

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES  
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges  
Eigentum

Internationales Büro

(43) Internationales  
Veröffentlichungsdatum  
12. Oktober 2017 (12.10.2017)



(10) Internationale Veröffentlichungsnummer  
**WO 2017/174200 A2**

(51) Internationale Patentklassifikation:  
**G06Q 20/20** (2012.01)

(21) Internationales Aktenzeichen: PCT/EP2017/000443

(22) Internationales Anmeldedatum:  
7. April 2017 (07.04.2017)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:  
10 2016 004 293.1 7. April 2016 (07.04.2016) DE

(71) Anmelder: **Q1 ENERGIE AG** [DE/DE]; Rheinstraße 82,  
49090 Osnabrück (DE).

(72) Erfinder: **HERKENHOFF, Sebastian**; Hasetorwall 21,  
49076 Osnabrück (DE). **SEIDEL, Kevin**; Falkenstraße 43,  
49124 Georgsmarienhütte (DE). **BECKMANN,**  
**Frederick**; Max-Reger-Straße 27, 49076 Osnabrück (DE).  
**HARTMANN, Georg**; Liebigstraße 35, 49074 Osnabrück  
(DE).

(74) Anwalt: **POTT, Ulrich**; Busse & Busse, Patent- und  
Rechtsanwälte Partnerschaft mbB, Großhandelsring 6,  
49084 Osnabrück (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für  
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,  
AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW,  
BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DJ, DK,  
DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM,  
GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH,  
KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,  
MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA,  
NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO,  
RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV,  
SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC,  
VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für  
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,  
GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST,  
SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG,  
KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR INITIATING AN AUTHENTICATION PROCESS, IN PARTICULAR SUITABLE FOR AUTHENTICATING A PERSON DURING A CASHLESS PAYMENT TRANSACTION, AND DATA PROCESSING TERMINAL FOR USE IN SAID TYPE OF METHOD

(54) Bezeichnung : VERFAHREN ZUR EINLEITUNG EINES AUTHENTIFIZIERUNGSPROZESSES, INSBESONDERE GEEIGNET ZUR PERSONENAUTHENTIFIZIERUNG IM RAHMEN EINES BARGELDLOSEN ZAHLUNGSVERKEHRS, UND DATENVERARBEITUNGSTERMINAL ZUR VERWENDUNG IN EINEM SOLCHEN VERFAHREN

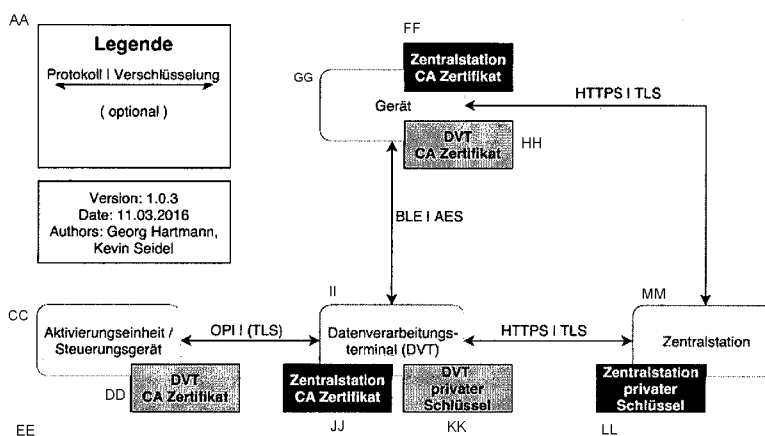


Fig. 1

(57) Abstract: The invention relates to a method for authenticating users and objects vis-a-vis an activation unit and/or a control unit, in particular for authenticating a person during a cashless payment transaction, for example, using a user/object-specific device such as a smartphone in which user/object-specific data are stored, and a central station, e.g. a server. Said type of method for authenticating users and objects involves the following method steps: the user/object-specific device is connected, via a radio link, to a data processing terminal that switches the connection and secures a communication with the central station; - the user/object-specific device sends encrypted system-specific data and user/object-specific data to the data processing terminal via the radio link; - the data processing terminal receives system-specific data sent by the device, verifies said data, applies a test seal (signature) to the user/object-specific data and transmits the signed user/object-specific data to the central station (server); - the central station (server) decrypts the received signed user/object-specific data and sends a positive or negative

authorization signal to the data processing terminal; - if the authorization signal sent by the central station is positive, the data processing terminal transmits an activation signal to the activation unit and/or the control device.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]



WO 2017/174200 A2



CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Veröffentlicht:**

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts (Regel 48 Absatz 2 Buchstabe g)*

---

Die Erfindung bezieht sich auf ein Verfahren zur Individuums- und Objektauthentifizierung gegenüber einer Aktivierungseinheit und / oder einem Steuerungsgerät, insbesondere zur Personenauthentifizierung beispielsweise im Rahmen eines bargeldlosen Zahlungsverkehrs, unter Verwendung von einem Individuums- / objektbezogenen Gerät wie z. B. einem Smartphone, auf dem Individuums- bzw. objektspezifische Daten hinterlegt sind, und einer Zentralstation, z. B. einem Server. Um ein solches Verfahren zur Individuums- und Objektauthentifizierung sind folgende Verfahrensschritte vorgesehen: - Das Individuums- / objektbezogene Gerät wird über eine Funkstrecke mit einem Datenverarbeitungsterminal verbunden, welches die Verbindung und Absicherung einer Kommunikation mit der Zentralstation vermittelt; - Das Individuums- / objektbezogene Gerät sendet verschlüsselt über die Funkstrecke an das Datenverarbeitungsterminal systemspezifische Daten und Individuums- / objektbezogene Daten; - Das Datenverarbeitungsterminal empfängt von dem Gerät gesendete systemspezifischen Daten, überprüft diese und versieht die Individuums- / objektbezogene Daten mit einem Prüfsiegel (Signatur) und leitet diese signierten Individuums- / objektbezogenen Daten an die Zentralstation (Server) weiter; - Die Zentralstation (Server) entschlüsselt die empfangenen signierten Individuums- / objektspezifischen Daten und sendet an das Datenverarbeitungsterminal ein positives oder negatives Autorisierungssignal. - Das Datenverarbeitungsterminal gibt im Falle eines von der Zentralstation positiv gemeldeten Autorisierungssignals ein Aktivierungssignal an die Aktivierungseinheit und/oder das Steuergerät weiter.

**Verfahren zur Einleitung eines Authentifizierungsprozesses,  
insbesondere geeignet zur Personenauthentifizierung im Rahmen  
eines bargeldlosen Zahlungsverkehrs, und Datenverarbeitungsterminal zur  
Verwendung in einem solchen Verfahren**

Die Erfindung bezieht sich auf ein Verfahren zur Objekt- und Individuumsauthentifizierung, insbesondere zur Personenauthentifizierung beispielsweise im Rahmen eines bargeldlosen Zahlungsverkehrs, unter Verwendung von einem individuum- oder objektbezogenen Gerät wie z.B. einem Smartphone, auf dem individuum- oder objektspezifische Daten hinterlegt sind, und einer Zentralstation, die den Authentifizierungsvorgang verifiziert, z.B. einem Server.

Der Zahlungsverkehr im stationären Handel erlebt durch veränderte regulatorische und technische Rahmenbedingungen einen tiefgreifenden Wandel. Herkömmliche Verfahren zur Einleitung eines bargeldlosen Zahlungsverkehrs setzen ein, in aller Regel an ein Kassensystem angeschlossenes, Lesegerät wie beispielsweise ein Kartenterminal voraus, das einerseits mit dem Kassensystem kommuniziert und andererseits mit dem Server einer Bank über ein speziell gesichertes Netz (VPN) verbunden ist. Für den Zahlvorgang wird eine Zwei-Faktor Authentifizierung vorgenommen, bestehend aus einem physisch vorhandenen Objekt (Karte) und einem kundenspezifischen Erkennungscode (PIN), mit deren Kombination sich der Kunde vor

- 2 -

Ort als Berechtigter für eine Zahlungsanweisung ausweist. Daneben sind neuere Verfahren zur Einleitung eines bargeldlosen Zahlungsverkehrs bekannt, bei denen eine Personenidentifizierung mittels eines Smartphones oder einer anderen tragbaren Elektronik einzuleiten ist, indem über ein Empfangsgerät (Lesegerät?) vom Smartphone erhaltene Identifizierungsdaten empfangen und Zahlungen mittels Eingabe eines PIN-Codes weitergegeben werden.

Ähnliches gilt auch für bislang angewendete Verfahren zur sonstigen Authentifizierung von Personen oder von Personen oder Gegenständen (Objekten), beispielsweise im Zuge von Personenkontrollen für Zugangssysteme z.B. für Gebäude. Bislang sind zwei Verfahren bekannt geworden, um einen bargeldlosen Zahlungsverkehr über Smartphones einzuleiten. Zum einen besteht die Möglichkeit, einen QR-Code, der von einem Kassensystem angezeigt wird, mittels einer Kamera des Smartphones zu erfassen. Zum anderen ist die Übertragung von kartenähnlichen Daten vom Smartphone durch eine Near-Field-Communication (NFC) möglich, wie sie auch in neueren, kontaktlosen Chipkarten eingesetzt wird.

QR-Codes übergeben eine Information vom einleitenden Gerät zu einer Software auf dem Smartphone, die diese Information verwendet um die Zahlung zu initiieren. Für die eigentliche Zahlung ist eine bestehende Internetverbindung auf dem Smartphone zwingende Voraussetzung. Außerdem kann der Nutzer anhand der QR-Codes optisch nicht verifizieren ob es sich um den erwarteten QR-Code handelt oder dieser durch einen Angreifer platziert wurde. Dadurch sind Phishing Attacken möglich.

NFC arbeitet mit zwei überlagerten Magnetfeldern, die in einer Nahdistanz von maximal 20 cm zur Deckung gebracht werden müssen. Dies ist dann von Nachteil, wenn die Zahlung auf Distanz durchgeführt werden soll (z.B. aus dem Inneren eines Fahrzeugs heraus). Weiterhin besteht auch keine Möglichkeit, das System z.B. über ortsabhängige Push-Benachrichtigungen aktiv zu bewerben. Des Weiteren können NFC-basierte Zahlungssysteme dadurch angegriffen werden, dass eine Zahlung gestartet wird, indem der Angreifer ein Zahlungsterminal in die physische Nähe des Smartphones des Opfers bringt und eine Zahlung auslöst, während das Opfer dies nicht erwartet. Nötwendige Schutzmaßnahmen wie Etais aus Aluminium stören jedoch auch erwünschte Funksignale wie WLAN oder Mobilfunk.

Die Tatsache, dass QR-Codes lediglich unidirektional Daten übergeben können und dass NFC sowohl von der Datenrate als auch von der maximalen Distanz zwischen den kommunizierenden Geräten stark eingeschränkt ist, limitiert die Einsatzbereiche dieser beiden Verfahren in der Verwendung als Verfahren zum lokalen Bezahlen (lokal = beide Kommunikationsteilnehmer befinden sich in einer räumlichen Nähe zueinander) und der Interaktion mit Maschinen z.B. im Kontext einer Anlagensteuerung oder Objektidentifikation.

Bei beiden Verfahren, QR-Code und NFC, kann das individuumbezogene Gerät zudem nicht verifizieren, ob es seine Daten an eine gültige, nicht kompromittierte Gegenstelle überträgt. Dies ist der Tatsache geschuldet, dass beide Verfahren keine ausreichend schnelle lokale, bidirektionale Datenübertragung ermöglichen, um beispielsweise zertifikatsbasierte Identitätsinformationen auszutauschen.

- 4 -

So ist es Aufgabe der vorliegenden Erfindung, ein Verfahren zur Individuums- und Objektauthentifizierung unter Verwendung eines individuums- bzw. objektbezogenen Geräts, im weiteren „Gerät“ genannt, zur Verfügung zu stellen, das die Erfassung und Übertragung von Daten, beispielsweise im Rahmen eines bargeldlosen Zahlungsverkehrs, schnell, mit einem hohen Sicherheitsfaktor und auf Distanz ermöglicht. Zudem soll es möglich sein, weitere Interaktionen, wie z.B. das Senden von Steuerungsbefehlen oder den Austausch digitaler Rechnungen und Belege, abzubilden.

Als personen- bzw. objektbezogene Geräte kommen insbesondere Smartphones in Betracht, die Dank der Anwendungsmarktplätze App Store (iOS) und Playstore (Android) in ihrer Softwareausstattung beliebig erweiterbar sind. Es soll jedoch auch möglich sein, andere Smart Devices wie z.B. Uhren und Armbänder, aber auch „Smarte“ Komponenten in Autos, die ebenfalls die Möglichkeiten bieten, in der Software erweitert zu werden, als personen- bzw. objektbezogene Geräte einzusetzen.

Das Verfahren ermöglicht die flexible, händlerindividuelle Anbindung einer variablen Anzahl von Zahlungsdienstleistern und weiteren Anwendungspartnern. Art und Anzahl der verfügbaren Zahlarten und Dienste können vom Händler selbsttätig über ein terminalspezifisches Administrationsdashboard festgelegt werden.

Physikalische Grundlage des Verfahrens ist, dass das Datenverarbeitungsterminal über eine Kurzfunkstrecke mit den Kurzstreckenfunkstandards Bluetooth Low Energy (BLE) oder einer Kombination aus einer Funkübertragung und einer Near-Field-

Communication, oder einer zukünftigen, schnelleren NFC Technik mit Mobiltelefonen und anderer tragbarer Elektronikgeräten kommunizieren kann.

Aufgrund der Verschlüsselung der ausgetauschten Daten auf der Funkstrecke durch die Kombination symmetrischer als auch ein asymmetrischer Verschlüsselungsverfahren ist eine sehr sichere Übertragung möglich, da sowohl Inhalt als auch Funkverbindung getrennt voneinander verschlüsselt sind.

Es ist möglich, Finanztransaktionen analog zu Funktionsweisen von Onlinezahlungen in Webshops durchzuführen, wobei Transaktionen nicht nur sequentiell, sondern auch parallel durchgeführt werden können, was eine entscheidende Verbesserung gegenüber herkömmlichen kartenbasierten Terminals darstellt. Basis dieser Flexibilität ist ein zertifikatbasiertes Identitätsmanagement, das allen Beteiligten des Transaktionsprozesses nur die für den jeweiligen Teilschritt benötigten Informationen zugänglich macht. Dieses Identitätsmanagement macht das Verfahren außerordentlich flexibel, sicher und schützt die Privatsphäre des Endanwenders bereits strukturell.

Im Rahmen des Paarungs-Prozesses (Pairing) ist es bei Bluetooth notwendig, dass der Nutzer einen Code zwischen den teilnehmenden Geräten manuell abgleicht, um eine „Man-In-The-Middle“-Attacke mit an Unmöglichkeit grenzender Wahrscheinlichkeit auszuschließen. Das vorgestellte Verfahren macht diesen Schritt überflüssig und macht Bluetooth somit erstmalig nutzbar für Vorgänge, die sowohl hohe Anforderungen an Sicherheit als auch Nutzungskomfort haben.

Durch die kombinierte Anwendung eines symmetrischen und eines asymmetrischen Verschlüsselungsverfahrens kann ein Schlüsselaustausch beim Verbindungsaufbau außerordentlich schnell und außerordentlich sicher durchgeführt werden. In Zukunft kann bei einer entsprechenden Leistungsfähigkeit der tragbaren elektronischen Geräte unter Umständen auch eine kombinierte Anwendung zweier asymmetrischer Verschlüsselungsverfahren oder die alleinige Verwendung eines einzelnen asymmetrischen Verschlüsselungsverfahrens stattfinden. Eine alleinige symmetrische Verschlüsselung kann nicht als ausreichend sicher und nicht als ausreichend praktisch angesehen werden, weil der Schlüssel vor der Übertragung beiden Kommunikationspartnern bekannt sein muss und bei Bekanntwerden bei allen Kommunikationspartnern zurückgezogen und/oder ausgetauscht werden muss.

Bei der symmetrischen Verschlüsselung verwenden die Teilnehmer einer Kommunikation zum Verschlüsseln und Entschlüsseln denselben Schlüssel. Dabei beruht die Sicherheit des Verfahrens darauf, dass der Aufwand zum Berechnen des Schlüssels so hoch ist, dass der Schlüssel mit der bestehenden Rechenleistung nicht mit vertretbarem Zeitaufwand ermittelt werden kann. Da jedoch der Inhaber des symmetrischen Schlüssels die mit ihm verschlüsselte Kommunikation entschlüsseln und lesen kann, muss der Austausch eines symmetrischen Schlüssels über einen sicheren Kanal oder durch Sicherung eines PIN-Codes erfolgen, der nur den Kommunikationsteilnehmern bekannt ist. Gleichwohl ist ein großer Vorteil einer symmetrischen Verschlüsselung die hohe Geschwindigkeit bei der Ver- und Entschlüsselung.

- 7 -

Bei der asymmetrischen Verschlüsselung, z.B. mittels der Public-Key-Kryptographie wird ein Paar aus zwei Schlüsseln generiert, wobei charakteristisch für dieses Schlüsselpaar ist, dass Daten, die mit einem Schlüssel verschlüsselt werden, nicht mit demselben Schlüssel wieder entschlüsselt werden können, sondern nur mit dem jeweils anderen. Der eine Schlüssel wird als öffentlich und der andere wird als privat definiert. Zur Signatur oder Verschlüsselung einer Kommunikation sendet ein Teilnehmer seinen öffentlichen Schlüssel an einen anderen Teilnehmer. Dieser andere Teilnehmer kann mit dem vom ersten Teilnehmer gesendeten öffentlichen Schlüssel beliebige Nachrichten für den ersten Teilnehmer verschlüsseln. Dann kann dieser erste Teilnehmer mit seinem privaten Schlüssel die Nachricht wieder entschlüsseln. Diese asymmetrische Verschlüsselung hat gegenüber der symmetrischen Verschlüsselung den Vorteil, dass der Schlüsselaustausch über eine unsichere Verbindung erfolgen kann und dass dabei keine Sicherung durch eine vorher vereinbarte PIN (Persönliche Identifikationsnummer) erfolgen muss. Damit sind bei dem erfindungsgemäßen Verfahren die ausgetauschten Daten auf der Funkstrecke außerordentlich sicher zu übermitteln.

Da die Überprüfung der Zertifikate ohne eine Internetverbindung erfolgen kann besteht keine Notwendigkeit zum Vorhandensein einer Internetverbindung über mobile Datennetze auf dem personen- und/oder objektbezogenen Gerät.

Das Datenverarbeitungsterminal steht aber nicht nur über die Funkstrecke mit dem personenbezogenen Gerät (z.B. Smartphone) in Verbindung, sondern auch z.B.

über eine Datenleitung mit einem Kassensystem. Das Datenverarbeitungsterminal hat ebenfalls einen öffentlichen Schlüssel und einen privaten Schlüssel.

Ein Datenverarbeitungsterminal, das zur Anwendung in dem erfindungsgemäßen Verfahren geeignet ist, ist in Anspruch 10 näher definiert, wobei vorteilhafte Ausgestaltungen dieses Datenverarbeitungsterminals in den Ansprüchen 11 bis 14 angegeben sind. Kern dieses Datenverarbeitungsterminals ist ein Kryptochip-System auf dem sich ein Mikroprozessor befindet, dem ein Identifizierungssicherheitsbaustein zugeordnet ist. Dieses Kryptochip-System kann modular aufgebaut sein. Im vorliegenden Fall befindet es sich auf einer Basisplatine, die die kabelgebundenen Verbindungen zur Außenwelt vermittelt. Des Weiteren befindet sich oberhalb des Kryptochipsystems eine Deckplatine, die alle Funkgebundenen Verbindungen zur Außenwelt vermittelt und über LED Bausteine zur visuellen Kommunikation mit dem Anwender verfügt. Über dieser Deckplatine ist eine gehärtete Glasoberfläche aufgebracht auf der sich der LED-Ring als Umgrenzung einer inneren Kreisfläche abzeichnet. Zudem weist das Datenverarbeitungsterminal einen Anschluss zur Verbindung mit einer weiteren Platine auf, über die das Datenverarbeitungsterminal Strom und Kabelgebundene Informationsströme erhält.

In dem in Fig. 1 gezeigten Schaubild wird eine Anwendung des individuellen Verfahrens näher dargestellt:

Fig. 1 (Abbildung a) zeigt einen Aufbau, wie er beispielsweise an einer Kasse am POS oder einem Zugangssystem vorliegt. Eine Aktivierungseinheit / ein Steuergerät

(AE) benötigt die Autorisierung einer Funktion, die die AE anbietet. Im Beispiel der Kasse könnte diese Funktion „Bezahlen“ sein, beim Zugangssystem „Tür öffnen“. Diese Autorisierung wird durch die Zentralstation vorgenommen, dafür muss diese jedoch das personenbezogene Gerät zunächst authentifizieren. Da AE und das personenbezogene Gerät allerdings keinerlei physische Verbindung zueinander haben, ist ein Datenverarbeitungsterminal (DVT) zwischengeschaltet, das sowohl über Nahfunk mit dem personenbezogenen Gerät als auch per Datenverbindung, über ein beliebiges Medium, mit AE und der Zentralstation verbunden ist.

Das DVT akzeptiert eine oder mehrere Verbindungen von einer auf dem personenbezogenen Gerät installierten Software (App). Diese Verbindung wird verschlüsselt, wobei das personenbezogene Gerät die Authentizität des Datenverarbeitungsterminals anhand in der App hinterlegter systemspezifischer Daten überprüft. Die Verbindung zwischen DVT und Zentralstation ist ebenfalls verschlüsselt, wobei sich beide Seiten einer Kommunikation gegenseitig authentifizieren. Die Zentralstation übernimmt in Abbildung a die Verwaltung von einem oder mehreren DVTs.

Zusätzlich übernimmt die Zentralstation in Abbildung a die Authentifizierung des Personenbezogenen Geräts. Zu diesem Zweck wurde während oder nach der Installation der App nutzerspezifische Daten auf dem personenbezogenen Gerät hinterlegt. In dem Moment, in dem eine die Autorisierung benötigende Funktion durch die AE ausgelöst werden soll, wird der Befehl zum Auslösen dieser Funktion von der AE über das DVT zur App geschickt. Durch kryptografische Verfahren wird der Befehl durch die App mit den nutzerspezifischen Daten unterschrieben (signiert) und Befehl

- 10 -

und Unterschrift (Signatur) werden an das DVT geschickt. Das DVT schickt die Daten an die Zentralstation. Dort wird zunächst anhand der nutzerspezifischen Daten das personenbezogene Gerät authentifiziert (identifiziert) und dann geprüft, ob das personenbezogene Gerät zur Ausführung des übermittelten Befehls autorisiert (berechtigt) ist.

Ist dies der Fall, sendet die Zentralstation die Autorisierung an das DVT. Dieses DVT sendet darauf hin ein Aktivierungssignal an die AE, welche darauf hin die die Autorisierung erfordernde Funktion ausführt.

Fig. 2 (Abbildung b) zeigt eine Variante von Abbildung a, deren Unterschied darin besteht, dass die Autorisierung der Funktion der Aktivierungseinheit / ein Steuergerät (AE) durch eine externe Station stattfindet, die nicht die Zentralstation ist. In Abbildung b nimmt diese Rolle ein Payment Service Provider (PSP) ein.

Ein wesentliches Merkmal des beschriebenen Verfahrens ist, dass die nutzerspezifischen Daten auf dem personenbezogenen Gerät für die externe Station verschlüsselt werden. Damit wird erreicht, dass das personenbezogene Gerät sich gegenüber der externen Station authentifizieren kann, für alle anderen an der Kommunikation beteiligten Geräte und potenzielle Angreifer jedoch nicht authentifizierbar (identifizierbar) ist.

Im Kontext der digitalen Bezahlungssysteme ist es aufgrund dieses Merkmals möglich, anonym / pseudonym zu bezahlen, wenn der gewählte PSP dies vorsieht ( wie

- 11 -

zum Beispiel im Falle digitaler Zahlungsmittel, z.B. mit der Digitalwährung BitCoin oder der Ethereum).

**Ansprüche:**

1. Verfahren zur Individuums- und Objektauthentifizierung gegenüber einer Aktivierungseinheit und / oder einem Steuerungsgerät, insbesondere zur Personenauthentifizierung beispielsweise im Rahmen eines bargeldlosen Zahlungsverkehrs, unter Verwendung von einem individuums- / objektbezogenen Gerät wie z.B. einem Smartphone, auf dem individuums- bzw. objektspezifische Daten hinterlegt sind, und einer Zentralstation, z.B. einem Server, gekennzeichnet durch folgende Verfahrensschritte:

- Das individuums- / objektbezogene Gerät wird über eine Funkstrecke mit einem Datenverarbeitungsterminal verbunden, welches die Verbindung und Absicherung einer Kommunikation mit der Zentralstation vermittelt;
- Das individuums- / objektbezogenen Gerät sendet verschlüsselt über die Funkstrecke an das Datenverarbeitungsterminal systemspezifische Daten und individuums- / objektbezogene Daten;
- Das Datenverarbeitungsterminal empfängt von dem Gerät gesendete systemspezifischen Daten, überprüft diese und versieht die individuums-/ objektbezogene Daten mit einem Prüfsiegel (Signatur) und leitet diese signierten individuums-/ objektbezogenen Daten an die Zentralstation (Server) weiter;

- 13 -

- Die Zentralstation (Server) entschlüsselt die empfangenen signierten individuals-/objektspezifischen Daten und sendet an das Datenverarbeitungsterminal ein positives oder negatives Autorisierungssignal.
- Das Datenverarbeitungsterminal gibt im Falle eines von der Zentralstation positiv gemeldeten Autorisierungssignals ein Aktivierungssignal an die Aktivierungseinheit und/oder das Steuergerät weiter.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das personen-/ objektbezogene Gerät über die Funkstrecke die Daten asymmetrisch oder asymmetrisch und symmetrisch verschlüsselt überträgt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass bei einer Kombination aus symmetrischen und asymmetrischen Verschlüsselungsverfahren das personenbezogene/ objektbezogene Gerät und das Datenverarbeitungsterminal zum Verschlüsseln und Entschlüsseln denselben Schlüssel verwenden und die Sicherung der asymmetrischen Verschlüsselung durch ein Paar aus zwei Schlüsseln dergestalt erfolgt, dass Signale, die mit einem Schlüssel verschlüsselt werden, nicht mit demselben Schlüssel wieder entschlüsselt werden können, sondern mit dem jeweils anderen Schlüssel, wobei der eine Schlüssel als öffentlich und der andere als privat definiert ist (Public-Key-Kryptographie).

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass als Funkstrecke ein Kurzstreckenfunkstandard (z.B. Bluetooth Low Energy oder Near Field Communication oder Wifi) verwendet wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass als individuum- /objektbezogenes Gerät eine mobile Elektronik wie ein Mobiltelefon (Smartphone), digitale Uhren oder dergleichen Smart-Devices benutzt werden.
6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass das personen-/ objektbezogene Gerät ohne mobile Datenverbindung über die Funkstrecke mit dem Datenverarbeitungsterminal kommuniziert.
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass das Verfahren durch Zonierung der Funkstrecke auslösbar ist.
8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass das Datenverarbeitungsterminal mit der Aktivierungseinheit und /oder dem Steuerungsgerät Daten über eine Datenverbindung austauscht und Daten zum Zwecke der Authentifizierung mit einer Zentralstation austauscht.
9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass eine Übergabe kundenrelevanter Informationen (z.B. einem digitalen Kaufbeleg) möglich ist.
10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass ein Austausch von Steuerungsinformationen erfolgt (z.B. Steuerungsbefehle und Statusinformationen zum Aktivieren und interaktiven Nutzung eines Waschportals für Kraftfahrzeuge

- 15 -

11. Datenverarbeitungsterminal zur Verwendung in einem Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass das Datenverarbeitungsterminal zumindest einen Anschluss für eine Datenverbindung und zumindest einen Anschluss für eine Funkstreckenverbindung (z.B. Bluetooth Low Energy, Near-Field-Communication, Wifi) und einen Speicher aufweist.

12. Datenverarbeitungsterminal nach Anspruch 11, dadurch gekennzeichnet, dass das Datenverarbeitungsterminal eine Deckplatine mit verschiedenen Funkstandards und optischen Signalgebern aufweist.

13. Datenverarbeitungsterminal nach Anspruch 12, dadurch gekennzeichnet, dass das Datenverarbeitungsterminal ein Kryptochipssystem in Gestalt eines Mikroprozessors und/oder eines Identifizierungssicherheitsbausteins enthält.

14. Datenverarbeitungsterminal nach Anspruch 12 oder 13, dadurch gekennzeichnet, dass der Deckplatine und dem Kryptochipssystem eine Basisplatine zugeordnet ist mit zumindest einem Anschluss für Datenverbindungen.

15. Datenverarbeitungsterminal nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, dass es eine gehärtete Glasoberfläche aufweist.

16. Datenverarbeitungsterminal nach einem der Ansprüche 12 bis 15, dadurch gekennzeichnet, dass in die Deckplatine ein LED-Ring zur Umgrenzung eines inneren Kreises integriert ist.

1 / 1

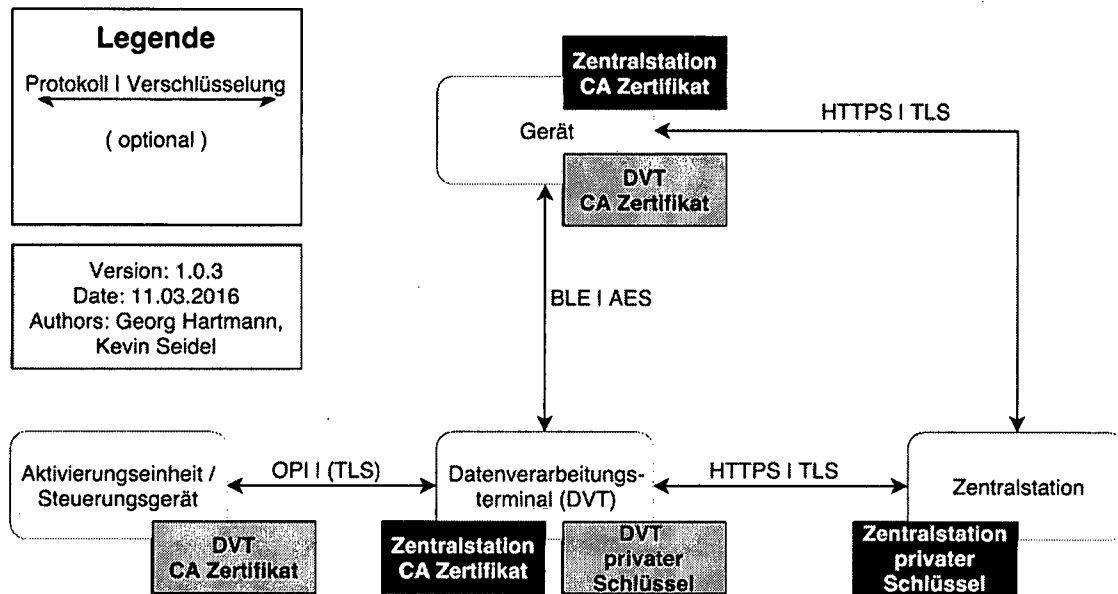


Abbildung a: Variante Zentralstation

Fig. 1

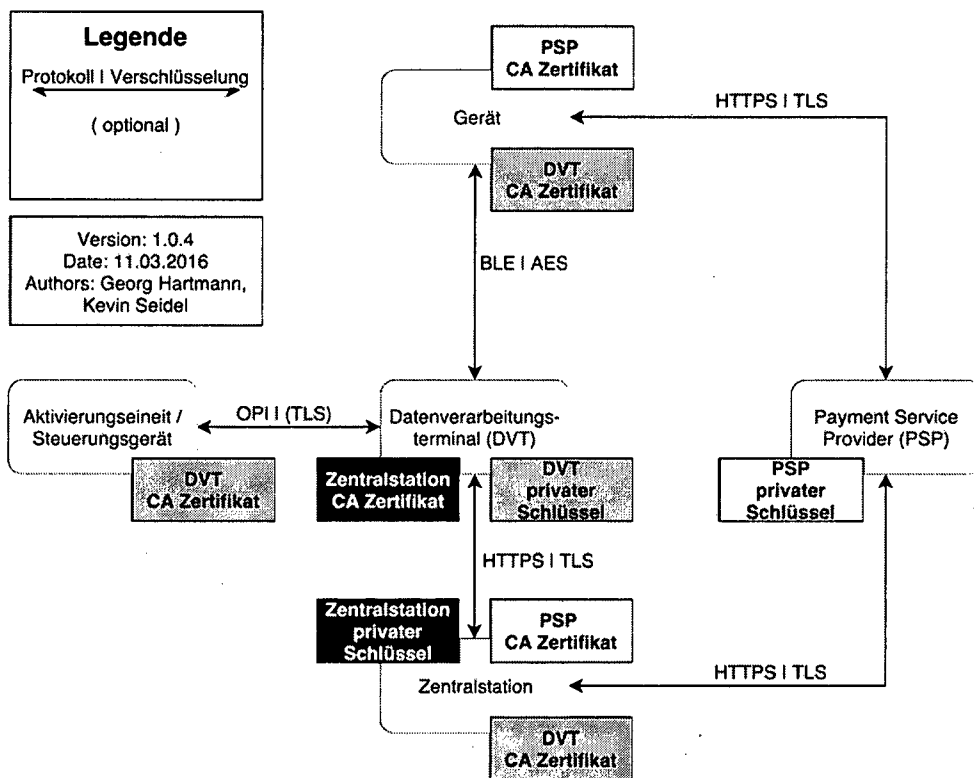


Abbildung b: Variante externe Autorisierung

Fig. 2