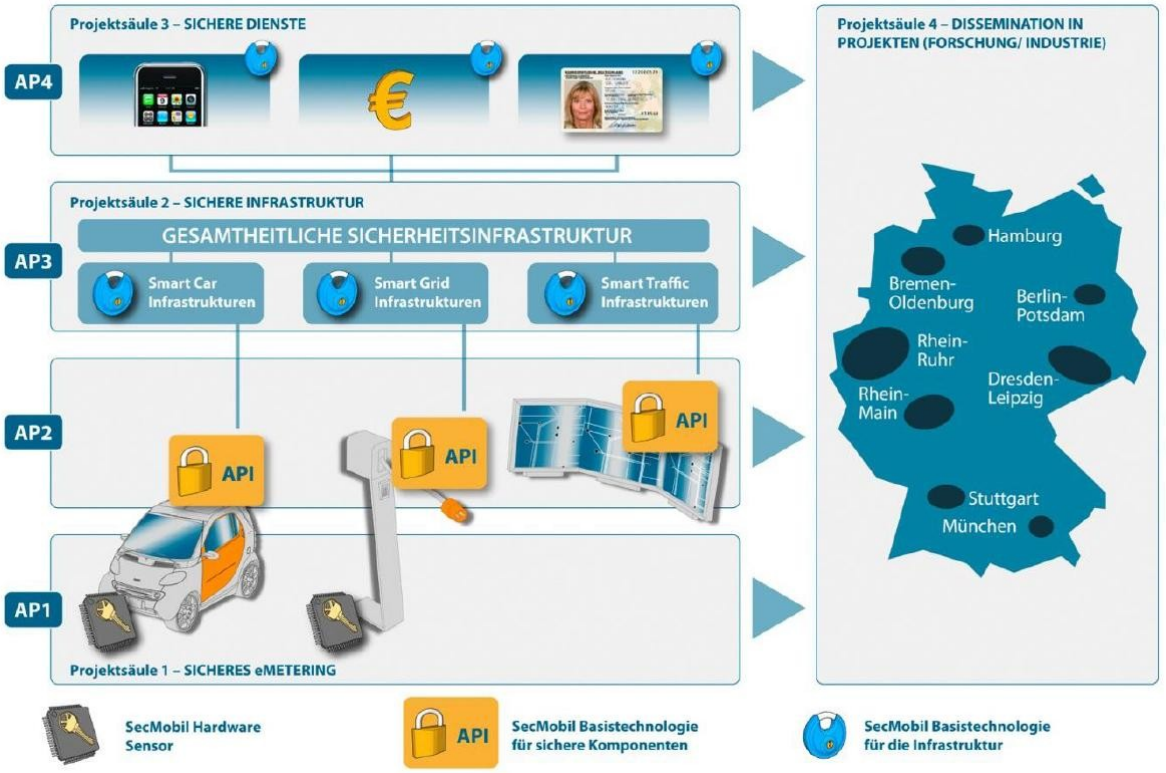
Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages

Secure eMobility (SecMobil)

„Sichere IKT für Elektromobilität – SmartCar, SmartGrid und SmartTraffic"

- Übergeordnetes Projektziel:
  standardisierte Sicherheitsarchitektur



- Unterschiedlichste Domänen treffen aufeinander
  - Benutzer (RFID (auch nPA), Smart Phone, ...)
  - Intelligente Automobile
  - Verkehrstelematik - (leitsysteme)
  - Intelligente Energieversorgungssysteme (National und international)
  - Abrechnungssysteme
  - Verschiedenste Stromanbieter
  - Gateway, Zapfsäule, Sensor, ...

ESCRYPT, Smartlab, RUB, DAIMLER, ELMOS, if(is)

Secure eMobility (SecMobil)

if(is) entwickelt Security-Basistechnologie für die Infrastruktur

- Das if(is) entwickelt für
  - Domänen
  - Komponenten
  - Identitäten
  - Clearing Center
  - Abrechnungssysteme
  - Gebäudebetreiber
  - ...
- → die **Infrastruktur zur vertrauenswürdigen Kommunikation**:
  - → PKI, Bridge CA, OpenID, SSO, ...
  - → Komponenten (auch Objekt-Identitäten) untereinander
  - → Benutzer: RFID (nPA, Smart Phone, …) zu anderen Identitäten

Secure eMobility (SecMobil)

if(is) entwickelt Security-Basistechnologie für die Infrastruktur

- Sämtliche vorhandene und zukünftige Domänen (PKI n) können vertrauenswürdig unter Beibehaltung Ihrer Unabhängigkeit eingebunden werden.
- Domänen (Private Unternehmen, Energieversorger, Automobilhersteller und -zulieferer, Finanzwelt, öffentliche Verwaltung, …) mit eigener PKI nutzen vorhandene BCA (könnte z.B. die European Bridge CA sein)
- Single Sign On (SSO) vereinfacht und fördert zusätzlich Geschäftsprozesse
  - Bezahlung per nPA
  - Bezahlung per Smartphone
  - Bezahlung mittels der Head Unit im Automobil
  - ...

- Die über Ihre Komponenten involvierten Domänen „wissen“ mit wem Sie kommunizieren und das die zum Teil lebenswichtigen Informationen nicht manipuliert sind:
  - Infrastruktur: Zähler, Zapfsäulen, Netzsteuerungskomponenten, Energieerzeuger, Safety kritische Informationen, Verkehrsinformationen, …
  - Betanken der Automobile (Ladesäule): Nutzer, Stromanbieter, Abrechnungsstellen, Banken, …
  - car2Infrastruktur: erhaltene bzw. versandte Verkehrsleit- und Umgebungsinformationen, Notfallmeldungen, ...
  - Car2car: Fahrzeuge dienen als Hop's für Verkehrs- und Umgebungsinformationen, lokale vor Ort Informationen, …
  - Gebäudezugriff („zu Hause“ und betriebliche) intelligente Vernetzung und Steuerung der Gebäude

- **Zusammenfassung der SecMobil Projekt Vorstellung**
  - if(is) und das Projekt Konsortium hat im Rahmen des Forschungsprojekts das Ziel eine standardisierte Sicherheits-Infrastruktur zu entwickeln
  - Vertrauenswürdige Kommunkation zwischen unabhägigen Partnern
  - Mittels PKI, Bridge CA, OpenID, SSO, RFID, nPA, ...

- **SecMobil Ziel**
  - Global verwendbare Forschungsergebnisse
  - Allgemein verwendbare Architektur für:
    Smart Car, Smart Grid, Smart Traffic, Smart Home, ...
  - jetzt schon für zukünftige Anforderungen ausgelegt

II. Beschreibung des „Betanken“ eines Elektroautos

- Authentifizierung an der Ladesäule

- Authentifizierung vom Auto aus

Authentifizierung an der Ladesäule

- Authentifizierung
- Ladesäule freischalten
- Identifizierung des Autos
- Autorisierung des Autos
- Ladevorgang
- Beenden des Ladevorganges
- Abrechnungsvorgang

Authentifizierung an der Ladesäule

- mit RFID Karte (aktuell)

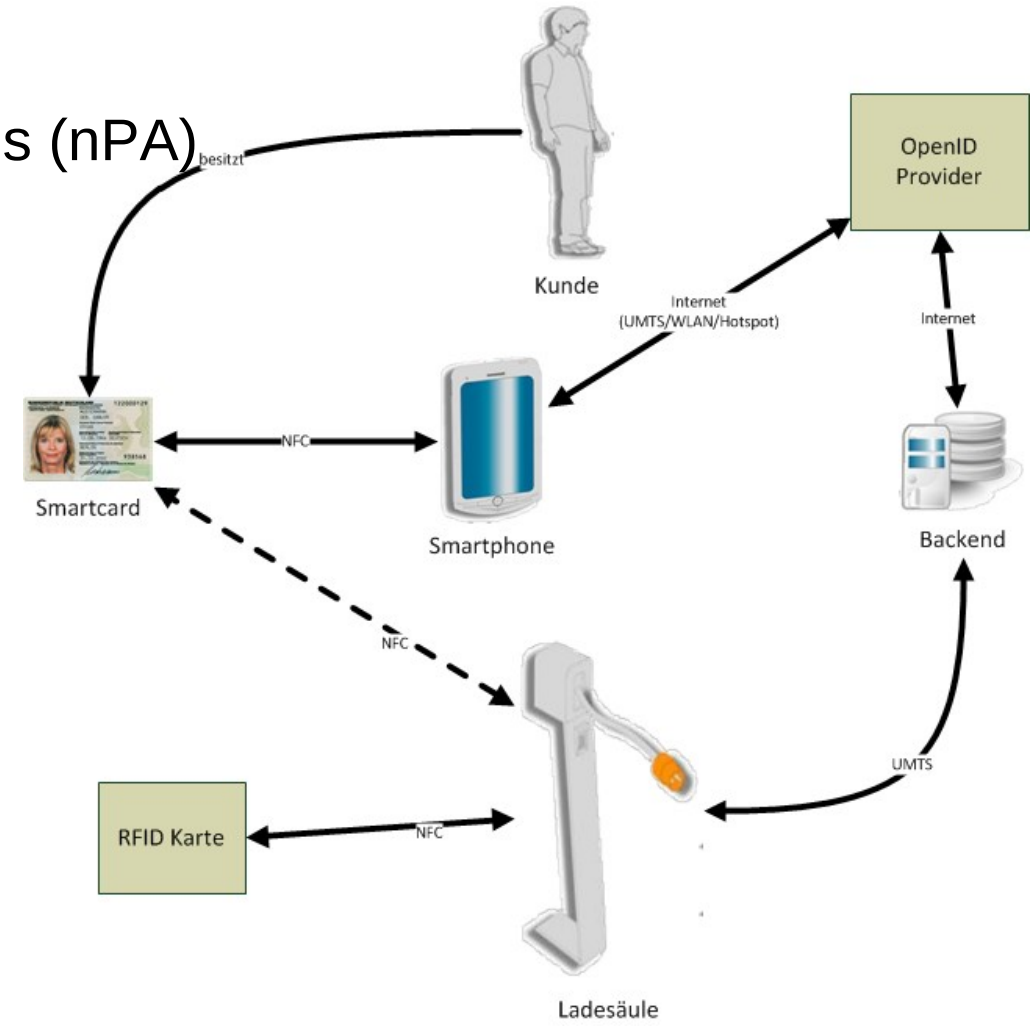
  Ladesäule ohne pinpad

- Ziel mit neuem Personalausweis (nPA)

  Ladesäule mit pinpad

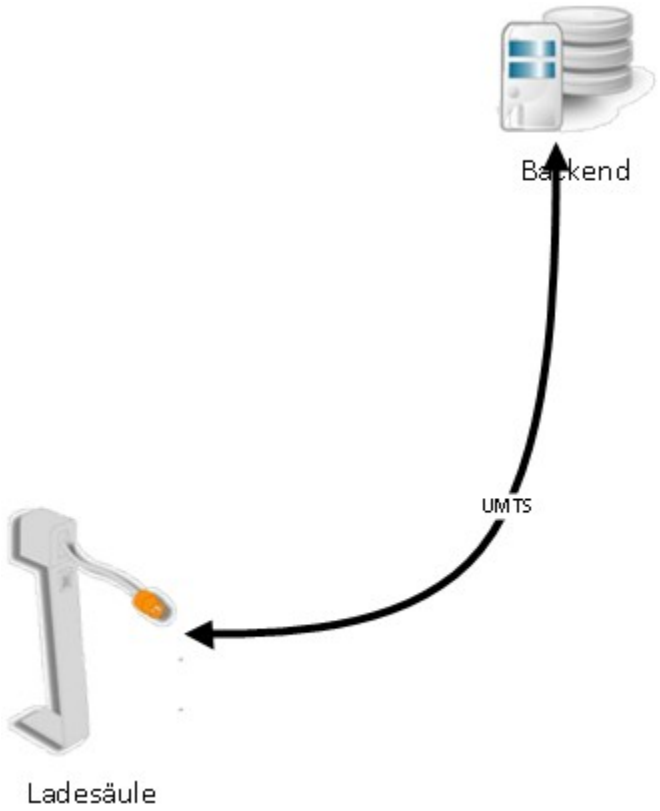
- Zusätzlich über Smart Phone

  und nPA unabhängig
  von Ladesäulenausstattung



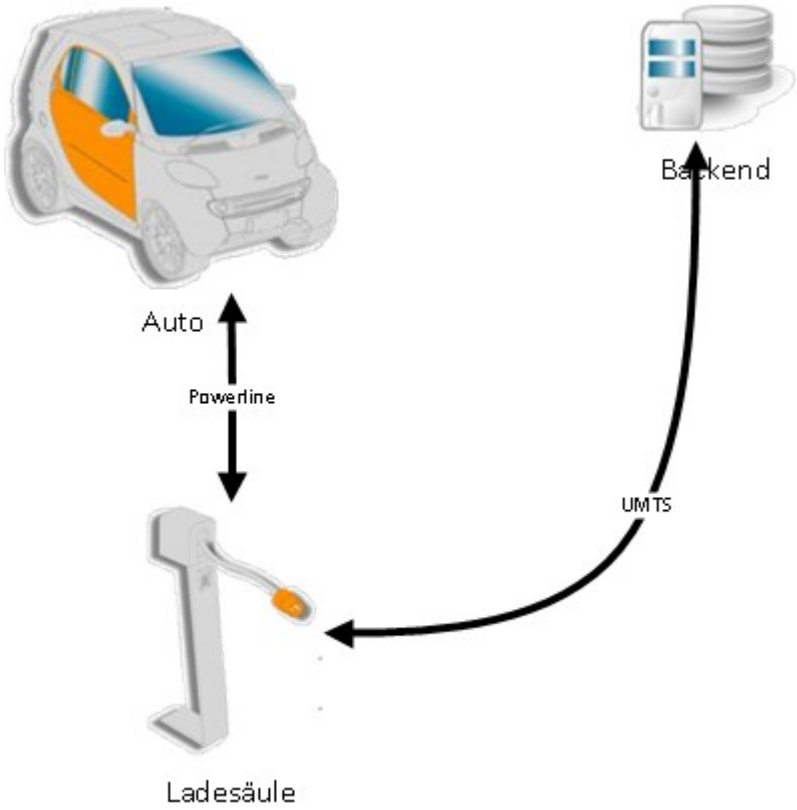
Ladesäule freischalten

- Backend schaltet die Säule für den Authentisierten Benutzer frei



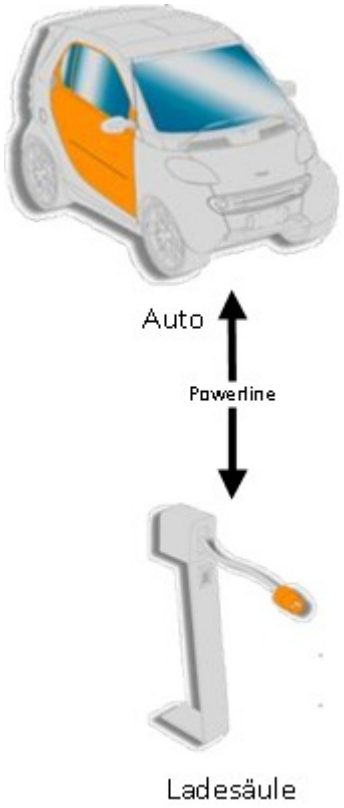
Identifizierung und Authorisierung des Autos

- Identifizierung
  (laut ISO15118 Batterie)
- Technische Voraussetzung
  - Phasenanzahl
  - z.B. Ladestrom/Ausgangsleistung
    1x16 A/3,7kW
    3x32 A/22kW
  - Andere technische Parameter



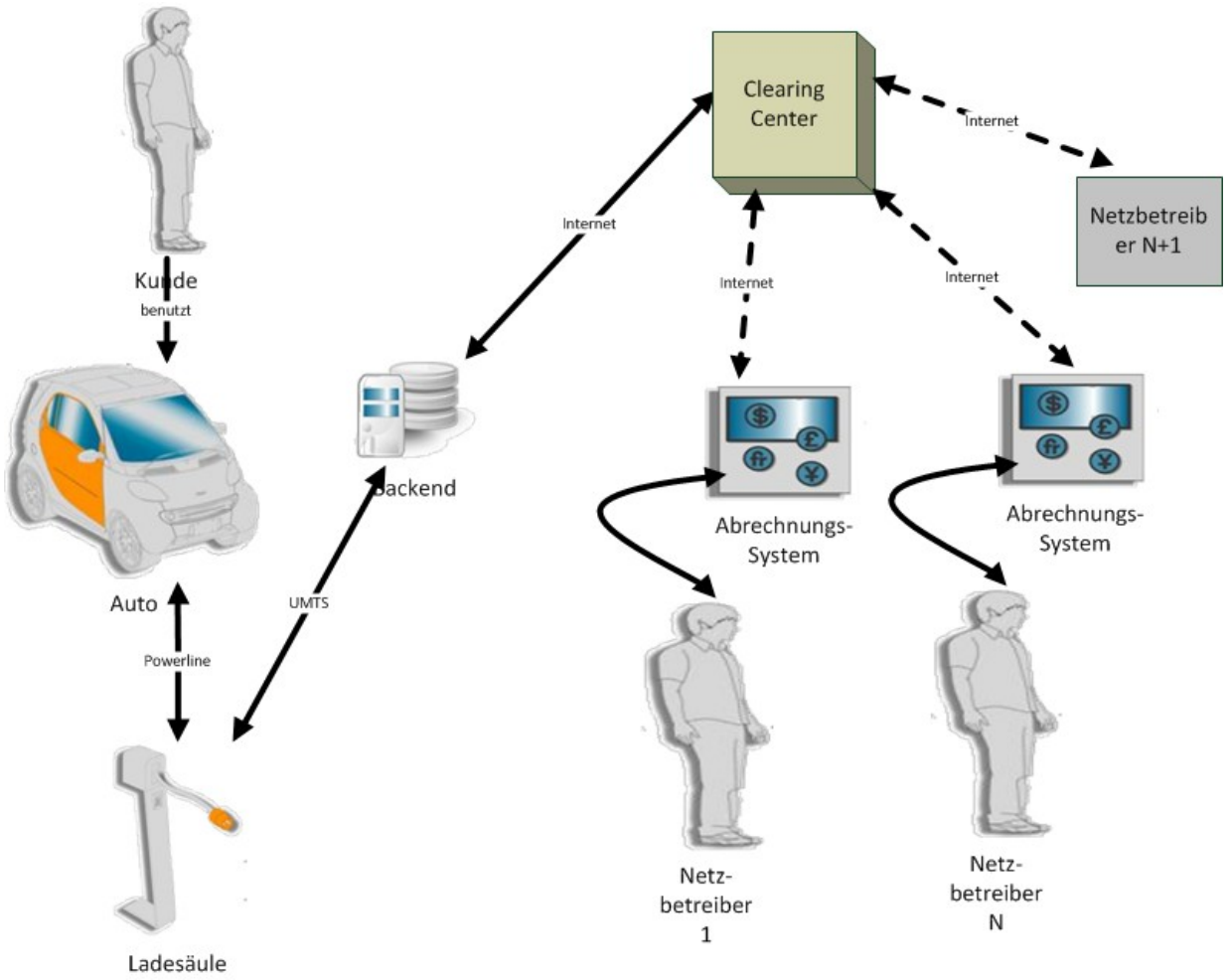
Ladenvorgang des Elektroautos

- Laden (ISO15118)
  - Quittieren beim Laden
  - ...
- Ladevorgang beenden
  - Benutzer beendet
  - System beendet da Akku voll
  - Stecker willkürlich gezogen
  - Fehler/Störung



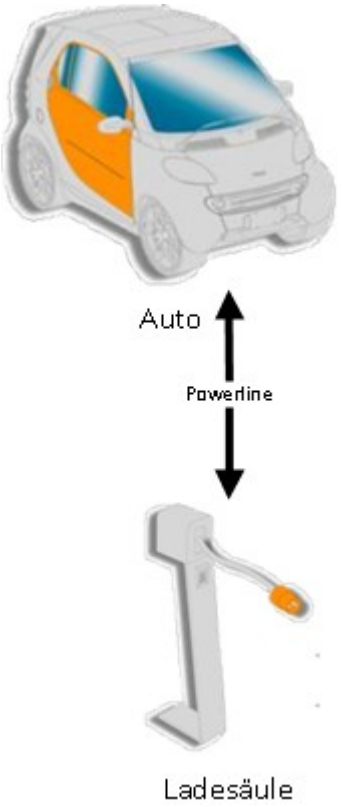
Abrechnung

- Abrechnungsvorgang:
  - Ladesäule online (direkt verschickt)
  - Ladesäule offline (später verschickt, max. T offline, dann kein Laden möglich)
- Clearing Center zur Anbindung verschiedener Abrechnungssysteme und Netzbetreiber



Authentifizierung vom Auto aus

- Benutzer authentisiert sich mittels nPA an der Head Unit
  - Integriertes Lesegerät
  - NFC SmartPhone mit Head Unit verbunden
- Von Head Unit entkoppelt mit nPA (Benutzer bezogen)
  - Smart Phone mit NFC
  - SSO OpenID per nPA



III. Domänen, Identitäten, Auto

- Domänen-Vielfalt
- Identitäten-Typen
- Das Auto wird zum Sicherheitsfall

Domänen-Vielfalt

- Domänen (Smart Car, Smart Grid, Smart Traffic, Smart Home, Smart Everything, ...)
  - Domänen-Vielfalt: Hersteller, Zulieferer, Energieversorger, Softwarehersteller, Verkehrsleitsysteme, Zugangssysteme, ...
- Identitäten-Flut: Jede der Domänen bringt verschiedene Identitäten-Typen mit sich:
  - Personen, Autos, Verkehrsleitkomponenten, Sensoren, Steuerungen, Stromverteiler, Gebäude, Batterie, Motor, Airbag, Feuermelder, Notfallstromsystem, Kühlschrank, Waschmaschine, Fernseher, Router, ...
- Domänen-übergreifende "Reise" der Identitäten
  - Identitäten sind in anderen Domänen aktiv
    - Alarmanlage Home schickt Meldung an den Bewohner
    - Home Stromverbraucher melden Bedarf an EVU an

Identitäten-Typen

- Personen haben Identitäten
  - Benutzername
  - Digitales Zertifikat (PKI)
  - nPA
- Objekte haben Identitäten (zunehmende Tendenz) (Internet der Dinge)
  - Seriennummer
  - Digitales Zertifikat (PKI)

Das Auto wird zum Sicherheitsfall

- Das Auto ist direkt und indirekt mit all diesen Domänen in Berührung
  - Das Auto ist einer Vielzahl von Zugriffsversuchen Domänen -naher und -fremder Identitäten ausgesetzt
  - Wem soll, kann bzw. darf das "Auto" vertrauen?

- Objekt IDs werden über Zertifikate (PKI) verifiziert
- Personen ID werden über nPA verifiziert
- => Die uneingeschränkte „Reise“ der beiden ID-Typen durch fremde Domänen bedarf eines hohen Aufwands, sowohl technisch wie administrativ.

Das Auto wird zum Sicherheitsfall

- Jede Domäne (PKI) muß mit jeder zu kommunizierenden Cross-Zertifiziert werden
- Jeder Dienst muß für den nPA einen eID Server haben
- Überschaubare Strukturen sind sowohl für Sicherheitsanbieter, Betreiber und Nutzer in doppelter Hinsicht Sicherheits fördernd:
  - Sicherheitsanbieter laufen weniger Gefahr strukturelle Risiken zu übersehen
  - Nutzer und Betreiber bauen ein höheres Vertrauensniveau auf
- Einfache aber effiziente Strukturen sind:
  - => Objekte: PKI + Bridge CA
  - => Personen: OpenID Provider (nPA)

IV. Zusammenfassung / Ausblick

- Identitätenmanagement:
  - Objekt-Identitäten mit asymmetrischem Verfahren (PKI)
    - Bridge CA
  - Personen-Authentifizierung mit dem nPA (neuen Personalausweis)
    - OpenID Provider für SSO (Single-Sign-On)
  - Aktuell: Personen haben zahlreiche Identitäten
- Erstellung standardisierter Sicherheitsarchitektur im Forschungsbereich:
  „Security for Smart Car, Smart Grid, Smart Traffic, Smart Home“
- if(is) plant Gateway nach BSI PP und Eichrecht konform

Referenzen

- Projekt: „Sichere IKT für Elektromobilität – SmartCar, SmartGrid und SmartTraffic"
- Master-Thesis: Sicherheitsanalyse eines OpenID-Provider mit Proxy-Funktionalität für den nPA, 11/2010
- IT-Sicherheit 6/2010: OpenID trifft elektronischen Personalausweis, Sichere Authentisierung im Internet.
  Prof. Dr. (TU NN) Norbert Pohlmann, B.Sc. Sebastian Feld, IT-Sicherheit, Ausgabe 6/2010
- Security Analysis of OpenID, followed by a Reference Implementation of an nPA-based OpenID-Provider.
  Sebastian Feld, Norbert Pohlmann. In ISSE 2010 Securing Electronic Business Processes. ISBN 978-3-8348-1438-8. pp 13-25. Vieweg+Teubner Verlag. 2010
- Ein OpenID-Provider mit Proxy-Funktionalität für den nPA. Sebastian Feld, Norbert Pohlmann. In D-A-CH Security 2010. ISBN 978-3-00-031441-4. pp 31-44. Technische Universität Wien. 2010
- Datenblatt der Siemens Ladesäule CP500A_D (260_110717_WS_CP500A_D.pdf)

Secure eMobility (SecMobil)

„Sichere IKT für Elektromobilität – SmartCar, SmartGrid und SmartTraffic"

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

Dipl.-Ing. Antonio González Robles
Projektleiter Secure eMobility
GonzalezRobles@internet-sicherheit.de

Institut für Internet-Sicherheit
https://www.internet-sicherheit.de
Westfälische Hochschule, Gelsenkirchen