Messsysteme für Ladeeinrichtungen: Ende-zu-Ende-Sicherungskonzept für eine eichrechtlich günstige Lösung („GL“) für die Übertragung von Messdaten auf Fernanzeigen

1 Einführung

Es gibt drei entscheidende Charaktermerkmale von Messgeräten im Anwendungsbereich Elektromobilität (MEMO):

a) MEMO sind öffentlich zugänglich.
b) Über MEMO werden mehrere Kunden abgerechnet.
c) MEMO benötigen in der Regel eine eichrechtkonforme Fernanzeige.

Vor diesem Hintergrund müssen bei MEMO zur Erzielung der Eichrechtkonformität geeignete technische und organisatorische Maßnahmen getroffen werden, um wesentliche Schutzziele bei der Übertragung von Messdaten auf Fernanzeigen zu erreichen. Die wesentlichen Schutzziele lauten:

1) Wahrheit
Der Wert der Messgröße muss von einem Messgerät entsprechend den physikalischen Konventionen der Messgröße richtig zugeordnet worden sein.

2) Integrität
Der Inhalt einer fernübertragenen Messwert-Nachricht darf nicht unerkannt verfälscht werden können.

3) Authentizität
Eine Messwert-Nachricht muss nach der Fernübertragung unzweifelhaft einer bestimmten Datenquelle zugeordnet werden können.

4) Zurechenbarkeit/Nichtabstreitbarkeit
Eine Messwert-Nachricht muss nach der Fernübertragung unzweifelhaft der Person zugeordnet werden können, die im Zusammenhang mit der Messung eine Rechnungsschuld verursacht hat.

5) Verfügbarkeit
Eine Messwert-Nachricht muss so lange für die Vertragspartner eines Geschäftsvorganges verfügbar sein, bis der Vorgang einschließlich der einvernehmlichen Bezahlung der Rechnungsschuld endgültig abgeschlossen ist.

Die Erreichung aller fünf Schutzziele ist notwendige Voraussetzung für die Richtigkeit eines Messergebnisses.

Das hiermit vorgelegte Dokument dient dem Zweck der Beschreibung eines Beispiels für eine eichrechtlich günstige Lösung zur Erreichung der Schutzziele. Der Term „Günstige Lösung“ wird in diesem Dokument mit den Versalien „GL“ abgekürzt und bedeutet:

- Die Lösung erfüllt die eichrechtlichen Anforderungen nach MessEV einschließlich deren Anlage 2
- Die Lösung lässt sich schnell und einfach durch Geräteentwickler realisieren.
- Die Lösung führt dazu, dass nur ein Minimum an Komponenten in einem verteilten Messgerät mit Systemcharakter in die eichrechtliche Prüfung, Bewertung und Zertifizierung mit einbezogen werden muss („minimalinvasiv“).
- Die Lösung lässt sich mit vergleichsweise geringem Aufwand eichrechtlich prüfen, bewerten und zertifizieren.

2 Kryptografische Ende-zu-Ende-Sicherung mit asymmetrischer Verschlüsselung

Ein GL nutzt das kryptografische Prinzip einer Ende-zu-Ende-Sicherung mittels einer digitalen Signatur auf Basis asymmetrischer Verschlüsselung, um die Messdatenübertragung von der Datenquelle bis zur Visualisierung mit eichrechtlich ausreichend niedrigem Risiko einer Kompromittierung zu übertragen. (Auf die grundsätzliche Wirkungsweise einer asymmetrischen

Verschlüsselung kann hier nicht weiter eingegangen werden. Es gibt zahlreiche ausführliche Beschreibungen dazu im Internet.)

Für die Realisierung der digitalen Signatur werden bei einer GL folgende kryptografischen Verfahren angewandt:

1) Bildung eines Hashwertes der zu signierenden Daten mit dem Algorithmus SHA 256 oder stärker

2) Asymmetrische Verschlüsselung des Hashwertes mit Elliptische-Kurven-Algorithmus ECC 192 oder stärker

Bei einer GL betrachtet das Eichrecht die Generierung eines einzigen Paares aus geheimem (Secret Key = SK) und öffentlichen Schlüssel (Public Key = PK) für die gesamte Lebensdauer des Messgerätes als ausreichend. Das gilt unter der Bedingung, dass der geheime Schlüssel nicht während der Lebensdauer des Gerätes erkennbar kompromittiert wurde. Dieser erleichterte Ansatz ermöglicht eine einfache Lösung eines „Direct-Trust-Konzepts“ zur Schaffung einer Public-Key-Infrastruktur für die eichrechtlich vertrauenswürdige Zuordnung eines PK zu einer Datenquelle. Der Direct-Trust-Ansatz funktioniert bei der GL so:

Im Rahmen des Produktionsprozesses erzeugt das Messgerät automatisch ein asymmetrisches Schlüsselpaar (SK + PK). Im Anschluss liest der Hersteller des Messgerätes, das mit ECC 192 signiert, den PK über die Fernanzeigeschnittstelle aus und druckt ihn auf das Typschild. Damit ist eine physische Zuordnung zwischen PK und Datenquelle geschaffen. Der Hersteller des Gerätes bescheinigt mit der Konformitätserklärung für das Geräteexemplar die Richtigkeit der Zuordnung. Das Messgerät ist so konstruiert, dass nach dem Inverkehrbringen eine Änderung bzw. ein Auslesen des SK nur nach Verletzung einer eichtechnischen Sicherung möglich ist. Der Verwender des Messgerätes, das einem Ladepunkt zugeordnet ist, teilt der BNetzA bei der Anmeldung des Ladepunktes den zugehörigen PK mit. Der Verwender des Messgerätes, also der Ladepunktbetreiber trägt die Verantwortung für die Richtigkeit der PK-Angabe bei der Ladepunkt-Anmeldung. Im Rahmen der Baumusterprüfbescheinigung wird festgelegt, dass eine eichrechtkonforme Verwendung des Messgerätes bedingt, die PK der Ladepunkte bei der BNetzA zusammen mit der Ladepunkt-Registrierung anzumelden.

Die zweite Säule der Vertrauenswürdigkeit der Zuordnung von PK zu Datenquelle besteht in der Möglichkeit für den Kunden, während des Ladevorgangs den PK vom Messgerät abzulesen und festzuhalten, z.B. durch ein Foto. Bei einer späteren Prüfung von signierten Daten, kann der Kunde dann den PK über die Webseite der BNetzA erhalten oder den selbst abgelesenen PK in die Prüfsoftware eingeben. Es gibt also eine doppelte Sicherung der Gewährleistung einer richtigen Zuordnung von PK zu Datenquelle. Aus eichrechtlicher Sicht erfüllt diese Lösung die Anforderungen an die Nachweisbarkeit der Zugehörigkeit eines PK zu einer Datenquelle.

3 Beispielerläuterung

Das Bild 1 erläutert, wie und warum die Ende-zu-Ende-Sicherung mittels einer digitalen Signatur auf Basis asymmetrischer Verschlüsselung zu einer GL führt. Der nachfolgende Text nimmt Bezug auf die im Bild aufgeführten Bezeichnungsnummern in Klammern. Zusätzlich ist die Bedeutung der Nummern auch in der
Tabelle 1 erklärt.

In einer Ladesäule (1) sind alle eichrechtlich relevanten Geräte in einer „Messkapsel“ zusammengefasst. Die Datenquelle (z.B. ein Elektrizitätszähler) für die eichrechtlich relevanten Messdaten signiert diese unter Verwendung des Hashverfahrens SHA 256 und des asymmetrischen Verschlüsselungsverfahren ECC 192. Der öffentliche Schlüssel ist auf den Zähler gedruckt (3). Der Zähler ist durch ein Fenster in der Ladesäule sichtbar. Der Zähler sendet die signierten Messdaten (4) durch das Internet, ggf. über einen CPO und einen Roamingdienst, zum EMSP (7).

Der Ladesäulenbetreiber übermittelt mit dem Anmeldeformular für die Ladepunkte der BNetzA die PK der Ladepunkte (5). Die BNetzA veröffentlicht die PK zusammen mit den übrigen Kenndaten des Ladepunktes über ihre Webseite (6).

Der EMSP liefert zum Zwecke der Abrechnung alle für Forderungen maßgeblichen Berechnungsfaktoren in digitaler Form zusammen mit der Rechnung an den ladevorgangsbedingten Zahlungsschuldner aus. Zu den Berechnungsfaktoren gehören die signierten Messdatensätze und ggf. die Tarifierungsvorschrift, sofern der EMSP Messwerte weiterverarbeitet hat, indem er sie Tarifzonen zugeordnet hat (8).

Dem Rechnungsschuldner stellt der EMSP die Transparenz- und Displaysoftware (9) zur Verfügung. Mit ihr kann der Rechnungsschuldner überprüfen, ob die in der Rechnung ausgewiesenen Messwerte tatsächlich aus dem Ladepunkt stammen, an dem Rechnungsschuld verursacht wurde und ob die Messwerte unverfälscht sind und vom EMSP entsprechend dem Service-Vertrag richtig tarifiert wurden. Die Software betreibt der Rechnungsschuldner auf seinem eigenen Endgerät, z.B. auf einem Smartphone oder Tablet (10). Für die Prüfung der Signatur benötigt der Rechnungsschuldner den PK, der zu dem Ladepunkt gehört. Den PK bekommt er von der Webseite der BNetzA (11). Zusätzliche Sicherheit liefern die selbst durchgeführten Erfassungen von PK an den Ladesäulen. Es gibt Anwendungsfälle, bei denen der Kunde an der Ladesäule und der Rechnungsschuldner verschiedene Personen sind („Ladekartenprinzip“). In diesem Fall ist zwischen Rechnungsschuldner Ladekartennutzer rechtlich zu klären, ob der Kartennutzer verpflichtet wird, die PK an den genutzten Ladepunkten zu erfassen oder ob der Rechnungsschuldner sich allein der BNetzA-Webseite bedient, um die PK für die Rechnungsprüfung zu erhalten.

Dieses Ende-zu-Ende-Sicherungskonzept hat den Vorteil, dass grundsätzlich nur die beiden rot markierten Systemkomponenten in die eichrechtlichen Betrachtungen mit einbezogen werden müssen. Übertragungswege und Backend-Systeme können ausgeklammert werden. Die beiden roten Komponenten bilden zusammen das zu prüfende und zu zertifizierende Messgerät im Anwendungsbereich Elektromobilität, sie bilden zusammen das „Target of Evaluation“ für eine Konformitätsbewertungsstelle. Da die Transparenz- und Display-Software notwendige Voraussetzung ist, um mit der Messkapsel eine eichrechtkonforme Messgerätelösung einschließlich eichrechtkonformer Anzeige zu realisieren, muss der Messkapselhersteller, im Rahmen des Baumusterprüfbescheinigungsverfahrens die Existenz der Transparenz- und Display-Software nachweisen, und zwar bei einer GL in einer Ausführung für mindestens ein Standard-Mobilgeräte-Betriebssystem (iOS oder Android) und für Hochsicherheitsprüfungen eine Ausführung für LINUX. Die Bereitstellung der Software beim Kunden oder Rechnungsschuldner ist dagegen gemäß MessEG, §3 Sache des EMSP, nicht des Messkapselherstellers.

4 Praxistipp für die Implementierung eichrechtkonformer Signatur-Algorithmen

Zitat von Dr. M. Esche, Leiter der AG 8.51 „Metrologische Software“ der PTB:

Die Bewertung einer vom Hersteller implementierten Bibliothek auf Basis eines standardisierten Kryptographiealgorithmus ist technisch möglich, allerdings mit großem Aufwand verbunden. Zu bevorzugen wäre die Verwendung bereits zertifizierter Bibliotheken/Module. Eine Open-Source-Referenzimplementierung des BSIs, die allen Anforderungen des Eichrechts genügen sollte und auch in kommerziellen Produkten frei genutzt werden kann, ist unter ***https://www.bsi.bund.de/DE/Themen/Kryptotechnologie/Kryptobibliothek/kryptobibliothek_node.html*** *zu finden.*

Der Fachbereich Elektrische Energiemesstechnik, über den die PTB die Baumusterprüfbescheinigungsverfahren für Messgeräte im Anwendungsbereich Elektromobilität abwickelt, empfiehlt Herstellern von Messkapseln dringend, sich an den Rat von Dr. Esche zu halten. Wird nicht die BSI-empfohlene Library verwendet, kann die Evaluierung Software der Messkapsel erheblich aufwändiger werden.

M. Kahmann, FB „Elektrische Energiemesstechnik“,
Tel.: 0531 592 2300
martin.kahmann@ptb.de

Dank an Dr. Esche, PTB für die Durchsicht dieses Dokumentes und die Bundesnetzagentur für die Unterstützung betreffend die Veröffentlichung der Public Keys.

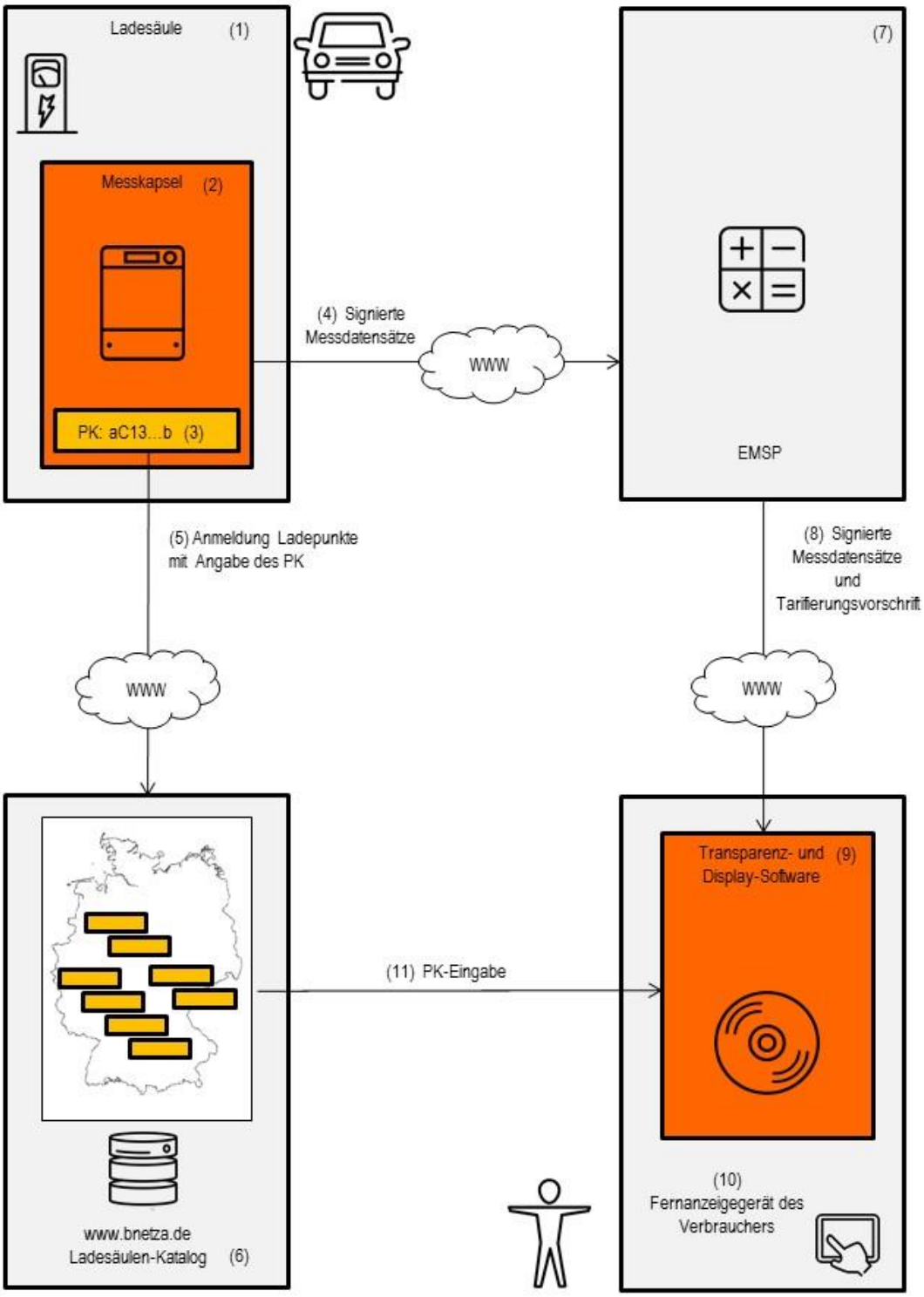
Ladesäule (1)
Messkapsel (2)
PK: aC13…b (3)
(4) Signierte Messdatensätze
WWW
(7)
EMSP
(5) Anmeldung Ladepunkte mit Angabe des PK
(8) Signierte Messdatensätze und Tarifierungsvorschrift
WWW
WWW
Transparenz- und Display-Software (9)
(11) PK-Eingabe
www.bnetza.de Ladesäulen-Katalog (6)
(10) Fernanzeigegerät des Verbrauchers

Bild 1

(1)	Bei einer GL sollte die Ladesäule so konstruiert sein, dass sie als ein elektrischer Betriebsraum betrachtet werden kann. Er sollte im Inneren bezüglich der Temperatur und der EMV- und Umweltbedingungen eine Einbauumgebung schaffen, innerhalb der ein MID-Zähler bestimmungsgemäß betrieben werden kann. Bei einer GL verfügt die Ladesäule über ein eigenes Abteil („Compartment"), in das eine Messkapsel einfach eingebaut oder noch besser eingesteckt werden kann („Cartridge"). Bei einer GL verfügt die Ladesäule über ein Fenster, das einen Blick auf die Anzeigen und Aufschriften der Messgeräte erlaubt, die zu der Messkapsel gehören.
(2)	Alle eichrechtlich relevanten Komponenten in einer Ladesäule können als in einer virtuellen Kapsel eingeschlossen betrachtet werden, die die virtuelle Abgrenzung gegen eine von der Eichpflicht ausgenommene Umwelt darstellt. Diese Kapsel wird in diesem Dokument „Messkapsel" genannt. Bei einer GL werden die Komponenten auch physisch in eine Kapsel eingebaut. Je kleiner die Kapsel, umso günstiger die Lösung. Bei einer GL verfügt die Messkapsel über eine eigene Systemzeit, deren Übereinstimmung mit der Tageszeit visuell über ein Display durch das Fenster in der Säule geprüft werden kann.
(3)	Bei einer GL ist der Public Key (PK) aller digital signierenden Datenquellen in einer Messkapsel visuell erfassbar und physisch mit der Datenquelle verbunden. Die Standardlösung ist, den PK mit in die Beschriftung des Typschildes aufzunehmen. Die Datenquelle kann z.B. ein Elektrizitätszähler sein. Die Datenquelle kann auch eine Zusatzeinrichtung sein, die die Messwerte von mehreren Elektrizitätszählern entgegennimmt, weiterverarbeitet und versendet. In diesem Fall muss für jeden Eingangskanal der Zusatzeinrichtung ein PK vorhanden sein. Bei einer GL erhält jeder Ladepunkt einen eigenen PK. Der Hersteller der Datenquelle muss im Rahmen des für sein Produkt gewählten Konformitätsbewertungsmoduls B oder F in der Produktionsstufe „Endabnahme und Prüfung" die richtige Zuordnung eines PK zu einem Geräteexemplar feststellen und erklären.
(4)	Die eichrechtlich relevanten Messdatensätze werden über Internet, ggf. via Charge-Point-Operator und/oder Roaming-Dienst an den Electromobility-Service-Provider versandt.
(5)	Bei einer GL meldet der Charge-Point-Operator der Ladesäulenverordnung folgend alle Ladepunkte bei der BNetzA an. Das Anmelde-Formular der BNetzA ermöglicht voraussichtlich ab Q1/2018 die Benennung der zu den Ladepunkten gehörenden PK.
(6)	Die BNetzA bietet ein vertrauenswürdiges, bundesweit zentral verwaltetes Portal zur Anmeldung von Ladepunkten nach der Ladesäulenverordnung. Die BNetzA wird voraussichtlich ab Q1/2018 über dieses Portal die Möglichkeit bieten, auf einer Landkarte alle dort gemeldeten Ladepunkte und die ggf. zugehörigen PK aufzufinden.
(7)	Der Electromobility-Service-Provider EMSP erhält die signierten Messdatensätze, um seinem Kunden entsprechend dem Service-Vertrag über die mit der Messkaspel ermittelten Messwerte eine Rechnung auszustellen. Der EMSP darf für die Abrechnung die Messwerte Tarifzonen zuordnen, z.B. nach Zeit oder nach Mengen, je nach den Vereinbarungen des Service-Vertrages. Allerdings darf er tarifierte Werte nur im geschäftlichen Verkehr für Abrechnungszwecke verwenden, wenn der Tarifierungsvorgang im Sinne des Eichrechts vertrauenswürdig ist. Bei einer GL wird die Vertrauenswürdigkeit durch Schaffung von Transparenz gegenüber dem Kunden erreicht. Bei einer GL wird die Schaffung von Transparenz erzeugt, indem der Kunde mit einer eichrechtlich evaluierten und zertifizierten „Transparenz- und Display-Software" versorgt wird, mit der der Kunde den Prozess der Tarifierung des EMSP zu Zwecken der Rechnungsprüfung rekonstruieren kann.
(8)	Der EMSP ist im Sinne des § 33 Abs. (3) des MessEG Messwerteverwender. Entsprechend verpflichtet sendet er dem Kunden auf sein mobiles Anzeigegerät die signierten Messdatensätze und die durch Transparenz- und Displaysoftware verarbeitbare Tarifierungsvorschrift

(9)	Bei einer GL erfolgt die Visualisierung der eichrechtlich relevanten Informationen mit einer PTB-evaluierten Transparenz- und Display-Software. Sie muss drei Hauptaufgaben erfüllen: a) Die Prüfung der Signatur der Messdatensätze aus der Messkapsel b) Die Anwendung der Tarifierungsvorschrift auf die Messdatensätze zur Rekonstruktion der Tarifierung in der eichrechtlich nicht sicheren Umgebung des EMSP c) Die eichrechtlich vertrauenswürdige Visualisierung der untarifierten und der tarifierten Messdatensätze unter Berücksichtigung software-ergonomischer Mindestanforderungen Bei einer GL steht die Transparenz- und Displaysoftware als App für das Smartphone/Tablet zur Verfügung. Zusätzlich steht die Transparenz- und Displaysoftware als Version für das Betriebssystem LINUX zur Verfügung. Für Hochsicherheitsprüfungen, z.B. im Rahmen einer Befundprüfung kann die Visualisierung dann außer auf dem Smartphone/Tablet auch auf dem sterilen Rechner mit garantiert nicht kompromittierten LINUX-Live-Betriebssystem erfolgen. Beide Ausführungsformen müssen von der PTB evaluiert bzw. zertifiziert sein.
(10)	Bei einer GL kommt die „Bring-Your-Own-Device“-Konzeption (BYOD) zur Anwendung. Als eichrechtlich relevantes Fernanzeigegerät dient das Smartphone oder Tablet des Kunden.
(11)	Zur Signaturprüfung ist es erforderlich, der Transparenz- und Displaysoftware den PK des Ladepunktes mitzuteilen. Er kann von der Webseite der BNetzA über eine https-Verbindung bezogen werden.

Tabelle 1: Erklärung der Bezeichnungsnummern in Bild 1 und Definitionen von Begriffen