(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
24. Januar 2019 (24.01.2019)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2019/015860 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2018/065020

(22) Internationales Anmeldedatum:
07. Juni 2018 (07.06.2018)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2017 212 474.1
20. Juli 2017 (20.07.2017) DE

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

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

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

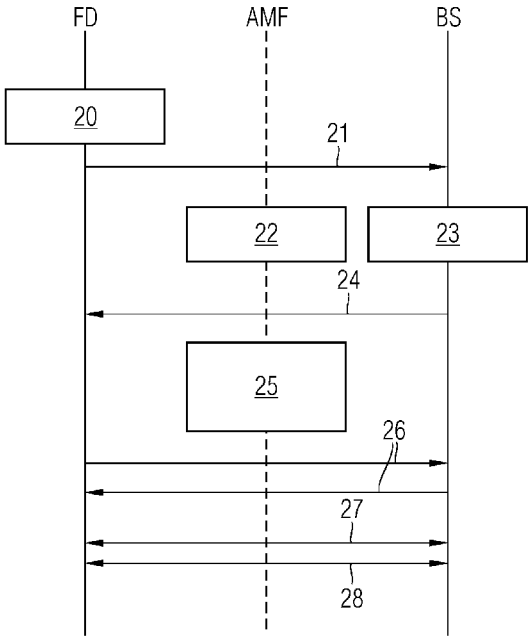
(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST,

WO 2019/015860 A1

(54) **Title:** METHOD, DEVICES AND COMPUTER PROGRAM PRODUCT FOR EXAMINING CONNECTION PARAMETERS OF A CRYPTOGRAPHICALLY PROTECTED COMMUNICATION CONNECTION DURING ESTABLISHING OF THE CONNECTION

(54) **Bezeichnung:** VERFAHREN, VORRICHTUNGEN UND COMPUTERPROGRAMMPRODUKT ZUR ÜBERPRÜFUNG VON VERBINDUNGSPARAMETERN EINER KRYPTOGRAPHISCH GESCHÜTZTEN KOMMUNIKATIONSVERBINDUNG WÄHREND DES VERBINDUNGSAUFBAUS

FIG 3



(57) Abstract: The invention relates to a method for examining connection parameters during establishing of a cryptographically protected communication connection between a first communication device (FD) and a second communication device (BS), comprising the method steps: - transmitting (11 and 20) an attestation data structure, which contains at least one connection parameter of the first and/or second communication device (FD, BS) as attestation information, from the first and/or second communications devices (FD, BS) to the second and/or first communication device (BS, FD), - eavesdropping (12 and 22) on the attestation data structure by means of a monitoring device (AMF, 47) arranged within a data transmission path of the communication connection, - examining (13 and 22) the attestation information in comparison to a specified guideline, and a corresponding communication system, a communication device, a monitoring device and a computer program product for carrying out the method.

(57) Zusammenfassung: Verfahren zur Überprüfung von Verbindungsparametern während des Aufbaus einer kryptographisch geschützten Kommunikationsverbindung zwischen einer ersten Kommunikationsvorrichtung (FD) und einer zweiten Kommunikationsvorrichtung (BS), mit den Verfahrensschritten: - Senden (11, 20) einer Attestierungsdatenstruktur, die mindestens einen Verbindungsparameter der ersten und/oder zweiten Kommunikationsvorrichtung (FD, BS) als Attestierungsinformation enthält, von der ersten und/oder zweiten Kommunikationsvorrichtungen (FD, BS) an die zweite und/oder erste Kommunikationsvorrichtung (BS, FD), - Mithören (12, 22) der Attestierungsdatenstruktur durch eine innerhalb eines

[Fortsetzung auf der nächsten Seite]

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)*

Datenübertragungspfads der Kommunikationsverbindung angeordnete Überwachungsvorrichtung (AMF, 47), - Überprüfen (13, 22) der Attestierungsinformation gegenüber einer vorgegebenen Richtlinie, sowie ein entsprechendes Kommunikationssystem, eine Kommunikationsvorrichtung, eine Überwachungsvorrichtung sowie ein Computerprogrammprodukt zur Durchführung des Verfahrens.

Beschreibung

VERFAHREN, VORRICHTUNGEN UND COMPUTERPROGRAMMPRODUKT ZUR ÜBERPRÜFUNG VON VERBINDUNGSPARAMETERN EINER KRYPTOGRAPHISCH GESCHÜTZTEN KOMMUNIKATIONSVERBINDUNG WÄHREND DES VERBINDUNGSAUFBAUS

Die Erfindung betrifft ein Verfahren, ein Kommunikationssystem, eine Kommunikationsvorrichtung sowie eine Überwachungsvorrichtung zur Überprüfung von Verbindungsparametern einer kryptographisch geschützten Kommunikationsverbindung zwischen einer ersten Kommunikationsvorrichtung und einer zweiten Kommunikationsvorrichtung während des Aufbaus der kryptographisch geschützten Kommunikationsverbindung.

Kryptographisch geschützte Kommunikationsprotokolle, wie beispielsweise ein IP-Sicherheitsprotokoll IPsec/IKE oder das Transportschichtsicherheitsprotokoll TLS, DTLS, QUIC, schützen zu übertragende Daten vor Manipulation und Ausspähen. Dabei erfolgen eine Authentisierung der Kommunikationspartner und eine Vereinbarung eines Sitzungsschlüssels. Bei einem Verbindungsaufbau über das TLS-Protokoll initiiert eine erste Kommunikationsvorrichtung als sogenannter TLS-Client eine Verbindung zu einer zweiten Kommunikationsvorrichtung, die als TLS-Server bezeichnet wird. Der TLS-Server authentifiziert sich typischerweise gegenüber dem TLS-Client mit einem Zertifikat. Der TLS-Client überprüft die Vertrauenswürdigkeit des Zertifikats und prüft, ob der Name des TLS-Servers, d.h. dessen DNS-Name, mit dem im Zertifikat angegebenen Namen übereinstimmt. Optional kann sich der TLS-Client mit einem eigenen Zertifikat auch gegenüber dem TLS-Server authentifizieren. Daraufhin sendet entweder der TLS-Client dem TLS-Server eine mit dem öffentlichen Schlüssel des TLS-Servers verschlüsselte geheime Zufallszahl, oder die beiden Parteien berechnen über einen Diffie-Hellman-Schlüsselaustausch ein gemeinsames Geheimnis. Aus dem Geheimnis wird dann ein kryptographischer Schlüssel abgeleitet, der zur Verschlüsselung der Payload-Nachrichten der Verbindung verwendet wird. Das TLS-Protokoll wird in einer Sitzungsschicht (Schicht 5) des

OSI-Referenzmodells für Netzwerkprotokolle ausgeführt, d.h. oberhalb des TCP-Protokolls oder UDP-Protokolls.

Das kryptographisch geschützte Internetprotokoll Security IPsec Protokoll ermöglicht eine gesicherte Kommunikation über potentiell unsichere Internetprotokoll (IP) Netze, wie das Internet. Zur Schlüsselverwaltung wird insbesondere das Internet Key Exchange Protokoll IKE, bevorzugt in der Version 2, verwendet. Das IPsec Protokoll arbeitet direkt auf der Internetschicht, die der Vermittlungsschicht (Schicht 3) des OSI-Referenzmodells entspricht.

Insbesondere in industriellen Umgebungen, wie beispielsweise in Automatisierungssystemen, besteht die Anforderung, die Kommunikation zwischen den einzelnen Geräten zu überwachen. Bekannte Ansätze zielen darauf ab, die übertragenen Nutzdaten überwachen zu können. Dies steht jedoch im Widerspruch zu einem Ende-zu-Ende Schutzes der übertragenen Daten. Es besteht der Bedarf, eine gewisse Überwachung von kryptographischen Verbindungen zu ermöglichen ohne den Schutz der Ende-zu-Ende Übertragung zu gefährden.

Aus der EP 3 171 570 A1 ist eine Vorrichtung bekannt, die es ermöglicht, von einem Endgerät unterstützte Optionen eines kryptographisch geschützte Kommunikationsprotokolls zu überprüfen. Dazu initiiert eine Kommunikationseinheit aktiv eine Kommunikationsverbindung zu dem Endgerät oder die Kommunikationseinheit empfängt eine Initiierungsnachricht vom Endgerät und baut eine Testkommunikation auf. Dabei kann die Konfiguration des Kommunikationsprotokolls auf dem Endgerät überprüft werden. Ein solcher zusätzlicher Aufbau einer Testkommunikation erzeugt einerseits zusätzliche Last auf einem Kommunikationsnetz, als auch auf dem zu überprüfenden Endgerät. Des Weiteren beschränken sich die prüfbaren Daten ausschließlich auf Informationen, die bei der Authentifizierung und Schlüsselvereinbarung vom Endgerät entsprechend dem Sicherheitsprotokoll übermittelt werden.

Vor diesem Hintergrund besteht eine Aufgabe der vorliegenden Erfindung darin, eine erweiterte Anzahl von Verbindungsparametern überwachen zu können, dabei die Kommunikationspartner sowie das Kommunikationsnetz möglichst wenig zu belasten und den Schutz der Ende-zu-Ende Übertragung nicht zu gefährden.

Die Aufgabe wird durch die in den unabhängigen Ansprüchen beschriebenen Maßnahmen gelöst. In den Unteransprüchen sind vorteilhafte Weiterbildungen der Erfindung dargestellt.

Gemäß einem ersten Aspekt betrifft die Erfindung ein Verfahren zur Überprüfung von Verbindungsparametern während des Aufbaus einer kryptographisch geschützten Kommunikationsverbindung zwischen einer ersten Kommunikationsvorrichtung und einer zweiten Kommunikationsvorrichtung, mit den Verfahrensschritten:
- Senden (11) einer Attestierungsdatenstruktur, die mindestens einen Verbindungsparameter der ersten und/oder zweiten Kommunikationsvorrichtung als Attestierungsinformation enthält, von der ersten und/oder zweiten Kommunikationsvorrichtungen an die zweite und/oder erste Kommunikationsvorrichtung,
- Mithören der Attestierungsdatenstruktur durch eine innerhalb der Datenübertragungsstrecke der Kommunikationsverbindung angeordnete Überwachungsvorrichtung und
- Überprüfen der Attestierungsinformation gegenüber einer vorgegebenen Richtlinie.

Dies ermöglicht es einem Dritten zu überwachen, ob das verwendete Sicherheitsprotokoll wie erwartet verwendet wird. Dies kann dabei während des Aufbaus einer Kommunikationsverbindung zwischen den tatsächlichen Kommunikationspartnern erfolgen, so dass keine zusätzliche Testkommunikation zu einer zusätzlichen Kommunikationseinheit aufgebaut werden muss. Es muss auch keine aktive Komponente in den Kommunikationspfad eingebracht werden, die die geschützte Kommunikationsverbindung beeinflussen könnte oder einen Einfluss auf die Antwortzeiten des Kommunikationspartners haben kann. Damit ist eine

Ende-zu-Ende Sicherheit der Kommunikationsverbindung nicht geschwächt. Es wird ebenfalls keine zusätzliche Kommunikationsverbindung aufgebaut, die das Kommunikationsgerät oder das Kommunikationsnetz belastet. Es wird lediglich eine durch Dritte überprüfbare Information zur aufgebauten kryptographisch gesicherten Kommunikationsverbindung bereitgestellt. Insbesondere bei der Nutzung in sicherheitskritischen industriellen Steuerungssystemen ist dies vorteilhaft, um sicherzustellen, dass eine kryptographisch geschützte Steuerungskommunikation nur so wie vorgesehen und zugelassen erfolgt. Insbesondere kann dadurch im laufenden Betrieb überprüft werden, dass eine abgenommene, freigegebene Anlagenkonfiguration nur so wie freigegeben im tatsächlichen operativen Betrieb verwendet wird. Diese Überwachung der Integrität bzw. der Einhaltung der vorgegebenen Sicherheitspolitik ist möglich, obwohl die Datenübertragung kryptographisch geschützt erfolgt.

In einer vorteilhaften Ausführungsform wird die kryptographisch geschützte Kommunikationsverbindung gemäß einem Transportschicht-Sicherheitsprotokoll TLS/DTLS/SSL oder einem Internet Protokoll-Sicherheitsprotokoll IPsec aufgebaut und die Attestierungsdatenstruktur als Erweiterung einer Protokollnachricht, insbesondere einer TLS-Handshake-Nachricht oder einer Internet-Schlüsselaustausch IKE Nachricht ausgebildet.

Dies hat den Vorteil, dass lediglich eine beziehungsweise mehrere Nachrichten durch die Attestierungsdatenstruktur ergänzt werden, der Ablauf des verwendeten Sicherheitsprotokolls aber unverändert bleibt. Solche Erweiterungen sind einfach implementierbar und werden von den Standards der genannten Sicherheitsprotokolle unterstützt. Um das passive Mitlesen zu ermöglichen, erfolgt die Übertragung der Attestierungsdatenstruktur vorzugsweise im lesbaren, nicht verschlüsselten Teil der Protokollnachrichten des Sicherheitsprotokolls. Im Falle von TLS können dazu insbesondere Handshake-Nachrichten für die Authentisierung und Schlüsselvereinbarung verwendet werden.

In einer vorteilhaften Ausführungsform wird eine Attestierungsdatenstruktur mit mindestens einem Verbindungsparameter der sendenden Kommunikationsvorrichtung als Attestierungsinformation sowohl von der ersten Kommunikationsvorrichtung als auch von der zweiten Kommunikationsvorrichtung zur jeweils anderen Kommunikationsvorrichtung gesendet.

Dadurch können nicht nur Verbindungsparameter der ersten Kommunikationsverbindung, die den Verbindungsaufbau veranlasst und üblicherweise als Client bezeichnet wird, überprüft werden, sondern auch Verbindungsparameter der zweiten Kommunikationsvorrichtung, die üblicherweise als Server bezeichnet wird.

In einer vorteilhaften Ausführungsform wird die Attestierungsdatenstruktur durch einen Attestierungsschlüssel kryptographisch geschützt.

Dies ermöglicht es, die Integrität der Attestierungsdatenstruktur und auch die Authentizität der sendenden Kommunikationsvorrichtung zu überwachen. Die kryptographisch geschützte Attestierungsdatenstruktur kann dabei insbesondere durch eine kryptographische Prüfsumme, insbesondere eine digitale Signatur oder durch einen kryptographischen Nachrichtenauthentisierungscode (message authentication code, MAC), geschützt sein. Ebenso ist es möglich, dass die kryptographisch geschützte Attestierungsdatenstruktur oder einzelne Felder der kryptographisch geschützten Attestierungsdatenstruktur verschlüsselt sind. Vorzugsweise ist die kryptographische Prüfsumme Teil der Attestierungsdatenstruktur, d.h. dass die Attestierungsdatenstruktur aus einer Attestierungsinformation und einer kryptographischen Attestierungsprüfsumme besteht. Es ist jedoch auch möglich, dass die kryptographische Attestierungsprüfsumme separat zur Attestierungsinformation vorliegt.

Beispielsweise kann als Attestierungsschlüssel der zur Authentisierung verwendete Schlüssel der sendenden Kommunikationsvorrichtung verwendet werden.

Dies hat den Vorteil, dass kein zusätzliches Schlüsselmaterial erzeugt werden muss. Bei einer Authentisierung der Kommunikationsvorrichtungen in einem TLS oder IPsec Protokoll werden die öffentlichen Schlüssel der Kommunikationspartner meist als Zertifikate unverschlüsselt übermittelt und können somit ebenso wie die Attestierungsdatenstruktur ausgekoppelt, verifiziert und zur weiteren kryptographischen Sicherung der Attestierungsdatenstruktur verwendet werden.

Mit „auskoppeln" ist im Weiteren insbesondere das Bereitstellen einer Datenstruktur an eine dritte Komponent außerhalb der eigentlichen Kommunikationsverbindung bezeichnet. Dabei ist die ausgekoppelte Information bevorzugt eine Kopie der von einer Kommunikationsvorrichtung empfangenen Datenstruktur sein. Die ursprüngliche Datenstruktur wird bevorzugt an die empfangende Kommunikationsvorrichtung über die Kommunikationsverbindung ausgegeben.

In einer vorteilhaften Ausführungsform wird der Attestierungsschlüssel einer Auswertevorrichtung über eine von der Kommunikationsverbindung unterschiedliche, separate Verbindung bereitgestellt.

Dies hat den Vorteil, dass die Auswertung der Attestierungsdatenstruktur nur von solchen Auswertevorrichtungen durchgeführt werden kann, die den Attestierungsschlüssel erhalten haben. Somit können explizit bestimmte Auswertevorrichtungen für die Auswertung einer Kommunikationsvorrichtung berechtigt werden. Der Attestierungsschlüssel kann dabei ein beliebiger kryptographischer Schlüssel sein. Als Kommunikationsverbindung wird die mit dem erfindungsgemäßen Verfahren überwachte Verbindung bezeichnet. Eine davon unterschiedliche, separate Verbindung kann eine über einen anderen Datenübertragungspfad

geführte Verbindung sein. Die separate Verbindung kann aber auch den gleichen Datenübertragungspfad wie die überwachte Kommunikationsverbindung nutzen, jedoch eine eigene, logisch getrennte Verbindung sein.

In einer vorteilhaften Ausführungsform wird die Attestierungsinformation von der senden Kommunikationsvorrichtung einer Speichereinrichtung, insbesondere einer Datenbank oder einem Logging-Server bereitgestellt.

Dies hat den Vorteil, dass die Auswertung der Attestierungsinformation zeitlich entkoppelt und beispielsweise zentralisiert durchgeführt werden kann.

In einer vorteilhaften Ausführungsform umfasst die Attestierungsdatenstruktur lediglich einen Referenzwert und über den Referenzwert wird die Attestierungsinformation auf der Speichereinrichtung ermittelt.

Dies hat den Vorteil, dass die Kommunikationsverbindung mit geringer zusätzlicher Last beaufschlagt wird. Andererseits kann die sendende Kommunikationsvorrichtung die Attestierungsinformation über eine andere, beispielsweise eine bereits vorhandene und/oder sichere Verbindung, auf einer Speichereinrichtung wie der vorgenannten Datenbank oder einem Logging-Server abgelegt werden kann. Der Referenzwert kann insbesondere ein kryptographischer Hash-Wert der Attestierungsinformation sein.

In einer vorteilhaften Ausführungsform werden vordefinierte Maßnahmen, insbesondere ein Ausgeben eines Warnsignals und/oder ein Blockieren der Kommunikationsverbindung, durchgeführt, wenn bei der Überprüfung eine Abweichung von der Richtlinie festgestellt wird.

Gemäß einem zweiten Aspekt betrifft die Erfindung ein Kommunikationssystem zur Überprüfung von Verbindungsparametern während des Aufbaus einer kryptographisch geschützten Kommu-

nikationsverbindung zwischen einer ersten Kommunikationsvorrichtung und einer zweiten Kommunikationsvorrichtung, wobei mindestens die erste und/oder zweite Kommunikationsvorrichtung, derart ausgebildet ist, eine Attestierungsdatenstruktur an die zweite und/oder erste Kommunikationsvorrichtung zu senden, und die Attestierungsdatenstruktur mindestens einen Verbindungsparameter der ersten und/oder zweiten Kommunikationsvorrichtung als Attestierungsinformation enthält, umfassend:

- eine Mithöreinheit, die innerhalb eines Datenübertragungspfads der Kommunikationsverbindung angeordnet ist und derart ausgebildet ist, die Attestierungsdatenstruktur auszukoppeln und
- eine Überprüfungseinheit, die derart ausgebildet ist, die Attestierungsinformation gegenüber einer vorgegebenen Richtlinie zu überprüfen.

Ein Datenübertragungspfad ist eine aus einem oder mehreren physikalischen Datenübertragungsstrecken zusammengesetzte physikalische Verbindungsstrecke zwischen der ersten und zweiten Kommunikationsvorrichtung. Der physikalische Datenübertragungspfad einer logischen Kommunikationsverbindung kann mehrere Datenübertragungsstrecken und Übertragungskomponenten, wie beispielsweise Router, Switche oder auch Firewalls, umfassen. Eine Überwachungsvorrichtung greift beispielsweise die Daten innerhalb einer Übertragungskomponente oder auch an einem Ausgang einer Übertragungskomponente die Protokollnachrichten ab und extrahiert daraus die Attestierungsdatenstruktur. Das Kommunikationssystem erlaubt es sicherheitsrelevante Informationen der Kommunikationsvorrichtungen und der Kommunikationsverbindung für Dritte zugänglich zu machen.

Gemäß einem dritten Aspekt betrifft die Erfindung eine Kommunikationsvorrichtung zur Überprüfung von Verbindungsparametern während des Aufbaus einer kryptographisch geschützten Kommunikationsverbindung zwischen der Kommunikationsvorrichtung und einer zweiten Kommunikationsvorrichtung, umfassend eine Sendevorrichtung, die derart ausgebildet ist, eine kryp-

tographisch geschützte Attestierungsdatenstruktur, die mindestens einen Verbindungsparameter als Attestierungsinformation enthält, an die zweite Kommunikationsvorrichtung zu senden.

Die Kommunikationsvorrichtung erlaubt somit Verbindungsparameter, die für die aktuell aufgebaute Kommunikationsverbindung verwendet werden, auf der Kommunikationsverbindung selbst bereitzustellen, so dass diese zu Überwachungszwecken ausgelesen werden können.

In einer vorteilhaften Ausführungsform ist die Kommunikationsvorrichtung als Client-Vorrichtung oder als Server-Vorrichtung ausgebildet.

Dies ermöglicht es, Attestierungsinformation von beiden Endkomponenten der Kommunikationsverbindung verwendete Verbindungsparameter Mithören zu können.

Gemäß einem vierten Aspekt betrifft die Erfindung eine Überwachungsvorrichtung zur Überprüfung von Verbindungsparametern während des Aufbaus einer kryptographisch geschützten Kommunikationsverbindung zwischen einer ersten Kommunikationsvorrichtung und einer zweiten Kommunikationsvorrichtung, umfassend eine Mithöreinheit, die innerhalb des Datenübertragungspfads der Kommunikationsverbindung anordenbar ist und derart ausgebildet ist, die Attestierungsdatenstruktur mitzuhören und die Attestierungsinformation einer Überprüfungseinrichtung bereitzustellen, sowie eine Überprüfungseinheit, die derart ausgebildet ist, die Attestierungsinformation gegenüber einer vorgegebenen Richtlinie zu überprüfen.

Mit Mithören ist ein passiver Vorgang bezeichnet, bei dem die Daten kopiert werden und diese Kopie an die Überprüfungseinheit ausgegeben wird. Die ursprünglichen Daten werden unverändert an den Kommunikationspartner ausgegeben. Durch das Mithören werden die ursprünglichen Daten nicht verändert und nicht ergänzt. Das Mithören verursacht keine oder eine ledig-

lich kurze Verzögerungszeit. Somit kann Attestierungsinformationen ohne signifikante Beeinflussung der ursprünglichen Kommunikationsverbindung abgegriffen werden.

In einer vorteilhaften Ausführungsform umfasst die Überwachungsvorrichtung zusätzlich eine Durchsetzungseinheit, die derart ausgebildet ist, vordefinierte Maßnahmen, insbesondere ein Signal auszugeben und/oder ein Blockieren der Kommunikationsverbindung, durchzuführen, wenn bei der Überprüfung eine Abweichung von der Richtlinie festgestellt wird.

Gemäß einem fünften Aspekt betrifft die Erfindung ein Computerprogrammprodukt, das direkt in einen Speicher eines digitalen Computers ladbar ist und Programmcodeteile umfasst, die dazu geeignet sind, die Schritte des vorbeschriebenen Verfahrens durchzuführen.

Ausführungsbeispiele des erfindungsgemäßen Verfahrens und der erfindungsgemäßen Vorrichtungen sind in den Zeichnungen beispielhaft dargestellt und werden anhand der nachfolgenden Beschreibung näher erläutert. Es zeigen:

Figur 1 ein Ausführungsbeispiel eines erfindungsgemäßen Kommunikationssystems in schematischer Darstellung;

Figur 2 ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens als Flussdiagramm;

Figur 3 ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens integriert in einen TLS-Handshake als Ablaufdiagramm;

Figur 4 ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens ausgeführt in einer Überwachungsvorrichtung als Flussdiagramm;

Figur 5 ein erstes Ausführungsbeispiel einer erfindungsgemäßen Überwachungsvorrichtung in schematischer Darstellung; und

Figur 6 ein zweites Ausführungsbeispiel einer erfindungsgemäßen Überwachungsvorrichtung in schematischer Darstellung.

Einander entsprechende Teile sind in allen Figuren mit den gleichen Bezugszeichen versehen.

Figur 1 zeigt ein Beispiel eines erfindungsgemäßen Kommunikationssystems, das beispielsweise als Automatisierungsnetzwerk mit mehreren Feldgeräten als Kommunikationsvorrichtungen FD1, FD2, FD3, ausgebildet ist. Die Kommunikationsvorrichtungen FD1, FD2, FD3 sind über ein Gateway GW und ein öffentliches Netzwerk 2 mit einem Backend-Server BS, beispielsweise einem Industrial Internet of Things Backend System, verbunden. Die Kommunikationsvorrichtungen FD1, FD2, FD3 übertragen insbesondere Diagnosedaten über eine Gateway GW zum Backend-Server BS. Bei einem kryptographisch geschützten Kommunikationsaufbau mittels eines TLS-Protokolls sendet die erste Kommunikationsvorrichtungen FD1 als TLS-Client zusätzlich zu den üblicherweise ausgetauschten Informationen eine Attestierungsdatenstruktur mit mindestens einem Verbindungsparameter als Attestierungsinformation an den Backend-Server als zweite Kommunikationsvorrichtung. Optional kann auch die zweite Kommunikationsvorrichtung als TLS-Server ihre Verbindungsparameter in einer Attestierungsdatenstruktur an die erste Kommunikationsvorrichtung senden. Die Attestierungsdatenstruktur wird beispielsweise als Erweiterung einer Nachricht des verwendeten TLS-Protokolls oder als eigenständige Nachricht über das Gateway an den Backend-Server BS als TLS-Server gesendet. In dem Gateway GW ist dabei eine Überwachungsvorrichtung AMF1 integriert, die die Attestierungsdatenstruktur ausliest und auswertet.

Dadurch kann das Gateway GW als am eigentlichen Verbindungsaufbau der geschützten Kommunikationsverbindung nicht beteiligte Komponente verlässlich beispielsweise überprüfen, welches Anwendungsprogramm auf welcher Kommunikationsvorrichtung die kryptographisch geschützte Kommunikationsverbindung initiiert beziehungsweise terminiert hat. Dadurch kann das Gateway GW insbesondere überprüfen, ob die Kommunikationsverbindung von einer freigegebenen Anwendung auf einem zulässigen Feldgerät mit aktuellem Firmware-Stand aufgebaut wird, und ob der kontaktierte Backend-Dienst tatsächlich der vorgegebene Dienst ist.

Beim Aufbau einer kryptographisch geschützten Kommunikationsverbindung zwischen einem Feldgerät FD1 und einem Feldgerät FD2 werden in gleicher Weise von dem die Kommunikationsverbindung initiierenden ersten Kommunikationspartner FD1 Verbindungsparameter als Attestierungsinformation in eine Attestierungsdatenstruktur codiert und an den zweiten Kommunikationspartner FD2 übermittelt. Eine Überwachungsvorrichtung AMF2, die innerhalb des Datenübertragungspfades der Kommunikationsverbindung angeordnet ist, kann diese Attestierungsdatenstruktur aus dem Datenübertragungspfad mithören und überprüfen.

In einer Variante senden die erste Kommunikationsvorrichtung und/oder zweite Kommunikationsvorrichtung FD1, FD2, FD3, BS lediglich einen Referenzwert der Attestierungsinformation. Die erste Kommunikationsvorrichtung FD1 übermittelt die Attestierungsinformation an eine Speichereinrichtung DB, beispielsweise über eine zweite geschützte Verbindung. Die Attestierungsinformation wird dort mit dem gleichen Referenzwert gekennzeichnet abgespeichert. Der Referenzwert kann beispielsweise ein Hashwert der Attestierungsinformation sein. Als Referenzwert kann aber auch eine Adressinformation beispielsweise eine Uniform Ressource Locator URL verwendet werden, über den die Attestierungsinformation ermittelt werden kann. Die Überprüfungseinheit AMF1, AMF2 kann anhand des Re-

ferenzwertes die eigentliche Attestierungsinformation in der Speichervorrichtung DB ermitteln und auswerten.

Die Attestierungsinformation kann einem Logging-Server bereitgestellt werden, der bestimmte oder auch alle übertragenen Nachrichten protokolliert. Ebenso kann die Attestierungsinformation einem Intrusion Detection System oder einer Artificial-Intelligence-Auswerteeinheit bereitgestellt werden.

In Figur 2 wird nun anhand eines Flussdiagramms das erfindungsgemäße Verfahren erläutert. Im Ausgangszustand 10 befindet sich eine erste Kommunikationsvorrichtung, die eine kryptographisch geschützte Kommunikationsverbindung zu einer zweiten Kommunikationsvorrichtung, bei FD2, über ein kryptographisches Authentisierungs- und Schlüsselvereinbarungsprotokoll aufbauen möchte. Ein solches Authentisierungs- und Schüsselvereinbarungsprotokoll ist beispielsweise ein Transportschichtsicherheitsprotokoll TLS oder auch dessen Vorgängerversion, die als sicheres Sockelschichtprotokoll SSL bezeichnet wird, ein Internetprotokollsicherheitsprotokoll IPsec mit dem Internetschlüsselaustauschprotokoll IKEv2, oder auch andere entsprechende Protokolle.

In einem ersten Verfahrensschritt 11 sendet eine erste Kommunikationsvorrichtung eine Attestierungsdatenstruktur, die mindestens einen Verbindungsparameter der sendenden Kommunikationsvorrichtung enthält, als Attestierungsinformation an die zweite Kommunikationsvorrichtung. Die erste Kommunikationsvorrichtung, die den Aufbau der kryptographisch geschützten Kommunikation veranlasst, wird üblicherweise als Client bezeichnet, die zweite Kommunikationsvorrichtung, die die Anforderung zu einer sicheren Kommunikationsverbindung erhält, wird üblicherweise als Server bezeichnet. Optional ermittelt die zweite Kommunikationsvorrichtung ebenfalls die in der zweiten Kommunikationsvorrichtung verwendeten Verbindungsparameter und sendet diese als Attestierungsdatenstruktur an die erste Kommunikationsvorrichtung.

Die über den Datenübertragungspfad zum jeweils anderen Kommunikationspartner übermittelte Attestierungsdatenstruktur wird nun im Verfahrensschritt 12 durch eine Überwachungsvorrichtung, beispielsweise AMF1 oder AMF2 in Figur 1, ausgekoppelt. Eine Kommunikationsverbindung, die logisch zwischen der ersten Kommunikationsvorrichtung und der zweiten Kommunikationsvorrichtung aufgebaut wird, wird physikalisch über einen Datenübertragungspfad, der aus mehreren Teilübertragungsstrecken zusammengesetzt sein kann, übertragen. Eine Datenübertragungsstrecke wird beispielsweise durch Übertragungskomponente, bspw. einen Router oder Switch terminiert. Diese führt Routingfunktionen oder andere Aktionen durch, die eigentliche kryptographisch geschützte Kommunikationsverbindung bleibt davon jedoch unberührt.

Eine Überwachungsvorrichtung kann beispielsweise als Teil einer solchen Übertragungskomponente ausgebildet sein oder in die Übertragungsstrecke zwischen zwei Übertragungskomponenten eingebracht werden. Bei einem Mithören der Attestierungsdatenstruktur werden die empfangenen Daten oder Nachrichten kopiert und die Kopie zur weiteren Auswertung ausgekoppelt. Die empfangenen Daten oder Nachrichten selbst werden unverändert über die Übertragungsstrecke weitergegeben.

Anschließend wird die Attestierungsinformation gegenüber einer vorgegebenen Richtline überprüft. Siehe Verfahrensschritt 13. Optional können in einem zusätzlichen Verfahrensschritt 14 vordefinierte Maßnahmen durchgeführt werden, wenn bei der Überprüfung eine Abweichung von der Richtlinie festgestellt wird.

Verbindungsparameter, die in einer erfindungsgemäßen Attestierungsinformation enthalten sind, sind beispielsweise ein verwendeter öffentlicher Schlüssel der ersten Kommunikationsvorrichtung oder dessen verwendetes Zertifikat, ein verwendeter öffentlicher Schlüssel der zweiten Kommunikationsvorrichtung beziehungsweise dessen Zertifikat. Die erste bzw. zweite Kommunikationsvorrichtung kann als Verbindungsparameter mitteilen, ob und wenn ja, welche durchgeführten Operationen zur

Zertifikatvalidierung verwendet wurden, z.B. ob eine Zertifikatspfadvalidierung oder eine Validierung unter Verwendung einer Zertifikatspositivliste (Certificate Whitelist) erfolgt ist. Eine Kommunikationsvorrichtung kann als Verbindungsparameter mitteilen, ob und mit welchem Verfahren sie ein Zertifikatswiderruf geprüft hat. Des Weiteren kann beispielsweise die vereinbarte Version des Sicherheitsprotokolls und/oder die ausgehandelte Verschlüsselungsfunktionen, die sog. Cipher Suite, enthalten sein.

Des Weiteren können erlaubte Optionen der Sicherheitsprotokolle, wie beispielsweise die Verwendung einer Session Resumption Funktion bei einem TLS-Protokoll angegeben werden. Als Verbindungsparameter kann eine verwendete Hash /Signatur-Algorithmuskombination für eine TLS-Handshake Operation, IP-Adresse sowie Port des TLS Clients oder IP-Adresse und Port des TLS-Servers, der Zeitpunkt des Verbindungsaufbaus, Anwendungen beziehungsweise Applikationen, die die TLS-Verbindung aufbaut, beispielsweise durch den Identifier, und Versionskennung angegeben werden. Dies betrifft sowohl den Client wie den Server. Des Weiteren kann als Verbindungsparameter die verwendete TLS-Bibliothek, beispielsweise durch eine entsprechende Kennung und die Versionsangabe für den Client sowie für den Server angegeben werden. Ein Verbindungsparameter kann eine zusätzliche Attestation eines lokalen Systemstatus, zum Beispiel ein TPM-Quote, zur Attestierung der aktuellen Plattformkonfiguration für den Client als auch den Server sein. Es kann dabei ein vertrauenswürdiges Plattformmodul, auch Trusted Platform Module TPM genannt, sein das eine Attestierung über den aktuellen Inhalt eines Plattformkonfigurationsregisters ausstellt.

Weiterhin kann eine Kommunikationsvorrichtung neben Anwendungen beziehungsweise Applikation selbst auch z.B. deren Version oder deren Herausgeber bestätigen. Dies ist insbesondere vorteilhaft, wenn die Kommunikationsvorrichtung ein Gateway zum Austausch von Industriedaten, z.B. ein Industrial Data Space Gateway, ist. Dabei werden Daten zwischen zwei Gateways

zum Austausch von Industriedaten übertragen, wobei z.B. eine Firewall am Rand eines Firmennetzes die Attestierungsdatenstruktur erfassen und prüfen kann. Dabei kann überwacht werden, welche Applikationen, die auch als App oder Service bezeichnet werden, einen Datenübertragungspfad verwenden. Weiterhin ist es möglich, dass die Attestierungsdatenstruktur eine Identifizierungsinformation der zu übertragenden Daten umfasst. Dies hat den Vorteil, dass überwachbar ist, welche Daten über den Datenübertragungspfad übertragen werden. Weiterhin ist es möglich, eine Information über die ausgetauschten Daten revisionssicher, d.h. aufbewahrungspflichtige oder aufbewahrungswürdige Informationen, zu erfassen und zu speichern.

Die Attestierungsdatenstruktur wird durch einen Attestierungsschlüssel der jeweils sendenden Kommunikationsvorrichtung kryptographisch geschützt. Der Attestierungsschlüssel kann beispielsweise der öffentliche Schlüssel der ersten beziehungsweise der zweiten Kommunikationsvorrichtung sein, die während des Aufbaus der kryptographisch geschützten Verbindung gegenseitig übermittelt werden. In einer Variante kann jedoch auch ein eigener Attestierungsschlüssel für eine bestimmte Verbindung oder spezifisch für eine Kommunikationsvorrichtung zur kryptographischen Sicherung der Attestierungsdatenstruktur verwendet werden. In diesem Fall muss dieser Attestierungsschlüssel der Überwachungsvorrichtung außerhalb der Kommunikationsverbindung mitgeteilt werden.

Ein beispielhafter Ablauf des Verfahrens wird nun am Beispiel einer Kommunikationsverbindung zwischen einem Feldgerät FD als erster Kommunikationsvorrichtung und einem Backend-Server BS als zweiter Kommunikationsvorrichtung in einem Automatisierungsnetz, wie in Figur 1 dargestellt, erläutert.

Die logische Kommunikationsverbindung zwischen der ersten und der zweiten Kommunikationsvorrichtung FD, BS wird über einen physikalischen Datenübertagungspfad des Automatisierungsnetzes 1 zur Gateway GW und von dort weiter über ein beispielsweise öffentliches Netz 2 zur zweiten Kommunikationsvorrich-

tung BS geführt. In der Gateway GW ist eine Mithör- und Überprüfungseinheit beispielsweise kombiniert in einer Überwachungsvorrichtung AMF angeordnet. Die Kommunikationsverbindung wird nun beispielhaft gemäß dem Transportschichtsicherheitsprotokoll TLS aufgebaut. Dazu werden in einem sogenannten TLS Handshake die Kommunikationsvorrichtungen gegenseitig authentisiert und ein Sitzungsschlüssel zur kryptographischen Absicherung der anschließenden Datenübertragung ausgehandelt. Dieser TLS Handshake wird nun wie folgt erweitert.

Die erste Kommunikationsvorrichtung FD generiert in Block 20 eine Attestierungsinformation und codiert dies als Erweiterung einer existierenden TLS Nachricht, beispielsweise in eine Client Hello Nachricht 21 ein. Die erste Kommunikationsvorrichtung FD oder auch die zweite Kommunikationsvorrichtung BS kann hierzu folgende Erweiterung im Server Hello unterstützen:

```
struct {
    senderPK        byte_string;
    receiverPK      byte_string;
    TLSversion      string;
    cipherSuite     string;
    senderIP        byte_string;
    receiverIP      byte_string;
    sigAlg          string;
    policy          string;
} SessionAttestation;
```

Diese Attestierungsdatenstruktur umfasst als Verbindungsparameter den öffentlichen Schlüssel des Senders sowie des Empfängers die TLS Version, die verwendete Cipher Suite, die IP-Adressen des Senders sowie des Empfängers, den verwendeten Signaturalgorithmus und zusätzliche Policy, also Richtlinieninformationen, wie beispielsweise das Datum der letzten Überprüfung der zurückgezogenen Zertifikate, verwendete TLS-Bibliotheken, Zeitpunkt des Verbindungsaufbaus oder auch In-

formationen über die Anwendung beziehungsweise das Anwendungsprogramm, das den TLS-Verbindungsaufbau veranlasst hat.

Alternativ kann die Authentisierungsdatenstruktur im TLS Handshake als zusätzliche Nachricht integriert werden. Hierbei wird die Attestierungsinformation in der Codierung als "Session Attestation" bezeichnet, als Teil eines neu zu definierenden Nachrichtentyps, beispielsweise "session_attestation" geschickt. Die Struktur der codierten Attestierungsinformation als SessionAttestation kann dabei der oben genannten Datenstruktur entsprechen.

Im Folgenden ist eine Erweiterung der Nachrichtentypen des Handshake-Protokolls um die Nachrichtentyp "session_attestation" dargestellt. Die Erweiterung entspricht dem Typ 21 und ist nachfolgend fettgedruckt, die Originaldefinition der Nachrichtentypen entspricht dem TLS Standard gemäß IETF RFC 4246, Kapitel 7.4.

```
enum {
    hello_request(0), client_hello(1), server_hello(2),
    certificate(11), server_key_exchange (12),
    certificate_request(13), server_hello_done(14),
    certificate_verify(15), client_key_exchange(16),
    finished(20), session_attestation (21), (255)
} HandshakeType;
```

```
struct {
     HandshakeType msg_type; /* handshake type */
     uint24 length; /* bytes in message */
     select (HandshakeType) {
          case hello_request: HelloRequest;
          case client_hello: ClientHello;
          case server_hello: ServerHello;
          case certificate: Certificate;
          case server_key_exchange: ServerKeyExchange;
          case certificate_request: CertificateRequest;
          case server_hello_done: ServerHelloDone;
          case certificate_verify: CertificateVerify;
          case client_key_exchange: ClientKeyExchange;
          case finished: Finished;
          case session_attestation: SessionAttestation;
     } body;
} Handshake;
```

Die Überwachungsvorrichtung AMF liest nun die TLS Nachricht als Ganzes oder die Attestierungsdatenstruktur alleine aus der ClientHello Nachricht 21 aus und überprüft diese, siehe Block 22. Bevorzugterweise erzeugt auch die zweite Kommunikationsvorrichtung BS eine Attestierungsinformation, siehe Block 23, mit Verbindungsparametern die die zweite Kommunikationsvorrichtung verwendet, beziehungsweise Sicherheitsmechanismen entsprechend der für die erste Kommunikationsvorrichtung generierten Information und sendet diese in einer ServerHello Nachricht 24 an die erste Kommunikationsvorrichtung FD. Die Attestierungsinformation wird durch die Überwachungsvorrichtung AMF ausgelesen und verifiziert, siehe Block 25. Anschließend wird im weiteren TLS Handshake-Ablauf der öffentliche Schlüssel der zweiten Kommunikationsvorrichtung an die erste Kommunikationsvorrichtung geschickt, und entsprechend kann der öffentliche Schlüssel der ersten Kommunikationsvorrichtung FD an die zweite Kommunikationsvorrichtung BS geschickt werden.

Nach dem Austausch bestätigen beide Kommunikationseinrichtungen mit einer ChangeCipherSpec, dass die folgenden Nachrich-

ten unter Nutzung der ausgehandelten Sicherheitsparameter geschützt werden, siehe Nachricht 26.
Am Ende des Handshakes erzeugt die erste Kommunikationsvorrichtung FD eine Prüfsumme, beispielsweise mittels einer Hashfunktion über alle vorher ausgetauschten Nachrichten. Diese Prüfsumme geht mit in eine Schlüsselableitung für den eigentlichen Sitzungsschlüssel ein. Die zweite Kommunikationsvorrichtung BS führt dieselbe Berechnung durch. Im Anschluss tauschen beide Kommunikationsvorrichtungen, FD und BS, mit einer Finish Nachricht 27 eine letzte Nachricht des Handshakes aus. Diese Nachricht ist verschlüsselt, so dass beide Kommunikationseinrichtungen durch Anwendung des lokal abgeleiteten Sitzungsschlüssels nachweisen, dass sie im Besitz des richtigen Schlüssels sind und implizit, dass alle Nachrichten des Handshakes auf beiden Seiten gleich waren. Anschließend werden Daten, siehe 28, über den ausgehandelten Schlüssel kryptographisch geschützt.

Die Überwachungsvorrichtung AMF überprüft die Attestierungsinformation gegenüber einer vorgegebenen Richtlinie, weicht die Attestierungsinformation von der Richtlinie ab, so wird bevorzugterweise ein Alarmsignal erzeugt und/oder der weitere Verbindungsaufbau blockiert.

Die Überprüfung der Attestierungsdatenstruktur in der Überwachungsvorrichtung AMF ist in Figur 4 anhand eines Ablaufdiagramms erläutert. Der Ablauf beginnt mit dem Startzustand 30, in dem die Überwachungsvorrichtung Verbindungsaufbaunachrichten, wie beispielsweise die genannten TLS Nachrichten, auskoppelt beziehungsweise mithört. Das Mithören umfasst ein Duplizieren der empfangenen Nachrichten und Ausgeben der Kopie der Nachrichten an eine Auswerteeinheit sowie das Weiterleiten der ursprünglichen Nachrichten an den Datenübertragungspfad zur empfangenden Kommunikationsvorrichtung. Dies wird in einer Mithöreinheit der Überwachungsvorrichtung durchgeführt.

Anschließend wird in einer Überprüfungseinheit die Attestierungsinformation gegenüber einer Sicherheitsrichtlinie überprüft, siehe 32. Entspricht die Attestierungsinformation nicht der Sicherheitsrichtlinie wird ein Fehlersignal bereitgestellt, siehe 33. Entspricht die Attestierungsinformation der Sicherheitsrichtlinie, so wird im nächsten Schritt 34 optional auch die Nachricht der zweiten Kommunikationsvorrichtung an die erste Kommunikationsvorrichtung ausgekoppelt und mitgehört und ebenfalls in Schritt 35 gegenüber der Sicherheitsregel überprüft. Stimmt die Attestierungsinformation nicht mit der Sicherheitsrichtlinie überein, wird ein Fehlersignal 33 bereitgestellt. Die als gültig geprüfte Attestierungsinformation wird an eine Durchsetzungseinheit weitergegeben. In der Durchsetzungseinheit werden gültige Attestierungsinformationen beispielsweise ausgewertet und/oder abgespeichert, siehe 36. Fehlersignale werden gemäß vordefinierten Maßnahmen umgesetzt. Beispielsweise werden Fehlersignale an eine zugeordnete Einheit bereitgestellt oder auch die Kommunikationsverbindung blockiert und beispielsweise abgebrochen. Damit ist der Endzustand 37 erreicht.

Eine Netzkomponente, die Funktionen einer Überwachungsvorrichtung integriert aufweist, ist in Figur 5 und Figur 6 dargestellt. Die Netzwerkkomponente 40, beispielsweise ein Router, Switch oder Access Point eines Kommunikationsnetzwerks empfängt Daten 45 einer Kommunikationsverbindung beispielsweise in einer Routingfunktion 41. Die Routingfunktion 41 enthält Routingtabellen, über die ein Ausgangsport zur nächsten Datenübertragungsstrecke 49 ermittelt wird und gibt die Daten entsprechend auf eine Datenübertragungsstrecke 49 aus. Die Überwachungsvorrichtung AMF greift über eine Mithöreinheit 47 die Verbindungsaufbaunachrichten ab. Die Mithöreinheit 47 kann beispielsweise als ein Mirroring Port eines Netzwerkswitches oder als eine Einwegkommunikationskomponente wie eine Datendiode ausgebildet sein. Die mitgehörten, beispielsweise gespiegelten Nachrichten werden nun an die Überprüfungseinheit 42 weiter gegeben. Dort wird die Attestierungsinformation gegenüber einer Sicherheitsrichtlinie über-

prüft. Die Sicherheitsrichtlinien werden dabei beispielsweise aus einer Richtliniendatenbank 44 der Überprüfungseinheit 42 bereitgestellt. Sicherheitsrichtlinien können dabei über eine Verbindung 46 von einer Richtliniendatenbank bereitgestellt oder aktualisiert werden.

Die Überprüfungseinheit 42 analysiert die Nachrichten des TLS Handshake, der im Klartext ausgeführt wird, auf das Vorliegen einer Attestierungsdatenstruktur in der Client Hello-Nachricht und/oder der Server Hello-Nachricht. Das Auswerteergebnis stellt die Überprüfungseinheit 42 einer Durchsetzungseinheit 43 bereit. Diese gibt entsprechend bei positivem Prüfungsergebnis die Daten unverändert an die Datenübertragungsstrecke 49 aus. Bei einem Verletzen der Richtlinien wird beispielsweise eine Fehlermeldung 48 von der Durchsetzungseinheit 43 ausgegeben. Optional kann die Datenausgabe bei einer Verletzung der Richtlinie zusätzlich blockiert werden. Das Blockieren beziehungsweise Sperren kann zum Beispiel dadurch erfolgen, dass die Netzwerkkonnektivität unterbrochen wird, indem eine Netzwerkfilterrichtlinie angepasst wird, das heißt ein Sperren der entsprechenden IP-Adresse beziehungsweise Portnummer die für den Aufbau der unzulässigen Kommunikationsverbindung verwendet werden, werden gesperrt. Es kann aber auch eine Verbindungsabbaunachricht an den Kommunikationspartner gesendet werden.

Die Überwachungsvorrichtung AMF3 besteht somit aus einer Mithöreinheit 47, einer Überprüfungseinheit 42 sowie einer Durchsetzungseinheit 43. In der Komponente 40 sind diese integriert ausgebildet.

Die Überwachungsvorrichtung AMF4 in Figur 6 umfasst eine kombinierte Mithör- und Überprüfungseinheit 52, die wiederum in einer Netzwerkkomponente 50 integriert ausgebildet ist. Die kombinierten Mithör- und Überprüfungseinheit 52 ist dabei direkt in der Datenübertragungsstrecke ausgebildet. Die Mithör- und Überprüfungseinheit 52 übernimmt die gleichen Funktionen wie die Einheiten 42 und 47 in der Netzwerkkomponente 40. Zur

Durchsetzung der Maßnahmen, die aus der Überprüfung resultieren umfasst die Überwachungsvorrichtung AMF4 die Durchsetzungseinheit 43 mit den Funktionen wie in Figur 5 für die Überwachungsvorrichtung AMF3 beschrieben.

Alle beschriebenen und/oder gezeichneten Merkmale können im Rahmen der Erfindung vorteilhaft miteinander kombiniert werden. Die Erfindung ist nicht auf die beschriebenen Ausführungsbeispiele, insbesondere auf die genannten Authentisierungs- und Schlüsselaushandlungsprotokolle, beschränkt.

Patentansprüche

1. Verfahren zur Überprüfung von Verbindungsparametern während des Aufbaus einer kryptographisch geschützten Kommunikationsverbindung zwischen einer ersten Kommunikationsvorrichtung (FD) und einer zweiten Kommunikationsvorrichtung (BS), mit den Verfahrensschritten:
- Senden (11) einer Attestierungsdatenstruktur, die mindestens einen Verbindungsparameter der ersten und/oder zweiten Kommunikationsvorrichtung (FD, BS) als Attestierungsinformation enthält, von der ersten und/oder zweiten Kommunikationsvorrichtungen (FD, BS) an die zweite und/oder erste Kommunikationsvorrichtung (BS, FD),
- Mithören (12) der Attestierungsdatenstruktur durch eine innerhalb eines Datenübertragungspfads der Kommunikationsverbindung angeordnete Überwachungsvorrichtung (AMF), und
- Überprüfen (13) der Attestierungsinformation gegenüber einer vorgegebenen Richtlinie.

2. Verfahren nach Anspruch 1, wobei die kryptographisch geschützte Kommunikationsverbindung gemäß einem Transportschicht-Sicherheitsprotokoll TLS/DTLS/SSL oder einem Internet Protokoll Sicherheitsprotokoll IPsec aufgebaut und die Attestierungsdatenstruktur als zusätzliche Protokollnachricht oder als Erweiterung einer Protokollnachricht (21, 24), insbesondere einer TLS Handshake Nachricht oder einer Internet-Schlüsselaustausch IKE Nachricht, ausgebildet wird.

3. Verfahren nach einem der vorhergehenden Ansprüche, wobei eine Attestierungsdatenstruktur mit mindestens einem Verbindungsparameter der sendenden Kommunikationsvorrichtung (FD, BS) als Attestierungsinformation sowohl von der ersten Kommunikationsvorrichtung (FD) als auch von der zweiten (BS) Kommunikationsvorrichtung zur jeweils anderen Kommunikationsvorrichtung (BS, FD) gesendet wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Attestierungsdatenstruktur durch einen Attestierungsschlüssel kryptographisch geschützt wird.

5. Verfahren nach Anspruch 4, wobei als Attestierungsschlüssel ein zur Authentisierung verwendeter Schlüssel der sendenden Kommunikationsvorrichtung (BS, FD) verwendet wird.

6. Verfahren nach Anspruch 4, wobei der Attestierungsschlüssel einer Auswertevorrichtung (AMF) über eine von der Kommunikationsverbindung unterschiedliche Verbindung bereitstellt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Attestierungsinformation von der sendenden Kommunikationsvorrichtung einer Speichereinrichtung (DB), insbesondere einer Datenbank oder einem Logging-Server, bereitgestellt wird.

8. Verfahren nach Anspruch 7, wobei die Attestierungsdatenstruktur lediglich einen Referenzwert umfasst und über den Referenzwert die Attestierungsinformation auf der Speichereinrichtung (DB) ermittelt wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei vordefinierte Maßnahmen, insbesondere ein Ausgeben eines Warnsignals und/oder ein Blockieren der Kommunikationsverbindung, durchgeführt (14) werden, wenn bei der Überprüfung eine Abweichung von der Richtlinie festgestellt wird.

10. Kommunikationssystem zur Überprüfung von Verbindungsparametern während des Aufbaus einer kryptographisch geschützten Kommunikationsverbindung zwischen einer ersten Kommunikationsvorrichtung (FD) und einer zweiten Kommunikationsvorrichtung (BS), wobei mindestens die erste und/oder zweite Kommunikationsvorrichtung (FD, BS), derart ausgebildet ist, eine Attestierungsdatenstruktur an die zweite und/oder erste Kommunikationsvorrichtung (BS, FD) zu senden, und die Attestie-

rungsdatenstruktur mindestens einen Verbindungsparameter der ersten und/oder zweiten Kommunikationsvorrichtung (FD, BS) als Attestierungsinformation enthält, umfassend:
- eine Mithöreinheit (AMF, 47, 52), die innerhalb eines Datenübertragungspfads der Kommunikationsverbindung angeordnet ist und derart ausgebildet ist, die Attestierungsdatenstruktur auszukoppeln, und
- eine Überprüfungseinheit(AMF, 42, 52) die derart ausgebildet ist, die Attestierungsinformation gegenüber einer vorgegebenen Richtlinie zu überprüfen.

11. Kommunikationsvorrichtung zur Überprüfung von Verbindungsparametern während des Aufbaus einer kryptographisch geschützten Kommunikationsverbindung zwischen der Kommunikationsvorrichtung und einer zweiten Kommunikationsvorrichtung, umfassend
- eine Sendeeinheit, die derart ausgebildet ist, eine kryptographisch geschützte Attestierungsdatenstruktur, die mindestens einen Verbindungsparameter als Attestierungsinformation enthält, an die zweite Kommunikationsvorrichtung zu senden.

12. Kommunikationsvorrichtung nach Anspruch 11, wobei die Kommunikationsvorrichtung als Client-Vorrichtung und/oder als Server-Vorrichtung ausgebildet ist und derart ausgebildet ist, das Verfahren gemäß Anspruch 1 bis 9 durchzuführen.

13. Überwachungsvorrichtung zur Überprüfung von Verbindungsparametern einer kryptographisch geschützten Kommunikationsverbindung zwischen einer ersten Kommunikationsvorrichtung (FD) und einer zweiten Kommunikationsvorrichtung (BS), umfassend
- eine Mithöreinheit (47, 52), die innerhalb des Datenübertragungspfads der Kommunikationsverbindung anordenbar ist und derart ausgebildet ist, eine Attestierungsdatenstruktur auszukoppeln und die Attestierungsinformation einer Überprüfungseinheit (bereitzustellen.

- eine Überprüfungseinheit (42, 52), die derart ausgebildet ist, die Attestierungsinformation gegenüber einer vorgegebenen Richtlinie zu überprüfen.

14. Überwachungsvorrichtung nach Anspruch 13, zusätzlich umfassend
eine Durchsetzungseinheit (43), die derart ausgebildet ist vordefinierte Maßnahmen, insbesondere ein Blockieren der Kommunikationsverbindung, durchzuführen, wenn bei der Überprüfung eine Abweichung von der Richtlinie festgestellt wird und derart ausgebildet ist, das Verfahren gemäß Anspruch 1 bis 9 durchzuführen.

15. Computerprogrammprodukt, das direkt in einen Speicher eines digitalen Computers ladbar ist, umfassend Programmcodeteile, die dazu geeignet sind, die Schritte des Verfahrens nach einem der Ansprüche 1 bis 9 durchzuführen.

FIG 1

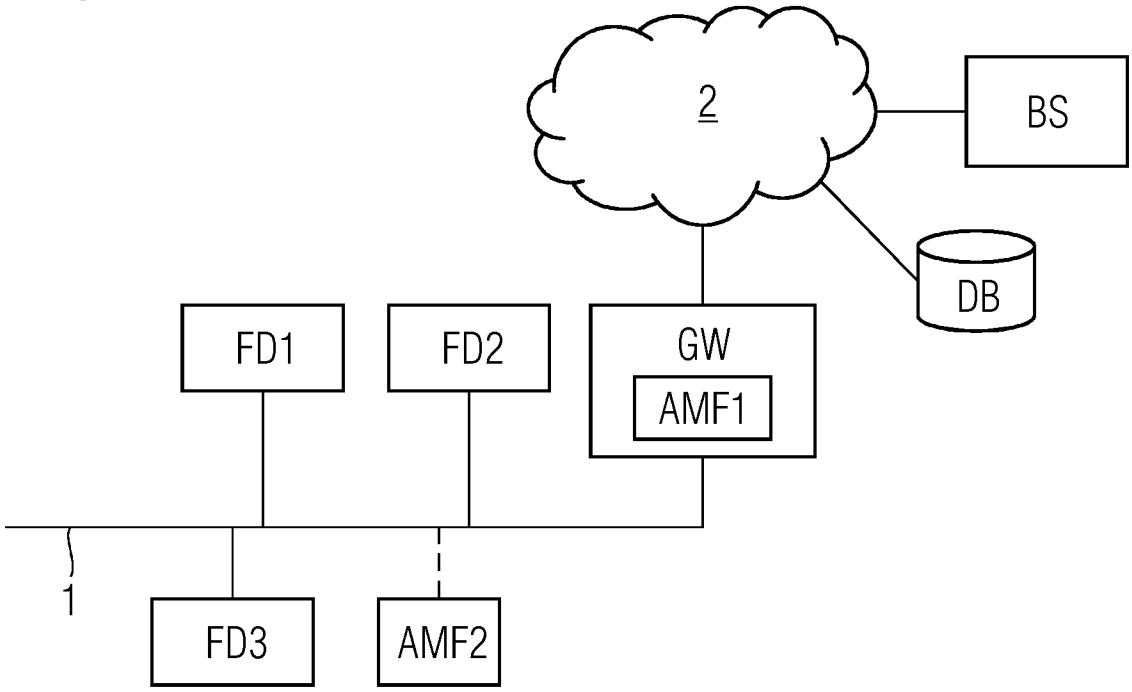


FIG 2

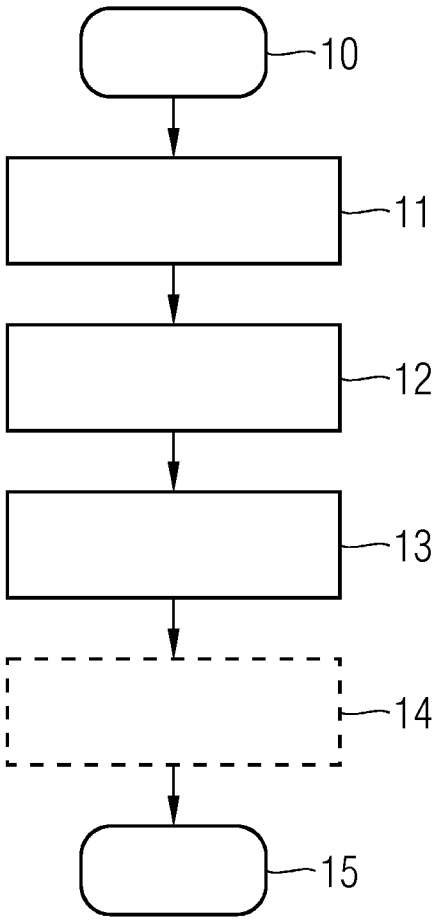


FIG 3

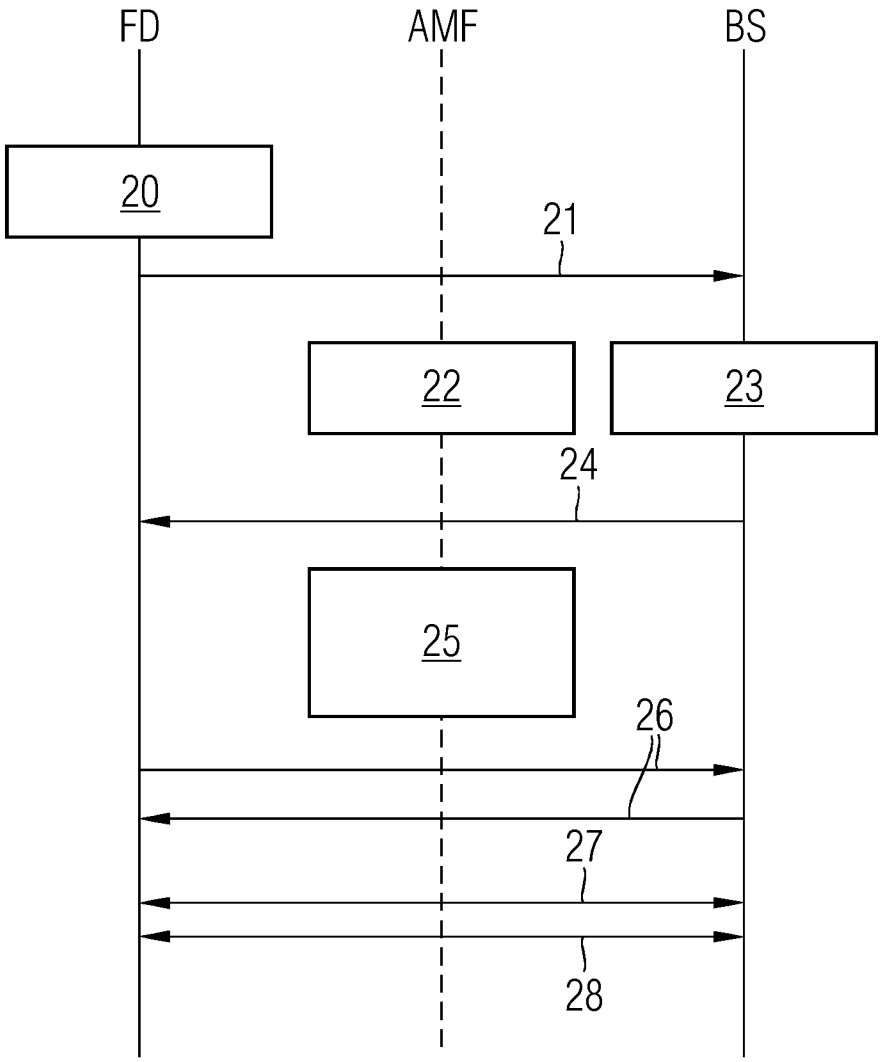


FIG 4

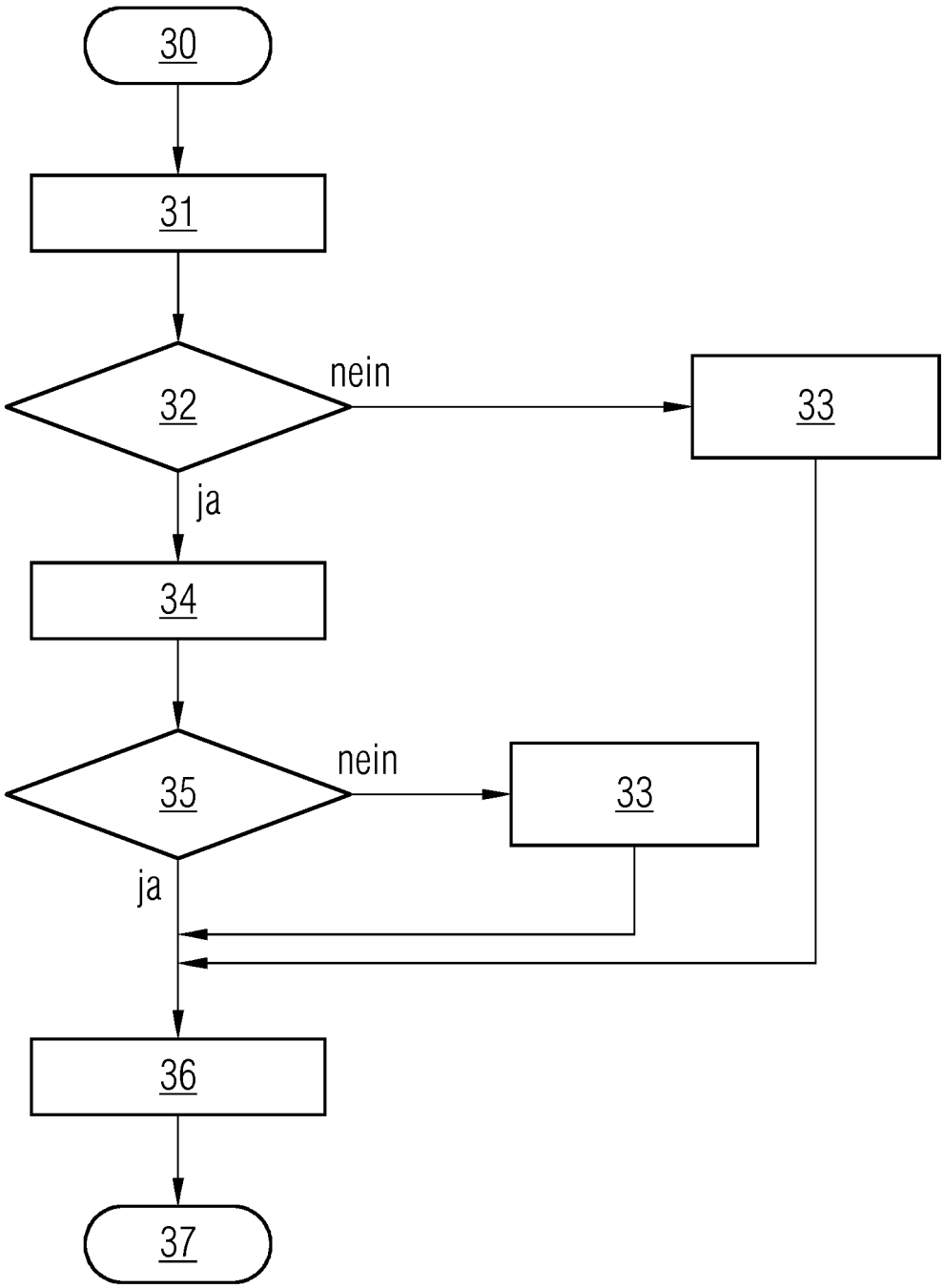


FIG 5

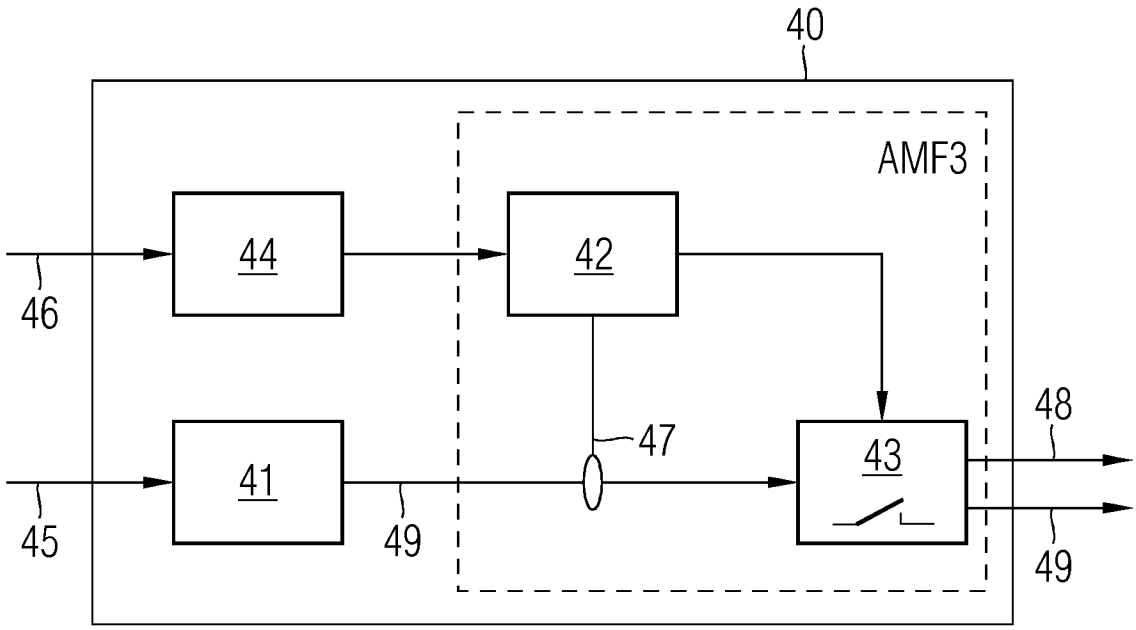
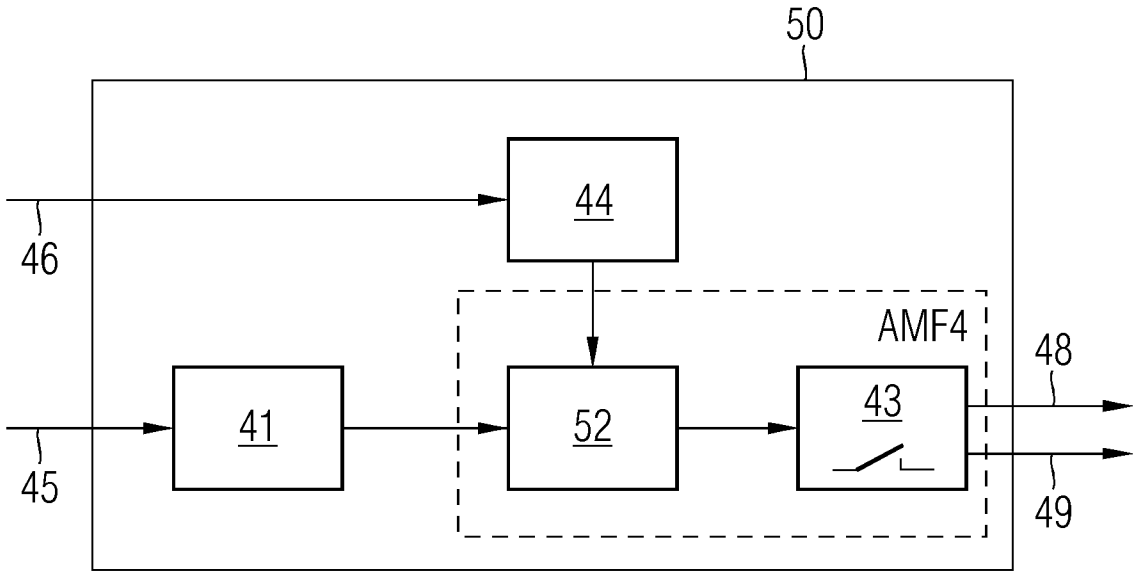


FIG 6



INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2018/065020

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; ***H04L 29/08***(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013094360 A1 (LUFT ACHIM [DE] ET AL) 18 April 2013 (2013-04-18) paragraphs [0004] - [0008], [0028] - [0035]; figure 1 paragraphs [0047], [0067], [0081] - [0093]; figure 5	1-15
X	RESCORLA RTFM E ET AL. "The Transport Layer Security (TLS) Protocol Version 1.3; draft-ietf-tls-tls13-21.txt" *THE TRANSPORT LAYER SECURITY (TLS) PROTOCOL VERSION 1.3; DRAFT-IETF-TLS-TLS13-21.TXT; INTERNET-DRAFT: NETWORK WORKING GROUP, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWI,* No. 21, 04 July 2017 (2017-07-04), pages 1-143 XP015120903 paragraph [0001] paragraphs [0004] - [04.2] paragraphs [04.3] - [04.4] paragraph [12.1]	11
A	US 2016219018 A1 (RAMAN RAJ [US] ET AL) 28 July 2016 (2016-07-28) paragraphs [0019] - [0036]; figure 3	1-15

☑ 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
29 August 2018	**06 September 2018**
Name and mailing address of the ISA/EP **European Patent Office** **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	Authorized officer **Günther, Steffen** Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2018/065020

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003163704 A1 (DICK KEVIN STEWART [US] ET AL) 28 August 2003 (2003-08-28) paragraphs [0041] - [0055]; figures 2-4	1-15

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2018/065020

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2013094360 A1	18 April 2013	DE 102012109395 A1	04 April 2013
		US 2013094360 A1	18 April 2013
US 2016219018 A1	28 July 2016	NONE	
US 2003163704 A1	28 August 2003	AT 555584 T	15 May 2012
		AU 2003257152 A1	25 February 2004
		CA 2494948 A1	19 February 2004
		EP 1543648 A2	22 June 2005
		IL 166660 A	17 May 2010
		US 2003163704 A1	28 August 2003
		US 2005091540 A1	28 April 2005
		WO 2004015524 A2	19 February 2004

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2018/065020

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06 H04L29/08
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

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

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2013/094360 A1 (LUFT ACHIM [DE] ET AL) 18. April 2013 (2013-04-18) Absätze [0004] - [0008], [0028] - [0035]; Abbildung 1 Absätze [0047], [0067], [0081] - [0093]; Abbildung 5 ----- -/--	1-15

[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
29. August 2018	06/09/2018

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

1

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	RESCORLA RTFM E ET AL: "The Transport Layer Security (TLS) Protocol Version 1.3; draft-ietf-tls-tls13-21.txt", THE TRANSPORT LAYER SECURITY (TLS) PROTOCOL VERSION 1.3; DRAFT-IETF-TLS-TLS13-21.TXT; INTERNET-DRAFT: NETWORK WORKING GROUP, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWI, Nr. 21, 4. Juli 2017 (2017-07-04), Seiten 1-143, XP015120903, [gefunden am 2017-07-04] Absatz [0001] Absätze [0004] - [04.2] Absätze [04.3] - [04.4] Absatz [12.1]	11
A	US 2016/219018 A1 (RAMAN RAJ [US] ET AL) 28. Juli 2016 (2016-07-28) Absätze [0019] - [0036]; Abbildung 3	1-15
A	US 2003/163704 A1 (DICK KEVIN STEWART [US] ET AL) 28. August 2003 (2003-08-28) Absätze [0041] - [0055]; Abbildungen 2-4	1-15

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2018/065020

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2013094360 A1	18-04-2013	DE 102012109395 A1	04-04-2013
		US 2013094360 A1	18-04-2013
US 2016219018 A1	28-07-2016	KEINE	
US 2003163704 A1	28-08-2003	AT 555584 T	15-05-2012
		AU 2003257152 A1	25-02-2004
		CA 2494948 A1	19-02-2004
		EP 1543648 A2	22-06-2005
		IL 166660 A	17-05-2010
		US 2003163704 A1	28-08-2003
		US 2005091540 A1	28-04-2005
		WO 2004015524 A2	19-02-2004