(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
08. Oktober 2020 (08.10.2020)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2020/200766 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2020/057276

(22) Internationales Anmeldedatum:
17. März 2020 (17.03.2020)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
19167507.3 05. April 2019 (05.04.2019) EP

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Werner-von-Siemens-Straße 1, 80333 München (DE).

(72) Erfinder: **FALK, Rainer**; Primelweg 9, 85586 Poing (DE).
FRIES, Steffen; Eberweg 3, 85598 Baldham (DE).

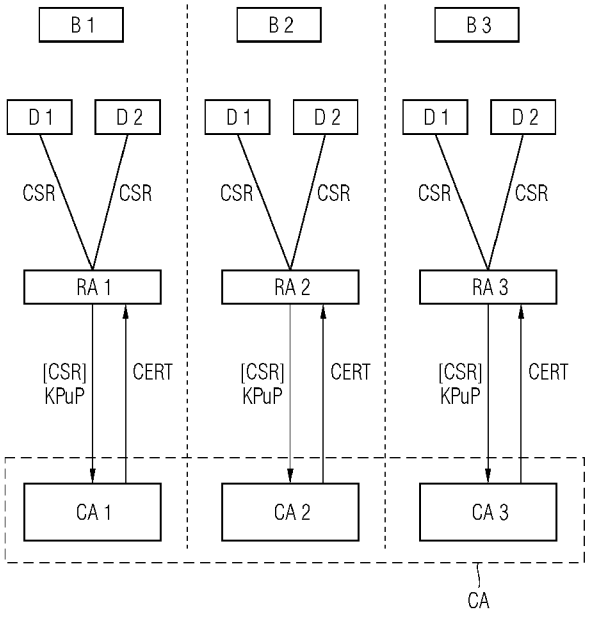
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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,

(54) **Title:** METHOD FOR ISSUING A CRYPTOGRAPHICALLY PROTECTED CERTIFICATE OF AUTHENTICITY FOR A USER

(54) **Bezeichnung:** VERFAHREN ZUM AUSSTELLEN EINER KRYPTOGRAPHISCH GESCHÜTZTEN AUTHENTIZITÄTSBESCHEINIGUNG FÜR EINEN BENUTZER

FIG 1



(57) **Abstract:** The invention claims a method for issuing a cryptographically protected certificate of authenticity (CERT) for a user (B1, B2, B3), having the following steps: - providing a public user key, - providing a public client key for a client assigned to the user, - forming a request (CSR) that contains the public user key and is protected and/or digitally signed using a private client key assigned to the provided public client key, and - issuing a cryptographically protected certificate of authenticity that contains the public user key and identifies the client. Preferably, the cryptographically protected certificate of authenticity contains or references a cryptographic client identifier (M-ID) that is formed on the basis of the public client key.

(57) **Zusammenfassung:** Die Erfindung beansprucht ein Verfahren zum Ausstellen einer kryptographisch geschützten Authentizitäts-

[Fortsetzung auf der nächsten Seite]

WO 2020/200766 A1

SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, 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:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

bescheinigung (CERT) für einen Benutzer (B1, B2, B3), aufweisend folgende Schritte: - Bereitstellen eines öffentlichen Benutzerschlüssels, - Bereitstellen eines öffentlichen Mandantenschlüssels für einen Mandanten, der dem Benutzer zugeordnet wird, - Bilden einer Anfrage (CSR), die den öffentlichen Benutzerschlüssel enthält und mit Hilfe eines dem bereitgestellten öffentlichen Mandantenschlüssel zugeordneten privaten Mandantenschlüssels geschützt und/oder digital signiert wird, und - Ausstellen einer kryptographisch geschützten Authentizitätsbescheinigung, die den öffentlichen Benutzerschlüssel enthält und den Mandanten identifiziert. Vorzugsweise enthält oder referenziert die kryptographisch geschützten Authentizitätsbescheinigung einen kryptographischen Mandantenidentifikator (M-ID), der abhängig vom öffentlichen Mandantenschlüssel gebildet wird.

Beschreibung

Verfahren zum Ausstellen einer kryptographisch geschützten Authentizitätsbescheinigung für einen Benutzer

Die Erfindung betrifft ein Verfahren zum Ausstellen einer kryptographisch geschützten Authentizitätsbescheinigung für einen Benutzer, wie z.B. eines digitalen Zertifikats, insbesondere eines Gerätezertifikats, für einen Benutzer sowie zugehörige Vorrichtungen.

Der Begriff „Security" bzw. „Sicherheit" bezieht sich im Rahmen der vorliegenden Beschreibung im Wesentlichen auf die Sicherheit bzw. Schutz, Vertraulichkeit und/oder Integrität von Daten sowie deren Übertragung und auch Sicherheit, Vertraulichkeit und/oder Integrität beim Zugriff auf entsprechende Daten. Auch die Authentifizierung bei Datenübertragungen beziehungsweise beim Datenzugriff gehört zum Begriff „Sicherheit", wie er im Rahmen der vorliegenden Beschreibung verwendet wird. Ein Modul kann hierbei als eine Hardware- und/oder Funktionseinheit, die software- und/oder firmwaremäßig ausgestaltet sein kann, ausgeprägt sein. Die Funktion kann beispielsweise mittels eines Prozessors und/oder einer Speichereinheit zum Speichern von Programmbefehlen ausgeführt werden.

In einem zertifikatbasierten System erhält jede Person oder jedes Objekt, z.B. ein Gerät oder ein Softwareprozess, eine Authentizitätsbescheinigung, wie beispielsweise ein digitales Zertifikat, eine Datenstruktur (oder ein Datensatz), welche Angaben zu seiner Identität und einen öffentlichen Schlüssel der Person bzw. des Benutzers bzw. des Objekts bzw. des Geräts enthält. Jedes Zertifikat ist von einer ausgebenden Stelle durch eine digitale Signatur beglaubigt, die ihrerseits wieder von höheren Stellen beglaubigt sein kann. Da die digitale Signatur die komplette Datenstruktur umfasst, wird deren Inhalt damit integritätsgeschützt. Das Vertrauenssystem einer solchen Private Key Infrastructure (PKI) ist hierarchisch. Den gemeinsamen Vertrauensanker bildet ein sogenann-

tes Wurzelzertifikat, auch Root Certificate genannt, welches in allen relevanten Systemkomponenten authentisch konfiguriert sein muss.

Auch die Authentizität und Integrität eines digitalen Zertifikats werden durch die digitale Signatur geprüft. Dazu wird mit Hilfe eines geheimen Signaturschlüssels, auch als privater Schlüssel bezeichnet, zu einem Datensatz ein Wert berechnet, der digitale Signatur genannt wird. Dieser Wert ermöglicht es jedem, mit Hilfe des zugehörigen öffentlichen Verifikationsschlüssels, auch als öffentlicher Schlüssel bezeichnet, die nichtabstreitbare Urheberschaft und Integrität des Datensatzes zu prüfen. Um eine mit einem Signaturschlüssel erstellte Signatur einem Benutzer zuordnen zu können, muss der zugehörige Verifikationsschlüssel diesem Benutzer zweifelsfrei zugeordnet sein.

Eine Zertifizierungsinstanz wird im Weiteren auch allgemein als Vorrichtung zur Ausgabe oder Ausgabevorrichtung von Zertifikaten bezeichnet.

Möglich ist ebenfalls die Speicherung von geheimen symmetrischen und privaten asymmetrischen Schlüsseln in physikalisch besonders geschützten Sicherheitsmodulen wie beispielsweise kryptographische Prozessoren, hardware security modules (HSM) oder trusted platform modules (TPM). Ein Sicherheitsmodul kann auch software-/firmwaremäßig implementiert sein. Geheime bzw. private Schlüssel können in das Sicherheitsmodul eingespielt oder darin erzeugt werden. Ein Auslesen der Schlüssel aus dem Sicherheitsmodul ist üblicherweise nicht oder nur sehr eingeschränkt möglich.

Für jedes Gerät, das einem Benutzer gehört, kann ein neues, asymmetrisches Schlüsselpaar erzeugt werden. Der private Schlüssel muss im Gerät verbleiben und gegen unberechtigte Nutzung und besonders gegen Auslesen und Kopieren zuverlässig geschützt werden; der öffentliche Schlüssel wird in authentischer Weise zu einer Certification Authority, abgekürzt CA,

die als Ausgabevorrichtung ausgestaltet sein kann, transportiert, welche ihn zusammen mit anderen Gerätedaten (Seriennummer, Typ, Herstellername, Produktionsdatum, usw.) in einer Datenstruktur digital signiert. Um sicherzustellen, dass der Besitzer des öffentlichen Schlüssels und der dazugehörigen Gerätedaten auch im Besitz des korrespondierenden privaten Schlüssels ist, ist der vom Gerät produzierte Datensatz ebenfalls häufig digital signiert, mit dem entsprechenden privaten Schlüssel des Geräts bzw. Benutzers, um den Transport vom Gerät zur CA zu schützen. Das Gerät kann ein IOT-Gerät oder anderes Gerät sein, das beispielsweise ein Sicherheitsmodul aufweist.

Digitale Zertifikate werden in der Regel zur Authentisierung von Benutzern benötigt, insbesondere auch zur Authentisierung von Geräten bzw. Komponenten eines industriellen Automatisierungs-/Steuerungssystems.

Ein digitales Zertifikat wird üblicherweise - wie oben beschrieben - von einer Public Key Infrastruktur (PKI) ausgestellt. Der Aufbau und Betrieb einer sicheren PKIs sind jedoch relativ aufwendig. Es ist möglich, dass eine technische PKI-Instanz von mehreren Mandanten gemeinsam benutzt wird. Obwohl die technische PKI-Infrastruktur gemeinsam durch mehrere Mandanten genutzt wird, erscheint es aus logischer Sicht so, als ob ein Mandant jeweils seine eigene PKI-Infrastruktur nutzen würde. Mandanten können beispielsweise unterschiedliche Betreiber von Automatisierungssystemen, unterschiedliche Automatisierungs-Anlagen oder unterschiedliche Firmen oder Geschäftsbereiche sein, die jeweils eine PKI-Infrastruktur benötigen. Benutzer, die einem Mandanten zugeordnet sind, können in diesem Zusammenhang Gerätehersteller-Servicepersonal oder auch Servicepersonal eines Automatisierungs-/Steuerungssystembetreibers sein. Hierbei übernehmen die Benutzer verschiedene Rollen, auf welche Weise sie Zugriff auf die Geräte und/oder Komponenten eines Benutzers bzw. eines Systems erhalten, um beispielsweise bestimmte Konfigurations- bzw. Wartungsarbeiten eines Mandanten zu erledigen. Über die-

se Rollen werden die Benutzer zu bestimmten Aufgabenerledigungen an Geräten des Benutzers bzw. des Systems autorisiert.

Jedoch ist es aufwendig, einen Mandanten sicher bei der PKI-Infrastruktur einzurichten und zu pflegen. Ein Mandant ist dabei typischerweise ein für einen Betreiber abgeschlossener Bereich der PKI, der nicht mit anderen Betreibern geteilt wird.

Es ist Aufgabe der vorliegenden Erfindung, Verfahren und Vor- bzw. Einrichtungen bzw. Geräten gegenüber dem oben genannten Stand der Technik zu verbessern.

Die Aufgabe wird durch die in den unabhängigen Ansprüchen angegebenen Merkmale gelöst. In den abhängigen Ansprüchen sind vorteilhafte Weiterbildungen der Erfindung dargestellt.

Die Erfindung beansprucht ein Verfahren zum Ausstellen einer kryptographisch geschützten Authentizitätsbescheinigung für einen Benutzer, aufweisend folgende Schritte:

- Bereitstellen eines öffentlichen Benutzerschlüssels (des Benutzers,
- Bereitstellen eines öffentlichen Mandantenschlüssels für einen Mandanten, der dem Benutzer zugeordnet wird,
- Bilden einer Anfrage zum Ausstellen der kryptographisch geschützten Authentizitätsbescheinigung,
wobei die Anfrage den öffentlichen Benutzerschlüssel enthält und mit Hilfe eines dem bereitgestellten öffentlichen Mandantenschlüssel zugeordneten privaten Mandantenschlüssels geschützt und/oder digital signiert wird, und
- Ausstellen einer kryptographisch geschützten Authentizitätsbescheinigung, die den öffentlichen Benutzerschlüssel enthält und den Mandanten identifiziert.

Der Mandant wird identifiert, indem die Zugehörigkeit der Anfrage zum Mandanten bestätigt wird oder ist oder positiv geprüft wird.

Dabei enthält die bereitgestellte Authentizitätsbescheinigung den öffentlichen Benutzerschlüssel, wie allgemein üblich. Zusätzlich enthält sie jedoch ein Informationselement zur Identifizierung bzw. Kennzeichnung desjenigen Mandanten, der die Anfrage mittels seines privaten Mandantenschlüssel geschützt und/oder digital signiert hat.

Die Erfindung bringt den Vorteil mit sich, dass kein explizites Einrichten von Mandanten in der PKI-Infrastruktur erforderlich ist. Mandanten sind implizit durch den öffentlichen Mandantenschlüssel gegeben, mit dem eine Zertifikatsanforderung überprüfbar ist. Dadurch kann ein Mandant vollautomatisch und ggf. „on the fly" für jede Zertifikatsanforderung eingerichtet werden. Trotzdem ist sichergestellt, dass die Authentizitätsbescheinigungen eines ersten Mandanten von solchen eines zweiten Mandanten zuverlässig unterschieden werden können.

Ein Mandant kann weitere öffentliche Schlüssel (public Keys) hinterlegen, die dem öffentlichen Mandantenschlüssel zugeordnet sind. Dann können Zertifikatsanforderungen dieses Mandanten auch mit den weiteren, jeweils dem öffentlichen Schlüssel zugeordneten privaten Schlüsseln geschützt werden.

Die Zertifizierungsanfrage für eine, den Benutzeridentifizierende Authentizitätsbescheinigung, enthält oder referenziert vorzugsweise einen kryptographischen Mandantenidentifikator, der abhängig vom öffentlichen Mandantenschlüssel gebildet wird. Es ist jedoch auch möglich, dass einer Zertifizierungsanfrage ein kryptographischen Mandantenidentifikator automatisch hinzugefügt wird.

Damit bestätigt/autorisiert der „Anfragende", d.h. der jeweilige Mandant, dass das Ausstellen des Zertifikats zulässig ist.

Die Anfrage kann einen vom öffentlichen Mandatenschlüssel abhängigen Mandantenidentifikator umfassen. Der Mandantenidentifikator kann aus dem Hashwert des öffentlichen Mandantenschlüssels gebildet werden.

Die Anfrage zum Ausstellen der kryptographisch geschützten Authentizitätsbescheinigung für einen Benutzer kann nach einer Authentifizierung des Mandanten gebildet und/oder übertragen werden, wobei die Anfrage über eine mit Hilfe einer Mandantenkennung oder mit Hilfe des gebildeten Mandantenidentifikators authentisierte Kommunikationsverbindung (z.B. TLS/IPsec/IKE) übertragen werden kann.

Bei einer die Anfrage bildenden und weiterleitenden Stelle z.B. eine Registration Authority (RA), kann die Authentisierung der Anfrage und basierend darauf die Autorisierung erfolgen. Letztendlich ist die Authentisierung eine Art "Zertifikatsaustellungsautorisierungs-Identifikator". Damit bestätigt der Benutzer bzw. die Anfrage bildende und weiterleitende Stelle (RA) die Zulässigkeit einer Zertifikatsausstellung.

Ein weiterer Aspekt der Erfindung ist eine Vorrichtung, insbesondere eine Certificate Authority (CA), zum Ausstellen einer kryptographisch geschützten Authentizitätsbescheinigung für einen Benutzer mit Hilfe eines bereitgestellten öffentlichen Benutzerschlüssels, aufweisend:
- eine Bestätigungseinheit, die dazu ausgelegt ist, eine kryptographisch geschützte Authentizitätsbescheinigung auszustellen, die den öffentlichen Benutzerschlüssel enthält und den Mandanten identifiziert, wobei sie die Zugehörigkeit und/oder die Zulässigkeit einer vorherigen Authentizitätsbescheinigungsanfrage zum Mandanten bestätigt (bzw. geprüft wird).

Ein weiterer Aspekt der Erfindung ist eine Vorrichtung, insbesondere eine Registration Authority (RA), zum Ausstellen einer kryptographisch geschützten Authentizitätsbescheinigung für einen Benutzer, aufweisend:

- eine Bereitstellungseinheit, die dazu ausgelegt ist, einen öffentlichen Mandantenschlüssel für einen Mandanten bereitzustellen, der dem Benutzer zugeordnet wird, und
- eine Erzeugungseinheit, die dazu ausgelegt ist, eine Anfrage zum Ausstellen der kryptographisch geschützten Authentizitätsbescheinigung zu bilden, wobei die Anfrage, die einen öffentlichen Benutzerschlüssel des Benutzers enthält oder mit diesem digital signiert ist, mit Hilfe des dem bereitgestellten öffentliche Mandantenschlüssels zugeordneten privaten Mandantenschlüssels schützbar und/oder digital signierbar ist.

Des Weiteren ist ein Computerprogramm(produkt) umfassend Programm-Code vorgesehen, der von mindestens einem Prozessor ausgeführt werden kann und der bewirkt, dass der mindestens eine Prozessor, das erfindungsgemäße (Betriebs-)Verfahren und dessen Ausführungsformen ausführt. Das Computerprogramm kann auf einer Vorrichtung der vorstehend genannten Art ablaufen oder als Computerprogrammprodukt auf einem computerlesbaren Medium gespeichert sein.

Die Vorrichtungen, Einrichtungen bzw. Geräte, Module und Computerprogramm(produkte) können entsprechend der Weiterbildungen/Ausführungsformen des vorgenannten Verfahrens und deren Weiterbildungen/Ausführungsformen und umgekehrt ausgebildet sein.

Die oben beschriebenen Eigenschaften, Merkmale und Vorteile dieser Erfindung sowie die Art und Weise, wie diese erreicht werden, werden klarer und deutlicher verständlich im Zusammenhang mit der folgenden Beschreibung der Ausführungsbeispiele, die im Zusammenhang mit den Figuren näher erläutert werden. Dabei zeigt in schematischer Darstellung:

Figur 1 ein Ausführungsbeispiel zur Anforderung bzw. zur Ausgabe von Authentizitätsbescheinigungen bzw. Zertifikaten,

Figur 2 ein Ausführungsbeispiel für eine Zertifikatsanforderungsnachricht und

Figur 3 ein Ausführungsbeispiel für ein angefordertes Zertifikats.

In Figur 1 zeigt erfindungsgemäß ein Vorgehen zur Anforderung bzw. zur Ausgabe von Authentizitätsbescheinigungen bzw. Zertifikaten,

Drei verschiedene Betreiber B1, B2, B3 bzw. Benutzer nutzen eine lokale Registrierungsstelle (Registration Authority) RA1, RA2, RA3, um Zertifikatsabfragen zu autorisieren. Alle drei Betreiber nutzen jeweils einen eigenen Zertifikatsaussteller CA1, CA2, CA3, der die Zertifikate betreiberspezifisch ausstellt. Die drei Betreiber können auch einen einzigen Zertifikatsaussteller CA (gestrichelt dargestellt) nutzen. Dazu hat jede Registrierungsstelle eine authentisierte Kommunikationsverbindung zum Aussteller z.B. CA, der auf Basis der für die Authentisierung genutzten privaten Mandantenschlüssel die Zertifikate ausstellen kann. Im Beispiel können Benutzer, die einem Mandanten zugeordnet sind, verschiedene Rollen übernehmen, wie sie Zugriff auf die Geräte D1 und D2 bzw. Komponenten eines Benutzers z.B. B1 bzw. eines Systems erhalten, um beispielsweise bestimmte Konfigurations- bzw. Wartungsarbeiten zu erledigen. Über die Rollen werden die Benutzer zu bestimmten Aufgabenerledigungen an Geräten des Benutzers bzw. des Systems eines Mandanten autorisiert.

Es wird ein öffentlicher Schlüssel (Public Key) KPUP eines Mandantenschlüsselpaares (öffentl., privater Schlüssel) verwendet, um einen Mandanten zu identifizieren. Automatisiert kann damit ein kryptographischer Mandanten-Identifier bzw. -Identifikator M-ID abhängig vom verwendeten Mandantenschlüsselpaar ermittelt werden (z.B. als Hash-Wert H des öffentlichen Mandantenschlüssels).

Die Anforderung bzw. Anfrage (Certificate Signing Request) CSR eines digitalen Zertifikats CERT ist durch den Mandantenschlüssel geschützt, das in Figur 1 durch die eckige Klammer angedeutet wird. Insbesondere kann eine Zertifikatsanforderung) durch den dem öffentlichen Mandantenschlüssel zugeordneten privaten Mandantenschlüssel digital signiert sein, das mit Sig gekennzeichnet wird. Die Zertifikatsanforderung CSR kann auch über eine mittels des privaten Mandantenschlüssels authentisierte Kommunikationsverbindung (z.B. TLS, IPsec/IKE) übertragen werden.

Der Schutz durch den privaten Mandantenschlüssels kann durch einen anfordernden Client-Knoten (Anfragesteller bzw. Requester) selbst erfolgen oder durch einen Zwischenknoten, insbesondere durch eine Registrierungsstelle RA, die eine Zertifikatsanforderungsnachricht nach einer Prüfung des Nachrichteninhalts an einen Zertifikatsaussteller CA weiterleitet. Der kryptographische Mandanten-Identifier bzw. Mandantenidentifikator ist in den ausgestellten Zertifikaten enthalten oder referenziert, die für diesen Mandanten angefordert werden. Er kann in dem Namen CN (siehe Figur 2) des ausgestellten Zertifikats und/oder in dem Namen eines Mandanten-SubCA-Zertifikats enthalten sein. Dadurch kann ein Mandant nur Zertifikate anfordern, die auch tatsächlich ihm (d.h. seinem kryptographischen Mandanten-Identifier) zugeordnet sind. Dabei kann geprüft werden, ob eine Zertifikatsanforderung den passenden kryptographischen Mandanten-Identifier enthält. Nur falls dies der Fall ist, wird das Zertifikat von Zertifikatsaussteller CA ausgestellt, d.h. die Zertifikatsanforderungsnachricht digital von Zertifikatsaussteller CA signiert bzw. ein entsprechend der Zertifikatsanforderungsnachricht CSR gebildetes Zertifikat CERT durch den Zertifikatsaussteller CA digital signiert. Es kann die Zertifikatsanforderungsnachricht auch - wie in Figur 2 angedeutet - modifiziert werden, indem der passende kryptographische Mandanten-Identifier eingetragen wird.

Zusammenfassend sind folgende Ausführungsformen möglich:

- Die Zertifikatsanfragenachricht kann mit dem privaten Mandantenkey digital signiert sein. Die Signatur ist mit dem öffentlichen Mandantenkey überprüfbar. Die Signatur kann durch den anfragenden Client, einen Zertifikatsmanagement-Proxy oder durch eine Registrierungsstelle RA erfolgen.

- Die Zertifikatsanfragenachricht kann zweifach digital signiert sein, einmal mit dem privaten Schlüssel des anfragenden Clients bzw. Benutzer (d.h. mit dem privaten Schlüssel, dessen zugeordneter öffentlicher Schlüssel PK durch das Zertifikat bestätigt werden soll), und einmal mit dem privaten Mandantenschlüssel. Für die digitale Signatur kann z.B. das Re-Signieren einer Zertifizierungsanfrage aus einem CMP-Protokoll (Certificate Management Protocol, IETF Standard RFC 4210)) genutzt werden.

- Bei der Nutzung einer authentisierten Kommunikationsverbindung zur Übermittlung der Zertifizierungsanfrage ist beispielsweise die Nutzung von EST (Enrollment over Secure Transport, IETF Standard RFC 7030) möglich. Hierbei wird eine TLS-Verbindung (Transport Layer Security, IETF Standard RFC 5246) zur Registrierungsstelle RA aufgebaut, die die Zertifizierungsanfrage des Anfragestellers prüft und autorisiert. Eine weitere TLS Verbindung wird von der RA zur ausstellenden CA aufgebaut, in der der private Mandantenschlüssel und ein Zertifikat des zugehörigen Mandanten zur Authentisierung genutzt wird. Ein den öffentlichen Mandantenschlüssel enthaltendes Zertifikat kann beispielsweise die Key Usage extension id-kp-cmcRA gesetzt haben.

Ein Mandant kann weitere öffentliche Schlüssel hinterlegen, die dem öffentlichen Mandantenschlüssel zugeordnet sind. Dann können Zertifikatsanforderungen dieses Mandanten auch mit den weiteren zugeordneten öffentlichen Schlüssel geschützt werden. Diese Anwendung ist flexibel.

Ein Zertifikat kann z.B. nur dann durch die CA ausgestellt (d.h. eine dem Inhalt des CSR entsprechende Datenstruktur signiert), wenn die Anfragenachricht einen Mandanten-Identifier entsprechendes Feld bereits enthält. Alternativ kann die CA diese Information auch aus dem öffentlichen Mandantenschlüssel (Zertifikat) ermitteln.

Der kryptographische Mandanten-Identifier kann grundsätzlich in ein beliebiges Attribut eines Zertifikats codiert bzw. eingefügt sein, z.B. Common Name CN - wie in Figur 3 gezeigt - , Organizational Unit (OU) oder AltName. Sie kann auch implizit enthalten (referenziert) sein, wenn das ausgestellte Zertifikat durch ein SubCA-Zertifikat (Sub)CA-CERT (siehe gestrichelt angedeutet in Figur 3) geschützt ist, das den kryptographischen Mandanten-Identifier M-ID enthält.

Vorzugsweise wird der Name im Zertifikat nicht nur abhängig von dem öffentlichen Schlüssel des Mandantenschlüssels gebildet, sondern auch abhängig von dem zu bestätigenden öffentlichen Schlüssels PK des Gerät D1, D2 (Device Key). Beispiele für das Bilden des Mandanten-Identifiers:

- ⇨ Konkatenieren der Teile KPUP | PK
- ⇨ H(KPUP | PK)
- ⇨ HMAC(KPUP, PK), wobei HMAC Key-Hashed Message Authentification Code bedeutet.

Vorzugsweise ist der CSR doppelt signiert:

- Mandanten Public Key (KPUP)
- Device Public Key (PK)

Vorzugsweise ist eine Zertifikatserweiterung (Certificate Extension) enthalten, die diese spezielle Art der Zertifikatsausstellung referenziert (über eine CA Policy Extension oder eine separate Certificate Extension).

Das folgende Beispiel zeigt eine solche Erweiterung:

```
id-on-MandantID   OBJECT IDENTIFIER ::= { id-on 3 }
MandantID  ::= SEQUENCE {
     MandantName            Name,
     MandantID              OCTET STRING,
     MandantCert            OCTET STRING OPTIONAL
}
```

Diese Erweiterung sollte im Zertifikat als „kritisch" markiert werden, da damit bei der Validierung immer die Extension auch mit verarbeitet wird. Damit wird sichergestellt, dass nicht nur die Signatur des Zertifikatsausstellers geprüft wird, sondern auch in wessen Auftrag die Zertifikatserstellung erfolgt ist. Über entsprechende Sicherheitsvorgaben (Security Policy) beim Überprüfer ist der Überprüfer damit in der Lage, ausschließlich Zertifikate, die für einen bestimmten Mandanten ausgestellt wurden, zu nutzen.

Der Parameter MandantID kann insbesondere der Hash-Wert (z.B. SHA256, SHA3) des öffentlichen Mandantenschlüssels sein. Der Mandantenidentifikator MandantID kann binär codiert werden oder als Zeichenkette (z.B. als ASCII-String des Hexadezimalwertes).

Die Zertifikatsvalidierung bzw. -prüfung kann wie folgt durchgeführt werden:

- Ermittle die kryptographische MandantID (whitelist), die z.B. explizit konfiguriert oder implizit aus einem eigenen Zertifikat („gehört die Anfragestelle (peer-node) zum gleichen Mandanten wie der prüfende Knoten bzw. ist der Mandant bekannt und akzeptiert?".
- Wenn ja, dann wird das Zertifikat akzeptiert.

Optional kann zusätzlich ein DNS-Name mit kryptographischem Namensteil entsprechend dem Zertifikat gebildet werden (z.B. für spontanen Web-Service/Dienst bei node.js: ein Knoten kann spontan einen HTTPS-Service aufsetzen für einen Web-Service,

d.h. dass ein zum ausgestellten Zertifikat passender Netzwerkname gebildet wird.)

Obwohl die Erfindung im Detail durch das bevorzugte Ausführungsbeispiel näher illustriert und beschrieben wurde, so ist die Erfindung nicht durch die offenbarten Beispiele eingeschränkt und andere Variationen können vom Fachmann hieraus abgeleitet werden, ohne den Schutzumfang der Erfindung zu verlassen.

Die Implementierung der vorstehend beschriebenen Prozesse oder Verfahrensabläufe kann anhand von Instruktionen erfolgen, die auf computerlesbaren Speichermedien oder in flüchtigen Computerspeichern (im Folgenden zusammenfassend als computerlesbare Speicher bezeichnet) vorliegen. Computerlesbare Speicher sind beispielsweise flüchtige Speicher wie Caches, Puffer oder RAM sowie nichtflüchtige Speicher wie Wechseldatenträger, Festplatten, usw.

Die vorstehend beschriebenen Funktionen oder Schritte können dabei in Form zumindest eines Instruktionssatzes in/auf einem computerlesbaren Speicher vorliegen. Die Funktionen oder Schritte sind dabei nicht an einen bestimmten Instruktionssatz oder an eine bestimmte Form von Instruktionssätzen oder an ein bestimmtes Speichermedium oder an einen bestimmten Prozessor oder an bestimmte Ausführungsschemata gebunden und können durch Software, Firmware, Microcode, Hardware, Prozessoren, integrierte Schaltungen usw. im Alleinbetrieb oder in beliebiger Kombination ausgeführt werden. Dabei können verschiedenste Verarbeitungsstrategien zum Einsatz kommen, beispielsweise serielle Verarbeitung durch einen einzelnen Prozessor oder Multiprocessing oder Multitasking oder Parallelverarbeitung usw.

Die Instruktionen können in lokalen Speichern abgelegt sein, es ist aber auch möglich, die Instruktionen auf einem entfernten System abzulegen und darauf via Netzwerk zuzugreifen.

Das Gerät oder auch die Vorrichtung können jeweils ein oder mehrere Prozessoren aufweisen. Der Begriff "Prozessor", "zentrale Signalverarbeitung", "Steuereinheit" oder "Datenauswertemittel", umfasst Verarbeitungsmittel im weitesten Sinne, also beispielsweise Server, Universalprozessoren, Grafikprozessoren, digitale Signalprozessoren, anwendungsspezifische integrierte Schaltungen (ASICs), programmierbare Logikschaltungen wie FPGAs, diskrete analoge oder digitale Schaltungen und beliebige Kombinationen davon, einschließlich aller anderen dem Fachmann bekannten oder in Zukunft entwickelten Verarbeitungsmittel. Prozessoren können dabei aus einer oder mehreren Vorrichtungen bzw. Einrichtungen bzw. Einheiten bestehen. Besteht ein Prozessor aus mehreren Vorrichtungen, können diese zur parallelen oder sequentiellen Verarbeitung bzw. Ausführung von Instruktionen ausgelegt bzw. konfiguriert sein.

Patentansprüche

1. Verfahren zum Ausstellen einer kryptographisch geschützten Authentizitätsbescheinigung (CERT) für einen Benutzer (B1, B2, B3), aufweisend folgende Schritte:
- Bereitstellen eines öffentlichen Benutzerschlüssels,

- Bereitstellen eines öffentlichen Mandantenschlüssels für einen Mandanten, der dem Benutzer zugeordnet wird,

- Bilden einer Anfrage (CSR), die den öffentlichen Benutzerschlüssel enthält und mit Hilfe eines dem bereitgestellten öffentlichen Mandantenschlüssel zugeordneten privaten Mandantenschlüssels geschützt und/oder digital signiert wird, und
- Ausstellen einer kryptographisch geschützten Authentizitätsbescheinigung, die den öffentlichen Benutzerschlüssel enthält und den Mandanten identifiziert, dadurch gekennzeichnet, dass die kryptographisch geschützten Authentizitätsbescheinigung einen kryptographischen Mandantenidentifikator (M-ID) enthält oder referenziert, der abhängig vom öffentlichen Mandantenschlüssel gebildet wird.

2. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die Anfrage einen vom öffentlichen Mandantenschlüssel abhängigen Mandantenidentifikator enthält.

3. Verfahren nach einem der vorhergehenden Ansprüche 1 oder 2, dadurch gekennzeichnet, dass der Mandantenidentifikator aus dem Hashwert des öffentlichen Mandantenschlüssels gebildet wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Anfrage zum Ausstellen der kryptographisch geschützten Authentizitätsbescheinigung nach einer Authentifizierung des Benutzers gebildet und/oder übertragen wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Anfrage über eine mit Hilfe einer Mandantenkennung oder mit Hilfe des gebildeten Mandantenidentifikators authentisierte Kommunikationsverbindung übertragen wird.

6. Vorrichtung (CA) zum Ausstellen einer kryptographisch geschützten Authentizitätsbescheinigung für einen Benutzer mit Hilfe eines bereitgestellten öffentlichen Benutzerschlüssels, aufweisend:
- eine Bestätigungseinheit, die dazu ausgelegt ist, eine kryptographisch geschützte Authentizitätsbescheinigung auszustellen, die den öffentlichen Benutzerschlüssel enthält und den Mandanten identifiziert, wobei sie die Zugehörigkeit einer vorherigen Authentizitätsbescheinigungsanfrage zum Mandanten bestätigt, dadurch gekennzeichnet, dass die den Mandanten identifizierende Authentizitätsbescheinigung einen kryptographischen Mandantenidentifikator enthält oder referenziert, der abhängig vom Mandantenschlüssel bildbar ist.

7. Vorrichtung (RA) zum Ausstellen einer kryptographisch geschützten Authentizitätsbescheinigung für einen Benutzer, aufweisend:
- eine Bereitstellungseinheit, die dazu ausgelegt ist, einen öffentlichen Mandantenschlüssel für einen Mandanten bereitzustellen, der dem Benutzer zugeordnet wird,
und
- eine Erzeugungseinheit, die dazu ausgelegt ist, eine Anfrage zum Ausstellen der kryptographisch geschützten Authentizitätsbescheinigung zu bilden, wobei die Anfrage, die einen öffentlichen Benutzerschlüssel für den Benutzer enthält, mit Hilfe des dem bereitgestellten öffentlichen Mandantenschlüssels zugeordneten privaten Mandantenschlüssels geschützt und/oder digital signiert wird und wobei die Anfrage einen vom öffentlichen Mandatenschlüssel abhängigen Mandantenidentifikator enthält.

8. Vorrichtung nach dem vorhergehenden Anspruch 7, dadurch gekennzeichnet, dass der Mandantenidentifikator aus dem Hashwert des öffentlichen Mandantenschlüssels bildbar ist.

9. Vorrichtung nach einem der vorhergehenden Ansprüche 7 oder 8, dadurch gekennzeichnet, dass die Anfrage zum Ausstellen der kryptographisch geschützten Authentizitätsbescheinigung nach einer Authentifizierung des Benutzers bildbar und/oder übertragbar ist.

10. Vorrichtung nach einem der vorhergehenden Ansprüche 7 bis 9, dadurch gekennzeichnet, dass die Anfrage über eine mit Hilfe einer Mandantenkennung oder mit Hilfe des gebildeten Mandantenidentifikators authentisierte Kommunikationsverbindung übertragbar ist.

11. Computerprogrammprodukt, das direkt in einen Speicher eines oder mehrerer digitaler Prozessoren ladbar ist, umfassend Programmcodeteile, die dazu geeignet sind, die Schritte des Verfahrens nach einem der vorhergehenden Verfahrensansprüche durchzuführen.

FIG 1

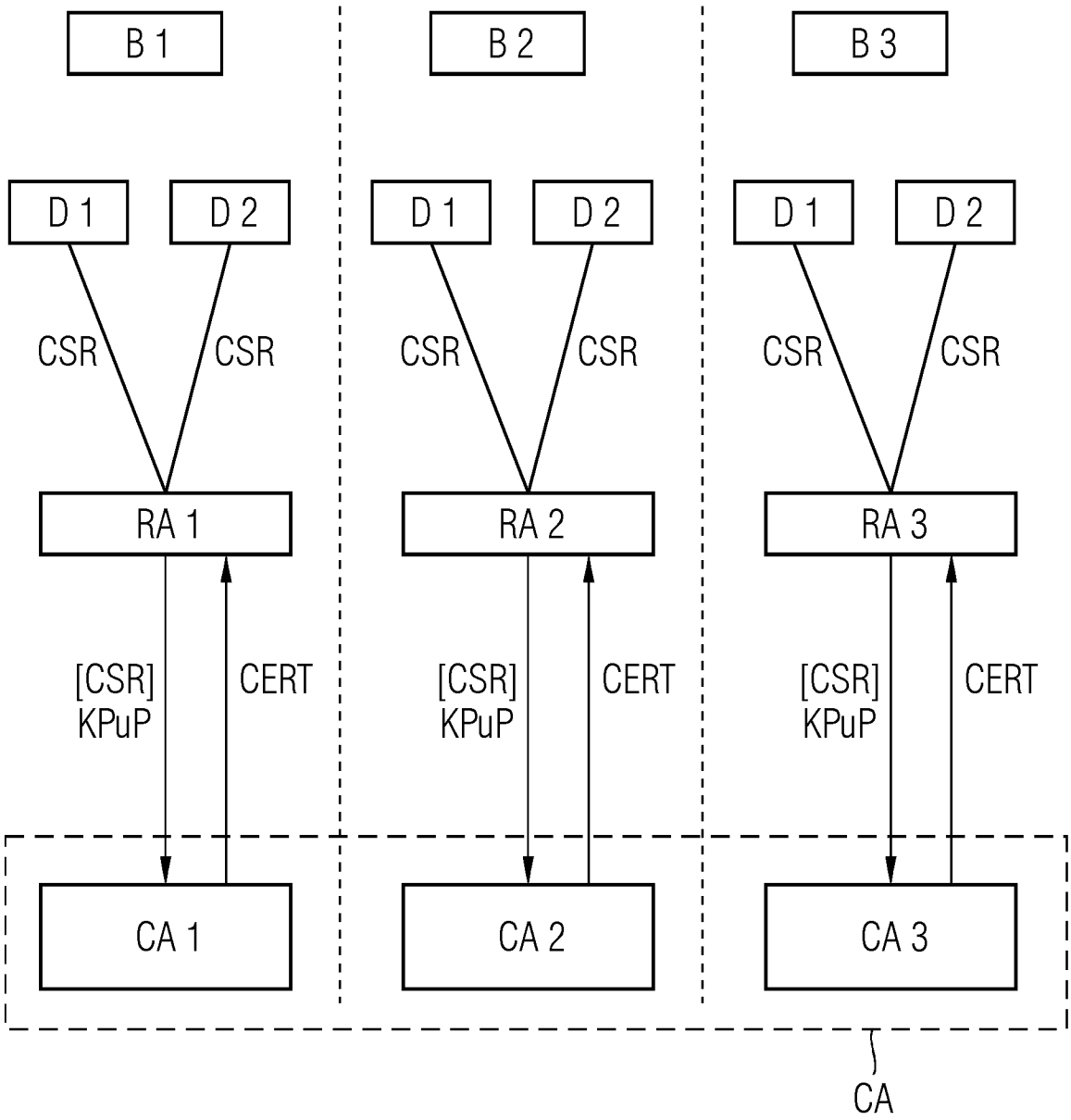

B 1
B 2
B 3
D 1
D 2
D 1
D 2
D 1
D 2
CSR
CSR
CSR
CSR
CSR
CSR
RA 1
RA 2
RA 3
[CSR]
KPuP
CERT
[CSR]
KPuP
CERT
[CSR]
KPuP
CERT
CA 1
CA 2
CA 3
CA

FIG 2

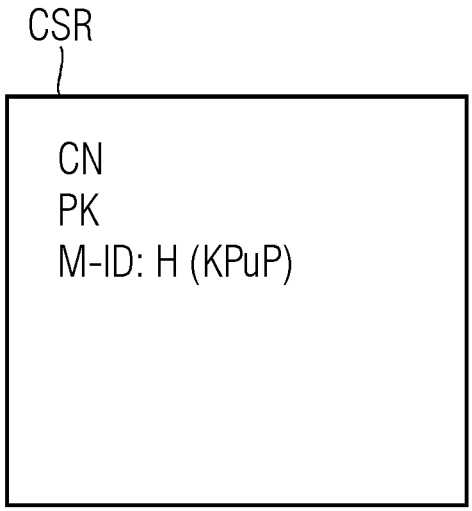
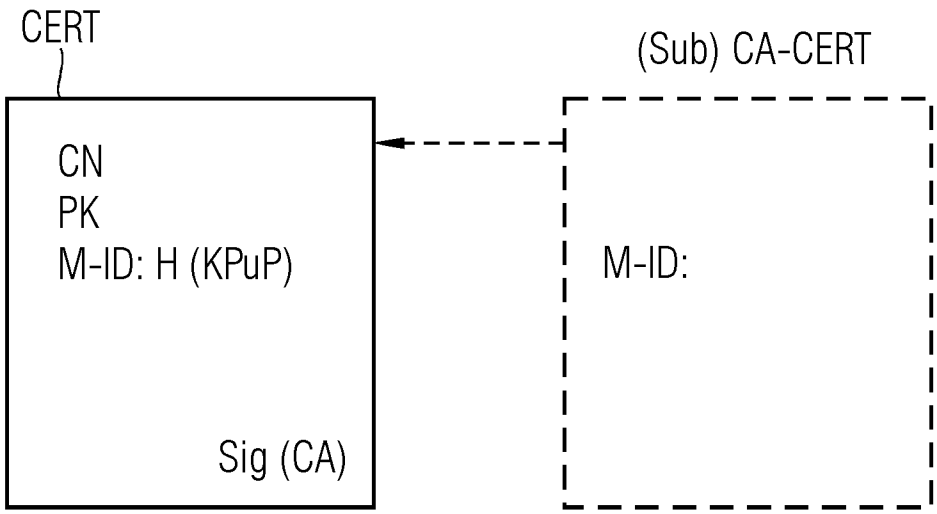


FIG 3



INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2020/057276

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 102013203101 A1 (SIEMENS AG [DE]) 28 August 2014 (2014-08-28) paragraph [0005]; figure 1 paragraph [0026] - paragraph [0040]; figure 3	1-11
A	DE 102015101014 A1 (BUNDESDRUCKEREI GMBH [DE]) 28 July 2016 (2016-07-28) paragraph [0004]	4,9

☐ Further documents are listed in the continuation of Box C.

☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 June 2020	**13 July 2020**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Vinck, Bart** Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2020/057276

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
DE 102013203101 A1	28 August 2014	DE 102013203101 A1	28 August 2014
		EP 2770467 A1	27 August 2014
		US 2014245409 A1	28 August 2014
DE 102015101014 A1	28 July 2016	DE 102015101014 A1	28 July 2016
		EP 3248357 A1	29 November 2017
		WO 2016116392 A1	28 July 2016

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2020/057276

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 10 2013 203101 A1 (SIEMENS AG [DE]) 28. August 2014 (2014-08-28) Absatz [0005]; Abbildung 1 Absatz [0026] - Absatz [0040]; Abbildung 3	1-11
A	DE 10 2015 101014 A1 (BUNDESDRUCKEREI GMBH [DE]) 28. Juli 2016 (2016-07-28) Absatz [0004]	4,9

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
4. Juni 2020	13/07/2020

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Vinck, Bart

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2020/057276

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102013203101 A1	28-08-2014	DE 102013203101 A1	28-08-2014
		EP 2770467 A1	27-08-2014
		US 2014245409 A1	28-08-2014
DE 102015101014 A1	28-07-2016	DE 102015101014 A1	28-07-2016
		EP 3248357 A1	29-11-2017
		WO 2016116392 A1	28-07-2016