White Paper „Ideen zu eichrechtskonformen Umgehungsmöglichkeiten für die Patente EP2531368B1 und EP2755846B1“

SAFE Technik AG
Christoph Lübke
Michael Haag
Hauke Hinrichs
Jo Wilkes
Heiko Bobzin
Alex Kaneppele
Thomas Bittner
Matthias Grote
et.al

PTB regelermittlungsausschuss

Dokument 6-A

EP 2 531 **368** B1

Weitere Erläuterungen zum Patent – vgl. ANLAGE

- Messwert: z.B. Anfangs- und Endzählerstand oder Differenz,
- Einheit des Messwerts,
- Zeitstempel,
- Eineindeutige ID der Ladevorrichtung (Beispiele nachstehend)
  - EVSE-ID (ID des Ladepunktes, der Energie an das Fahrzeug abgibt) oder
  - Meter-ID (ID des Zählers),
- Identifikation des Kunden (Beispiele nachstehend)
  - EMAID oder
  - Session-ID oder
  - UID, RFID oder
  - Transaktions-ID,
- Kryptographische Signatur des gesamten Datensatzes zur Gewährleistung der Prüfbarkeit von Integrität und Authentizität des Datensatzes (LS2-4 bzw. DK2-4).

Anspruch 1

	Merkmale
1.1	**Verfahren** zur Zuordnung eines von einer Ladestation erfassten Messwertes zu einem Nutzer mit:
1.2	*Erfassen* zumindest eines die von einem Fahrzeug (6) von der Ladestation (2) bezogene Energiemenge repräsentierenden Messgerätezählerstands *in einem Messgerät (10) innerhalb der Ladestation (2)*,
1.3	*Erfassen* einer Nutzeridentifikation (19) *durch die Ladestation (2)*,
1.4	Erstellen eines Datenpakets (34) umfassend zumindest den Messgerätezählerstand, die Nutzeridentifikation (19) und einen eindeutigen Bezeichner der Ladestation (34c),
1.5	Erstellen einer eindeutigen Beschreibung des Datenpakets (34) *in dem Messgerät (10)*,
1.6	Übermitteln zumindest des Datenpakets (34) und der Beschreibung (36) von der Ladestation (2) *an das Elektrofahrzeug (6)* und / oder *eine Abrechnungszentrale (22)*.

Lösungsidee #1: Weglassen der EVSE-ID aus dem signierten Datenpaket, da durch Public Key Ladepunkt eindeutig beschrieben

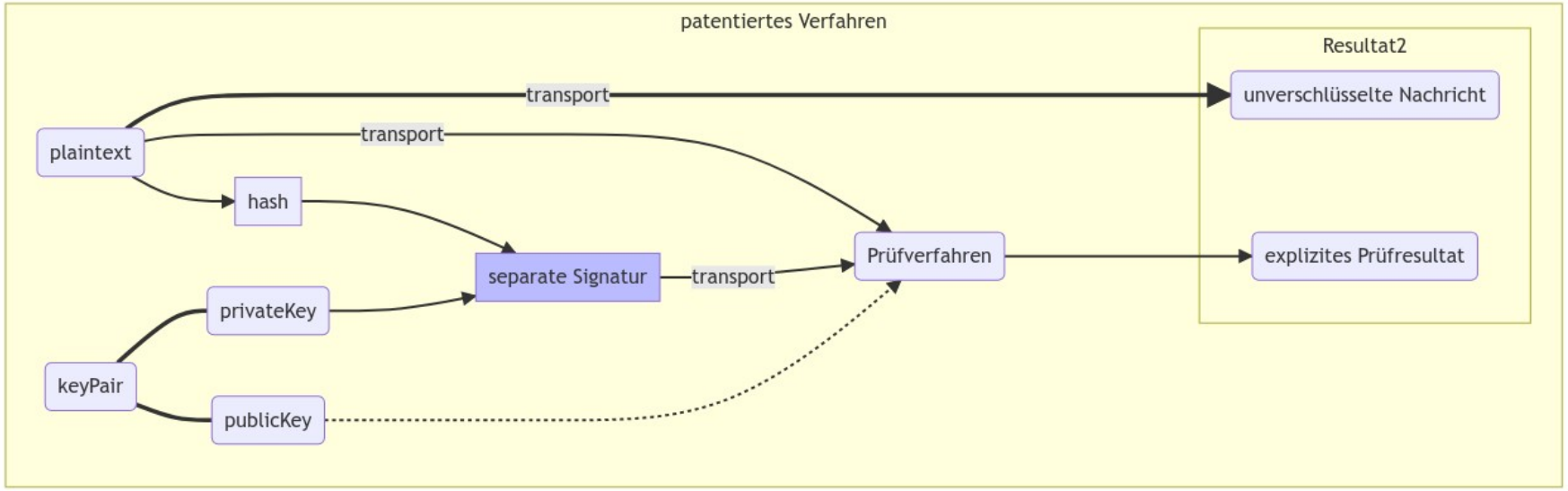
- Der Public Key der Signiereinheit kann im OCMF mit übertragen werden oder
- Der Endverbraucher kann anhand der übertragenen EVSE-ID den Public-Key aus der Datenbank der Bundesnetzagentur abrufen. Die EVSE-ID ist ihm durch den CDRs bzw. Abrechnungsinformationen bekannt.
- Optional: Public Key wird unsigniert zum backend übertragen
- Optional: Public Key wird in der Transparenzsoftware als editierbarer Vorschlag angegeben
- Endverbraucher kann signierten Datensatz mit Hilfe des Public-Key prüfen
- Ist die Signaturprüfung positiv, dann ist sowohl die Authentizität (durch die 1:1 Verknüpfung von Public-Key und EVSE-ID) als auch die Integrität des signierten Datensatzes sichergestellt
- Hierbei ist sicherzustellen, dass jeder Ladepunkt einen eindeutigen Public-Key besitzt.
- Zu prüfen: Wahrscheinlichkeit, dass trotzdem zwei Ladepunkte zufällig denselben Public-Key aufweisen.

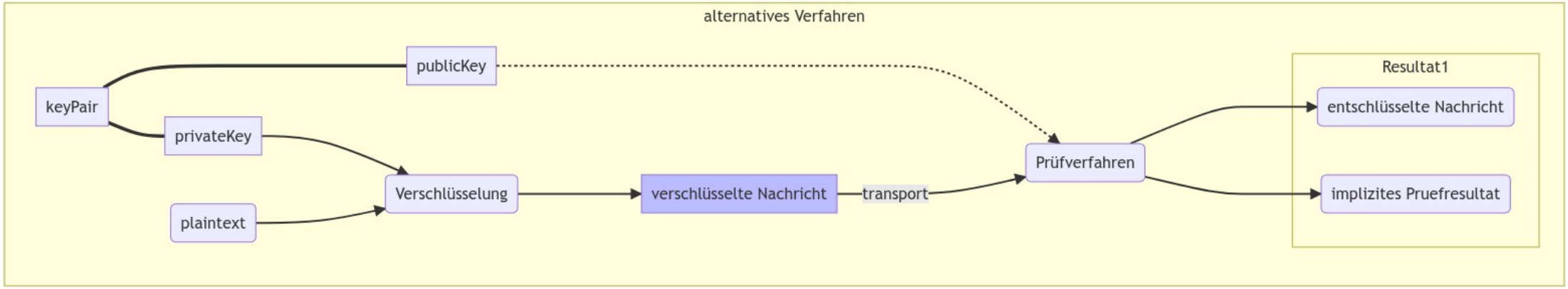
Lösungsidee #2: Reine Übertragung der Signatur nur Übertragung des mit dem Private-Key verschlüsselten Datenpakets

- Endverbraucher kann Datensatz überprüfen, indem das Datenpaket mit Hilfe des Public-Keys des Ladepunktes entschlüsselt
- Optional: Public Key wird unsigniert zum backend übertragen
- Optional: Public Key wird in der Transparenzsoftware als editierbarer Vorschlag angegeben

Lösungsidee #2

Gegenüberstellung der Verfahren





Lösungsidee #2

Gegenüberstellung der Verfahren

Patentiertes Verfahren

- Es wird über den Inhalt (plaintext) ein Hash berechnet; dieser wird dann mit dem Private Key verschlüsselt, um eine Signatur zum Inhalt zu bilden.
- Plaintext und separate Signatur werden übertragen.
- Zwecks Prüfung wird über den Plaintext wiederum der Hash gebildet, die Signatur mit dem public key entschlüsselt, und der enthaltene Hash mit dem vom Prüfverfahren ermittelten Hash verglichen.
- Das Resultat ist Übereinstimmung (Gültigkeit) oder Abweichung (Ungültigkeit); der Plaintext liegt bereits separat vor.

Alternatives Verfahren

- Der Inhalt (plaintext) wird in Gänze mit dem private key verschlüsselt.
- Die verschlüsselte Nachricht wird übertragen.
- Zwecks Prüfung wird die verschlüsselte Nachricht mit dem erwarteten Public Key entschlüsselt. Schlägt der Entschlüsselungsvorgang fehl, wird Ungültigkeit festgestellt; erfolgreiche Entschlüsselung hingegen weist nach, dass der passende private key des Public Keys verwendet wurde.
- Das Resultat der Entschlüsselung ist der plaintext; dieser kommt nur erfolgreich zustande, wenn die Gültigkeit gegeben ist.

(Der zum Private Key zugehörige Public Key wird generell dem Empfänger zugänglich gemacht)

Lösungsidee #3: Bauliche Trennung von Zähler (im Patent: „Messgerät“) und Signatureinheit

- Hilft aber nur Patent EP 2 531 **368** B1, nicht bei EP 2 755 **846** B1