(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
25. Juni 2020 (25.06.2020)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2020/126923 A1

(51) Internationale Patentklassifikation:
*H04L 29/06* (2006.01) *H04L 29/08* (2006.01)
*G06F 21/44* (2013.01) *H04W 4/70* (2018.01)
*G06F 21/60* (2013.01) *H04W 12/00* (2009.01)

(21) Internationales Aktenzeichen: PCT/EP2019/085122

(22) Internationales Anmeldedatum:
13. Dezember 2019 (13.12.2019)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2018 222 464.1
20. Dezember 2018 (20.12.2018) DE

(71) Anmelder: **ROBERT BOSCH GMBH** [DE/DE]; Postfach 30 02 20, 70442 Stuttgart (DE).

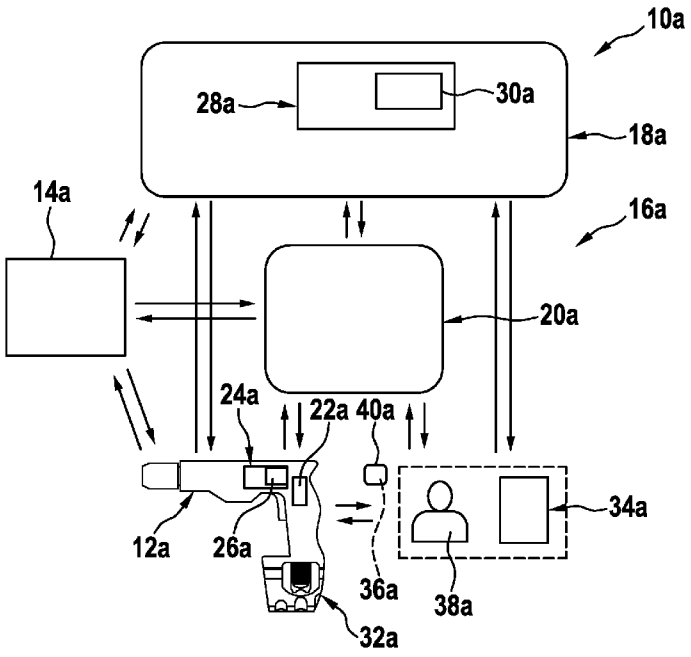
(72) Erfinder: **BERNING, Sebastian**; Ahornstr. 18, 70597 Stuttgart (DE). **ALTUN, Cankal**; Stoefflerweg 28, 70567 Stuttgart (DE).

(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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) **Title:** METHOD FOR COMMUNICATION BETWEEN MACHINE TOOLS IN A NETWORK

(54) **Bezeichnung:** VERFAHREN ZUR KOMMUNIKATION VON WERKZEUGMASCHINEN IN EINEM NETZWERK

**Fig. 1**




(57) **Abstract:** The invention relates to a method for communication between machine tools in a network using asymmetrical cryptography, in particular using a public key infrastructure. In at least one method step (58a), a data packet is encrypted and/or decrypted by means of at least one communication unit (22a; 22b; 22c; 22d; 22e) and/or at least one control and/or regulating unit (24a; 24b; 24c; 24d; 24e), in particular using at least one cryptoprocessor (26a; 26b; 26c; 26d; 26e), of at least one machine tool (12a; 12b; 12c; 12d; 12e) via a public key function (82a; 82b; 82c; 82d; 82e) and/or a private key function (84a; 84b; 84c; 84d; 84e), in particular a key function which is specific to the machine tool, during a data transmission and/or authentication of the at least one machine tool (12a; 12b; 12c; 12d; 12e) by means of a server unit (18a; 18b; 18c; 18d; 18e), at least one additional machine tool (12a; 12b; 12c; 12d; 12e),

WO 2020/126923 A1

*[Fortsetzung auf der nächsten Seite]*

**(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, 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)*

and/or at least one external unit (34a; 34b; 34c; 34d; 34e) via a network unit (20a; 20b; 20c; 20d; 20e).

**(57) Zusammenfassung:** Die Erfindung geht aus von einem Verfahren zur Kommunikation von Werkzeugmaschinen in einem Netzwerkmittels asymmetrischer Kryptografie,insbesondere mittels einer Public-Key-Infrastruktur. Es wird vorgeschlagen, dass in zumindest einem Verfahrensschritt (58a) bei einer Datenübertragung und/oder einer Authentifizierung zumindest einer Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) über eine Netzwerkeinheit (20a; 20b; 20c; 20d; 20e) mit einer Servereinheit (18a; 18b; 18c; 18d; 18e), zumindest einer weiteren Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) und/oder zumindest einer externen Einheit (34a; 34b; 34c; 34d; 34e) ein Datenpaket mittelszumindest einer Kommunikationseinheit (22a; 22b; 22c; 22d; 22e) und/oder zumindest einer Steuer-und/oder Regeleinheit (24a; 24b; 24c; 24d; 24e), insbesondere mittels zumindest eines Krypto-Prozessors(26a; 26b; 26c; 26d; 26e), der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) über eine, insbesondere werkzeugmaschinenspezifische, öffentliche Schlüsselfunktion (82a; 82b; 82c; 82d; 82e) und/oder private Schlüsselfunktion (84a; 84b; 84c; 84d; 84e) verschlüsselt und/oder entschlüsselt wird.

Beschreibung

Verfahren zur Kommunikation von Werkzeugmaschinen in einem Netzwerk

Stand der Technik

In US 2017/0364360 A1 ist bereits ein Verfahren zur Kommunikation von Werkzeugmaschinen mittels asymmetrischer Kryptografie vorgeschlagen worden.

Offenbarung der Erfindung

Die Erfindung geht aus von einem Verfahren zur Kommunikation von Werkzeugmaschinen in einem Netzwerk mittels asymmetrischer Kryptografie, insbesondere mittels einer Public-Key-Infrastruktur.

Es wird vorgeschlagen, dass in zumindest einem Verfahrensschritt bei einer Datenübertragung und/oder einer Authentifizierung zumindest einer Werkzeugmaschine über eine Netzwerkeinheit mit einer Servereinheit, zumindest einer weiteren Werkzeugmaschine und/oder zumindest einer externen Einheit ein Datenpaket mittels zumindest einer Kommunikationseinheit und/oder zumindest einer Steuer- und/oder Regeleinheit, insbesondere mittels zumindest eines Krypto-Prozessor, der Werkzeugmaschine über eine, insbesondere werkzeugmaschinenspezifische, öffentliche Schlüsselfunktion und/oder private Schlüsselfunktion verschlüsselt und/oder entschlüsselt wird.

Vorzugsweise ist das Verfahren dazu eingerichtet, die Kommunikation der Werkzeugmaschinen in dem Netzwerk, insbesondere gegen äußere und/oder unbefugte Eingriffe, zu sichern. Unter „asymmetrischer Kryptografie“ soll insbesondere

eine Verschlüsselungsmethode für zwischen zwei Identitäten zu kommunizierenden Daten verstanden werden, wobei jede Identität jeweils unterschiedliche Informationen für eine Verschlüsselung und/oder eine Entschlüsselung der Daten aufweist. Unter einer „Public-Key-Infrastruktur" soll insbesondere eine Verschlüsselungsmethode verstanden werden, welche auf der asymmetrischen Kryptografie basiert, wobei zu einer als Empfänger von Daten eingerichteten Identität jeweils zumindest ein privater Schlüssel und zumindest ein öffentlicher Schlüssel existiert und wobei der öffentliche Schlüssel dazu eingerichtet ist, Daten zu verschlüsseln und der private Schlüssel dazu eingerichtet ist, die mit dem öffentlichen Schlüssel verschlüsselten Daten zu entschlüsseln. Unter „eingerichtet" soll insbesondere speziell programmiert, speziell ausgelegt und/oder speziell ausgestattet verstanden werden. Darunter, dass ein Objekt zu einer bestimmten Funktion eingerichtet ist, soll insbesondere verstanden werden, dass das Objekt diese bestimmte Funktion in zumindest einem Anwendungs- und/oder Betriebszustand erfüllt und/oder ausführt. Beispielsweise erfolgt eine Authentifizierung der Werkzeugmaschine in zumindest einem Verfahrensschritt insbesondere bei einer Inbetriebnahme der Werkzeugmaschine, bei einer Verwendung einer Werkzeugmaschine mit einer Sperr- und/oder Diebstahlsicherungsfunktion, bei einer Verwendung einer Werkzeugüberwachungsfunktion der Werkzeugmaschine, bei einer Benutzerkontenverwaltung der Werkzeugmaschine o. dgl. Bevorzugterweise ist das Netzwerk als ein Intranet als ein Internet, als ein Bluetooth-, VLC-, NFC-, LAN-, USB-, WPAN-, WUSB-, Powerline-, CAN Bus- und/oder ein anderes, einem Fachmann bekanntes Netzwerk o. dgl. ausgebildet. Vorzugsweise ist die Netzwerkeinheit beispielsweise als ein Router, als ein Modem, als ein LAN-Switch, als ein Gateway o. dgl. ausgebildet. Bevorzugt wird über die Servereinheit die Kommunikation, insbesondere eine Authentifizierung und/oder eine Datenübertragung, der Werkzeugmaschine mit der Servereinheit und/oder der weiteren Werkzeugmaschine verwaltet. Vorzugsweise erfolgen/erfolgt eine Authentifizierung und/oder eine Datenübertragung der Werkzeugmaschine durch/an die Servereinheit über eine Verbindung der Werkzeugmaschine mit der Servereinheit über die Netzwerkeinheit. Es ist aber auch denkbar, dass eine Authentifizierung und/oder eine Datenübertragung der Werkzeugmaschine direkt durch/an die Servereinheit erfolgen/erfolgt.

Unter einer „Steuer- und/oder Regeleinheit“ soll insbesondere eine Einheit mit zumindest einer Steuerelektronik verstanden werden. Unter einer „Steuerelektronik“ soll insbesondere eine Einheit mit einer Prozessoreinheit und mit einer Speichereinheit sowie mit einem in der Speichereinheit gespeicherten Betriebsprogramm verstanden werden. Unter einem „Krypto-Prozessor“ soll insbesondere eine Einheit verstanden werden, die zumindest einen Mikroprozessor umfasst und welche dazu eingerichtet ist, Grundfunktionen einer mittels Kryptografie gesicherten Datenkommunikation, insbesondere beispielsweise eine Authentifizierung, kryptografische Algorithmen, eine Verwaltung von Kryptologie-Schlüsseln und/oder Netzwerkprotokollen o. dgl., auszuführen. Vorzugsweise sind/ist die Steuer- und/oder Regeleinheit und/oder der Krypto-Prozessor zumindest im Wesentlichen manipulationssicher ausgebildet. Darunter dass eine elektronische Einheit, insbesondere die Steuer- und/oder Regeleinheit und/oder der Krypto-Prozessor, „zumindest im Wesentlichen manipulationssicher ausgebildet“ sind, soll insbesondere verstanden werden, dass die Einheit derart ausgebildet ist, dass ein unbefugter, insbesondere physischer und/oder digitaler, Eingriff zur Änderung zumindest eines Betriebsparameters der Einheit, insbesondere einen Programmierbefehl und/oder einen Befehlsparameter der Steuer- und/oder Regeleinheit und/oder des Krypto-Prozessors, zumindest erschwert wird. Vorzugsweise weisen/weist die Steuer- und/oder Regeleinheit und/oder der Krypto-Prozessor fest belegte Schnittstellen zu anderen Bauteilen auf, wobei ein Anschließen eines externen Geräts zumindest erschwert wird.

Vorzugsweise sind/ist die öffentliche und/oder private Schlüsselfunktion als eine, insbesondere digitale, Information ausgebildet, die dazu eingerichtet ist, einen kryptografischen Algorithmus zu parametrisieren. Besonders bevorzugt sind/ist die öffentliche und/oder private Schlüsselfunktion als eine Bitfolge ausgebildet. Vorzugsweise wird in zumindest einem Verfahrensschritt die öffentliche und/oder private Schlüsselfunktion der Werkzeugmaschine mittels der Servereinheit zugeordnet. Bevorzugt ist die öffentliche Schlüsselfunktion dazu eingerichtet, das Datenpaket zu verschlüsseln. Vorzugsweise ist die private Schlüsselfunktion dazu eingerichtet, ein mittels der korrespondiert ausgebildeten öffentlichen Schlüsselfunktion verschlüsselte Datenpaket zu entschlüsseln. Bevorzugt erfolgt ein Entschlüsseln des Datenpakets mittels einer Komponente, insbesondere der/einer Steuer- und/oder Regeleinheit, der Werkzeugmaschine oder der Servereinheit,

der die private und öffentliche Schlüsselfunktion zugeordnet ist. Vorteilhafterweise ist das zu verschlüsselnde und/oder zu entschlüsselnde Datenpaket als eine Authentifikationsabfrage, als eine werkzeugspezifische und/oder betriebssystemrelevante Datei o. dgl. ausgebildet. Besonders bevorzugt erfolgt in zumindest einem Verfahrensschritt eine Authentifizierung der Werkzeugmaschine mittels der Kommunikationseinheit und/oder der Steuer- und/oder Regeleinheit, insbesondere mittels des Krypto-Prozessors, der Werkzeugmaschine vor einer Datenübertragung. Vorzugsweise umfasst die Servereinheit zumindest eine Überwachungsfunktion, die dazu eingerichtet ist, ein Gerät, insbesondere die Werkzeugmaschine, in dem Netzwerk zu erfassen und/oder das Netzwerk periodisch oder kontinuierlich auf Geräte, insbesondere Werkzeugmaschinen, zu überprüfen. Bevorzugterweise erfolgt eine Authentifizierung der Geräte, insbesondere der Werkzeugmaschine in Abhängigkeit von einem Referenzzeitintervall, über den sich die erfasste Werkzeugmaschine in dem Netzwerk befindet. Bevorzugterweise wird mittels der Servereinheit, insbesondere über die Netzwerkeinheit, bei einer Überschreitung des Referenzzeitintervalls durch eine Aufenthaltsdauer der Werkzeugmaschine im Netzwerk eine Authentifizierungsanfrage an die Werkzeugmaschine gesendet. Es ist denkbar, dass in zumindest einem Verfahrensschritt die Authentifizierungsanfrage der Servereinheit einem Benutzer der Werkzeugmaschine, insbesondere über eine Ausgabeeinheit der Werkzeugmaschine, ausgegeben wird. Vorzugsweise wird bei oder nach einer erfolgreichen Authentifizierung der Werkzeugmaschine im Netzwerk einem Benutzer über die Ausgabeeinheit ein optisches, haptisches und/oder akustisches Signal ausgegeben.

Durch die erfindungsgemäße Ausgestaltung des Verfahrens kann eine vorteilhaft sichere Kommunikation zwischen mehreren Werkzeugmaschinen und/oder einer Werkzeugmaschine und einer Servereinheit ermöglicht werden. Es kann eine vorteilhaft hohe Flexibilität ermöglicht werden, insbesondere da eine sichere Kommunikation unabhängig von verwendeten Übertragungskanälen erfolgen kann. Durch die erfindungsgemäße Ausgestaltung kann eine vorteilhaft hohe Geheimhaltung eines Datenpakets ermöglicht werden. Es kann eine vorteilhaft genaue und einfache Zuordnung von Werkzeugmaschinen im Netzwerk erfolgen.

Des Weiteren wird vorgeschlagen, dass in zumindest einem Verfahrensschritt der Werkzeugmaschine mittels der Servereinheit genau eine werkzeugmaschinenspezifische Kenngröße, die öffentliche Schlüsselfunktion und die private Schlüsselfunktion zugeordnet und übertragen werden, wobei die werkzeugmaschinenspezifische Kenngröße, die öffentliche Schlüsselfunktion und die private Schlüsselfunktion in zumindest einer Speichereinheit der Werkzeugmaschine hinterlegt werden. Bevorzugt ist die werkzeugmaschinenspezifische Kenngröße als eine Bitfolge, als eine Nummernfolge, als eine Wortfolge o. dgl. ausgebildet. Es ist auch denkbar, dass die werkzeugmaschinenspezifische Kenngröße als eine Kombination von zumindest einer Wortfolge und zumindest einer Nummernfolge o. dgl. ausgebildet ist. Vorteilhafterweise wird die öffentliche Schlüsselfunktion mittels der Servereinheit der werkzeugspezifischen Kenngröße zugeordnet und in der Servereinheit, insbesondere einer Speichereinheit der Servereinheit, hinterlegt. Vorzugsweise erfolgt in zumindest einem Verfahrensschritt bei einer Verschlüsselung des Datenpakets mittels der Steuer- und/oder Regeleinheit, insbesondere dem Krypto-Prozessor, eine Signatur des Datenpakets mit der werkzeugmaschinenspezifischen Kenngröße. Bevorzugt wird bei der Signatur des Datenpakets mittels der Steuer- und/oder Regeleinheit die werkzeugmaschinenspezifische Kenngröße dem, insbesondere verschlüsselten Datenpaket hinzugefügt. Besonders bevorzugt wird in zumindest einem Verfahrensschritt mittels der Servereinheit eine weitere öffentliche Schlüsselfunktion der Servereinheit an die Werkzeugmaschine übertragen und in der Speichereinheit der Werkzeugmaschine hinterlegt. Vorzugsweise wird in zumindest einem Verfahrensschritt ein Datenpaket mittels der Steuer- und/oder Regeleinheit, insbesondere dem Krypto-Prozessor, über die weitere öffentliche Schlüsselfunktion verschlüsselt und, insbesondere über die Netzwerkeinheit, an die Servereinheit übertragen. Vorteilhafterweise erfolgt eine Übertragung der weiteren öffentlichen Schlüsselfunktion der Servereinheit an die Werkzeugmaschine, die Netzwerkeinheit und/oder die weitere Werkzeugmaschine vor oder während einer Authentifizierung der Werkzeugmaschine und/oder der weiteren Werkzeugmaschine durch die Servereinheit in dem Netzwerk. Bevorzugt erfolgen/erfolgt eine Zuordnung und/oder eine Übertragung der werkzeugmaschinenspezifischen Kenngröße, der öffentlichen Schlüsselfunktion und der privaten Schlüsselfunktion mittels der Servereinheit während oder nach einem Herstellungsprozess der Werkzeugmaschine. Bevorzugterweise wird die öffentliche Schlüsselfunktion der Werkzeugmaschine vor oder während

einer Authentifizierung der Werkzeugmaschine durch die Servereinheit in dem Netzwerk an die Servereinheit, die Netzwerkeinheit und/oder die weitere Werkzeugmaschine übertragen. Durch die erfindungsgemäße Ausgestaltung des Verfahrens kann eine vorteilhaft genaue und einfache Zuordnung von Datenpaketen und Werkzeugmaschinen im Netzwerk erfolgen. Durch die erfindungsgemäße Ausgestaltung kann eine vorteilhaft sichere Kommunikation erreicht werden, insbesondere da Datenpakete werkzeugmaschinenspezifisch verschlüsselt und/oder entschlüsselt werden können.

Zudem wird vorgeschlagen, dass in zumindest einem Verfahrensschritt mittels der Servereinheit und/oder der externen Einheit zumindest ein digitales Zertifikat generiert wird, welches zumindest eine werkzeugmaschinenspezifische Kenngröße, die öffentliche Schlüsselfunktion, die private Schlüsselfunktion und/oder zumindest eine Benutzerinformation umfasst und in der Speichereinheit der Werkzeugmaschine hinterlegt wird. Vorzugsweise erfolgt in zumindest einem Verfahrensschritt mittels der Servereinheit eine Authentifizierung der Werkzeugmaschine über eine Überprüfung des digitalen Zertifikats, wobei zumindest eine Komponente des digitalen Zertifikats mittels der Servereinheit mit zumindest einem in der Servereinheit hinterlegten Referenzwert der Komponente verglichen wird. Bevorzugt ist das digitale Zertifikat als eine Bitfolge, als ein Datensatz o. dgl. ausgebildet. Es ist denkbar, dass das digitale Zertifikat, insbesondere bei einer Authentifizierung, mittels der Servereinheit und/oder der Werkzeugmaschine über eine kryptografische Schlüsselfunktion, insbesondere der Servereinheit, verschlüsselt und/oder entschlüsselt wird. Alternativ oder zusätzlich ist denkbar, dass in zumindest einem Verfahrensschritt in der Speichereinheit der Werkzeugmaschine eine Vielzahl von digitalen Zertifikaten hinterlegt werden, insbesondere zur Authentifizierung der Werkzeugmaschine mit einer Vielzahl von Servereinheiten, Netzwerkeinheiten, anderen Werkzeugmaschinen und/oder externen Einheiten, insbesondere zur Kommunikation der Werkzeugmaschine mit Einheiten in einer Vielzahl von Netzwerken. Vorzugsweise erfolgt eine Generierung des digitalen Zertifikats mittels der Servereinheit und/oder der externen Einheit während oder nach einem Herstellungsprozess der Werkzeugmaschine oder bei oder vor einer Authentifizierung der Werkzeugmaschine durch die Servereinheit in dem Netzwerk. Durch die erfindungsgemäße Ausgestaltung des Verfahrens kann eine vorteilhaft einfache und schnelle Authentifizierung in einem Netzwerk erreicht

werden. Es kann ein vorteilhaft geringer Rechenaufwand im Netzwerk, insbesondere der Servereinheit und/oder der Werkzeugmaschine, erreicht werden, da insbesondere zu einer Authentifizierung lediglich das digitale Zertifikat überprüft wird.

Ferner wird vorgeschlagen, dass in zumindest einem Verfahrensschritt mittels der Werkzeugmaschine, der Servereinheit und/oder der externen Einheit zumindest ein digitaler Marker erstellt wird, welcher dazu eingerichtet ist, zumindest einen Benutzer und/oder zumindest eine externe Einheit über die Kommunikationseinheit und/oder die Steuer- und/oder Regeleinheit, insbesondere den Krypto-Prozessor, für zumindest eine Anwendung mit der Werkzeugmaschine und/oder der Servereinheit zu verifizieren. Vorzugsweise erfolgt in zumindest einem Verfahrensschritt vor einer Verwendung der Werkzeugmaschine und/oder der Servereinheit durch einen Benutzer und/oder eine externe Einheit eine Überprüfung des digitalen Markers mittels der Werkzeugmaschine und/oder der Servereinheit. Bevorzugt wird über die Werkzeugmaschine, insbesondere die Ausgabeeinheit der Werkzeugmaschine, und/oder die Servereinheit vor einer Verwendung eine Eingabeaufforderung zur Verfügungsstellung des digitalen Markers ausgegeben. Insbesondere erfolgt die Eingabeaufforderung über zumindest ein haptisches, akustisches und/oder optisches Signal die Ausgabeeinheit der Werkzeugmaschine und/oder eine Ausgabeeinheit der Servereinheit. Vorteilhafterweise ist der digitale Marker als eine Bitfolge, als eine Nummernfolge, als eine Wortfolge o. dgl. ausgebildet. Es ist denkbar, dass der digitale Marker, insbesondere der digitale Marker eines Benutzers, in einer externen Speichereinheit hinterlegt wird. Bevorzugt erfolgt eine Erstellung des digitalen Markers vor oder bei einer ersten Anwendung eines Benutzers und/oder einer externen Einheit mit der Werkzeugmaschine. Vorzugsweise erfolgt eine Erstellung des in der externen Speichereinheit hinterlegten digitalen Markers und die Überprüfung des digitalen Markers über die Werkzeugmaschine und/oder die Servereinheit über zumindest eine Schnittstelle der Werkzeugmaschine und/oder der Servereinheit. Besonders bevorzugt ist die Schnittstelle der Werkzeugmaschine und/oder der Servereinheit zumindest im Wesentlichen manipulationssicher ausgebildet. Vorteilhafterweise ist die externe Speichereinheit zumindest im Wesentlichen manipulationssicher ausgebildet. Durch die erfindungsgemäße Ausgestaltung des Verfahrens kann

eine vorteilhaft einfache und sichere Identitätskontrolle erreicht werden, insbesondere da zu einer Verwendung der Werkzeugmaschine und/oder der Servereinheit lediglich der vorher generierte digitale Marker überprüft werden kann. Es kann eine vorteilhaft hohe Sicherheit ermöglicht werden, insbesondere da eine unbefugte Verwendung von Werkzeugmaschinen vorteilhaft vermieden werden kann.

Des Weiteren wird vorgeschlagen, dass die Datenübertragung und/oder die Authentifizierung der Werkzeugmaschine mit der Netzwerkeinheit, der Servereinheit und/oder der weiteren Werkzeugmaschine über die Kommunikationseinheit und/oder die Steuer- und/oder Regeleinheit, insbesondere den Krypto-Prozessor, mittels zumindest einem auf Transport Layer Security (TLS) basierenden Verschlüsselungsprotokoll gesichert wird. Insbesondere ist das Verschlüsselungsprotokoll als TLS 1.3 und/oder als eine andere, insbesondere aktuellere, einem Fachmann bekannte Version eines Transport Layer Security (TLS)-Protokolls ausgebildet. Besonders bevorzugt erfolgt in zumindest einem Verfahrensschritt die Authentifizierung und/oder die Datenübertragung der Werkzeugmaschine durch die Netzwerkeinheit, die Servereinheit und/oder die weitere Werkzeugmaschine mittels dem auf Transport Layer Security (TLS) basierenden Verschlüsselungsprotokoll und einer vorhergehenden Überprüfung eines digitalen Zertifikats der Werkzeugmaschine, der Netzwerkeinheit, der Servereinheit und/oder der weiteren Werkzeugmaschine. Durch die erfindungsgemäße Ausgestaltung des Verfahrens kann eine vorteilhaft sichere Authentifizierung und/oder Datenübertragung in dem Netzwerk ermöglicht werden. Durch die erfindungsgemäße Ausgestaltung können vorteilhaft sogenannte „Man-in-the-Middle-Angriffe“ vorteilhaft vermieden werden.

Zudem wird vorgeschlagen, dass in zumindest einem Verfahrensschritt über die Kommunikationseinheit und/oder die Steuer- und/oder Regeleinheit, insbesondere den Krypto-Prozessor, zumindest eine Authentifizierung zumindest eines Benutzers und/oder der externen Einheit mit der Werkzeugmaschine, der Netzwerkeinheit und/oder der Servereinheit als Challenge-Response-Authentifizierung erfolgt. Vorzugsweise wird bei der Challenge Response-Authentifizierung dem Benutzer und/oder der externen Einheit eine Aufgabe gestellt, welche zur Authentifizierung mittels zumindest einer Information beantwortet werden muss.

Vorteilhafterweise erfolgt eine Ausgabe der Aufgabe mittels zumindest einem akustischen, haptischen und/oder optischen Signal über die Ausgabeeinheit der Werkzeugmaschine. Es ist auch denkbar, dass die Ausgabe der Aufgabe über die Servereinheit erfolgt. Bevorzugt ist die Information als eine vordefinierte, insbesondere geheime, Information ausgebildet. Vorteilhafterweise wird in zumindest einem Verfahrensschritt, insbesondere vor einer Authentifizierung, die Information an den Benutzer und/oder die externe Einheit, insbesondere verschlüsselt, ausgegeben und/oder übertragen. Alternativ oder zusätzlich ist denkbar, dass die Aufgabe mittels der Servereinheit über zumindest ein statistisches Verfahren ermittelt wird, wobei insbesondere die Information auf einem logischen Prinzip und/oder einem Allgemeinwissen eines Benutzers basiert. Durch die erfindungsgemäße Ausgestaltung des Verfahrens kann eine vorteilhaft einfache und schnelle Authentifizierung im Netzwerk ermöglicht werden.

Ferner wird vorgeschlagen, dass in zumindest einem Verfahrensschritt zu einer Authentifizierung von zumindest einer Werkzeugzubehöreinheit, insbesondere bei einem Verbinden der Werkzeugzubehöreinheit mit der Werkzeugmaschine, mittels der Kommunikationseinheit, der Steuer- und/oder Regeleinheit, insbesondere dem Krypto-Prozessor, und/oder der Servereinheit, insbesondere automatisch, zumindest ein digitales Zertifikat der Werkzeugzubehöreinheit überprüft wird. Vorzugsweise erfolgt die Authentifizierung der Werkzeugzubehöreinheit durch die Servereinheit vor, bei oder nach einem Befestigen und/oder einem Verbinden der Werkzeugzubehöreinheit mit der Werkzeugmaschine. Insbesondere ist die Werkzeugzubehöreinheit als ein Akku, als ein Diagnosewerkzeug, als eine Staubsaugereinheit, als eine Leuchte und/oder eine andere, einem Fachmann bekannte Werkzeugzubehöreinheit für die Werkzeugmaschine ausgebildet. Vorzugsweise wird in zumindest einem Verfahrensschritt, insbesondere bei einer Produktion der Werkzeugmaschine und/oder einer Authentifizierung der Werkzeugmaschine in dem Netzwerk durch die Servereinheit, das digitale Zertifikat der Werkzeugzubehöreinheit in einer Speichereinheit der Werkzeugmaschine hinterlegt. Bevorzugt wird bei einer Authentifizierung der Werkzeugzubehöreinheit durch die Servereinheit zumindest ein elektrisches und/oder elektronisches Signal, insbesondere ein Datenpaket, an die Servereinheit gesendet. Vorzugsweise werden über die Servereinheit, insbesondere die Sensoreinheit der Servereinheit, zumindest alle Werkzeugmaschinen und Werkzeugzubehöreinheiten im

Netzwerk überwacht. Bevorzugterweise wird bei der Authentifizierung der Werkzeugzubehöreinheit zumindest ein Zeitpunkt der Authentifizierung in der Servereinheit hinterlegt und in ein Register der Servereinheit, insbesondere zeitlich, werkzeugzubehörtypspezifisch, nach Relevanz o.dgl., eingeordnet. Insbesondere ist das Register durch einen Benutzer über die Kommunikationseinheit der Werkzeugmaschine und/oder eine Bedieneinheit der Servereinheit abrufbar. Durch die erfindungsgemäße Ausgestaltung des Verfahrens kann eine vorteilhaft genaue Überwachung der Werkzeugmaschinen im Netzwerk ermöglicht werden. Es kann eine vorteilhaft hohe Sicherheit erreicht werden, insbesondere da eine Beeinflussung durch unauthentifizierte Zubehöreinheiten an der Werkzeugmaschine vorteilhaft vermieden werden können. Durch die erfindungsgemäße Ausgestaltung kann eine Überwachung der Werkzeugzubehöreinheiten ermöglicht werden.

Des Weiteren wird vorgeschlagen, dass in zumindest einem Verfahrensschritt über die Netzwerkeinheit und/oder die Servereinheit, insbesondere mittels der öffentlichen Schlüsselfunktion, verschlüsselte betriebssystembezogene Daten an die Werkzeugmaschine übermittelt werden, welche mittels der Kommunikationseinheit und/oder der Steuer- und/oder Regeleinheit, insbesondere dem Krypto-Prozessor, insbesondere mittels der privaten Schlüsselfunktion, entschlüsselt und mit zumindest einer Recheneinheit der Werkzeugmaschine verarbeitet werden. Bevorzugt sind die betriebssystembezogenen Daten als ein Betriebssystemupdate, als eine Änderung von Betriebsparameters o. dgl. ausgebildet. Bevorzugt erfolgt eine Verarbeitung der entschlüsselten betriebssystembezogenen Daten in einem passiven und/oder inaktiven Zustand der Werkzeugmaschine, insbesondere während ein Motor der Werkzeugmaschine deaktiviert ist. Vorzugsweise erfolgt eine Übermittelung der verschlüsselten betriebssystembezogenen Daten durch die Servereinheit an alle Werkzeugmaschinen im Netzwerk, insbesondere zumindest im Wesentlichen zeitgleich. Darunter, dass Ereignisse, insbesondere Datenübermittelungen, „zumindest im Wesentlichen zeitgleich“ erfolgen, soll insbesondere verstanden werden, dass die Ereignisse, insbesondere jeweils ein Startzeitpunkt der Ereignisse, höchstens 60 s, vorzugsweise höchstens 30 s, besonders bevorzugt höchstens 10 s, zeitlich versetzt voneinander stattfinden. Es ist aber auch denkbar, dass die verschlüsselten betriebssystembezogenen Daten bei einer erfolgreichen Authentifizierung der Werkzeugmaschine durch die

Servereinheit an die Werkzeugmaschine übertragen werden. Vorzugsweise erfolgt in zumindest einem Verfahrensschritt eine Übermittlung von Sicherheitskopien des Betriebssystems der Werkzeugmaschine, insbesondere über die Netzwerkeinheit, an die Servereinheit, wobei die Sicherheitskopien des Betriebssystems über die Steuer- und/oder Regeleinheit der Werkzeugmaschine mittels der weiteren öffentlichen Schlüsselfunktion verschlüsselt werden. Bevorzugt werden die verschlüsselten Sicherheitskopien des Betriebssystems der Werkzeugmaschine über die weitere Steuer- und/oder Regeleinheit der Servereinheit mittels der weiteren privaten Schlüsselfunktion entschlüsselt. Es ist denkbar, dass die entschlüsselten Sicherheitskopien des Betriebssystems in zumindest einem Verfahrensschritt mittels eines Abgleichs von Referenzsystemdaten des Betriebssystems über die weitere Steuer- und/oder Regeleinheit der Servereinheit auf eine, insbesondere vergangene, unbefugte Manipulation der Werkzeugmaschine überprüft werden. Vorzugsweise erfolgt bei einer Erkennung einer unbefugten Manipulation der Werkzeugmaschine eine Ausgabe eines haptischen, akustischen und/oder optischen Signals an einen Benutzer und/oder eine Ausgabe eines elektrischen und/oder elektronischen Signals an eine externe Einheit und/oder die Werkzeugmaschine, insbesondere zu einer Deaktivierung der Werkzeugmaschine. Alternativ oder zusätzlich erfolgt bei einer Erkennung einer unbefugten Manipulation der Werkzeugmaschine ein, insbesondere temporärer, Ausschluss der Werkzeugmaschine aus dem Netzwerk, wobei eine Authentifizierung und eine Datenübertragung der Werkzeugmaschine mit anderen Einheiten im Netzwerk unterbunden wird. Durch die erfindungsgemäße Ausgestaltung des Verfahrens kann eine vorteilhaft einfache und sichere Übertragung von Systemupdates ermöglicht werden. Es kann eine vorteilhaft sichere Kommunikation im Netzwerk ermöglicht werden, insbesondere da das Betriebssystem der Werkzeugmaschine über eine sichere Verbindung aktualisiert werden kann.

Zudem wird vorgeschlagen, dass in zumindest einem Verfahrensschritt mittels der Servereinheit zumindest eine weitere öffentliche Schlüsselfunktion, insbesondere die oben beschriebene weitere Schlüsselfunktion, an die Werkzeugmaschine und/oder die Netzwerkeinheit ausgegeben wird, wobei, insbesondere in zumindest einem weiteren Verfahrensschritt, zur Datenübertragung und/oder Authentifizierung der Werkzeugmaschine und/oder der Netzwerkeinheit mit der Ser-

vereinheit zumindest ein Datenpaket mittels der weiteren öffentlichen Schlüsselfunktion verschlüsselt wird und mittels zumindest einer weiteren privaten Schlüsselfunktion von der Servereinheit entschlüsselt wird. Vorzugsweise werden in zumindest einem Verfahrensschritt benutzerbezogene und/oder anwendungsbezogene Datenpakete der Werkzeugmaschine mittels der Steuer- und/oder Regeleinheit, insbesondere periodisch oder kontinuierlich, verschlüsselt an die Servereinheit übertragen. Vorzugsweise werden in zumindest einem Verfahrensschritt von der Werkzeugmaschine und/oder der Netzwerkeinheit zur Servereinheit zu übertragene Datenpakete mittels der Steuer- und/oder Regeleinheit der Werkzeugmaschine mit dem digitalen Zertifikat, insbesondere der werkzeugmaschinenspezifischen Kenngröße, der Werkzeugmaschine signiert. Bevorzugt werden in zumindest einem Verfahren mit der weiteren öffentlichen Schlüsselfunktion verschlüsselte netzwerkbezogene Datenpakete von der Netzwerkeinheit an die Servereinheit übertragen. Durch die erfindungsgemäße Ausgestaltung des Verfahrens kann eine vorteilhaft sichere Authentifizierung und/oder Datenübertragung durch die Servereinheit erreicht werden.

Ferner wird vorgeschlagen, dass in zumindest einem Verfahrensschritt bei der Datenübertragung und/oder der Authentifizierung der Werkzeugmaschine das, insbesondere verschlüsselte, Datenpaket mit zumindest einer, insbesondere der oben beschriebenen, werkzeugmaschinenspezifischen Kenngröße gekennzeichnet wird, wobei, insbesondere in zumindest einem weiteren Verfahrensschritt, das Datenpaket über die Servereinheit mittels zumindest einer der werkzeugspezifischen Kenngröße zugeordneten, insbesondere der oben beschriebenen, öffentlichen Schlüsselfunktion entschlüsselt wird. Vorzugsweise wird in zumindest einem Verfahrensschritt mittels der Servereinheit das digitale Zertifikat der Werkzeugmaschine der werkzeugmaschinenspezifischen Kenngröße zugeordnet und in der Servereinheit hinterlegt. Es ist aber auch denkbar, dass die werkzeugmaschinenspezifische Kenngröße und/oder die öffentliche Schlüsselfunktion mittels der Servereinheit anhand des digitalen Zertifikats zugeordnet werden. Vorteilhafterweise werden die werkzeugmaschinenspezifische Kenngröße, die öffentliche Schlüsselfunktion und/oder das digitale Zertifikat auf einer zumindest im Wesentlichen manipulationssicheren Speichereinheit der Servereinheit hinterlegt. Alternativ oder zusätzlich ist denkbar, dass mittels der Servereinheit, periodisch oder kontinuierlich, mit werkzeugspezifischen Kenngrößen signierte und/oder mittels

der weiteren öffentlichen Schlüsselfunktion von der Netzwerkeinheit abgerufen werden. Vorzugsweise ist die Netzwerkeinheit dazu eingerichtet, Datenpakete in Abhängigkeit von einer Signatur und/oder einer Verschlüsselungsart zu unterscheiden und zu sortieren. Durch die erfindungsgemäße Ausgestaltung des Verfahrens kann eine vorteilhaft schnelle Entschlüsselung eines übertragenen Datenpakets erreicht werden. Es kann eine vorteilhaft einfache Zuordnung der werkzeugspezifischen Daten erfolgen.

Außerdem wird ein System zur Kommunikation von Werkzeugmaschinen in einem Netzwerk mittels asymmetrischer Kryptografie, insbesondere mittels zumindest einer Public-Key-Infrastruktur, insbesondere gemäß einem erfindungsgemäßen Verfahren, mit zumindest einer erfindungsgemäßen Werkzeugmaschine, mit zumindest einer Servereinheit und mit zumindest einer Netzwerkeinheit vorgeschlagen. Vorzugsweise ist die Netzwerkeinheit dazu eingerichtet, eine Kommunikation zu einer Authentifizierung und/oder einer Datenübertragung zwischen der Werkzeugmaschine und der Servereinheit zu ermöglichen. Es ist denkbar, insbesondere wenn ein Abstand der Werkzeugmaschine von der Servereinheit innerhalb einer Verbindungsreichweite einer Art der Kommunikation im Netzwerk aufweist, dass die Werkzeugmaschine und die Servereinheit direkt miteinander kommunizieren. Vorzugsweise umfasst das System eine Vielzahl von Werkzeugmaschinen. Bevorzugt umfasst das System zumindest eine Werkzeugzubehöreinheit, die insbesondere modular ausgebildet ist. Vorteilhafterweise ist die Werkzeugzubehöreinheit zu zumindest einer Anwendung mit der Werkzeugmaschine eingerichtet, wobei insbesondere die Werkzeugmaschine und/oder die Servereinheit dazu eingerichtet sind, die Werkzeugzubehöreinheit vor der Anwendung mit der Werkzeugmaschine zu authentifizieren. Bevorzugt weist das System für jede Werkzeugmaschine und jede Servereinheit des Systems genau eine öffentliche und genau eine private Schlüsselfunktion auf. Vorzugsweise ist die Servereinheit beispielsweise als ein Cloud-Server, als eine Blockchain, als ein lokaler Server, als ein Intranet-Server o. dgl. ausgebildet. Besonders bevorzugt umfasst die Servereinheit zumindest eine weitere Steuer- und/oder Regeleinheit, insbesondere einen weiteren Krypto-Prozessor, zur Verschlüsselung und Entschlüsselung von Datenpaketen. Bevorzugt ist die weitere Steuer- und/oder Regeleinheit, insbesondere der weitere Krypto-Prozessor, zumindest im Wesentlichen manipulationssicher ausgebildet. Vorzugsweise weist die weitere

Steuer- und/oder Regeleinheit zumindest eine Speichereinheit auf. Besonders bevorzugt ist zumindest eine Komponente der Speichereinheit als nichtflüchtiger Datenspeicher ausgebildet. Bevorzugterweise sind in der Speichereinheit öffentliche Schlüsselfunktionen aller Werkzeugmaschinen des Systems und eine weitere öffentliche Schlüsselfunktion und eine weitere private Schlüsselfunktion der Servereinheit hinterlegt. Bevorzugt ist die Servereinheit dazu eingerichtet die weitere öffentliche Schlüsselfunktion, insbesondere bei oder vor einer Authentifizierung der Werkzeugmaschine an die Netzwerkeinheit und/oder an, insbesondere eine Kommunikationseinheit, der Werkzeugmaschine zu übertragen. Durch die erfindungsgemäße Ausgestaltung des Systems kann eine vorteilhaft sichere Kommunikation zwischen der Werkzeugmaschine und der Servereinheit erreicht werden. Es kann eine vorteilhaft hohe Funktionalität der Werkzeugmaschine erreicht werden, insbesondere da eine sichere Vernetzung der Werkzeugmaschine mit einem Internet und/oder einem Intranet ermöglicht werden kann.

Weiterhin wird eine Werkzeugmaschine zur Kommunikation in einem Netzwerk mittels asymmetrischer Kryptografie, insbesondere mittels zumindest einer Public-Key-Infrastruktur, insbesondere gemäß einem erfindungsgemäßen Verfahren, vorgeschlagen, wobei die Werkzeugmaschine zumindest eine Kommunikationseinheit zu einer, insbesondere drahtlosen, Übertragung von elektronischen Daten und zumindest eine mit der Kommunikationseinheit verbundene Steuer- und/oder Regeleinheit zu einer Auswertung und/oder Bearbeitung von übertragenen und/oder zu übertragenen Daten umfasst. Es ist denkbar, dass die Steuer- und/oder Regeleinheit zumindest eine Krypto-Schaltung umfasst, wobei insbesondere die Krypto-Schaltung den Krypto-Prozessor umfasst. Die Krypto-Schaltung ist bevorzugt als eine Platine ausgebildet, die zumindest eine elektrische Leitung, eine Speichereinheit, einen Authenticator und/oder weitere, einem Fachmann als sinnvoll erscheinende Bauteile zur Verschlüsselung und/oder Entschlüsselung von Daten aufweist. Vorzugsweise ist die Krypto-Schaltung zumindest im Wesentlichen manipulationssicher ausgebildet. Insbesondere weist die Steuer- und/oder Regeleinheit zumindest eine Speichereinheit auf, die zumindest eine Komponente aufweist, die als nichtflüchtiger Datenspeicher ausgebildet ist. Vorzugsweise umfasst die Steuer- und/oder Regeleinheit zumindest eine Gehäuseeinheit, die dazu eingerichtet ist, die Steuer- und/oder Regeleinheit, insbeson-

dere die Krypto Schaltung und/oder den Krypto-Prozessor, vor physischen unbefugten Einflüssen zu sichern. Bevorzugt umschließt die Gehäuseeinheit die Krypto-Schaltung und/oder den Krypto-Prozessor zumindest im Wesentlichen vollständig. Bevorzugterweise ist die Gehäuseeinheit zumindest im Wesentlichen verliersicher mit einer Komponente der Steuer- und/oder Regeleinheit, insbesondere der Krypto-Schaltung und/oder dem Krypto-Prozessor, verbunden. Darunter, dass eine Einheit, insbesondere die Gehäuseeinheit, mit einer weiteren Einheit, insbesondere der Komponente der Steuer- und/oder Regeleinheit, „zumindest im Wesentlichen verliersicher verbunden ist“ soll insbesondere verstanden werden, dass die Einheit lediglich unter der Zuhilfenahme von Trennwerkzeugen, wie beispielsweise einer Säge, insbesondere einer mechanischen Säge usw., chemischen Trennmitteln, wie beispielsweise Lösungsmittel usw. und/oder einem einheitenspezifischen Werkzeug von der weiteren Einheit trennbar ist. Vorzugsweise umfasst die Werkzeugmaschine zumindest eine Schnittstelle, welche zu einer Verbindung der Werkzeugmaschine mit einer Werkzeugzubehöreinheit eingerichtet ist. Bevorzugt ist die Kommunikationseinheit und/oder die Steuer- und/oder Regeleinheit, insbesondere der Krypto-Prozessor dazu eingerichtet, die Werkzeugzubehöreinheit für zumindest eine Anwendung mit der Werkzeugmaschine und/oder der Servereinheit zu verifizieren. Vorteilhafterweise weist die Werkzeugmaschine zumindest eine Eingabeeinheit zur Interaktion mit einem Benutzer und/oder einer externen Einheit auf. Bevorzugt weist die Werkzeugmaschine zumindest die Ausgabeeinheit zur Ausgabe von zumindest einer Information, insbesondere einem akustischen, optischen und/oder haptischen Signal, auf. Vorzugsweise ist die Ausgabeeinheit dazu eingerichtet, zumindest eine Eingabeaufforderung zu signalisieren und/oder Betriebsinformationen der Werkzeugmaschine an einen Benutzer auszugeben. Die Eingabeeinheit kann einteilig mit der Ausgabeeinheit ausgebildet sein, insbesondere bei einer Ausgestaltung der Eingabeeinheit als berührungsempfindliches Display o. dgl. Durch die erfindungsgemäße Ausgestaltung kann eine vorteilhaft sichere Kommunikation mit einer Servereinheit und/oder einer weiteren Werkzeugmaschine ermöglicht werden. Durch die erfindungsgemäße Ausgestaltung der Werkzeugmaschine kann eine vorteilhaft hohe Funktionalität erreicht werden, insbesondere da die Werkzeugmaschine über eine sichere Verbindung im Internet oder einem Intranet eingebunden werden kann. Es kann eine vorteilhaft genaue Überwachung der

Werkzeugmaschine ermöglicht werden, insbesondere bei einer Verwendung innerhalb eines Systems und/oder in einem Netzwerk.

Des Weiteren wird vorgeschlagen, dass die Steuer- und/oder Regeleinheit dazu eingerichtet ist, übertragene und/oder zu übertragene Daten zu entschlüsseln oder zu verschlüsseln. Vorzugsweise ist die Steuer- und/oder Regeleinheit dazu eingerichtet, die zu übertragenen Daten mittels einer weiteren öffentlichen Schlüsselfunktion einer Sendereinheit, insbesondere der Servereinheit, zu verschlüsseln. Bevorzugt ist die Steuer- und/oder Regeleinheit dazu eingerichtet, insbesondere über die Kommunikationseinheit, übertragene Daten mittels einer privaten Schlüsselfunktion der Werkzeugmaschine zu entschlüsseln. Vorteilhafterweise sind die private Schlüsselfunktion und die öffentliche Schlüsselfunktion auf der Speichereinheit der Werkzeugmaschine hinterlegt. Durch die erfindungsgemäße Ausgestaltung der Werkzeugmaschine kann eine vorteilhaft sichere Kommunikation erreicht werden. Es kann eine vorteilhaft hohe Sicherheit erreicht werden, insbesondere da eine Steuerung der Werkzeugmaschine durch unbefugte Einflüsse vorteilhaft vermieden werden kann.

Das erfindungsgemäße Verfahren, das erfindungsgemäße System und/oder die erfindungsgemäße Werkzeugmaschine sollen/soll hierbei nicht auf die oben beschriebene Anwendung und Ausführungsform beschränkt sein. Insbesondere können/kann das erfindungsgemäße Verfahren, das erfindungsgemäße System und/oder die erfindungsgemäße Werkzeugmaschine zu einer Erfüllung einer hierin beschriebenen Funktionsweise eine von einer hierin genannten Anzahl von einzelnen Elementen, Bauteilen und Einheiten sowie Verfahrensschritten abweichende Anzahl aufweisen. Zudem sollen bei den in dieser Offenbarung angegebenen Wertebereichen auch innerhalb der genannten Grenzen liegende Werte als offenbart und als beliebig einsetzbar gelten.

## Zeichnung

Weitere Vorteile ergeben sich aus der folgenden Zeichnungsbeschreibung. In der Zeichnung sind fünf Ausführungsbeispiele der Erfindung dargestellt. Die Zeichnung, die Beschreibung und die Ansprüche enthalten zahlreiche Merkmale in

Kombination. Der Fachmann wird die Merkmale zweckmäßigerweise auch einzeln betrachten und zu sinnvollen weiteren Kombinationen zusammenfassen.

Es zeigen:

Fig. 1 eine schematische Darstellung eines erfindungsgemäßen Systems zur Kommunikation von Werkzeugmaschinen in einem Netzwerk mit einer erfindungsgemäßen Werkzeugmaschine zur Durchführung eines erfindungsgemäßen Verfahrens,

Fig. 2 eine weitere schematische Darstellung des erfindungsgemäßen Systems mit einer Zuteilung der kryptografischen Elemente,

Fig. 3 eine schematische Darstellung der erfindungsgemäßen Werkzeugmaschine,

Fig. 4 eine schematische Darstellung eines Ablaufs des erfindungsgemäßen Verfahrens,

Fig. 5 eine schematische Darstellung einer ersten alternativen Ausgestaltung eines erfindungsgemäßen Systems mit einer erfindungsgemäßen Werkzeugmaschine zur Durchführung eines erfindungsgemäßen Verfahrens,

Fig. 6 eine schematische Darstellung einer zweiten alternativen Ausgestaltung eines erfindungsgemäßen Systems mit einer erfindungsgemäßen Werkzeugmaschine zur Durchführung eines erfindungsgemäßen Verfahrens,

Fig. 7 eine schematische Darstellung einer dritten alternativen Ausgestaltung eines erfindungsgemäßen Systems mit einer erfindungsgemäßen Werkzeugmaschine zur Durchführung eines erfindungsgemäßen Verfahrens und

Fig. 8 eine schematische Darstellung einer vierten alternativen Ausgestaltung eines erfindungsgemäßen Systems mit einer erfindungsgemäßen Werkzeugmaschine zur Durchführung eines erfindungsgemäßen Verfahrens.

Beschreibung der Ausführungsbeispiele

Figur 1 zeigt ein System 10a zur Kommunikation von Werkzeugmaschinen 12a, 14a in einem Netzwerk 16a mittels asymmetrischer Kryptografie, insbesondere mittels zumindest einer Public-Key-Infrastruktur. Das System 10a umfasst eine Werkzeugmaschine 12a, eine Servereinheit 18a und eine Netzwerkeinheit 20a. Die Werkzeugmaschine 12a weist eine Kommunikationseinheit 22a und eine Steuer- und/oder Regeleinheit 24a auf, welche einen Krypto-Prozessor 26a umfasst. Die Servereinheit 18a weist eine weitere Steuer- und/oder Regeleinheit 28a auf, die einen weiteren Krypto-Prozessor 30a umfasst. Vorzugsweise sind die Werkzeugmaschine 12a, die Netzwerkeinheit 20a und die Servereinheit 18a kabelgebunden und/oder kabellos miteinander über das Netzwerk 16a verbunden. Vorzugsweise erfolgt eine Authentifizierung und/oder eine Datenübertragung von und/oder mit der Werkzeugmaschine 12a, der Servereinheit 18a und/oder einer weiteren Werkzeugmaschine 14a des Systems 10a über die Netzwerkeinheit 20a. Es ist denkbar, dass, insbesondere falls der Abstand zwischen der Werkzeugmaschine 12a und der Servereinheit 18a und/oder der weiteren Werkzeugmaschine 14a gering ist, die Authentifizierung und/oder die Datenübertragung direkt erfolgt. Vorzugsweise umfasst das System 10a zumindest eine Werkzeugzubehöreinheit 32a, die insbesondere zu einer Anwendung mit der Werkzeugmaschine 12a zusammenwirkt. In Figur 1 ist eine als Akku ausgebildete Werkzeugzubehöreinheit 32a dargestellt. Es sind jedoch auch andere Ausgestaltungen der Werkzeugzubehöreinheit 32a denkbar. Vorzugsweise ist die Werkzeugmaschine 12a, die Servereinheit 18a und/oder eine externe Einheit 34a dazu eingerichtet einen digitalen Marker 36a zu generieren, wobei der digitale Marker 36a dazu eingerichtet ist, einen Benutzer 38a und/oder die Steuer- und/oder Regeleinheit 24a, insbesondere den Krypto-Prozessor 26a, der Werkzeugmaschine 12a für zumindest eine Anwendung mit der Werkzeugmaschine 12a und/oder der Servereinheit 18a zu verifizieren. Der digitale Marker 36a ist auf einer externen Speichereinheit 40a hinterlegt, welche insbesondere nichtflüchtig und manipulationssicher ausgebildet ist.

Figur 2 zeigt eine schematische Darstellung des Systems 10a mit einer Zuteilung der kryptografischen Elemente, insbesondere Schlüsselfunktionen 82a, 84a, 86a,

88a, 90a, 92a, digitale Zertifikate 94a, 96a, 98a und einem digitalen Marker 100a. Vorzugsweise sind öffentliche Schlüsselfunktionen 82a, 86a, 90a der Werkzeugmaschine 12a, der Servereinheit 18a und der weiteren Werkzeugmaschine 14a in jeweils einer Speichereinheit der Servereinheit 18a, der Werkzeugmaschine 12a und der weiteren Werkzeugmaschine 14a hinterlegt. Bevorzugt ist eine private Schlüsselfunktion 84a der Werkzeugmaschine 12a lediglich in einer Speichereinheit 55a der Werkzeugmaschine 12a hinterlegt. Vorteilhafterweise ist eine private Schlüsselfunktion 88a der Servereinheit 18a lediglich in der Speichereinheit der Servereinheit 18a hinterlegt. Vorzugsweise ist eine private Schlüsselfunktion 92a der weiteren Werkzeugmaschine 14a lediglich in der Speichereinheit 55a der weiteren Werkzeugmaschine 14a hinterlegt. Bevorzugt ist der digitale Marker 100a auf der externen Speichereinheit 40a gespeichert und in den Speichereinheiten der Werkzeugmaschine 12a und der Servereinheit 18a hinterlegt, insbesondere zu einer Verifizierung einer Anwendung mit der Werkzeugmaschine 12a und/oder der Servereinheit 18a durch einen Benutzer 38a und/oder eine externe Einheit 34a. Vorzugsweise sind digitale Zertifikate 94a, 96a der Werkzeugmaschine 12a und der weiteren Werkzeugmaschine 14a, insbesondere zur Authentifizierung mit der Servereinheit 18a, der Netzwerkeinheit 20a und/oder der Werkzeugmaschine 12a und/oder der weiteren Werkzeugmaschine 14a, auf den Speichereinheiten der Servereinheit 18a, der Werkzeugmaschine 12a und der weiteren Werkzeugmaschine 14a und einer Speichereinheit der Netzwerkeinheit 20a hinterlegt. Die Werkzeugzubehöreinheit 32a weist ein anderes digitales Zertifikat 98a auf, insbesondere zur Authentifizierung mit der Werkzeugmaschine 12a und/oder der Servereinheit 18a, insbesondere über das Netzwerk 16a. Das andere digitale Zertifikat 98a ist insbesondere in den Speichereinheiten der Werkzeugmaschine 12a, der Netzwerkeinheit 20a und der Servereinheit 18a hinterlegt. Es ist auch denkbar, dass die Werkzeugzubehöreinheit 32a mit einer Vielzahl von Werkzeugmaschinen 12a, 14a des Systems 10a, insbesondere der weiteren Werkzeugmaschine 14a, verbunden und/oder verwendet werden kann, wobei das andere digitale Zertifikat 98a in der Speichereinheit der weiteren Werkzeugmaschine 14a hinterlegt ist. Die Werkzeugmaschine 12a und die weitere Werkzeugmaschine 14a weisen jeweils eine werkzeugmaschinenspezifische Kenngröße 102a, 104a auf, welche jeweils in der Speichereinheit 55a der Werkzeugmaschine 12a und der weiteren Werkzeugmaschine 14a hinterlegt sind. Vor-

zugsweise sind die werkzeugmaschinenspezifischen Kenngrößen 102a, 104a zumindest in der Speichereinheit der Servereinheit 18a hinterlegt, insbesondere zur eindeutigen Zuordnung der Werkzeugmaschinen 12a, 14a, insbesondere der Daten von Werkzeugmaschinen 12a, 14a, im System 10a.

Figur 3 zeigt die Werkzeugmaschine 12a zur Kommunikation in dem Netzwerk 16a mittels asymmetrischer Kryptografie, insbesondere mittels zumindest einer Public-Key-Infrastruktur. Die Kommunikationseinheit 22a der Werkzeugmaschine 12a ist zu einer, insbesondere drahtlosen, Übertragung von elektronischen Daten eingerichtet. Die Werkzeugmaschine 12a umfasst einen Motor 42a zum Antreiben eines Werkzeugs der Werkzeugmaschine 12a. Die Steuer- und/oder Regeleinheit 24a der Werkzeugmaschine 12a ist mit der Kommunikationseinheit 22a verbunden und insbesondere zu einer Auswertung und/oder Bearbeitung von übertragenen und/oder zu übertragenen Daten eingerichtet. Die Steuer- und/oder Regeleinheit 24a umfasst eine Krypto-Schaltung 44a und einen Krypto-Prozessor 26a. Vorzugsweise ist die Steuer- und/oder Regeleinheit 24a, insbesondere der Krypto-Prozessor 26a dazu eingerichtet, übertragene und/oder zu übertragene Daten zu entschlüsseln oder zu verschlüsseln. Die Steuer- und/oder Regeleinheit 24a umfasst eine Gehäuseeinheit 46a, die die Krypto-Schaltung 44a zumindest im Wesentlichen vollständig umschließt. Bevorzugt ist die Steuer- und/oder Regeleinheit 24a dazu eingerichtet, zumindest den Motor 42a der Werkzeugmaschine 12a, insbesondere in Abhängigkeit von einer Benutzersteuerung, zu steuern und/oder zu regeln. Die Werkzeugmaschine 12a umfasst eine als Display ausgebildete Ausgabeeinheit 48a zur Ausgabe von zumindest einer Information, insbesondere einem akustischen, optischen und/oder haptischen Signal, insbesondere zur Übermittlung von Betriebsinformationen der Werkzeugmaschine 12a an einen Benutzer 38a und/oder zur Signalisierung einer Eingabeaufforderung. Es sind jedoch auch andere Ausgestaltungen der Ausgabeeinheit 48a denkbar. Die Werkzeugmaschine 12a umfasst eine als Bedienfeld ausgebildete Eingabeeinheit 50a zur Interaktion mit einem Benutzer 38a und/oder einer externen Einheit 34a. Es sind jedoch auch andere Ausgestaltungen der Eingabeeinheit 50a denkbar. Alternativ oder zusätzlich ist denkbar, dass die Eingabeeinheit 50a und die Ausgabeeinheit 48a einstückig ausgebildet sind. Die Ausgabeeinheit 48a und die Eingabeeinheit 50a sind mit der Steuer- und/oder Regeleinheit 24a verbunden. Vorzugsweise ist die Steuer- und/oder Regeleinheit 24a dazu eingerichtet,

die Ausgabeeinheit 48a und die Eingabeeinheit 50a, insbesondere in Abhängigkeit von einem Betriebsparameter der Werkzeugmaschine 12a und/oder einer Kommunikation mit der Servereinheit 18a, der Netzwerkeinheit 20a und/oder der weiteren Werkzeugmaschine 14a über die Kommunikationseinheit 22a, zu steuern und/oder zu regeln. Die Werkzeugmaschine 12a umfasst eine Bedieneinheit 52a zu einer Bedienung der Werkzeugmaschine 12a durch einen Benutzer 38a, insbesondere in einer Anwendung der Werkzeugmaschine 12a. Die Werkzeugmaschine 12a weist eine Schnittstelle 54a auf, die insbesondere zu einer Verbindung der Werkzeugmaschine 12a mit der externen Speichereinheit 40a eingerichtet ist, insbesondere zu einer Verifizierung eines Benutzers 38a und/oder einer externen Einheit 34a mittels dem digitalen Marker 36a. Vorzugsweise ist die Schnittstelle 54a zumindest teilweise als USB-Port ausgebildet. Es sind aber auch andere Ausgestaltungen der Schnittstelle 54a denkbar. In Figur 3 ist die Werkzeugmaschine 12a zusammen mit der als Akku ausgebildeten Werkzeugzubehöreinheit 32a dargestellt, welche insbesondere über eine weitere Schnittstelle (in Figur 3 nicht gezeigt) mit der Werkzeugmaschine 12a verbunden ist. Die Steuer- und/oder Regeleinheit 24a umfasst eine Speichereinheit 55a, die insbesondere nichtflüchtig und manipulationssicher ausgebildet ist. Es ist denkbar, dass die Speichereinheit 55a an der Krypto-Schaltung 44a angeordnet ist.

Figur 4 zeigt einen Ablauf eines Verfahrens 56a zur Kommunikation von Werkzeugmaschinen 12a, 14a in einem Netzwerk 16a mittels asymmetrischer Kryptografie, insbesondere mittels einer Public-Key-Infrastruktur. In zumindest einem Verfahrensschritt 58a des Verfahrens 56a wird bei einer Datenübertragung und/oder einer Authentifizierung zumindest einer Werkzeugmaschine 12a über eine Netzwerkeinheit 20a mit einer Servereinheit 18a, zumindest einer weiteren Werkzeugmaschine 14a und/oder zumindest einer externen Einheit 34a ein Datenpaket mittels zumindest einer Kommunikationseinheit 22a und/oder zumindest einer Steuer- und/oder Regeleinheit 24a, insbesondere mittels zumindest eines Krypto-Prozessors 26a, der Werkzeugmaschine 12a über eine, insbesondere werkzeugmaschinenspezifische, öffentliche Schlüsselfunktion 82a und/oder private Schlüsselfunktion 84a verschlüsselt und/oder entschlüsselt. In zumindest einem weiteren Verfahrensschritt 60a des Verfahrens 56a werden der Werkzeugmaschine 12a mittels der Servereinheit 18a genau eine werkzeugmaschinenspezifische Kenngröße 102a, die öffentliche Schlüsselfunktion 82a und die private

Schlüsselfunktion 84a zugeordnet und übertragen, wobei die werkzeugmaschinenspezifische Kenngröße 102a, die öffentliche Schlüsselfunktion 82a und die private Schlüsselfunktion 84a in zumindest einer Speichereinheit 55a der Werkzeugmaschine 12a hinterlegt werden. In zumindest einem weiteren Verfahrensschritt 62a des Verfahrens 56a wird mittels der Servereinheit 18a und/oder der externen Einheit 34a zumindest ein digitales Zertifikat 94a generiert, welches zumindest eine werkzeugmaschinenspezifische Kenngröße 102a, die öffentliche Schlüsselfunktion 82a, die private Schlüsselfunktion 84a und/oder zumindest eine Benutzerinformation umfasst und in der Speichereinheit 55a der Werkzeugmaschine 12a hinterlegt wird. In zumindest einem weiteren Verfahrensschritt 64a des Verfahrens 56a wird mittels der Werkzeugmaschine 12a, der Servereinheit 18a und/oder der externen Einheit 34a zumindest ein digitaler Marker 100a erstellt, welcher dazu eingerichtet ist, zumindest einen Benutzer 38a und/oder zumindest eine externe Einheit 34a über die Kommunikationseinheit 22a und/oder die Steuer- und/oder Regeleinheit 24a, insbesondere den Krypto-Prozessor 26a, für zumindest eine Anwendung mit der Werkzeugmaschine 12a und/oder der Servereinheit 18a zu verifizieren. Vorzugsweise wird in zumindest einem Verfahrensschritt 66a des Verfahrens 56a die Datenübertragung und/oder die Authentifizierung der Werkzeugmaschine 12a mit der Netzwerkeinheit 20a, der Servereinheit 18a und/oder der weiteren Werkzeugmaschine 12a über die Kommunikationseinheit 22a und/oder die Steuer- und/oder Regeleinheit 24a, insbesondere den Krypto-Prozessor 26a, mittels zumindest einem auf Transport Layer Security (TLS) basierenden Verschlüsselungsprotokoll gesichert. In zumindest einem weiteren Verfahrensschritt 68a des Verfahrens 56a erfolgt über die Kommunikationseinheit 22a und/oder die Steuer- und/oder Regeleinheit 24a, insbesondere den Krypto-Prozessor 26a, zumindest eine Authentifizierung zumindest eines Benutzers 38a und/oder der externen Einheit 34a mit der Werkzeugmaschine 12a, der Netzwerkeinheit 20a und/oder der Servereinheit 18a als Challenge-Response-Authentifizierung. In zumindest einem weiteren Verfahrensschritt 70a des Verfahrens 56a wird zu einer Authentifizierung von zumindest einer Werkzeugzubehöreinheit 32a, insbesondere bei einem Verbinden der Werkzeugzubehöreinheit 32a mit der Werkzeugmaschine 12a, mittels der Kommunikationseinheit 22a, der Steuer- und/oder Regeleinheit 24a, insbesondere dem Krypto-Prozessor 26a, und/oder der Servereinheit 18a, insbesondere automatisch, zumindest ein digitales Zertifikat 98a der Werkzeugzubehöreinheit 32a überprüft. In zumindest einem

weiteren Verfahrensschritt 72a des Verfahrens 56a werden über die Netzwerkeinheit 20a und/oder die Servereinheit 18a, insbesondere mittels der öffentlichen Schlüsselfunktion 82a, verschlüsselte betriebssystembezogene Daten an die Werkzeugmaschine 12a übermittelt, welche mittels der Kommunikationseinheit 22a und/oder der Steuer- und/oder Regeleinheit 24a, insbesondere dem Krypto-Prozessor 26a, insbesondere mittels der privaten Schlüsselfunktion 84a, entschlüsselt und mit zumindest einer Recheneinheit der Werkzeugmaschine 12a verarbeitet werden. In zumindest einem weiteren Verfahrensschritt 74a des Verfahrens 56a wird mittels der Servereinheit 18a zumindest eine weitere öffentliche Schlüsselfunktion 86a an die Werkzeugmaschine 12a und/oder die Netzwerkeinheit 20a ausgegeben. In zumindest einem weiteren Verfahrensschritt 76a des Verfahrens 56a wird zur Datenübertragung und/oder Authentifizierung der Werkzeugmaschine 12a und/oder der Netzwerkeinheit 20a mit der Servereinheit 18a zumindest ein Datenpaket mittels der weiteren öffentlichen Schlüsselfunktion 86a verschlüsselt und mittels zumindest einer weiteren privaten Schlüsselfunktion 88a von der Servereinheit 18a entschlüsselt. In zumindest einem weiteren Verfahrensschritt 78a des Verfahrens 56a wird bei der Datenübertragung und/oder der Authentifizierung der Werkzeugmaschine 12a das, insbesondere verschlüsselte, Datenpaket mit zumindest einer werkzeugmaschinenspezifische Kenngröße 102a gekennzeichnet. In zumindest einem weiteren Verfahrensschritt 80a des Verfahrens 56a wird das Datenpaket über die Servereinheit 18a mittels zumindest einer der werkzeugspezifischen Kenngröße 102a zugeordneten öffentlichen Schlüsselfunktion 92a entschlüsselt.

In den Figuren 5 bis 8 sind weitere Ausführungsbeispiele der Erfindung gezeigt. Die nachfolgenden Beschreibungen und die Zeichnungen beschränken sich im Wesentlichen auf die Unterschiede zwischen den Ausführungsbeispielen, wobei bezüglich gleich bezeichneter Bauteile, insbesondere in Bezug auf Bauteile mit gleichen Bezugszeichen, grundsätzlich auch auf die Zeichnungen und/oder die Beschreibung der anderen Ausführungsbeispiele, insbesondere der Figuren 1 bis 4, verwiesen werden kann. Zur Unterscheidung der Ausführungsbeispiele ist der Buchstabe a den Bezugszeichen des Ausführungsbeispiels in den Figuren 1 bis 4 nachgestellt. In den Ausführungsbeispielen der Figuren 5 bis 8 ist der Buchstabe a durch die Buchstaben b bis e ersetzt.

Figur 5 zeigt eine erste alternative Ausgestaltung eines Systems 10b zur Kommunikation von Werkzeugmaschinen 12b in einem Netzwerk 16b mittels asymmetrischer Kryptografie, insbesondere mittels zumindest einer Public-Key-Infrastruktur. Das in der Figur 5 dargestellte System 10b weist eine zumindest im Wesentlichen analoge Ausgestaltung zu dem in der Beschreibung der Figuren 1 bis 4 beschriebenen System 10a auf, so dass bezüglich einer Ausgestaltung des in der Figur 5 dargestellten Systems 10b zumindest im Wesentlichen auf die Beschreibung der Figuren 1 bis 4 verwiesen werden kann. Im Unterschied zu dem in der Beschreibung der Figuren 1 bis 4 beschriebenen System 10a weist das in der Figur 5 dargestellte System 10b zwei weitere Servereinheiten 106b, 108b auf, die dazu eingerichtet sind, mit einer Servereinheit 18b, der Werkzeugmaschine 12b und einer Werkzeugzubehöreinheit 32b zu kommunizieren. Es ist denkbar, dass eine Kommunikation im Netzwerk 16b des Systems 10b über Netzwerkeinheiten 20b erfolgt, welche in der Figur 5 jedoch nicht dargestellt sind. Die zwei weiteren Servereinheiten 106b, 108b weisen jeweils eine öffentliche Schlüsselfunktion 112b, 116b und jeweils eine private Schlüsselfunktion 114b, 118b auf, wobei die öffentlichen Schlüsselfunktionen 112b, 116b der weiteren Servereinheiten 106b, 108b zumindest in Speichereinheiten der Servereinheit 18b, der Werkzeugmaschine 12b, der Werkzeugzubehöreinheit 32b hinterlegt sind. Vorzugsweise ist eine der weiteren Servereinheiten 108b dazu eingerichtet, die Werkzeugmaschine 12a, insbesondere eine Anwendung der Werkzeugmaschine 12b, zu authentifizieren und/oder eine Kommunikation mit der Werkzeugmaschine 12b zu ermöglichen. Bevorzugt ist ein digitales Zertifikat 94b der Werkzeugmaschine 12b in einer Speichereinheit der einen weiteren Servereinheit 108b hinterlegt. Vorteilhafterweise ist die andere der weiteren Servereinheiten 106b dazu eingerichtet, die Werkzeugzubehöreinheit 32a, insbesondere eine Anwendung der Werkzeugzubehöreinheit 32a mit der Werkzeugmaschine 12b, zu authentifizieren und/oder eine Kommunikation mit der Werkzeugzubehöreinheit 32b zu ermöglichen. Bevorzugt ist ein digitales Zertifikat 110b der Werkzeugzubehöreinheit 32b in einer Speichereinheit der einen weiteren Servereinheit 106b hinterlegt. Die Werkzeugzubehöreinheit 32b weist ein weiteres digitales Zertifikat 98b auf, insbesondere zur Authentifizierung der Werkzeugzubehöreinheit 32b mit der Werkzeugmaschine 12b. Besonders bevorzugt ist die Servereinheit 18b dazu eingerichtet, die weiteren Servereinheiten 106b, 108b, insbesondere im Netzwerk 16b, zu authentifizieren und/oder Authentifizierungszertifikate an die weiteren

Servereinheiten 106b, 108b zu verteilen und/oder zuzuordnen. Vorzugsweise erfolgt in zumindest einem Verfahrensschritt bei einer Datenübertragung und/oder einer Authentifizierung der Werkzeugmaschine 12b über eine Netzwerkeinheit 20b mit einer Servereinheit 18b, 108b, zumindest einer weiteren Werkzeugmaschine 14b (in Figur 5 nicht gezeigt) und/oder zumindest einer externen Einheit 34b (in Figur 5 nicht gezeigt) eine Verschlüsselung und/oder eine Entschlüsselung eines Datenpaket mittels zumindest einer Kommunikationseinheit 22b (in Figur 5 nicht gezeigt) und/oder zumindest einer Steuer- und/oder Regeleinheit 24b (in Figur 5 nicht gezeigt), insbesondere mittels zumindest eines Krypto-Prozessors 26b (in Figur 5 nicht gezeigt), der Werkzeugmaschine 12b über eine, insbesondere werkzeugmaschinenspezifische, öffentliche Schlüsselfunktion 82b und/oder private Schlüsselfunktion 84b (in Figur 5 nicht gezeigt).

Figur 6 zeigt eine zweite alternative Ausgestaltung eines Systems 10c zur Kommunikation von Werkzeugmaschinen 12c in einem Netzwerk 16c mittels asymmetrischer Kryptografie, insbesondere mittels zumindest einer Public-Key-Infrastruktur. Das in der Figur 6 dargestellte System 10c weist eine zumindest im Wesentlichen analoge Ausgestaltung zu dem in der Beschreibung der Figuren 1 bis 4 beschriebenen System 10a auf, so dass bezüglich einer Ausgestaltung des in der Figur 6 dargestellten Systems 10c zumindest im Wesentlichen auf die Beschreibung der Figuren 1 bis 4 verwiesen werden kann. Im Unterschied zu dem in der Beschreibung der Figuren 1 bis 4 beschriebenen System 10a weist das in der Figur 6 dargestellte System 10c zwei weitere Servereinheiten 106c, 108c auf, die dazu eingerichtet sind, von der Servereinheit 18c authentifizierte Zertifikate an die Werkzeugmaschine 12c und zumindest eine Werkzeugzubehöreinheit 32c zu verteilen und/oder zu übermitteln. Vorzugsweise ist eine der weiteren Servereinheiten 108c dazu eingerichtet, von der Servereinheit 18c authentifizierte Zertifikate an die Werkzeugmaschine 12c zu verteilen und/oder zu übermitteln, wobei insbesondere die andere der beiden weiteren Servereinheiten 106c dazu eingerichtet ist von der Servereinheit 18c authentifizierte Zertifikate an die Werkzeugzubehöreinheit 32c zu verteilen und/oder zu übermitteln. Die Servereinheit 18c weist eine weitere öffentliche Schlüsselfunktion 86c und eine weitere private Schlüsselfunktion 88c auf, insbesondere zu einer Verschlüsselung und/oder einer Entschlüsselung von Datenpaketen, die zwischen der Servereinheit 18c und den

zwei weiteren Servereinheiten 106c, 108c übertragen werden. Die Werkzeugzubehöreinheit 32c weist ein weiteres digitales Zertifikat 98c auf, insbesondere zur Authentifizierung der Werkzeugzubehöreinheit 32c mit der Werkzeugmaschine 12c. Vorzugsweise erfolgt in zumindest einem Verfahrensschritt bei einer Datenübertragung und/oder einer Authentifizierung der Werkzeugmaschine 12c über eine Netzwerkeinheit 20c (in Figur 6 nicht gezeigt) mit einer Servereinheit 18c, 108c, zumindest einer weiteren Werkzeugmaschine 14c (in Figur 6 nicht gezeigt) und/oder zumindest einer externen Einheit 34c (in Figur 6 nicht gezeigt) eine Verschlüsselung und/oder eine Entschlüsselung eines Datenpaket mittels zumindest einer Kommunikationseinheit 22c (in Figur 6 nicht gezeigt) und/oder zumindest einer Steuer- und/oder Regeleinheit 24c (in Figur 6 nicht gezeigt), insbesondere mittels zumindest eines Krypto-Prozessors 26c (in Figur 6 nicht gezeigt), der Werkzeugmaschine 12c über eine, insbesondere werkzeugmaschinenspezifische, öffentliche Schlüsselfunktion 82c und/oder private Schlüsselfunktion 84c (in Figur 6 nicht gezeigt).

Figur 7 zeigt eine dritte alternative Ausgestaltung eines Systems 10d zur Kommunikation von Werkzeugmaschinen 12d in einem Netzwerk 16d mittels asymmetrischer Kryptografie, insbesondere mittels zumindest einer Public-Key-Infrastruktur. Das in der Figur 7 dargestellte System 10d weist eine zumindest im Wesentlichen analoge Ausgestaltung zu dem in der Beschreibung der Figuren 1 bis 4 beschriebenen System 10a auf, so dass bezüglich einer Ausgestaltung des in der Figur 7 dargestellten Systems 10d zumindest im Wesentlichen auf die Beschreibung der Figuren 1 bis 4 verwiesen werden kann. Im Unterschied zu dem in der Beschreibung der Figuren 1 bis 4 beschriebenen System 10a weist das in der Figur 7 dargestellte System 10d eine Servereinheit 18d auf, die eine weitere Steuer- und/oder Regeleinheit 28d umfasst. Die weitere Steuer- und/oder Regeleinheit 28d weist eine Datenbank 120d auf, in welcher insbesondere eine werkzeugmaschinenspezifische Kenngröße 102d der Werkzeugmaschine 12d, eine öffentliche Schlüsselfunktion 82d der Werkzeugmaschine 12d und eine private Schlüsselfunktion 84d der Werkzeugmaschine 12d hinterlegt sind. Vorzugsweise ist die Datenbank dazu eingerichtet, die öffentliche Schlüsselfunktion 82d und die private Schlüsselfunktion 84d mittels der werkzeugspezifischen Kenngröße 102d der Werkzeugmaschine 12d zuzuordnen, insbesondere zu einer Auswahl der öffentlichen Schlüsselfunktion 82d zu einem Verschlüsseln eines an die

Werkzeugmaschine 12d zu übertragenden Datenpakets. Vorteilhafterweise erfolgt eine Authentifizierung und/oder eine Datenübertragung in dem Netzwerk 16d des Systems 10d unabhängig von digitalen Zertifikaten. Vorzugsweise erfolgt in zumindest einem Verfahrensschritt bei einer Datenübertragung und/oder einer Authentifizierung der Werkzeugmaschine 12d über eine Netzwerkeinheit 20d (in Figur 7 nicht gezeigt) mit einer Servereinheit 18d, zumindest einer weiteren Werkzeugmaschine 14d (in Figur 7 nicht gezeigt) und/oder zumindest einer externen Einheit 34d (in Figur 7 nicht gezeigt) eine Verschlüsselung und/oder eine Entschlüsselung eines Datenpakets mittels zumindest einer Kommunikationseinheit 22d und/oder zumindest einer Steuer- und/oder Regeleinheit 24d, insbesondere mittels zumindest eines Krypto-Prozessors 26d (in Figur 7 nicht gezeigt), der Werkzeugmaschine 12d über eine, insbesondere werkzeugmaschinenspezifische, öffentliche Schlüsselfunktion 82d und/oder private Schlüsselfunktion 84d.

Figur 8 zeigt eine vierte alternative Ausgestaltung eines Systems 10e zur Kommunikation von Werkzeugmaschinen 12e in einem Netzwerk 16e mittels asymmetrischer Kryptografie, insbesondere mittels zumindest einer Public-Key-Infrastruktur. Das in der Figur 8 dargestellte System 10e weist eine zumindest im Wesentlichen analoge Ausgestaltung zu dem in der Beschreibung der Figur 7 beschriebenen System 10d auf, so dass bezüglich einer Ausgestaltung des in der Figur 8 dargestellten Systems 10e zumindest im Wesentlichen auf die Beschreibung der Figur 7 verwiesen werden kann. Im Unterschied zu dem in der Beschreibung der Figur 7 beschriebenen System 10d weist das in der Figur 8 dargestellte System 10e eine Servereinheit 18e auf, die eine weitere Steuer- und/oder Regeleinheit 28e umfasst. Die weitere Steuer- und/oder Regeleinheit 28e weist eine Datenbank 120e auf, in der eine werkzeugspezifische Kenngröße 102e der Werkzeugmaschine 12e hinterlegt ist. Die Datenbank 120e ist insbesondere dazu eingerichtet, ein von der Werkzeugmaschine 12e übermitteltes, insbesondere mittels einer weiteren öffentlichen Schlüsselfunktion 86e verschlüsseltes, Datenpaket bei einem Entschlüsseln mittels einer weiteren privaten Schlüsselfunktion 88e der Werkzeugmaschine 12e zuzuordnen. Vorzugsweise erfolgt eine Authentifizierung und/oder eine Datenübertragung in dem Netzwerk 16e des Systems 10e lediglich über mittels der weiteren öffentlichen Schlüsselfunktion 86e und der weiteren privaten Schlüsselfunktion 88e verschlüsselten und/oder entschlüsselten Datenpaketen. Bevorzugt erfolgt eine Authentifizierung

und/oder eine Datenübertragung in dem Netzwerk 16e des Systems 10e unabhängig von von der weiteren öffentlichen Schlüsselfunktion 86e und der weiteren privaten Schlüsselfunktion 88e verschiedenen Schlüsselfunktionen 82e, 84e, 90e, 92e (in der Figur 8 nicht gezeigt). Vorzugsweise erfolgt in zumindest einem Verfahrensschritt bei einer Datenübertragung und/oder einer Authentifizierung der Werkzeugmaschine 12d über eine Netzwerkeinheit 20d (in Figur 8 nicht gezeigt) mit einer Servereinheit 18d, zumindest einer weiteren Werkzeugmaschine 14d (in Figur 8 nicht gezeigt) und/oder zumindest einer externen Einheit 34d (in Figur 8 nicht gezeigt) eine Verschlüsselung und/oder eine Entschlüsselung eines Datenpaket mittels zumindest einer Kommunikationseinheit 22d und/oder zumindest einer Steuer- und/oder Regeleinheit 24d, insbesondere mittels zumindest eines Krypto-Prozessor 26d (in Figur 8 nicht gezeigt), der Werkzeugmaschine 12d über eine, insbesondere werkzeugmaschinenspezifische, öffentliche Schlüsselfunktion 82d und/oder private Schlüsselfunktion 84d (in Figur 8 nicht gezeigt).

Ansprüche

1. Verfahren zur Kommunikation von Werkzeugmaschinen in einem Netzwerk mittels asymmetrischer Kryptografie, insbesondere mittels einer Public-Key-Infrastruktur, **dadurch gekennzeichnet, dass** in zumindest einem Verfahrensschritt (58a) bei einer Datenübertragung und/oder einer Authentifizierung zumindest einer Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) über eine Netzwerkeinheit (20a; 20b; 20c; 20d; 20e) mit einer Servereinheit (18a; 18b; 18c; 18d; 18e), zumindest einer weiteren Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) und/oder zumindest einer externen Einheit (34a; 34b; 34c; 34d; 34e) ein Datenpaket mittels zumindest einer Kommunikationseinheit (22a; 22b; 22c; 22d; 22e) und/oder zumindest einer Steuer- und/oder Regeleinheit (24a; 24b; 24c; 24d; 24e), insbesondere mittels zumindest eines Krypto-Prozessors (26a; 26b; 26c; 26d; 26e), der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) über eine, insbesondere werkzeugmaschinenspezifische, öffentliche Schlüsselfunktion (82a; 82b; 82c; 82d; 82e) und/oder private Schlüsselfunktion (84a; 84b; 84c; 84d; 84e) verschlüsselt und/oder entschlüsselt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** in zumindest einem Verfahrensschritt (60) der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) mittels der Servereinheit (18a; 18b; 18c; 18d; 18e) genau eine werkzeugmaschinenspezifische Kenngröße (102a; 102d; 102e), die öffentliche Schlüsselfunktion (82a; 82b; 82c; 82d; 82e) und die private Schlüsselfunktion (84a; 84b; 84c; 84d; 84e) zugeordnet und übertragen werden, wobei die werkzeugmaschinenspezifische Kenngröße (102a; 102d; 102e), die öffentliche Schlüsselfunktion (82a; 82b; 82c; 82d; 82e) und die private Schlüsselfunktion (84a; 84b; 84c; 84d; 84e) in zumindest einer Speichereinheit der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) hinterlegt werden.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** in zumindest einem Verfahrensschritt (62) mittels der Servereinheit (18a; 18b; 18c; 18d; 18e) und/oder der externen Einheit (34a; 34b; 34c; 34d; 34e) zumindest ein digitales Zertifikat (94a; 94b; 94c; 94d; 94e) generiert wird, welches zumindest eine werkzeugmaschinenspezifische Kenngröße (102a; 102d; 102e), die öffentliche Schlüsselfunktion (82a; 82b; 82c; 82d; 82e), die private Schlüsselfunktion (84a; 84b; 84c; 84d; 84e) und/oder zumindest eine Benutzerinformation umfasst und in der Speichereinheit (55a; 55b; 55c; 55d; 55e) der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) hinterlegt wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** in zumindest einem Verfahrensschritt (64) mittels der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e), der Servereinheit (18a; 18b; 18c; 18d; 18e) und/oder der externen Einheit (34a; 34b; 34c; 34d; 34e) zumindest ein digitaler Marker (100a; 100b; 100c; 100d; 100e) erstellt wird, welcher dazu eingerichtet ist, zumindest einen Benutzer (38a; 38b; 38c; 38d; 38e) und/oder zumindest eine externe Einheit (34a; 34b; 34c; 34d; 34e) über die Kommunikationseinheit (22a; 22b; 22c; 22d; 22e) und/oder die Steuer- und/oder Regeleinheit (24a; 24b; 24c; 24d; 24e), insbesondere den Krypto-Prozessor (26a; 26b; 26c; 26d; 26e), für zumindest eine Anwendung mit der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) und/oder der Servereinheit (18a; 18b; 18c; 18d; 18e) zu verifizieren.

5. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Datenübertragung und/oder die Authentifizierung der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) mit der Netzwerkeinheit (20a; 20b; 20c; 20d; 20e), der Servereinheit (18a; 18b; 18c; 18d; 18e) und/oder der weiteren Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) über die Kommunikationseinheit (22a; 22b; 22c; 22d; 22e) und/oder die Steuer- und/oder Regeleinheit (24a; 24b; 24c; 24d; 24e), insbesondere den Krypto-Prozessor (26a; 26b; 26c; 26d; 26e), mittels zumindest einem auf Transport Layer Security (TLS) basierenden Verschlüsselungsprotokoll gesichert wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** in zumindest einem Verfahrensschritt (68) über die Kommunikationseinheit (22a; 22b; 22c; 22d; 22e) und/oder die Steuer- und/oder Regeleinheit (24a; 24b; 24c; 24d; 24e), insbesondere den Krypto-Prozessor (26a; 26b; 26c; 26d; 26e), zumindest eine Authentifizierung zumindest eines Benutzers (38a; 38b; 38c; 38d; 38e) und/oder der externen Einheit (34a; 34b; 34c; 34d; 34e) mit der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e), der Netzwerkeinheit (20a; 20b; 20c; 20d; 20e) und/oder der Servereinheit (18a; 18b; 18c; 18d; 18e) als Challenge-Response-Authentifizierung erfolgt.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** in zumindest einem Verfahrensschritt (70) zu einer Authentifizierung von zumindest einer Werkzeugzubehöreinheit (32a; 32b; 32c; 32d; 32e), insbesondere bei einem Verbinden der Werkzeugzubehöreinheit (32a; 32b; 32c; 32d; 32e) mit der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e), mittels der Kommunikationseinheit (22a; 22b; 22c; 22d; 22e), der Steuer- und/oder Regeleinheit (24a; 24b; 24c; 24d; 24e), insbesondere dem Krypto-Prozessor (26a; 26b; 26c; 26d; 26e), und/oder der Servereinheit (18a; 18b; 18c; 18d; 18e), insbesondere automatisch, zumindest ein digitales Zertifikat (98a; 98b; 98c; 98d; 98e) der Werkzeugzubehöreinheit (32a; 32b; 32c; 32d; 32e) überprüft wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** in zumindest einem Verfahrensschritt (72) über die Netzwerkeinheit (20a; 20b; 20c; 20d; 20e) und/oder die Servereinheit (18a; 18b; 18c; 18d; 18e), insbesondere mittels der öffentlichen Schlüsselfunktion (82a; 82b; 82c; 82d; 82e), verschlüsselte betriebssystembezogene Daten an die Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) übermittelt werden, welche mittels der Kommunikationseinheit (22a; 22b; 22c; 22d; 22e) und/oder der Steuer- und/oder Regeleinheit (24a; 24b; 24c; 24d; 24e), insbesondere dem Krypto-Prozessor (26a; 26b; 26c; 26d; 26e), insbesondere mittels der privaten Schlüsselfunktion (84a; 84b; 84c; 84d; 84e), entschlüsselt und mit zumindest einer Recheneinheit der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) verarbeitet werden.

9. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** in zumindest einem Verfahrensschritt (74) mittels der Servereinheit (18a; 18b; 18c; 18d; 18e) zumindest eine weitere öffentliche Schlüsselfunktion (86a; 86b; 86c; 86d; 86e) an die Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) und/oder die Netzwerkeinheit (20a; 20b; 20c; 20d; 20e) ausgegeben wird, wobei, insbesondere in zumindest einem weiteren Verfahrensschritt (76), zur Datenübertragung und/oder Authentifizierung der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) und/oder der Netzwerkeinheit (20a; 20b; 20c; 20d; 20e) mit der Servereinheit (18a; 18b; 18c; 18d; 18e) zumindest ein Datenpaket mittels der weiteren öffentlichen Schlüsselfunktion (86a; 86b; 86c; 86d; 86e) verschlüsselt wird und mittels zumindest einer weiteren privaten Schlüsselfunktion (88a; 88b; 88c; 88d; 88e) von der Servereinheit (18a; 18b; 18c; 18d; 18e) entschlüsselt wird.

10. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** in zumindest einem Verfahrensschritt (78) bei der Datenübertragung und/oder der Authentifizierung der Werkzeugmaschine (12a; 12b; 12c; 12d; 12e) das, insbesondere verschlüsselte, Datenpaket mit zumindest einer werkzeugmaschinenspezifischen Kenngröße (102a; 102d; 102e) gekennzeichnet wird, wobei, insbesondere in zumindest einem weiteren Verfahrensschritt (80), das Datenpaket über die Servereinheit (18a; 18b; 18c; 18d; 18e) mittels zumindest einer der werkzeugspezifischen Kenngröße (102a; 102d; 102e) zugeordneten öffentlichen Schlüsselfunktion (82a; 82b; 82c; 82d; 82e) entschlüsselt wird.

11. System zur Kommunikation von Werkzeugmaschinen in einem Netzwerk mittels asymmetrischer Kryptografie, insbesondere mittels zumindest einer Public-Key-Infrastruktur, insbesondere gemäß einem Verfahren nach einem der Ansprüche 1 bis 8, mit zumindest einer Werkzeugmaschine (12a; 12b; 12c; 12d; 12e), mit zumindest einer Servereinheit (18a; 18b; 18c; 18d; 18e) und mit zumindest einer Netzwerkeinheit (20a; 20b; 20c; 20d; 20e).

12. Werkzeugmaschine zur Kommunikation in einem Netzwerk mittels asymmetrischer Kryptografie, insbesondere mittels zumindest einer Public-Key-

Infrastruktur, insbesondere gemäß einem Verfahren nach einem der Ansprüche 1 bis 8, mit zumindest einer Kommunikationseinheit (22a; 22b; 22c; 22d; 22e) zu einer, insbesondere drahtlosen, Übertragung von elektronischen Daten und mit zumindest einer mit der Kommunikationseinheit (22a; 22b; 22c; 22d; 22e) verbundenen Steuer- und/oder Regeleinheit (24a; 24b; 24c; 24d; 24e) zu einer Auswertung und/oder Bearbeitung von übertragenen und/oder zu übertragenen Daten, **dadurch gekennzeichnet, dass** die Steuer- und/oder Regeleinheit (24a; 24b; 24c; 24d; 24e) dazu eingerichtet ist, übertragene und/oder zu übertragene Daten zu entschlüsseln oder zu verschlüsseln.

Fig. 1

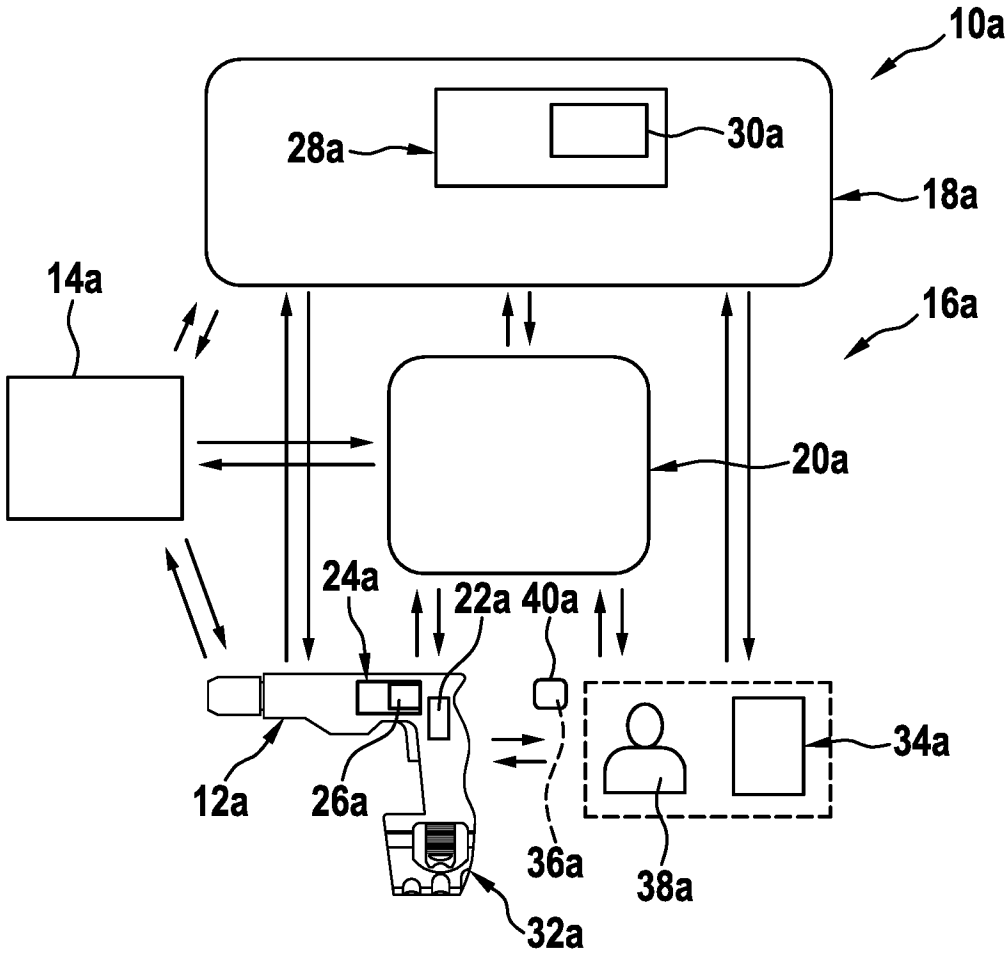


Fig. 2

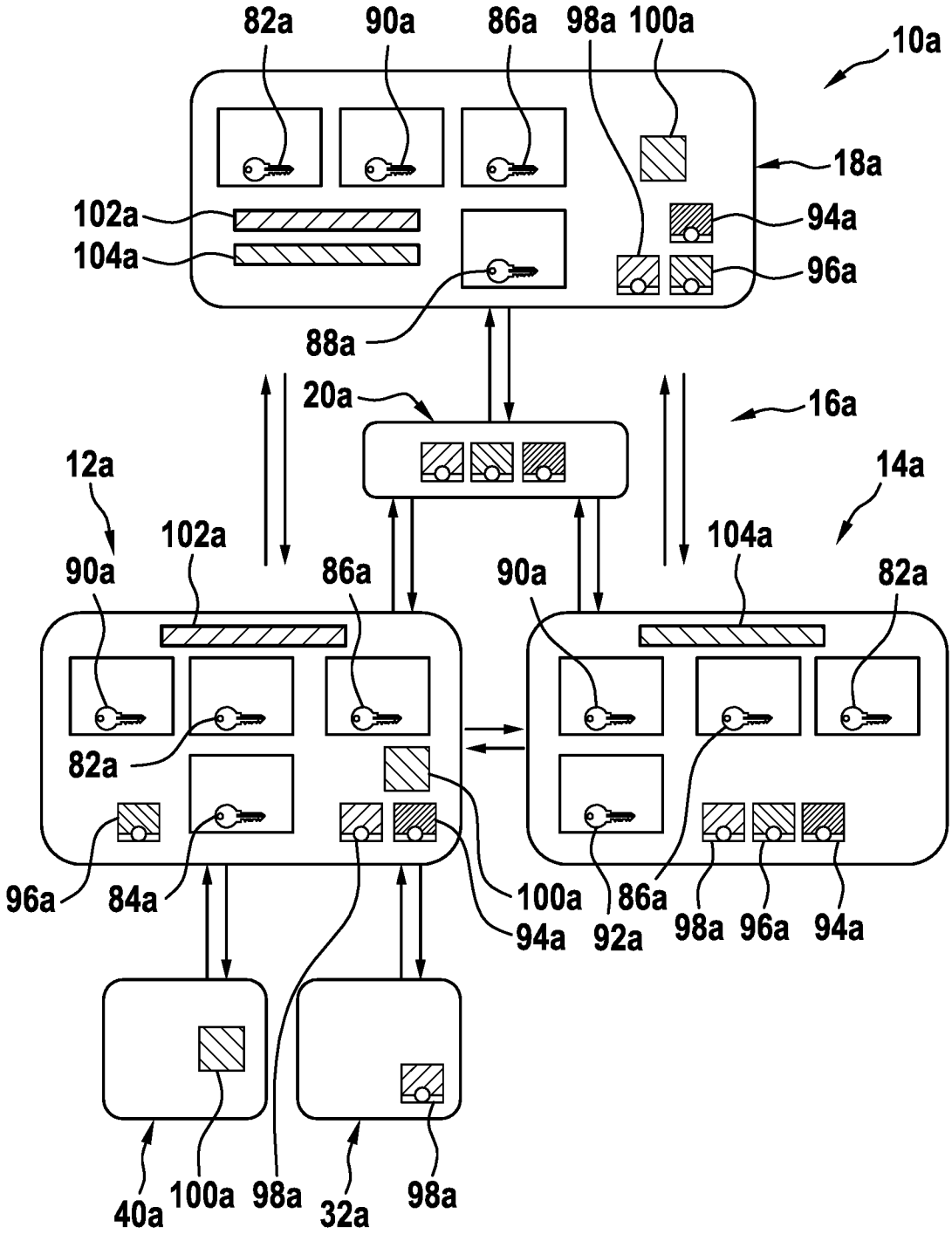

82a
90a
86a
98a
100a
10a
18a
102a
104a
94a
96a
88a
20a
16a
12a
14a
102a
104a
90a
86a
90a
82a
82a
96a
84a
100a
94a
86a
92a
98a
96a
94a
40a
100a
98a
32a
98a

Fig. 3

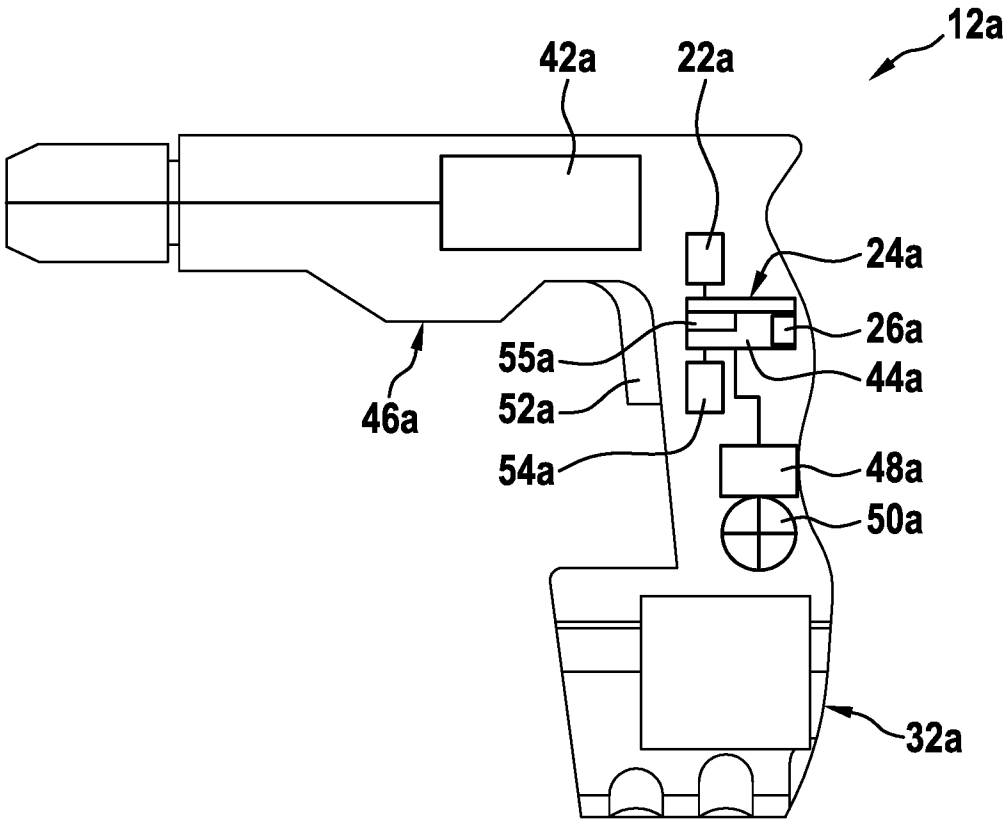


Fig. 4

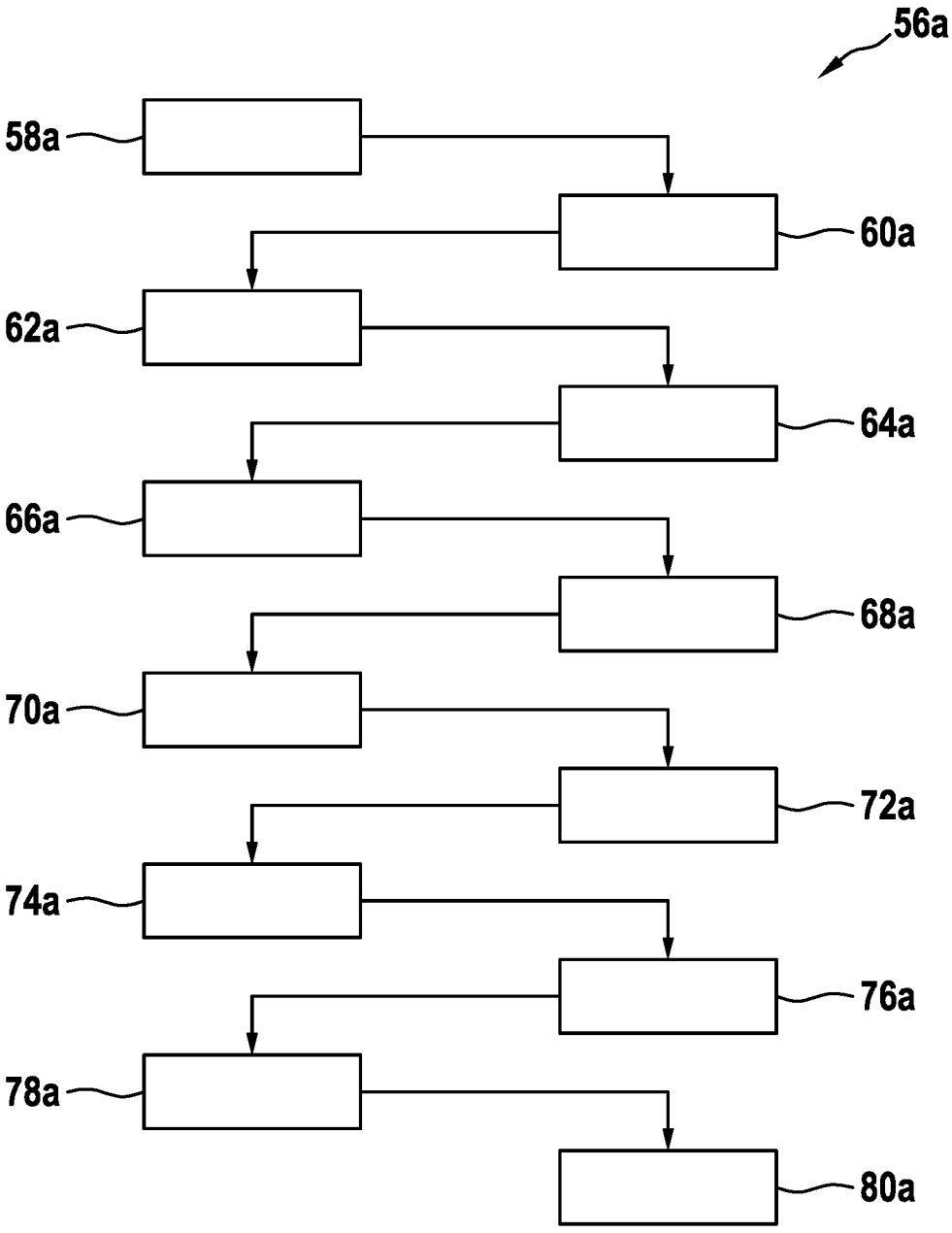


Fig. 5

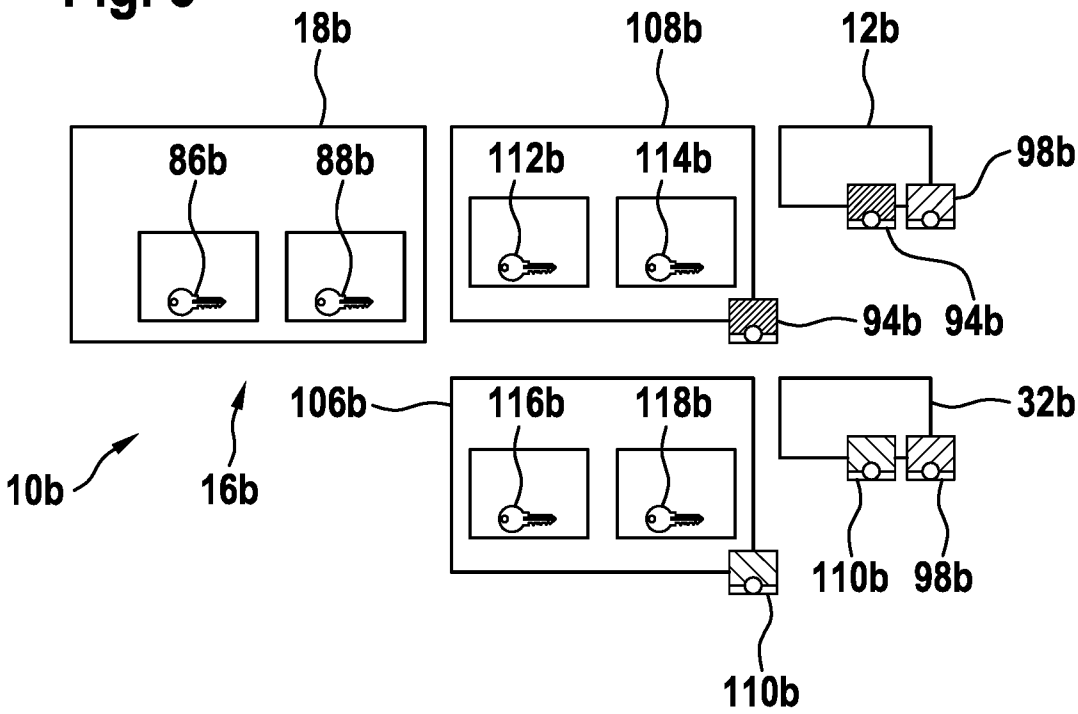

18b
108b
12b
86b
88b
112b
114b
98b
94b
94b
106b
116b
118b
32b
10b
16b
110b
98b
110b

Fig. 6

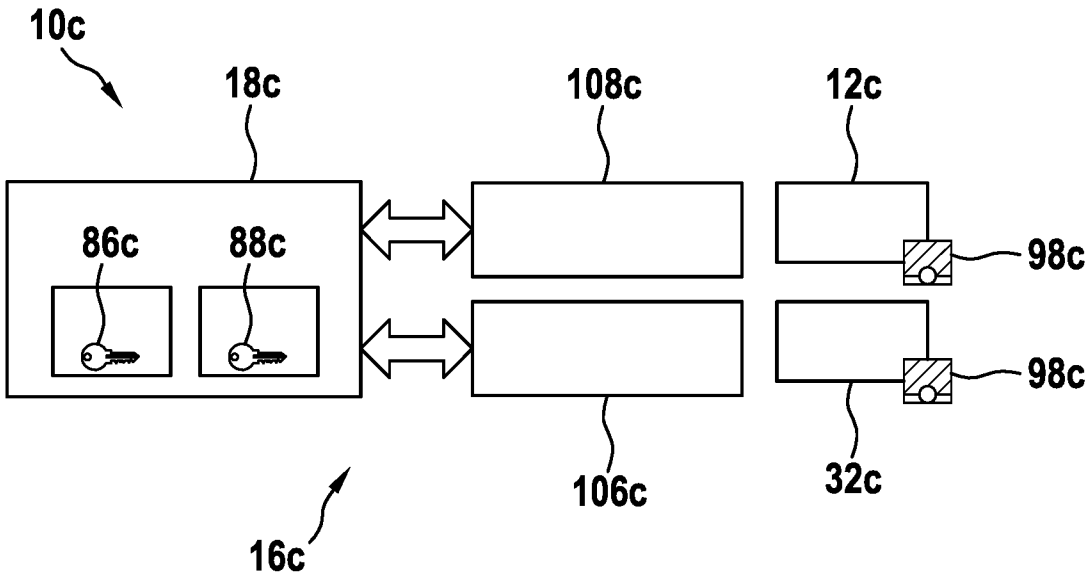

10c
18c
108c
12c
86c
88c
98c
98c
106c
32c
16c

Fig. 7

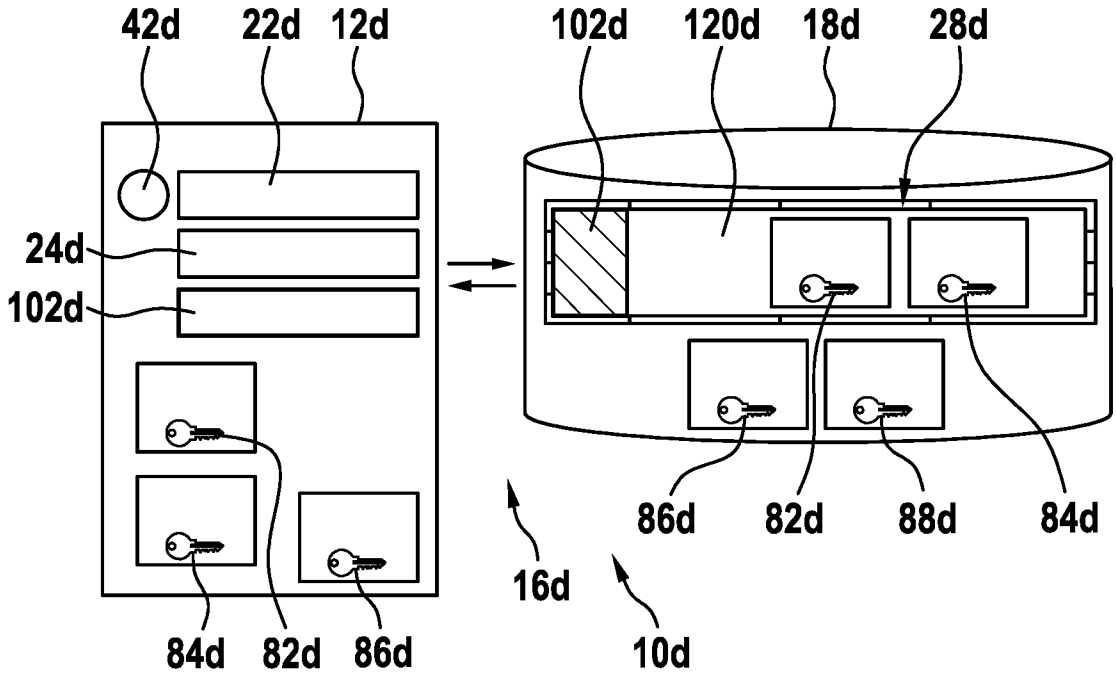
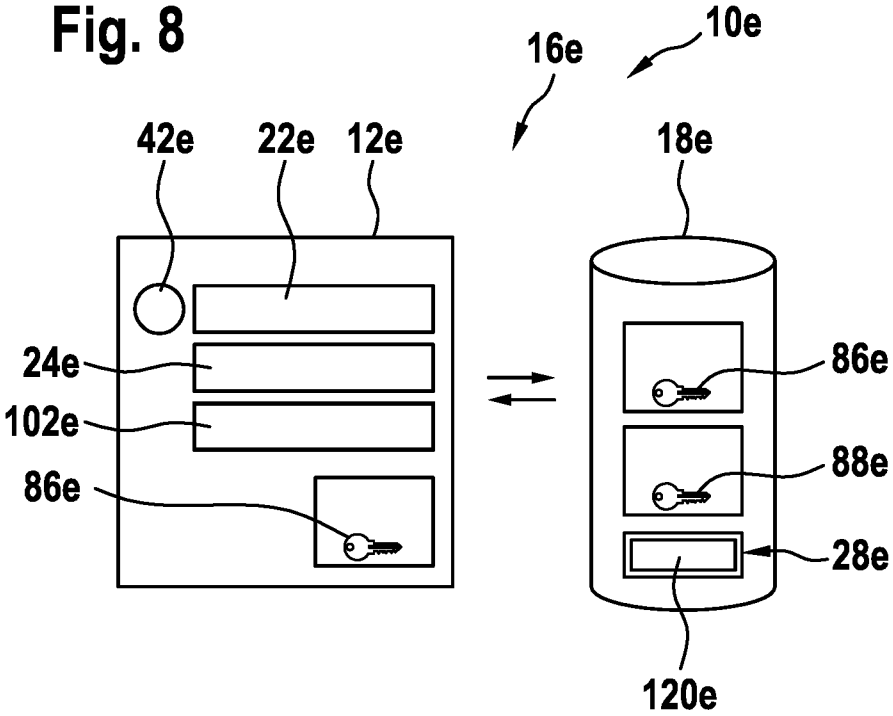

42d
22d
12d
102d
120d
18d
28d
24d
102d
86d
82d
88d
84d
16d
10d
84d
82d
86d

Fig. 8



# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/EP2019/085122**

## A. CLASSIFICATION OF SUBJECT MATTER

***H04L 29/06***(2006.01)i; ***G06F 21/44***(2013.01)i; ***G06F 21/60***(2013.01)i; ***H04L 29/08***(2006.01)i; ***H04W 4/70***(2018.01)i; ***H04W 12/00***(2009.01)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; G06F; H04W

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 | US 2004054630 A1 (GINTER KARL L [US] ET AL) 18 March 2004 (2004-03-18)<br>paragraphs [0147], [0437], [0450] - [0453], [0457], [0462] - [0467], [0474] - [0457], [1451] - [1453], [1613], [1630] - [1637] | 1-12 |
| X | US 2017068266 A1 (ENYEDY EDWARD A [US]) 09 March 2017 (2017-03-09)<br>paragraphs [0026] - [0030], [0046] - [0047], [0058] - [0059]; figure 1 | 1-12 |
| X | US 2018248704 A1 (COODE DAVID [CA] ET AL) 30 August 2018 (2018-08-30)<br>paragraphs [0033] - [0035], [0039], [0074], [0085] - [0086], [0101] - [0107] | 1-12 |
| X | DE 102014218475 A1 (BOSCH GMBH ROBERT [DE]) 17 March 2016 (2016-03-17)<br>paragraphs [0003] - [0011], [0025], [0030] - [0031]; figures 1,3 | 1-12 |
| X | US 2007055731 A1 (THIBEAULT JASON [US]) 08 March 2007 (2007-03-08)<br>paragraphs [0070] - [0074], [0163] | 1-12 |

☐ 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 |
|---|---|
| **02 March 2020** | **18 March 2020** |
| Name and mailing address of the ISA/EP<br>**European Patent Office**<br>**p.b. 5818, Patentlaan 2, 2280 HV Rijswijk**<br>**Netherlands**<br>Telephone No. **(+31-70)340-2040**<br>Facsimile No. **(+31-70)340-3016** | Authorized officer<br>**Betz, Sebastian**<br>Telephone No. |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/EP2019/085122**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| US 2004054630 A1 | 18 March 2004 | US 7069451 B1 | 27 June 2006 |
| | | US 2004054630 A1 | 18 March 2004 |
| US 2017068266 A1 | 09 March 2017 | CN 106502146 A | 15 March 2017 |
| | | DE 202016005360 U1 | 08 December 2017 |
| | | US 2017068266 A1 | 09 March 2017 |
| | | US 2019041888 A1 | 07 February 2019 |
| US 2018248704 A1 | 30 August 2018 | NONE | |
| DE 102014218475 A1 | 17 March 2016 | CN 105426934 A | 23 March 2016 |
| | | DE 102014218475 A1 | 17 March 2016 |
| | | US 2016080038 A1 | 17 March 2016 |
| US 2007055731 A1 | 08 March 2007 | NONE | |

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2019/085122

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06 G06F21/44 G06F21/60 H04L29/08 H04W4/70
H04W12/00
ADD.
Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole )
H04L G06F H04W

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 | US 2004/054630 A1 (GINTER KARL L [US] ET AL) 18. März 2004 (2004-03-18) Absätze [0147], [0437], [0450] - [0453], [0457], [0462] - [0467], [0474] - [0457], [1451] - [1453], [1613], [1630] - [1637] | 1-12 |
| X | US 2017/068266 A1 (ENYEDY EDWARD A [US]) 9. März 2017 (2017-03-09) Absätze [0026] - [0030], [0046] - [0047], [0058] - [0059]; Abbildung 1 | 1-12 |
| X | US 2018/248704 A1 (COODE DAVID [CA] ET AL) 30. August 2018 (2018-08-30) Absätze [0033] - [0035], [0039], [0074], [0085] - [0086], [0101] - [0107] | 1-12 |

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] 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 |
|---|---|
| 2. März 2020 | 18/03/2020 |

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

2

Formblatt PCT/ISA/210 (Blatt 2) (April 2005)

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| X | DE 10 2014 218475 A1 (BOSCH GMBH ROBERT [DE]) 17. März 2016 (2016-03-17) Absätze [0003] - [0011], [0025], [0030] - [0031]; Abbildungen 1,3 | 1-12 |
| X | US 2007/055731 A1 (THIBEAULT JASON [US]) 8. März 2007 (2007-03-08) Absätze [0070] - [0074], [0163] | 1-12 |

## INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2019/085122

| Im Recherchenbericht angeführtes Patentdokument | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | Datum der Veröffentlichung |
|---|---|---|---|
| US 2004054630 A1 | 18-03-2004 | US 7069451 B1 | 27-06-2006 |
| | | US 2004054630 A1 | 18-03-2004 |
| US 2017068266 A1 | 09-03-2017 | CN 106502146 A | 15-03-2017 |
| | | DE 202016005360 U1 | 08-12-2017 |
| | | US 2017068266 A1 | 09-03-2017 |
| | | US 2019041888 A1 | 07-02-2019 |
| US 2018248704 A1 | 30-08-2018 | KEINE | |
| DE 102014218475 A1 | 17-03-2016 | CN 105426934 A | 23-03-2016 |
| | | DE 102014218475 A1 | 17-03-2016 |
| | | US 2016080038 A1 | 17-03-2016 |
| US 2007055731 A1 | 08-03-2007 | KEINE | |