Antonio González Robles, Norbert Pohlmann

Sichere mobile Identifizierung und Authentisierung

Das Roaming in der eMobility am Beispiel von Ladesäulen

Die vorgestellte „Sichere mobile Identifizierung und Authentisierung" für das eMobility Umfeld kombiniert hierfür das Security Token, die Smartphone AuthService-App, NFC-Technologie, QR-Code und einen über das Internet sicher zu erreichenden Webservice AuthService. Die Reichweite von Elektroautos erlaubt derart weite Fahrten, dass das Beladen an Ladesäulen, die nicht zum eigenen Vertrags-Stromanbieter gehören, notwendig wird. Das Stromanbieter-Ladesäulen Roaming kann mit dem an die Stromkunden ausgeteilten Security Token umgesetzt werden, da über Policy und technisch einstellbare Vertrauensstellungen über eine BridgeCA [5] für PKIs [4,5] Stromkunden mit dem Security Token ihres Anbieters und dem eigenen SmartPhone an Ladesäulen anderer Stromanbieter laden können. Abschließend wird die Anwendbarkeit der vorgestellten Lösung auf andere Bereiche, wie Versicherungen, Banken, Behörden, Soziale Netzwerke oder Internetunternehmen, betrachtet.

1 Motivation/Problemstellung

In Zuge der Umsetzung der Energiewende nimmt die Elektromobilität (eMobility) eine immer wichtiger werdende Rolle ein.

Dipl.-Ing. Antonio González Robles

ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen. Er betreut dort den Forschungsbereich „Security for Smart Car, Smart Grid, Smart Traffic und Smart Home" und ist Projektleiter für „Secure eMobility", in dem das „Identity Management" einen Schwerpunkt bildet.
E-Mail: GonzalezRobles@internet-sicherheit.de

Norbert Pohlmann

Professor für Informationssicherheit und geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Westfälische Hochschule Gelsenkirchen sowie Vorstandsvorsitzender des TeleTrusT – Bundesverband IT-Sicherheit.
E-Mail: pohlmann@internet-sicherheit.de

Der Weg von fossilen primären Energieressourcen hin zu regenerativen und umweltfreundlichen Energieformen findet einerseits durch das Ersetzen der fossilen Rohstoffe zur Erzeugung der elektrischen Energie in Kraftwerken, andererseits auch im Alltag statt, sodass für den Antrieb direkt elektrische Energie statt fossiler Rohstoffe verwendet wird.

Die gesellschaftlich sichtbare Substitution der fossilen Rohstoffe durch elektrische Energie ist im Umfeld der Elektromobilität am deutlichsten zu sehen. Im Straßenverkehr werden viele zuvor mit fossilen Kraftstoffen (z.B. Benzin und Diesel) betriebene Fahrzeuge auf innovative Elektroantriebe umgestellt. Die Elektrifizierung des Antriebs zieht sich durch eine Großzahl an Fahrzeugklassen, unterschiedlichste Wirtschaftszweige und behördliche Einrichtungen. Es werden PKWs, Busse, LKWs und auch Zweiräder, elektrisch betrieben, vermehrt eingesetzt.

Die Versorgung mit elektrischer Energie für die eMobility wird von einer Vielzahl von Stromanbietern gewährleistet. Es sind große überregionale Unternehmen wie RWE, EON und die regionalen Stadtwerke, nahezu jeder deutschen Stadt, die vorrangig die Versorgung mit elektrischer Energie sicherstellen. Die zur Verfügung zu stellende Ladesäulen-Infrastruktur erfordert allein für die elektrotechnische Umsetzung hohe Investitionen, die gerade bei modernen Energienetzen auch schon einen sehr hohen Anteil für Informations- und Kommunikationstechnologie (IKT) erfordert. Moderne Energienetze umfassen hier unter anderem den Industrie-, Privat- und Öffentlichen Bereich, zu letzterem gehört z.B. der Straßenverkehr.

Die geforderte Energiewende kann nur durch den Einsatz technologisch hoch ausgereifter IKT umgesetzt werden. Schon heute

ist ein hoher Teil des Energieversorgungsnetzes über das Internet erreichbar, bzw. ist das Internet der Energie im Aufbau, und die Weichen für das Internet der Dinge sind schon gestellt. Vor diesem Hintergrund betrachtet ist es nicht verwunderlich, dass die im Aufbau befindliche Ladeinfrastruktur für Elektroautos schon jetzt remote über das Internet steuer- und wartbar ist. Die Elektromobilität hat in den letzten Jahren große Fortschritte gemacht, die unter anderem eine höhere Reichweite der Elektroautos mit einer Akkuladung ermöglichen. Der Elektroautofahrer wird sein Elektrofahrzeug nicht nur lokal im heimischen Einzugsbereich nutzen und somit zum Laden nicht immer die Ladesäulen seines lokalen Stromanbieters verwenden können.

Im Rahmen der höheren Reichweite der Elektroautos stellt sich die Frage, wie der Stromkunde an anderen Ladesäulen, als die seines Stromanbieters, erstens Zugang und zweitens Strom zu seinen Stromanbietertarifen erhalten kann.

Die Stromanbieter ihrerseits müssen an den eigenen Ladesäulen die Stromkunden anderer Stromanbieter, erstens als solche identifizieren und zweitens, die geladene elektrische Energie mit dem Stromanbieter des Roaming Kunden abrechnen können.

Die Ladesäulen-Infrastruktur muss also in der Lage sein, die Nutzung durch lokale und überregionale Stromkunden zu gewährleisten und dabei sicherzustellen, dass Kunden eindeutig identifizierbar und deren Abrechnungsdaten fehlerfrei dem zugehörigen Stromanbieter bereitgestellt werden können.

Die Erfüllung dieser Forderungen darf die Kosten der Ladesäulen nicht noch weiter in die Höhe schnellen zu lassen.

Idealerweise würde eine Ladesäule, wie sie heute schon mit Internetanschluss aufgestellt worden ist, mit nur ganz minimalem oder keinem zusätzlichen Aufwand, die überregionale Nutzung durch Stromkunden erlauben.

2 Aufgabenstellung

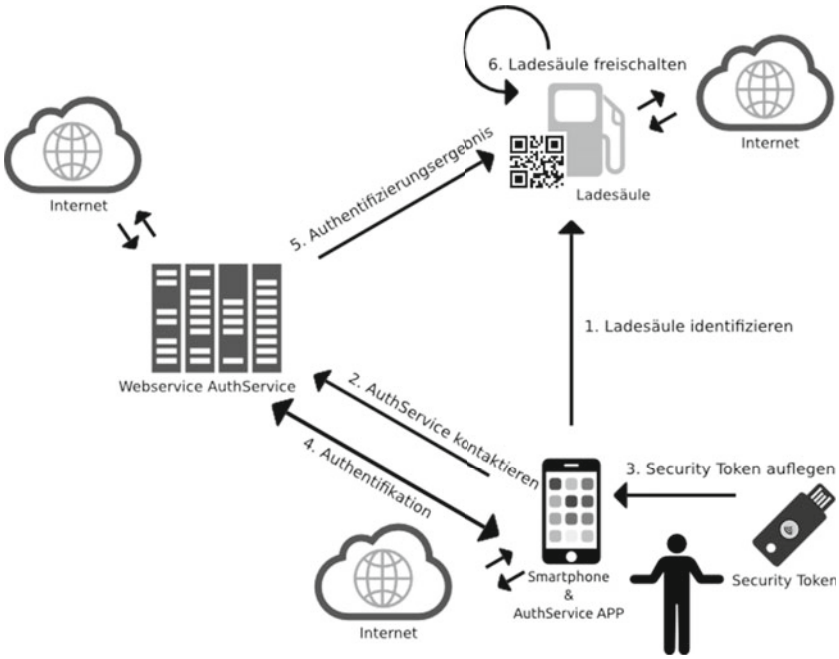
Im Umfeld der Nutzung der Ladesäulen-Infrastruktur durch Stromkunden unterschiedlicher Stromanbieter ergibt sich folgende zu lösende Aufgabenstellung:

- Alle am Ladevorgang beteiligten Parteien und Komponenten müssen eindeutig identifiziert und zweifelsfrei authentifiziert werden.
- Zusätzliche Kosten dürfen nicht anfallen

Die Abbildung 1 zeigt schematisch den Ladevorgang mit den beteiligten Komponenten und Parteien, wenn ein Stromkunde an der Ladesäule seines Stromanbieters Strom lädt. Der gezeigte Ladevorgang verwendet die vom Institut für Internet-Sicherheit – if(is) erarbeitete „Sichere mobile Identifizierung und Authentifizierung".

Die zuverlässige Identifizierung, wie auch die Authentisierung, werden im Folgenden anhand obiger Abbildung 1 generisch dargestellt.

Abb. 1 | Generischer Authentifizierungs-Ablauf



Ladesäulen werden zur Identifikation [2] mit einem QR-Code (oder NFC-Chip) versehen. In diesem QR-Code sind vom Stromanbieter hinterlegte Informationen zur Ladesäule selbst und zum Standort eingebracht.

Kunden erhalten von ihrem Stromanbieter für sie personalisierte Security Token zur sicheren Authentikation, mit digitalen Zertifikaten der Stromanbieter PKI.

Die Stromanbieter betreiben selbst die zugehörige PKI oder nehmen den Dienst einer PKI-Betreiber-Instanz in Anspruch, die dann auch die personalisierten Security Token ausstellt und von den Stromanbietern den Stromkunden bei Ausgabe zugeordnet werden.

Der Stromanbieter versieht seine Ladesäulen zur Identifikation mit QR-Codes. Die Ladesäulen benötigen keine Monitore, Tastaturen oder Mäuse/Trackballs. Diese können, müssen aber nicht, vorhanden sein.

Der Webservice AuthService ist über das Internet erreichbar und kann von mehreren Stromanbietern gemeinsam genutzt werden.

Der Kunde erhält sein Security Token zur sicheren Authentikation und installiert zu dessen Verwendung die AuthService-APP auf dem Smartphone seiner Wahl.

Der Ablauf der Identifikation der Ladesäule und anschließende Authentikation des Kunden gestalten sich im weiteren Verlauf so einfach, wie heute schon ein beliebiger QR-Code eingelesen wird. Das Security Token wird mit der rechten Hand an das Smartphone in der linken Hand gehalten und über die NFC Kommunikation miteinander verbunden.

Ob der Kunde an einer Ladesäule seines oder eines anderen Stromanbieters Strom laden möchte, hat auf den beschriebenen Identifikations- und Authentikationsablauf keinen Einfluss. Dieser bleibt weiterhin einfach und simple.

Die organisationsübergreifende Nutzung von Ladesäulen unterschiedlicher Stromanbieter wird durch Einhaltung gemeinsam von den Stromanbietern dafür vereinbarter Policies und durch die Einrichtung der Vertrauensstellung der Stromanbieter PKI zu einer existierenden BridgeCA ermöglicht.

Anders ausgedrückt, heißt das nichts anderes, als dass z.B. Kunden eines Stromanbieters aus München an Ladesäulen eines Stromanbieters in Frankfurt mit demselben sicheren Security Token seines heimischen Stromanbieters genau so einfach Strom laden können.

Die zusätzlichen Kosten für den Stromanbieter sind gering:

- Einfache Ladesäulen, wie bisher
- Legacy-Ladesäulen weiterhin nutzbar
- Webservice im Internet mit einfacher Standard-Schnittstelle
- sichere und günstige Smartcard-Technologie

Die sichere Identifizierung und Authentifizierung der Kunden stellt die Grundlage für eine sich anschließende Abrechnung der geladenen elektrischen Energie, da eindeutig nachvollziehbar ist, welcher Kunde wie viel elektrische Energie geladen hat.

Zusammenfassend ergibt sich die zu lösende Aufgabenstellung wie folgt:

- zuverlässige Identifikation der Ladesäulen
- eindeutige Identifikation des Stromkunden
- sichere Authentisierung des Stromkunden
- organisations übergreifendes Roaming beim Laden ermöglichen

3 Identifikations- und Authentikations-Provider in der eMobility

Im Folgenden wird der aus dem eMobilty Umfeld entstandene Identifikations- und Authentikations-Provider beschrieben.

Die Identifikation und Authentikation der beteiligten Komponenten und Akteure basiert auf asymmetrischen Schlüsselpaaren und zugehörigen Zertifikaten, die von einer PKI bereitgestellt werden. Das Security Token ist das sichere Authentifizierungs Token, auf dem das Stromkunden Zertifikat und Schlüsselpaar geschützt gespeichert vorliegen.

Ergänzende vertrauensbildende Maßnahmen zur Identifizierung im Ladesäulenumfeld sind die Einbeziehung der Standorte der Ladesäule und des Stromkunden während des Authentifizierungsvorgangs. Des Weiteren werden dem Kunden im Verlauf der Authentikation, zur Steigerung des Vertrauens, Informationen der digitalen Zertifikate der Ladesäule auf dem Smartphone angezeigt.

3.1 Identifikation und Authentifikation der Komponenten und Akteure

Zu allen Komponenten und zugehörigen Akteuren hat der Stromanbieter ein asymmetrisches kryptografisches Schlüsselpaar und durch eine PKI ausgestelltes zugehöriges digitales Zertifikat, sodass alle miteinander kommunizierenden Komponenten, wie der Webservice AuthService, Ladesäule und Kunden Security Token eine vertrauenswürdige Kommunikation aufbauen können. Das verwendete Authentisierungsprotokoll ist Challenge Response basiert und erfüllt die notwendigen IT-Sicherheitskriterien und -anforderungen. Sie basieren auf asymmetrischen Schlüsselpaaren, um passende Vertrauensmodelle nutzen zu können.

Die aufgestellten **Ladesäulen** sind mit einem **QR-Code** versehen. Der QR-Code beinhaltet alle relevanten Informationen der Ladesäule.

- Webservice AuthService-URL, Standort, Ladesäulen-ID, TYP, context, Zertifikatsinfo, ...

Die **Stromkunden erhalten** ein durch den Stromanbieter für sie **personalisiertes Security Token**, das eine starke Authentikation des Stromkunden ermöglicht.

Die Stromkunden nutzen das Security Token in Kombination mit ihrem **Smartphone**, auf dem die **AuthService-App** zur Verwendung des Token installiert ist. Die Smartphone AuthService-App wird bei Ausgabe einmalig für das personalisierte Security Token konfiguriert.

Die Kombination aus Smartphone, AuthService-APP und Security Token stellt dem Stromkunden ein einfach, schnell und sicher zu nutzendes Identifizierungs- und Authentifizierungswerkzeug zur Verfügung. Der Stromanbieter seinerseits erhält das sicherste verfügbare Kunden-Authentifizierungs-Token zu günstigsten Preisen.

Schematisch lassen sich Identifizierung und Authentifizierung wie folgt darstellen:

Identifizierung:

- Der Stromkunde identifiziert die Ladesäule durch das Einlesen des QR-Codes mit dem Smartphone und der AuthService-APP
- Dem Stromkunden werden Informationen, wie z.B. Standort, Aufsteller, Zertifizierungs-Instanz zur Ladesäule angezeigt, die im umgesetzten Protokollablauf berücksichtigt werden.

Authentifizierung:

- Webservice AuthService URL wird dem Kunden angezeigt: (Stromkunde wird über den zu startenden Authentifizierungsvorgang informiert)
  - Zur Authentifizierung wird ein personalisiertes Security Token an das Smartphone gehalten
- Der Webservice AuthService authentifiziert den Kunden
  - Ladesäule erhält Information zum authentifizierten Kunden
  - Der Kunde erhält Information über die erfolgreiche Authentifizierung

Die Einbindung des vorliegenden Identifizierungs- und Authentifizierungs-Providers ist für den Stromanbieter kostengünstig in jeder vorhandenen Ladeinfrastrukturtechnologie durchführbar, sodass sich der hier beschriebenen Authentifizierung die Autorisierung, des Stromkunden durch die Ladeinfrastruktur dann unverändert (wie schon umgesetzt), anschließt.

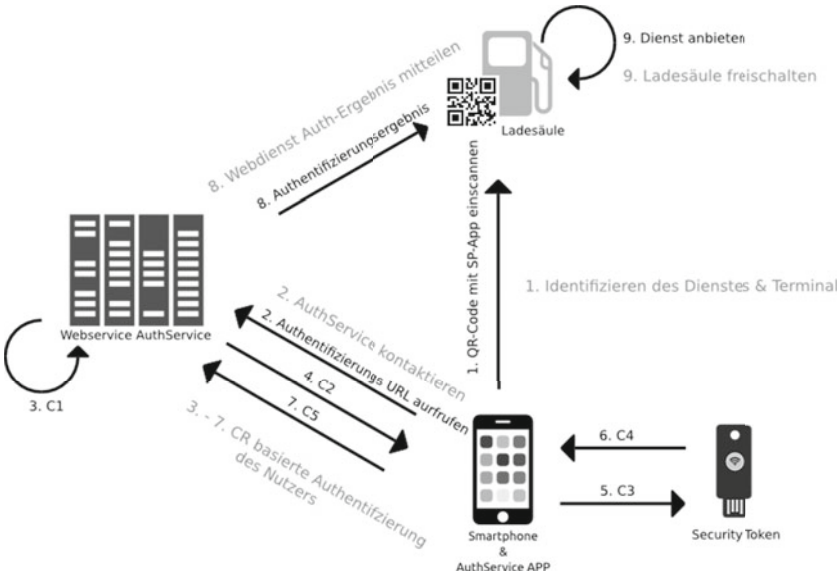
3.2 Protokollablauf, HW, SW und Schnittstellen

In Abbildung 2 wird der Authentifizierungsvorgang dargestellt. Der Abbildung 2 ist zu entnehmen, dass innerhalb der Ladeinfrastruktur nur eine geringfügige Ergänzung notwendig ist, um die Mitteilung über die erfolgreiche Authentifizierung des Stromkunden vom Webservice AuthService entgegennehmen zu können. In die vorhandene Infrastruktur wird ein den Webservice AuthService bereitstellender Server eingebunden. Die übrige Ladeinfrastruktur, wie auch die Ladesäulen selbst, bleiben unverändert und in ihrer übrigen Funktionalität unberührt.

Der **Protokollablauf** für Identifizierung und Authentifizierung stellt sich wie in Abbildung 2 gezeigt dar:

1. QR-Code mit der Smartphone AuthService-App einlesen
2. Webservice AuthService wird von der Smartphone AuthService-App aufgerufen
3. Webservice AuthService initiiert Challenge Response (CR) basiertes Protokoll
4. Webservice AuthService Auth Anfrage an Smartphone
5. Das Security Token wird vom Stromkunden an das Smartphone gehalten

Abb. 2 | Detaillierter Authentifizierungs-Ablauf



6. Das Security Token bestätigt die Auth-Anfrage des Webservice AuthService
7. Smartphone leitet die Security Token Bestätigung der Auth-Anfrage an den Webservice AuthService
8. Webservice AuthService leitet das Ergebnis der Authentifizierung an die Ladesäule
9. Ladesäule für den Ladevorgang freigeschaltet

Die Betrachtung der notwendigen Hardware, Software und einhergehender Schnittstellen fällt kurz aus, da die an der vorhandenen Ladeinfrastruktur notwendigen Änderungen zur Einbindung sehr gering sind.

In der Ladeinfrastruktur wird an einer beliebigen Stelle ein neuer Webservice AuthService, siehe Abb. 2, bereitgestellt. Die Ladesäulen erhalten einen QR-Code und sofern sie nicht schon remote frei geschaltet werden können, kann eine ergänzende Software-Komponente eingespielt werden (siehe Abb. 2). Die AuthService-APP wird auf dem Samrtphone des Benutzers bei der Aushändigung des Security Token und dessen Personalisierung installiert und eingerichtet.

In der Ladeinfrastruktur wird keine neue Hardware benötigt. Einzig auf der Stromkundenseite wird mit dem Security Token bewährte NFC-fähige Smartcard Technologie für die starke Authentikation ausgerollt, die mit der AuthService-App verwendet wird.

3.3 Innovative und einfache Authentikations-Methode

In dem vorliegenden eMobility Umfeld haben sowohl der Stromanbieter wie auch der Stromkunde das berechtigte Interesse, eine Kommunikation erst nach einer sicheren Authentikation aufzubauen. Die starke Authentikation ist hierfür eine seit langem bewährte Methode, mit der sich beteiligte Kommunikationspartner gegenseitig authentifizieren.

Die Bereitstellung einer klassischen starken Authentikation geht einerseits bei dem Infrastruktur Betreiber mit einem hohen Aufwand, andererseits für den Anwender (Benutzer) mit einem bei jeder Verwendung gleich bleibenden hohen Aufwand einher; z.B. sei hier das Verfahren erwähnt, bei dem zu jeder durchzuführenden Authentikation ein sich minütlich änderndes Passwort-Fragment abgelesen und kombiniert mit einem persönlichen PIN eingetippt werden müssen.

Die Verwendung der klassischen starken Authentikations-Methoden haben zudem den Nachteil, dass sie nur unter hohem Aufwand organisationsübergreifend einsetzbar wären und dieses somit zur Folge hat, dass Benutzer oft innerhalb eines Unternehmens mehrere Token mit sich führen müssten. Das Security Token erlaubt eine einfache organisations übergreifende Verwendung für einen Benutzer und wird im nächsten Kapitel genauer betrachtet.

Die Vorteile des Security Token sind die eingesetzte innovative Technologie und die einfache Verwendung für den Stromkunden.

Innovativ ist die verwendete NFC fähige Smartcard Technologie unter Verwendung von Secure Elements zum Ablegen des schützenswerten Schlüsselmaterials und weiterer Informationen in Kombination mit PKI Zertifikaten.

Der für den Benutzer ersichtlichste Vorteil ist die simple Verwendung des Security Token, da sich dieser so einfach nutzen lässt wie der Benutzer das Security Token (in der linken Hand haltend) an die Rückseite des Smartphones (SP) (in der rechten Hand haltend) hält.

Vorteile für die **Stromanbieter**, also für den Betreiber, sind:

- Beibehaltung der bisherigen Infrastruktur
- kostengünstige und einfache Webservice AuthService Einbindung
- Sichere Identifizierung der Stromkunden
- Grundlage für die sich anschließende Abrechnung

Die **Vorteile** des Security Token **für** den **Stromkunden**:

- Das Security Token ist speziell für den Stromkunden konfiguriert
- Smartphone AuthService-APP für den persönlichen Security Token konfiguriert
- Security Token und AuthService-APP sind PIN geschützt
- Authentikation durch simples aneinander halten des Smartphones und Security Token
- Höhere Sicherheit, wenn zur Bestätigung besonderer Transaktionen (Bezahltoken signieren) auch die PIN Eingabe erforderlich ist
- FIDO Alliance: Einbindung und Zertifizierung geplant

3.4 Security Token

Im vorliegenden Projekt entwickelt das Institut für Internet-Sicherheit – if(is) ein auf einem Security Token basierenden Authentifizierungs Webservice AuthService. In dem vorgestellten Projekt wird das Security Token mit dem YubiKey Neo der Firma [1] Yubico umgesetzt.

Das gewählte Security Token genügt hohen sicherheitstechnischen Ansprüchen und stellt unter anderem folgende Features bereit:

- Secure Element: sicherer Speicher für asymmetrische Schlüsselpaare und Zertifikate
- JAVACARD (jcop v3) integriert
- NFC kontaktlos Technologie (NDEF type 4)
- Common Criteria zertifizierte ICs

- CCID compliant
- MIFARE Classic (1k) Unterstützung

Die Umsetzung kann auch mit einer entsprechenden JAVACARD (Smartcard) umgesetzt werden, da der YubiKey Neo zusätzlich zu anderen Komponenten auch eine JAVACARD beinhaltet.

Die Umsetzung mit einer Smartcard bietet dem Stromanbieter die Möglichkeit weiterhin, sofern bisher so umgesetzt, eine **Smartcard im Corporate Identity design** an die Kunden bei der Registrierung und Personalisierung auszugeben.

Wo kann zukünftig die hier beschriebene Chip Technologie eingesetzt werden?

Die für die Identifikation und Authentikation der Kunden verwendete Technologie, sei sie in einem YubiKey Neo oder in einer Smartcard „verpackt", ist keine andere Technologie, als die die, große Unternehmen überwiegend für ihre **Mitarbeiterausweise** einsetzen bzw. beim anstehenden Kartengenerationswechsel zukünftig verwenden werden. In diesem Zusammenhang seien exemplarisch als Beispiel Unternehmen wie z.B. Siemens, RWE und Deutsche Bank genannt.

3.5 Benutzer Vertrauen steigernde Maßnahmen

Der vorliegende Identifizierungs- und Authentifizierungs-Provider verwendet ein kryptographisch gesichertes Security Token. Der Stromanbieter, der das Security Token an seine Stromkunden zur sicheren Authentifizierung ausgegeben hat, kennt die eingesetzte Technologie und hat vollstes Vertrauen in die angebotene Lösung.

An dieser Stelle werden Maßnahmen zusammengefasst dargestellt, die in der vorhandenen Lösung primär eingesetzt werden, um das subjektive empfundene Vertrauen beim Stromkunden zu steigern.

Es werden in der APP auf dem Smartphone Informationen zu dem Stromanbieter und zu dem Standort der Ladesäule angezeigt, die dieser selbst verifizieren kann.

Im Normalfall werden die angezeigten Informationen dem Stromkunden plausibel erscheinen und somit die Zuversicht und das Vertrauen des Kunden steigern. Die dem Kunden angezeigten Informationen stellen eine zusätzliche Darstellung selbiger dar, da diese in der vorliegenden Umsetzung zur Sicherung des Authentifizierungsvorgangs in jedem Fall Berücksichtigung finden. Die dem Kunden angezeigten Stromanbieter Informationen entstammen der kryptographisch gesicherten Kommunikation mit dem AuthService des Stromanbieters, sodass der Stromkunde zusätzlich angezeigt bekommt, mit wem er gerade eine Authentifizierung vornimmt.

Sollten diese Informationen nicht stimmen, käme es gar nicht zur erfolgreichen Authenitfizierung.

Des Weiteren werden dem Stromkunden Informationen zu dem QR-Code, Standort der Ladesäule und dem im Smartphone tatsächlich ermittelten Standort angezeigt, siehe hierzu im Anschluss an Tabelle 1 die Erläuterung.

In Tabelle 1 sind die Benutzer Vertrauen bildende Maßnahmen aufgeführt.

Tab. 1 | Benutzer Vertrauen steigernde Maßnahmen

	Benutzer Vertrauen steigernde Maßnahmen		
Maßnahme	Besitz	Wissen (PIN)	**Anzeige am Smartphone**
Smartphone	x	x	
Security Token	x	x	
Smart Phone APP	x	x	
QR-Code			**x**
Anbieter-Zertifikats-Info			**x**
Standort (Karte)			**x**

Obige Tabelle 1 zeigt die dem Kunden angezeigten Vertrauen bildenden Informationen.

- Zu dem Stromanbieter werden Firmenname, Anschrift und Zertifikats Fingerprint angezeigt.
- Zu der Ladesäule wird der Standort mit Angabe der Anschrift und Lokalisierung in dem angezeigten Kartenausschnitt angezeigt.

Im Normalfall werden die Angaben zum Standort des Kunden und der Ladesäule in der APP übereinstimmen und entsprechend als zum Login bereit angezeigt. Sollten in der Authentifizierung an obigen zwei Größen im technischen Ablauf Zweifel auftreten, werden diese technischen Zweifel, entsprechend farblich hervorgehoben (z.B. rot), dem Kunden angezeigt.

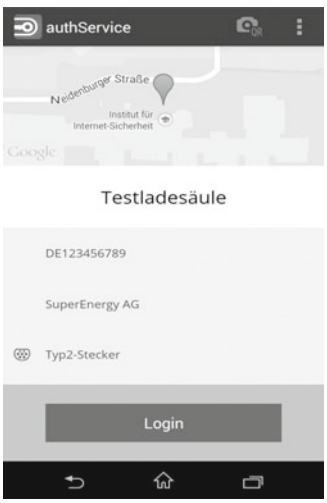
Stromanbieter Informationen (Abb. 3):

- Sind die Stromanbieter Informationen richtig, wird dies dem Stromkunden bei der Authentifizierung angezeigt.
- Sind die Stromanbieter Informationen falsch, wird dem Stromkunden dieses in rotem Text angezeigt und dann der Authentifizierungsvorgang abgebrochen.

Standort der Ladesäule (Abb. 3):

- Stimmen der Standort der Ladesäule des QR-Code und der von dem Smartphone festgestellte Standort tatsächliche überein, wird dieses entsprechend auf dem Kartenausschnitt angezeigt und der Benutzer hat trotzdem die Möglichkeit, sich hiervon zu überzeugen.
- Stimmen der Ladesäulen Standort aus dem QR-Code und der vom Smartphone erfasste und angezeigte Standort nicht überein, wird der Ladevorgang, mit entsprechender farblich gekennzeichneter Meldung an den Benutzer, abgebrochen.

Abb. 3 | Benutzer und Ladesäulen Standort



4 Organisations- und bereichsübergreifender Einsatz des eMobility Identifikations-Authentikations-Provider

Die vorgestellte starke Authentikations-Methode kombiniert die Smartphone AuthService-APP und den personalisierten Stromkunden Security Token. Die zuvor beschriebene Authentifikation basiert auf den folgenden Komponenten:

- Security Token => personalisierte PKI basierte Ausstellung
- AuthService-APP => Konfiguration basierend auf Kunden Security Token

Die Personalisierung der Security Token findet bei der Registrierung und einhergehenden Identitätsfeststellung des Stromkunden statt. Das Security Token beinhaltet ein Smartcard-Chip basiertes Security-Modul, in dem nach Abschluss der Personalisierung, ein asymmetrisches Schlüsselpaar, PKI basiertes Zertifikat und Unternehmens bezogene Daten zugriffsgeschützt vorliegen und für die spätere Abrechnung verwendet werden können.

Die vorliegenden personalisierten und mit PKI Zertifikaten versehenen Security Token sind die Grundlage für den im Folgenden gezeigten organisations- und bereichsübergreifenden Einsatz.

In Abhängigkeit von der Größe des Stromanbieters und somit der für die Umsetzung der Security Token basierten starken Authentikation vorhandenen Mittel bieten sich zwei verschiedene Bereitstellungsmodelle an.

- Stromanbieter betreibt selbst eine PKI bzw. Schnittstellenanbindung zu einer PKI
- Stromanbieter nutzt die Dienste eines PKI-Betreibers

4.1 Interoperabilität von eMobilty Identifikations-Authentikations-Provider

In Abbildung 4 werden zwei eMobility Anbieter gezeigt. Der grüne Anbieter ist z.B. die Stadtwerke A und der rote Anbieter die Stadtwerke B. Jeder Anbieter stellt seinen Kunden ein Security Token zur Verwendung an den eigenen Stromladesäulen aus.

Jeder Benutzer wird an den Ladesäulen des eigenen eMobility Anbieters unter Verwendung des Security Token in Kombination mit der Smartphone AuthService-APP sein Elektroauto nach erfolgreicher Authentifizierung mit Strom laden können.

In dem vorliegenden Fall müssen für die Umsetzung des Roamings Abkommen getroffen werden. Das Roaming gliedert sich in die Bereiche Abrechnung und technische Umsetzung.

Die Abkommen zur Abrechnung regeln wie und zu welchen Bedingungen sich die Stromanbieter untereinander die von Stromkunden anderer Stromanbieter geladene elektrische Energie gegenseitig in Rechnung stellen bzw. gegeneinander Verrechnen.

Auf technischer Ebene werden über eine Policy die Bedingungen zur Anbindung an eine BridgeCA festgelegt. Die BridgeCA ermöglicht den Stromkunden der teilnehmenden Stromanbieter das krytographische Roaming. Krytographisches Roaming bedeutet, dass der Stromkunde das von seinem Stromanbieter erhaltene Security Token ohne jegliche Veränderung auch an Ladesäulen fremder Stromanbieter zur Identifizierung und Authentifizierung und somit Freischaltung der Ladesäule verwenden kann.

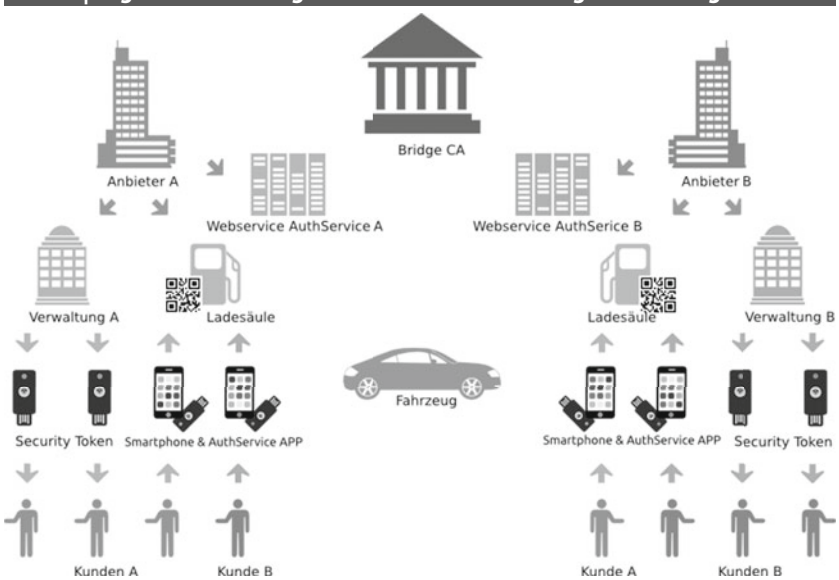
Die Grundlage zur Nutzung einer BridgeCA, ist die von allen Beteiligten zu unterzeichnende Policy, sodass das gewählte Vertrauensmodell umgesetzt werden kann. Die Policy definiert organisatorische und technische Rahmenbedingungen, sodass alle Beteiligten (Stromkunden und Stromanbieter) einerseits Vertrauen aufbauen können, andererseits bei Einhaltung der technischen Anforderungen, organisationsübergreifend den eigenen Security Token einsetzen können.

Technisch gesehen findet im Hintergrund und für den Stromkunden völlig transparent jeweils eine einmalige zentralisierte Cross-Zertifizierung jeder einzelnen Stromanbieter PKI mit der BridgeCA statt, wodurch ein pragmatisches und sicheres Vertrauensmodell umgesetzt wird. Dieses Vertrauensmodell gewährleistet, dass bei der Authentifizierung mit dem Security Token des Anbieters B an der Ladesäule des Anbieters A die jeweils fremden Zertifikate der anderen Stromanbieter PKI als vertrauenswürdig verifiziert werden können.

4.2 Identifikations-Authentikations-Provider Einsatz im Internet

Die im Bereich der eMobility eingeführte starke Authentikation kann auf alle Internet basierten Dienste angewandt werden. Der QR-Code der Ladesäule kann auch auf einer beliebigen Webseite angezeigt und zur Authentifizierung mit einem Security Token verwendet werden. Die Betrachtung der Ausweitung der vorgestellten starken Authentikations-Methode aus dem eMobility Umfeld wird hier für Unternehmen und deren Dienste aus dem klassischen Internet kurz skizziert:

Abb. 4 | Organisationsübergreifende Authentifizierung für Roaming



- Klassisches Internet Unternehmen: google, facebook, …
  - Auf der Startseite der Webseite wird auch ein QR-Code angezeigt
  - Der Benutzer gibt seine Benutzerkennung ein
  - Der Nutzer kann wie gewohnt den Dienst nutzen

=> Nutzung am PC, Notebook, Internetcafe

- Traditionelle Unternehmen: Lufthansa, Bundesbahn, Behörde, => am PC oder Terminal genutzt
  - Auf der Startseite der Webseite wird auch ein QR-Code angezeigt
  - Der Benutzer gibt seine Benutzerkennung ein
  - Der Nutzer kann wie gewohnt den Dienst nutzen

=> Nutzung wie oben, aber auch an „Automaten". Tickets, Check-In, etc. ...

- BridgeCA ermöglicht auch hier organisations übergreifenden Einsatz
  - z.B. Google Nutzer könnten ihr Security Token (YubiKey Neo) wahlweise auch an einem Lufthansa Terminal einsetzen
  - z.B. Behörden Nutzer könnten ihr Security Token auch wahlweise an einem Bahn-Automaten oder Facebook-Dienst verwenden.

5 Ausblick

Die Umsetzung des eMobility Identifikations- und Authentikations-Providers ermöglicht durch eine starke Authentikation ein sicheres Roaming der Stromkunden beim Strom laden an Ladesäulen fremder Stromanbieter.

Gerade die ursprünglich als unvereinbar erscheinenden Anforderungen des eMobility Umfelds haben die Erarbeitung des vorliegenden Ergebnisses beflügelt.

Die im Gegensatz zu anderen Bereichen spartanisch anmutenden technischen Gegebenheiten und der in der Branche typische immense betriebswirtschaftliche Spardruck haben erst die Konzipierung der vorgestellten sicheren Identifizierung und Authentifizierung inspiriert.

Zusammengefasst **die aktuellen Vorteile der Lösung**:

- Ladesäulen können kostengünstig gehalten werden
  - Legacy Ladesäulen ohne Terminal nutzbar
  - Neue Ladesäulen mit und ohne Monitor einsetzbar
- Stromkunde verwendet einfach das personalisierte Security Token und sein Smartphone
- Stromanbieter integriert den Webservice AuthService als weiteren Dienst in seine Infrastruktur
- Organisations übergreifende Nutzung ermöglicht Roaming beim Strom laden

Der Einsatz modernster Smartcard Chip-Technologie im Security Token eröffnet weitere auf dieser Technologie basierende Features. Die Untersuchung des Ladevorgangs an einer eMobility Ladesäule legt in den bisherigen technischen Umsetzungen zwei wichtige und noch nicht umgesetzte Aspekte offen. Diese zwei Aspekte sind auf der einen Seite, die Bestätigung des Bezahlvorgangs mittels eines Bezahltoken durch den Benutzer, andererseits eine Neukunden Vertragsunterzeichnung an der Ladesäule.

Überblick des Security Token Einsatzes an der Ladesäule:
Bisheriger Einsatz:

- **Identifikation** der Ladesäule und des Stromkunden
- **Authentifizierung** des Stromkunden an der Ladesäule

Zukünftiger in Entwicklung befindlicher Einsatz:

- **Bezahltoken** (durch den Kunden digital signierte Rechnung)
- **Vertragsunterzeichung** (durch den Kunden digital signierten Vertragsabschluss)

Die vorgestellte „Sichere Identifizierung und Authentifizierung" mit Security Token und Smartphone unter Verwendung eines QR-Codes an der Ladesäule kann schon jetzt von den unterschiedlichsten Unternehmensarten (Internetfirmen, Luftfahrt, Behörden, etc.) für die sichere Identifizierung und Authentifizierung ihrer Kunden und Mitarbeiter bei der Nutzung von Internet- und Intranetdiensten eingesetzt werden.

Die vorgestellte Lösung kann somit an beliebigen Dienstzugangspunkten von jedem Unternehmen eingesetzt werden, da es heute keinen unternehmerischen Bereich gibt, der nicht seine Dienste über das Internet bzw. Telematic basiert anbietet. Der Einsatz der vorliegenden Lösung ist auch bei klassischen Zugangskontrollsystemen einsetzbar, wie sie von darauf spezialisierten Unternehmen für Gebäude eingesetzt werden. Das Einsatzfeld ist schier unbegrenzt!

Acknowledgements

Das dieser Veröffentlichung zugrunde liegende Forschungs- und Entwicklungsprojekt „Secure eMobility (SecMobil)" wird mit Mitteln des Bundesministeriums für Wirtschaft und Energie (BMWi) innerhalb des Technologieprogramms „IKT für Elektromobilität" unter dem Förderkennzeichen 01ME12024 gefördert.

Literaturverzeichnis

[1] YubiKey Neo, Stand 18. Juli 2014 http://www.yubico.com/products/yubikey-hardware/yubikey-neo/

[2] A. González Robles, N. Pohlmann: „Smart Objects und Objekt-Identitäten im globalen Internet – Risiken der Standard-IT-Vernetzung in kritischen Infrastrukturen und in der Industrie". IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 4/2012

[3] S. Feld, N. Pohlmann: „Security analysis of OpenID, followed by a reference implementation of an nPA-based OpenID provider". In Proceedings of the ISSE 2010 – Securing Electronic Business Processes – Highlights of the Information Security Solutions Europe 2010 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Vieweg-Teubner Verlag, Wiesbaden 2010

[4] M. Hesse, N. Pohlmann: „Kryptographie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (VI) – Zweck und grundlegende Funktionsweise von Public-Key-Infrastrukturen (PKI)", IT-Sicherheit & Datenschutz, Supplement in DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 04/2007

[5] M. Hesse, N. Pohlmann: „Kryptographie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (VII) – Vertrauensmodelle von Public-Key-Infrastrukturen(PKI)", IT-Sicherheit & Datenschutz, Supplement in DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 04/2007

[6] M. Linnemann, N. Pohlmann: „Identitätskrisen in der IT", IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 05/2005

[7] N. Pohlmann: „Nutzen und Chancen von Public-Key-Infrastrukturen". In Proceedings der IT-Security Konferenz -Sicherheitsinfrastrukturen in Wirtschaft und Verwaltung, Hrsg.: Patrick Horster, IT Verlag, 2002