(19) Deutsches Patent- und Markenamt

(10) **DE 10 2017 202 002 A1** 2018.08.09

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2017 202 002.4**
(22) Anmeldetag: **08.02.2017**
(43) Offenlegungstag: **09.08.2018**

(51) Int Cl.: ***H04L 9/00*** (2006.01)

(71) Anmelder:
Siemens Aktiengesellschaft, 80333 München, DE

(72) Erfinder:
Falk, Rainer, 85586 Poing, DE

(56) Ermittelter Stand der Technik:

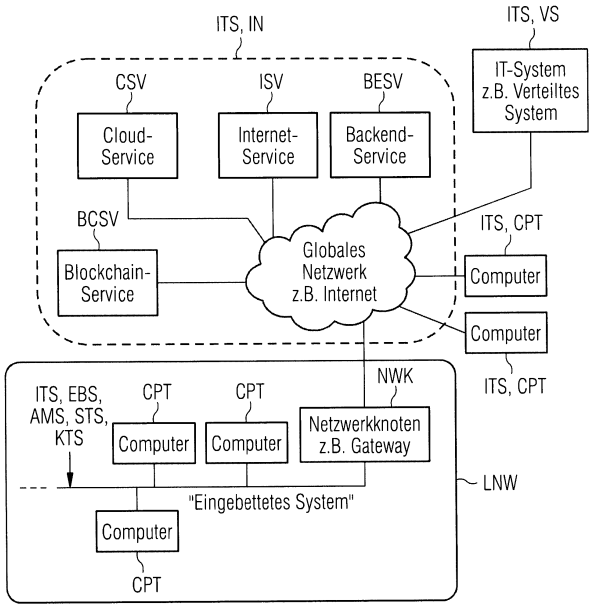
US	**6 202 157**	**B1**
US	**7 849 497**	**B1**
US	**2004 / 0 117 624**	**A1**
US	**2005 / 0 044 418**	**A1**
US	**2013 / 0 104 236**	**A1**

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren und Computer zum kryptografischen Schützen von Steuerungskommunikation in und/oder Service-Zugang zu IT-Systemen, insbesondere im Zusammenhang mit der Diagnose und Konfiguration in einem Automatisierungs-, Steuerungs- oder Kontrollsystem**

(57) Zusammenfassung: Um den kryptografische Schutz der Steuerungskommunikation in einem und/oder des Service-Zugangs zu einem IT-System (ITS, EBS, VS, IN) zu verbessern, wird es vorgeschlagen automatisch und dynamisch, insbesondere regelmäßig oder ereignisgesteuert, oder manuell, insbesondere auf Nutzeraufforderung hin, durch Autokonfiguration zu ermitteln, ob benutzte oder aktivierte und benutzbare Cipher Suites und/oder Schlüssellängen für einen aktuellen kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs ausreichend stark sind, indem
1) durch Abfrage von im Netz/System verfügbaren „Cipher Suite“-bezogenen/-spezifischen Informationen Referenz-Cipher Suites und/oder
2) durch Abfrage oder Ermittlung von im Netz/System verfügbaren Blockchain-Informationen mit als „Proof of Work“ bezeichneten Datensätzen zur Lösung von komplexen Rechenaufgaben mit der Ermittlung von Blockchain-Difficulty-Parameter als Schlüssellängen-Abschätzparameter angemessene Referenz-Schlüssellängen, insbesondere für Krypto-Algorithmen erforderliche Referenz-Mindestschlüssellängen, ermittelt werden sowie
3) die ermittelten Referenz-Cipher Suites und/oder die durch die Schlüssellängen-Abschätzparameter ermittelten Referenz-Schlüssellängen mit den benutzten oder aktivierten und benutzbaren Cipher Suites und/oder Schlüssellängen abgeglichen werden.



Beschreibung

[0001] Die Erfindung bezieht sich auf ein Verfahren zum kryptografischen Schützen von Steuerungskommunikation in und/oder Service-Zugang zu IT-Systemen, insbesondere im Zusammenhang mit der Diagnose und Konfiguration in einem Automatisierungs-, Steuerungs- oder Kontrollsystem gemäß dem Oberbegriff des Patentanspruches 1 und ein Computer zum kryptografischen Schützen von Steuerungskommunikation in und/oder Service-Zugang zu IT-Systemen, insbesondere im Zusammenhang mit der Diagnose und Konfiguration in einem Automatisierungs-, Steuerungs- oder Kontrollsystem gemäß dem Oberbegriff des Patentanspruches 7.

[0002] Ein integrierter kryptographischer Schutz für Komponenten von Informationstechnischen Systemen, so genannten IT-Systemen, insbesondere den von industriellen Datenverarbeitungs- und Steuerkomponenten in Automatisierungs-, Steuerungs- oder Kontrollsystemen und entsprechenden Systemlösungen, ist erforderlich, um Angriffe (z.B. Manipulation, Ausspähen etc.) gegen die Informationssicherheit solcher Systeme abzuwehren.

[0003] Ein IT-System ist ein elektronisch-datenverarbeitendes System, zu dem weil VNA-basierend (beruht auf der Basis einer Von-Neumann-Architektur) z.B. jegliche Art von Verteilten Systemen und Eingebetteten Systemen, aber auch auf einer Harvard-Architektur basierende elektronisch-datenverarbeitende Systeme, einzelne Computer, Großrechner, Hochleistungsrechner etc., teilweise auch Kommunikationssysteme sowie das Internet in seiner Gesamtheit zu zählen sind.

[0004] Eine wesentliche systemspezifische Funktionalität ist dabei der kryptographische Schutz von Steuerungskommunikation in IT-Systemen (z.B. „MACsec“ gemäß IEEE-Spezifikation IEEE 802.1 AE; „IPsec/IKEv2“ ein „Internet Protocol security“basierter Protokollstapel mit dem über ein „Internet-Key-Exchange“-Protokoll der Version 2 (aktuell Version) eine gesicherte Kommunikation über potentiell unsichere Netze wie das Internet ermöglicht werden soll; „TLS“ ein „Transport Layer Security“-basiertes hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet) und/oder Service-Zugängen zu IT-Systemen.

[0005] Dabei werden unterschiedliche kryptographische Algorithmen und Nutzungsarten unterstützt in Form von Cipher Suites und/oder Schlüssellängen der Krypto-Algorithmen. Es besteht ein Bedarf sicherzustellen, dass ausreichend starke Cipher Suites und/oder gewisse Mindestschlüssellängen über die gesamte Nutzungsdauer eines Computer-basierten Gerätes in dem System verwendet werden.

[0006] Es gibt bekannte Empfehlungen von unterschiedlichen Institutionen zu angemessenen Schlüssellängen. So sind z.B. unter https://www.keylength.com Schlüssellängen verfügbar. Diese basieren aber nur auf Schätzungen. Bis wann ein kryptographisches Verfahren mit einer bestimmten Schlüssellänge tatsächlich sicher ist, hängt auch von unvorhergesehenen Ereignissen ab, z.B. neuen Angriffsmethoden. Auch decken die Empfehlungen nur einen begrenzten Zeitraum ab [z.B. die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) bis zum Jahr 2021]. Für System-Geräte, z.B. mit langer Nutzungsdauer von 10 oder 20 Jahren, wie das beispielsweise in Automatisierungssystemen der Fall ist, sind solche Aussagen aus heutiger Sicht daher nicht ausreichend.

[0007] Weiterhin ist es bekannt, dass technische Implementierungen von kryptographischen Verfahren (wie „OpenSSL“ für das TLS-Protokoll oder „StrongSwan“ für Authentisierung und Schlüsselvereinbarung bei IPsec) konfiguriert werden können. Dadurch kann eingeschränkt werden, welche Cipher Suites unterstützt werden.

[0008] Dieses wird heute jedoch speziell bei eingebetteten Systemen bei der Entwicklung oder Inbetriebnahme festgelegt, wohingegen die Empfehlungen zu Schlüssellängen manuell berücksichtigt werden können.

[0009] Es besteht daher die Gefahr, dass die Konfiguration nicht an eine geänderte Lage angepasst wird. Auch besteht die Gefahr, dass ein Nutzer bzw. Administrator schwache Verfahren aktiviert.

[0010] Speziell in Bezug auf Blockchains ist ein „Proof-of-Work“ bekannt, bei dem Knoten zur Bestätigung eines Blocks der Blockchain eine komplexe Rechenaufgabe lösen müssen. Dabei wird die Komplexität der Rechenaufgabe adaptiv an die verfügbare Rechenleistung angepasst. (vgl. https://en.bitcoin.it/wiki/Proof of work).

[0011] Ein „Difficulty“-Parameter wird bei Bitcon dabei so gewählt, dass etwa alle 10 Minuten ein neuer Block der Blockchain gebildet wird. Einen Überblick über die zeitliche Entwicklung der „Difficulty“ gibt z.B. http://bitcoindifficulty.com. Weitere Informationen zur Bitcon-Difficulty ist unter https://en.bitcoin.it/wiki/Difficulty verfügbar.

[0012] Die der Erfindung zugrundeliegende Aufgabe besteht darin, ein Verfahren und Computer zum kryptografischen Schützen von Steuerungskommunikation in und/oder Service-Zugang zu IT-Systemen, insbesondere im Zusammenhang mit der Diagnose und Konfiguration in einem Automatisierungs-, Steuerungs- oder Kontrollsystem, anzugeben, bei dem der kryptografische Schutz der Steuerungskom-

munikation und/oder des Service-Zugangs verbessert wird.

[0013] Diese Aufgabe wird ausgehend von dem im Oberbegriff des Patentanspruchs 1 definierten Verfahren durch die im Kennzeichen des Patentanspruches 1 angegebenen Merkmale gelöst.

[0014] Darüber hinaus wird die Aufgabe ausgehend von dem im Oberbegriff des Patentanspruchs 7 definierten Computer durch die im Kennzeichen des Patentanspruches 7 angegebenen Merkmale gelöst.

[0015] Die der Erfindung zugrundeliegende Idee gemäß der in den Ansprüchen 1 und 7 jeweils angegebenen technischen Lehre besteht darin, dass zum kryptografischen Schützen von Steuerungskommunikation in und/oder Service-Zugang zu IT-Systemen automatisch und dynamisch, insbesondere regelmäßig oder ereignisgesteuert, oder manuell, insbesondere auf Nutzeraufforderung hin, durch Autokonfiguration ermittelt wird, ob benutzte oder aktivierte und benutzbare Cipher Suites und/oder Schlüssellängen für einen aktuellen kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs ausreichend stark sind, indem

1) durch Abfrage von im Netz/System verfügbaren „Cipher Suite“-bezogenen/-spezifischen Informationen Referenz-Cipher Suites und/oder

2) durch Abfrage oder Ermittlung von im Netz/System verfügbaren Blockchain-Informationen mit als „Proof of Work“ bezeichneten Datensätzen zur Lösung von komplexen Rechenaufgaben mit der Ermittlung von Blockchain-Difficulty-Parameter als Schlüssellängen-Abschätzparameter angemessene Referenz-Schlüssellängen, insbesondere für Krypto-Algorithmen erforderliche Referenz-Mindestschlüssellängen, ermittelt werden sowie

3) die ermittelten Referenz-Cipher Suites und/oder die durch die Schlüssellängen-Abschätzparameter ermittelten Referenz-Schlüssellängen mit den benutzten oder aktivierten und benutzbaren Cipher Suites und/oder Schlüssellängen abgeglichen werden.

[0016] Dabei wird ohne explizite Administration ermittelt, welche Schlüssellänge bzw. Cipher Suites aktuell angemessen sind. Dazu wird in dem Netz, z.B. dem Internet, verfügbare Informationen, die „Cipher Suite“-bezogenen/-spezifischen Informationen und/oder die Blockchain-Informationen, verwendet und ausgewertet. Diese sind kaum manipulierbar:

[0017] Authentisierte, wohlbekannte Internet-Dienste werden produktiv verwendet. Die Sicherheit des jeweiligen Internet-Dienstes hängt an dessen Konfiguration. Daher ist es unplausibel, dass diese unsicher konfiguriert sind. Darüber hinaus kann durch einen Mehrheitsentscheid unter Verwendung von mehreren Internet-Diensten eine erhöhte Robustheit erreicht werden.

[0018] Die Blockchain-Difficulty bzw. der Blockchain-Difficulty-Parameter kann nicht nach unten manipuliert werden, da die Komplexität dezentral abhängig von der Rechenkapazität angepasst wird. Es gibt hier keine einzelne Instanz, die dies manipulieren könnte.

[0019] Dies kann gemäß dem Anspruch 7 in vorteilhafter Weise und ganz allgemein durch einen Computer geschehen, wobei dieser vorzugsweise als ein Feldgerät, Steuergerät, IoT-Gerät („Internet-of-Things“-Gerät), Projektierungs-, Service-, Test- oder Diagnosewerkzeug ausgebildet sein kann. Abhängig von der ermittelten Information können - gemäß den Ansprüchen 3 und 9 - die von dem Computer unterstützten Cipher Suites eingeschränkt werden (z.B. unsichere Cipher Suites sperren).

[0020] In einer anderen Variante - gemäß den Ansprüchen 3 und 9 - wird ein Warnhinweis ausgegeben, z.B. als akustisches Warnsignal oder der Hinweis wird optisch auf einem Display oder als elektrisches Schaltsignal angezeigt, z.B. in einem Service-Menü oder in Log-Eintrag, dass, z.B. in dem Computer, als unsicher bzw. nicht mehr zeitgemäß erkannte Cipher Suites aktiviert sind.

[0021] In einer weiteren Variante können aktivierbare bzw. aktivierte Ciphersuites als aktuell angemessen oder nicht angemessen gekennzeichnet (oder mehrstufig, z.B. rot, gelb grün gekennzeichnet) werden. Dadurch wird einem Nutzer, der selbst kein Security-Experte ist, eine Information bereitgestellt, welche Cipher Suites aktuell noch angemessen sind.

[0022] Es können weiterhin in vorteilhafter Weise unterschiedliche Aktionen zur Verwendung von Cipher Suites für die Steuerungskommunikation und/oder den Service-Zugang (beispielsweise zum Zweck der Diagnose und der Konfiguration) definiert sein. So kann z.B. die operative Kommunikation bei Verwendung einer als schwach klassifizierten Cipher Suite nur geloggt werden (Warnhinweis). Dagegen kann bei einem Service-Zugang bei Verwendung einer als schwach klassifizierten Cipher Suite nur noch ein Anzeigemöglichkeit bestehen, aber keine Änderung der Konfiguration möglich sein (es wird also abhängig von der verwendeten Cipher Suite eingeschränkt, welche Rollen bzw. Zugriffsberechtigung gewährbar sind).

[0023] Die Information, welche Cipher Suites als angemessen gelten, wird im Betrieb automatisch ermittelt bzw. aktualisiert. Dies kann auf unterschiedliche Art erfolgen (einzeln oder in Kombination) :

[0024] Es wird zu bekannten, als vertrauenswürdigen Internet-Diensten, eine kryptographisch geschützte Verbindung probeweise aufgebaut bzw. probeweise ein Verbindungsaufbau initiiert, um die von diesem Internet-Dienst unterstützten Cipher Suites abzufragen.

[0025] Es können mehrere Dienste abgefragt werden. Die Entscheidung kann als Schnittmenge oder Vereinigungsmenge der jeweils unterstützen Cipher Suites gebildet werden.

[0026] In einer anderen Variante wird ein Quorum oder Mehrheitsentscheid der unterstützen Cipher Suites gebildet. Dadurch kann von professionell administrierten Internet-Diensten gelernt werden, welche Cipher Suites aktuell von diesen unterstützt werden.

[0027] Die Abschätzung einer erforderlichen Mindestschlüssellänge erfolgt vorzugsweise unter Verwendung einer Blockchain. Blockchains, wie insbesondere Bitcoin, realisieren einen „Proof of Work“, bei dem mindestens eine komplexe Rechenaufgaben gelöst werden muss. Abhängig von aktueller Blockchain-Komplexität (Bitcoin Difficulty), die ein Maß für die zur Verfügung stehende Rechenkapazität ist, wird eine Mindestschlüssellänge festgesetzt. Dazu wird die aktuelle Difficulty ermittelt und spezifisch für einen Kryptoalgorithmus [wie z.B. Advanced Encryption Standard (AES); RSA-Kryptosystem (nach Rivest, Shamir, Adleman); Digital Signature Algorithm (DSA) ; Elliptic Curve Digital Signature Algorithm (ECDSA), Secure Hash Algorithmus 2 (SHA2), Diffie-Hellman-Schlüsselvereinbarung (DH), Elliptic Curve Diffie-Hellman-Schlüsselvereinbarung (ECDH)] die jeweilige Mindestschlüssellänge bestimmt.

[0028] Weitere Vorteile der Erfindung ergeben sich aus der nachfolgenden Beschreibung eines Ausführungsbeispieles der Erfindung anhand der **Fig. 1** bis **Fig. 4**. Diese zeigen:

Fig. 1 ein typisches Netzwerkszenario im IT-Umfeld mit einer computerbasierten Steuerungskommunikation, z.B. zum Zweck von Diagnose und Konfiguration, in einem z.B. als Automatisierungs-, Steuerungs- oder Kontrollsystem ausgebildeten IT-System und/oder einem computerbasierten Service-Zugang zu einem weiteren IT-System,

Fig. 2 den prinzipiellen Aufbau eines für die Steuerungskommunikation und/oder den Service-Zugang in dem Netzwerkszenario gemäß der **Fig. 1** verwendeten Computers,

Fig. 3 ein erstes Ablaufdiagramm zum Prüfen des kryptografischen Schutzes der Steuerungskommunikation und/oder des Service-Zugangs auf der Basis von Cipher Suites,

Fig. 4 ein zweites Ablaufdiagramm zum Prüfen des kryptografischen Schutzes der Steuerungskommunikation und/oder des Service-Zugangs auf der Basis von Schlüssellängen, insbesondere für Krypto-Algorithmen erforderliche Mindestschlüssellängen.

[0029] **Fig. 1** zeigt ein typisches Netzwerkszenario im IT-Umfeld mit einer computerbasierten Steuerungskommunikation, z.B. zum Zweck von Diagnose und Konfiguration, in einem, z.B. als Automatisierungssystem AMS, Steuerungssystem STS oder Kontrollsystem KTS ausgebildeten, IT-System ITS und/oder einem computerbasierten Service-Zugang zu einem weiteren IT-System ITS. Gemäß der in dem einleitenden Teil der vorliegenden Anmeldung gegebenen Definition für ein Informationstechnisches System kann das IT-System ITS ganz allgemein ein Verteiltes System, ein Eingebettetes System, ein Internet oder aber auch einen einzelnen Computer verkörpern. Dies ist in der **Fig. 1** ebenfalls exemplarisch gezeigt.

[0030] Danach verkörpert das Automatisierungssystem AMS, Steuerungssystem STS oder Kontrollsystem KTS ein Eingebettetes System EBS, das als ein drahtgebundenes oder drahtloses Lokalen Netzwerk LNW, insbesondere als ein Ethernet- oder WLANbasiertes Netzwerk, ausgebildet ist und in dem die computerbasierte Steuerungskommunikation stattfindet.

[0031] Weiterhin gibt es gemäß dem Netzwerkszenario ein vorzugsweise als Internet fungierendes Globales Netzwerk GNW, das in einem das IT-System verkörpernde Internet IN den Zugang zu diversen Services ermöglicht, als da vorzugsweise sind gemäß der **Fig. 1** zumindest ein Internet-Service ISV, zumindest ein Cloud-Service CSV, zumindest ein Backend-Service BESV und/oder zumindest ein Blockchain-Service BCSV, und das die computerbasierte Steuerungskommunikation innerhalb des Globalen Netzwerkes GNW, sprich netzwerkbeschränkt, zwischen einem das IT-System verkörpernden einzelnen Computer CPT („Einzel-Computer-System“) und einem das IT-System verkörpernden Verteilten System VS sowie netzübergreifend zwischen einerseits dem einzelnen Computer CPT und/oder dem Verteilten System VS und andererseits dem als Lokales Netzwerk LNW ausgebildeten Eingebetteten System EBS möglich macht.

[0032] Das Verteilte System VS als auch das Eingebettete System EBS sind gewöhnlich „Mehr-Computer-Systeme“ (in der **Fig. 1** ist dies stellvertretend für beide Systeme nur bezüglich des Eingebetteten Systems EBS veranschaulicht), in dem jeweils wie beim „Einzel-Computer-System“ die netzwerkbeschränkte oder netzwerkübergreifende Steuerungskommunikation und/oder der Service-Zugang computerbasiert erfolgt. So ist in beiden Systemen EBS, VS

jeweils pro netzwerkübergreifende Steuerungskommunikation und/oder pro Service-Zugang wie beim Einzel-Computer-System ein Computer CPT maßgeblich beteiligt. Die netzwerkübergreifende Steuerungskommunikation als auch der Service-Zugang wird dabei über einen Netzwerkknoten NWK, der beispielsweise als Gateway ausgebildet sein kann, in dem untergeordneten Netzwerk, gemäß der **Fig. 1** in dem Lokalen Netzwerk LNW, zu dem übergeordneten Netzwerk, gemäß der **Fig. 1** zu dem Globalen Netzwerk GNW, abgewickelt.

[0033] Bei der netzwerkbeschränkte Steuerungskommunikation hingegen können mindestens zwei der in dem System EBS, VS vorhandenen Computer CPT beteiligt sein.

[0034] In dem als „Mehr-Computer-System“ ausgebildeten Eingebetteten System EBS ist der Computer CPT vorzugsweise als Feldgerät, Steuergerät, IoT-Gerät, Projektierungs-, Service-, Test- oder Diagnosewerkzeug ausgestaltet, um in dem Automatisierungssystem AMS, Steuerungssystem STS oder Kontrollsystem KTS anfallenden Aufgaben und Funktionen, z.B. System-Diagnose und System-Konfiguration, zu steuern. So z.B. in einem Automatisierungssystem AMS mit mehreren Feldgeräten und Services (z.B. Cloud Services, Internet Services, Backend-Services etc.), wobei das Feldgerät mit einem Backend-Service regelmäßig kommuniziert, um z.B. Statusdaten des Gerätes für eine vorausschauende Wartung „Predictive Maintenance“ zu übertragen.

[0035] Diese Steuerungskommunikation kann z.B. durch das „IPsec/IKEv2“-Kommunikationsprotokoll oder das „TLS“-Verschlüsselungsprotokoll geschützt sein. Darüber hinaus können auch mehrere Feldgeräte in dem Automatisierungssystem AMS miteinander geschützt, z.B. über Ethernet-MACsec („MACsec“ gemäß IEEE-Spezifikation IEEE **802.1** AE) oder WLAN (Wireless Local Area Network gemäß IEEE **802.11**), kommunizieren.

[0036] In dem „Einzel-Computer-System“ hingegen ist der Computer CPT vorzugsweise ein ganz gewöhnlicher Desktop-Personal-Computer oder ein Notebook mit Zugriffsmöglichkeit ins Globale Netzwerk GNW respektive Internet.

[0037] Für den im einleitenden Teil der vorliegenden Anmeldung erläuterten systemrelevanten Aspekt, nämlich die computerbasierte Steuerungskommunikation und/oder den computerbasierten Service-Zugang kryptografisch hinreichend sicher zu schützen, sind in dem Computer CPT zunächst Cipher Suites und/oder Schlüssellängen aktiviert und benutzbar oder aber die Cipher Suites und/oder Schlüssellängen werden schon explizit eingesetzt. Dabei haben insbesondere die aktivierten und benutzbaren oder benutzten Schlüssellängen für Krypto-Algorithmen erforderliche Mindestschlüssellängen. Für einen hinreichend sicheren Schutz ist dies aber häufig zu wenig, weil nicht sichergestellt werden kann, dass die Cipher Suites und/oder Schlüssellängen ausreichend stark sind. Anhand der nachfolgenden Beschreibung der **Fig. 2** bis **Fig. 4** wird erläuter wie in dem Computer CPT (**Fig. 2**) durch entsprechende Maßnahmen oder durch eine entsprechend methodische Vorgehensweise (**Fig. 3** und **Fig. 4**) die Verwendung von ausreichend starken Cipher Suites und/oder Schlüssellängen sichergestellt ist.

[0038] **Fig. 2** zeigt den prinzipiellen Aufbau eines für die Steuerungskommunikation und/oder den Service-Zugang in dem Netzwerkszenario gemäß der **Fig. 1** verwendeten Computers CPT. So weist der Computer CPT einen nicht-flüchtigen, lesbaren Speicher SP, in dem prozessorlesbare Steuerprogrammbefehle eines den kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs steuernden Programm-Moduls PGM gespeichert sind, einen mit dem Speicher SP verbundenen, vorzugsweise als Mikro-Prozessor „µP“ ausgebildeten, Prozessor PZ, der die Steuerprogrammbefehle des Programm-Moduls PGM ausführt, einen mit dem Prozessor PZ verbundenen Konfigurationsspeicher KSP, in dem die in dem Computer CPT aktivierten und benutzbaren oder aber die von diesem benutzten Cipher Suites und/oder Schlüssellängen Cipher Suites und/oder Schlüssellängen, vorzugsweise in einer Liste, gespeichert sind, eine mit dem Prozessor PZ verbundene Netzwerkschnittstelle NWSS, über die netzwerkbezogene bidirektionale Datenverkehr des Computers CPT hinsichtlich der computerbasierten Steuerungskommunikation und/oder des computerbasierten Service-Zugangs läuft und die zu diesem Zweck mit dem Netzwerkknoten NWK eine Funktionseinheit bildet, sowie eine Eingabeschnittstelle ESS und eine Ausgabeschnittstelle ASS für benutzerspezifische Vorgänge im Zusammenhang mit dem kryptografischen Schützen der Steuerungskommunikation in und/oder des Service-Zugang zu dem IT-Systemen ITS.

[0039] Die vorstehend aufgeführten Komponenten des Computers CPT bilden eine Funktionseinheit und sind derart ausgebildet, dass entweder automatisch und dynamisch oder manuell durch Autokonfiguration ermittelt wird, ob die benutzten oder aktivierten und benutzbaren Cipher Suites und/oder Schlüssellängen für einen aktuellen kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs ausreichend stark sind.

[0040] Die automatisch und dynamisch eingeleitete Ermittlung erfolgt vorzugsweise in regelmäßigen Abständen oder kann bei bestimmten auftretenden Ereignissen passieren (Ereignissteuerung). Unabhängig hiervon ist es vorteilhaft, wenn die Ermittlung in einem dedizierten Betriebsmodus des Computers

CPT, z.B. im Wartungsmodus, erfolgt, um nicht andere Vorgänge oder Prozesse, die auf dem Computer laufen, zu beeinträchtigen Bei der manuell eingeleiteten Ermittlung wird z.B. auf eine Aufforderung (z.B. Eingabe von Steuerkommandos) des Benutzers des Computers CPT über eine Eingabeschnittstelle ESS hin, die Autokonfiguration gestartet.

[0041] Über die Eingabeschnittstelle ESS ist es auch möglich, durch manuelle Konfiguration eine „Cipher Suite"-mäßig zumindest eingeschränkte Liste von aktivierten Cipher Suites oder die aktuell benutzte oder aktivierte und benutzbare Cipher Suite und/oder Schlüssellänge zu aktivieren.

[0042] Die Bestimmung, ob die benutzten oder aktivierten und benutzbaren Cipher Suites und/oder Schlüssellängen ausreichend stark sind, geschieht dadurch, dass

1) bei einem „Internet-Service (ISV)"-Zugang zu mindestens einem Anbieter von Internet-Diensten jeweils eine erste Kommunikationsverbindung und/oder bei einem „Blockchain-Service (BCSV)"-Zugang zu einem Anbieter von Blockchain-Services eine zweite Kommunikationsverbindung aufgebaut wird,

2) von dem Internet-Dienst des Internet-Anbieters verfügbare Informationen abgefragt werden, um für den kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs angemessene Referenz-Cipher Suites zu ermitteln und/oder

3) zu den Blockchain-Services des Blockchain-Anbieters verfügbare Blockchain-Informationen mit als „Proof of Work" bezeichneten Datensätzen zur Lösung von komplexen Rechenaufgaben abgefragt oder ermittelt werden, um für den kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs aus den Blockchain-Informationen durch die Ermittlung von Blockchain-Difficulty-Parameter als Schlüssellängen-Abschätzparameter angemessene Referenz-Schlüssellängen, z.B. die für Krypto-Algorithmen erforderliche Referenz-Mindestschlüssellängen, zu ermitteln und

4) die ermittelten Referenz-Cipher Suites und/oder die durch die Schlüssellängen-Abschätzparameter ermittelten Referenz-Schlüssellängen mit den in dem Konfigurationsspeicher KSP gespeicherten, benutzten oder aktivierten und benutzbaren Cipher Suites und/oder Schlüssellängen abgeglichen werden.

[0043] Bei den Informationen, die gemäß der Punkte **1**) und 2) abgefragt werden, handelt es sich um z.B. Parameter/Informationen mit einem eindeutigen „Cipher Suite"-Bezug, die in Internet Diensten von Internet-Anbietern verwendet werden. Werden bei der Abfrage Informationen von mehreren Internet-Dienstanbietern abgefragt, dass dann diese Informationen für die Ermittlung der angemessenen Referenz-Cipher Suites gewichtet werden.

[0044] Bei den Blockchain-Informationen, die gemäß dem Punkt **3**) abgefragt bzw. ermittelt werden, wird entweder der Block der Blockchain direkt oder ein Metadienst über eine Blockchain abgefragt, um einen aktuellen Blockchain-Difficulty-Parameter zu ermitteln.

[0045] Das Aufbauen der Verbindungen muss nicht gewollt oder absichtlich zum Zweck der Datenübertragung motiviert sein, sondern erfolgt vorzugsweise probeweise oder probehalber. Das bedeutet, dass der Computer CPT ohne eigentliche Nutzdatenkommunikation eine sichere Kommunikationsverbindung zu Internet-Diensten, wie z.B. Microsoft®, Amazon®, Google®, IBM®, Siemens®, etc., aufbaut. Diese Kommunikation kann z.B. wieder durch das „IPsec/IKEv2"-Kommunikationsprotokoll oder das „TLS"-Verschlüsselungsprotokoll geschützt sein.

[0046] Das Abfragen der Informationen muss nicht zwingend auf der aufgebauten ersten und zweiten Kommunikationsverbindung erfolgen, sondern kann auch auf einer Verbindung mit Nutzdatenkommunikation passieren.

[0047] Das Speichern der ermittelten Referenz-Cipher Suites und/oder Referenz-Schlüssellängen kann wie das Speichern der in dem Computer CPT aktivierten und benutzbaren oder aber der von diesem benutzten Cipher Suites und/oder Schlüssellängen auch in einer Liste, vorzugsweise in einer Referenz-Liste, passieren. In diesem Fall bietet es sich an und ist auch zweckmäßig, dass der Abgleich listenweise durchgeführt wird.

[0048] Ergibt der gemäß dem Punkt **4**) durchgeführte Abgleich einer dedizierten, aktuell benutzten oder aktivierten und benutzbaren Cipher Suite und/oder Schlüssellänge der in dem Konfigurationsspeicher KSP gespeicherten Cipher Suites und/oder Schlüssellängen mit den ermittelten Referenz-Cipher Suites und/oder den bestimmten Referenz-Schlüssellängen, dass die aktuell benutzte oder aktivierte und benutzbare Cipher Suite und/oder Schlüssellänge nicht unter den ermittelten Referenz-Cipher Suites und/oder den bestimmten Referenz-Schlüssellängen ist, dass dann

a) ein an den Benutzer des Computers CPT adressierter Warnhinweis erzeugt und über die Ausgabeschnittstelle ASS ausgegeben wird,

b) die aktuell benutzte Cipher Suite und/oder Schlüssellänge unverzüglich gesperrt wird, und/oder

c) die aktuell benutzte Cipher Suite und/oder Schlüssellänge nach einer Karenzzeit des ausgegebenen Warnhinweises gesperrt wird.

[0049] Der Warnhinweis kann dabei akustisch, z.B. als Warnsignal, oder aber optisch auf einem Display oder als elektrisches Schaltsignal ausgegeben werden.

[0050] Kommt es aufgrund des durchgeführten Abgleichs zu einer Sperrung der aktuell benutzten oder aktivierten und benutzbaren Cipher Suite und/oder Schlüssellänge, so wird entweder automatisch nach einer Wartezeit oder nach Bestätigung durch einen Servicetechniker über die Eingabeschnittstelle ESS die für den Abgleich herangezogene Referenz-Cipher Suite und/oder Referenz-Schlüssellänge für die Benutzung/Aktivierung in dem Computer CPT übernommen.

[0051] **Fig. 3** zeigt ein erstes Ablaufdiagramm mit mehreren Ablaufzuständen $AZ1_{FIG3}$...$AZ6_{FIG3}$ zum Prüfen des kryptografischen Schutzes der Steuerungskommunikation und/oder des Service-Zugangs auf der Basis von Cipher Suites. In einem ersten Ablaufzustand $AZ1_{FIG3}$ wird die Prüfung des kryptografischen Schutzes der Steuerungskommunikation und/oder des Service-Zugangs gestartet.

[0052] Danach werden in einem zweiten Ablaufzustand $AZ2_{FIG3}$ „Cipher Suite“-bezogene Informationen/Parameter, die in Internet Diensten von Internet-Anbietern verwendet werden, abgefragt. Dabei werden vorzugsweise Informationen aus mehreren als Referenz dienenden Quellen (Internet Diensten von Internet-Anbietern) durch Abfrage ermittelt, um daraus und in Abhängigkeit von den durch Abfrage ermittelten Daten/Informationen in einem dritten Ablaufzustand $AZ3_{FIG3}$ eine, z.B. plausibilisierte, Referenz-Liste aktuell angemessener Referenz-Cipher Suites zu bestimmen. Dabei können z.B. unterschiedliche Informationsquellen gewichtet werden, z.B. Aufnahme in die Referenz-Liste, wenn eine Referenz-Cipher Suite von mindestens 3 Quellen (Internet-Dienste von 3 Internet-Anbietern) unterstützt wird, oder wenn mindestens 50% der Quellen (Internet-Dienste von mehreren Internet-Anbietern) die Referenz-Cipher Suite unterstützen.

[0053] Es kann weiterhin eine Filterung nach einer Mindestschlüssellänge erfolgen, die abhängig von der Difficulty einer Blockchain ermittelt wird (vgl. **Fig. 4**).

[0054] Die Referenz-Liste aktueller Referenz-Cipher Suites kann zudem für das gleiche Kommunikationsprotokoll gelten, das für die Abfrage der aktuellen Referenz-Cipher Suites verwendet wurde - z.B. das von Google verwendete „Transport Layer Security“-basierte hybride Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet, um die von Google® verwendeten Referenz-Cipher Suites bei Nutzung des TLS-Protokolls zu ermitteln.

[0055] Vorzugsweise erfolgt die Verwendung aber für weitere Anwendungen, z.B. Referenz-Cipher Suites, die für ein anderes Protokoll ermittelt werden. So können aktuell zulässige Referenz-Cipher Suites für „MACsec“ oder „IKEv2/IPsec“ abhängig davon bestimmt werden, welche Referenz-Cipher Suites Google® bei „TLS“ unterstützt und welche Difficulty bei einer Bitcon Blockchain aktuell gilt. Auch können zulässige Referenz-Cipher Suites für weitere Sicherheitsanwendungen wie Dateisystemverschlüsselung, Nachrichtenschutz bei Publish/Subscribe-Messaging-Diensten, XML-Security etc. angepasst werden.

[0056] Anschließend wird diese Referenz-Liste aktueller Referenz-Cipher Suites in einem vierten Ablaufzustand $AZ4_{FIG3}$ mit der, z.B. in dem Konfigurationsspeicher KSP des Computers CPT (vgl. **Fig. 2**) gespeicherten, Liste mit den in dem Computer benutzten oder aktivierten und benutzbaren Cipher Suites - d.h. die auf dem Computer technisch unterstützen Cipher Suites bzw. die durch manuelle Konfiguration aktivierten Cipher Suites - abgeglichen. Mit dem Abgleichergebnis erfolgt dabei die Abfrage nach der Maßgabe: „Enthält eine Liste von aktuell benutzten oder aktivierten und benutzbaren Cipher Suites zumindest einen Eintrag, der nicht in der Referenz-Liste der aktuell ermittelten Referenz-Cipher Suites ist?“

[0057] Lautet die Antwort auf diese Abfrage „JA“, dann wird in einem fünften Ablaufzustand $AZ5_{FIG3}$ ein Warnhinweis, z.B. akustisch als Warnsignal oder optisch auf einem Display oder als elektrisches Schaltsignal, ausgegeben. Im anderen Fall, wenn die Antwort auf diese Abfrage „NEIN“ ist, dann ist in einem sechsten Ablaufzustand $AZ6_{FIG3}$ die Prüfung des kryptografischen Schutzes der Steuerungskommunikation und/oder des Service-Zugangs beendet.

[0058] Bei dieser Abfrage wird mit anderen Worten geklärt, ob eine Cipher Suite unterstützt wird, die nicht in der Referenz-Liste aktuell angemessener Referenz-Cipher Suites enthalten ist. Ist das der Fall, so erfolgt z.B. eine Warnung, vorzugsweise in Form eines Warnhinweises im Service-Menü des Computers, als Logging-Event bei Erkennen, als Logging-Event bei Nutzung. In einer anderen alternativen Variante wird diese Cipher Suite automatisch gesperrt, z.B. sofort oder nach einer gewissen Karenzzeit nach Ausgabe des Warnhinweises.

[0059] Die in der **Fig. 3** dargestellte Prüfung erfolgt - wie auch die gemäß **Fig. 2** mit der dazugehörigen Figurenbeschreibung durchgeführten Ermittlungen zum kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs - vorzugsweise regelmäßig oder ereignisgesteuert. Außerdem findet die Prüfung vorzugsweise in einem bestimmten Betriebsmodus des Computers statt (z.B. im Wartungsmodus). Zudem können die Änderungen auch automatisch übernommen werden, automatisch nach einer Wartezeit, oder nach Bestätigung durch einen Servicetechniker (z.B. Bestätigung in den Konfigurationseinstellungen in einem Service-Menü des Computers).

[0060] **Fig. 4** zeigt ein zweites Ablaufdiagramm mit mehreren Ablaufzuständen $AZ1_{FIG4}$...$AZ6_{FIG4}$ zum Prüfen des kryptografischen Schutzes der Steuerungskommunikation und/oder des Service-Zugangs auf der Basis von Schlüssellängen, insbesondere für Krypto-Algorithmen erforderliche Mindestschlüssellängen. In einem ersten Ablaufzustand $AZ1_{FIG4}$ wird die Prüfung des kryptografischen Schutzes der Steuerungskommunikation und/oder des Service-Zugangs gestartet.

[0061] Danach werden in einem zweiten Ablaufzustand $AZ2_{FIG4}$ Blockchain-Informationen mit als „Proof of Work“ bezeichneten Datensätzen zur Lösung von komplexen Rechenaufgaben, die in Blockchain-Services eines Blockchain-Anbieters verwendet werden, abgefragt. Dabei werden vorzugsweise Informationen aus mehreren als Referenz dienenden Quellen (Blockchain-Services von Blockchain-Anbietern oder von eine Blockchain realisierenden Blockchain-Knoten) durch Abfrage ermittelt, um daraus und in Abhängigkeit von den durch Abfrage ermittelten Daten/Informationen in einem vierten Ablaufzustand $AZ3_{FIG4}$ eine, z.B. plausibilisierte, Referenz-Liste aktuell angemessener Referenz-Schlüssellängen, z.B. Referenz-Mindestschlüssellängen für Krypto-Algorithmen, zu bestimmen. Dabei können z.B. unterschiedliche Informationsquellen gewichtet werden, z.B. Aufnahme in die Referenz-Liste, wenn eine Referenz-Schlüssellänge, insbesondere Referenz-Mindestschlüssellänge, von mindestens 3 Quellen (Blockchain-Services von 3 Blockchain-Anbietern oder von eine Blockchain realisierenden Blockchain-Knoten) unterstützt wird, oder wenn mindestens 50% der Quellen (Blockchain-Services von mehreren Blockchain-Anbietern oder von einer Mehrzahl von eine Blockchain realisierenden Blockchain-Knoten) die Referenz-Schlüssellänge, insbesondere Referenz-Mindestschlüssellänge, unterstützen. Dabei können unterschiedliche Blockchains geprüft werden, z.B. Bitcoin, Ethereum und Hyperledger.

[0062] Es kann weiterhin eine Filterung nach einer Mindestschlüssellänge erfolgen, die abhängig von der Difficulty einer Blockchain ermittelt wird.

[0063] Anschließend wird diese Referenz-Liste aktueller Referenz-Schlüssellängen, insbesondere Referenz-Mindestschlüssellängen, in einem vierten Ablaufzustand $AZ4_{FIG4}$ mit der, z.B. in dem Konfigurationsspeicher KSP des Computers CPT (vgl. **Fig. 2**) gespeicherten, Liste mit den in dem Computer benutzten oder aktivierten und benutzbaren Schlüssellängen, insbesondere Mindestschlüssellängen, - d.h. die auf dem Computer technisch unterstützen Schlüssellängen, insbesondere Mindestschlüssellängen, bzw. die durch manuelle Konfiguration aktivierten Schlüssellängen, insbesondere Mindestschlüssellängen, - abgeglichen. Mit dem Abgleichergebnis erfolgt dabei die Abfrage nach der Maßgabe: „Enthält eine Liste von aktuell benutzten oder aktivierten und benutzbaren Schlüssellängen, insbesondere Mindestschlüssellängen, zumindest einen Eintrag, der nicht in der Referenz-Liste der aktuell ermittelten Referenz-Schlüssellängen, insbesondere Referenz-Mindestschlüssellängen, ist?“

[0064] Lautet die Antwort auf diese Abfrage „JA“, dann wird in einem fünften Ablaufzustand $AZ5_{FIG4}$ ein Warnhinweis, z.B. akustisch als Warnsignal oder optisch auf einem Display oder als elektrisches Schaltsignal, ausgegeben. Im anderen Fall, wenn die Antwort auf diese Abfrage „NEIN“ ist, dann ist in einem sechsten Ablaufzustand $AZ6_{FIG4}$ die Prüfung des kryptografischen Schutzes der Steuerungskommunikation und/oder des Service-Zugangs beendet.

[0065] Bei dieser Abfrage wird mit anderen Worten geklärt, ob eine Schlüssellänge, insbesondere Mindestschlüssellänge, unterstützt wird, die nicht in der Referenz-Liste aktuell angemessener Referenz-Schlüssellängen, insbesondere Referenz-Mindestschlüssellängen, enthalten ist. Ist das der Fall, so erfolgt z.B. eine Warnung, vorzugsweise in Form eines Warnhinweises im Service-Menü des Computers, als Logging-Event bei Erkennen, als Logging-Event bei Nutzung. In einer anderen alternativen Variante wird diese Schlüssellänge, insbesondere Mindestschlüssellänge, automatisch gesperrt, z.B. sofort oder nach einer gewissen Karenzzeit nach Ausgabe des Warnhinweises.

[0066] Die in der **Fig. 4** dargestellte Prüfung erfolgt - wie auch die gemäß **Fig. 2** mit der dazugehörigen Figurenbeschreibung durchgeführten Ermittlungen zum kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs - wieder (wie die in der **Fig. 3** dargestellte Prüfung) vorzugsweise regelmäßig oder ereignisgesteuert. Außerdem findet die Prüfung wieder vorzugsweise in einem bestimmten Betriebsmodus des Computers statt (z.B. im Wartungsmodus). Zudem können die Änderungen auch wieder automatisch übernommen werden, automatisch nach einer Wartezeit, oder nach Bestätigung durch einen Servicetechniker (z.B. Be-

stätigung in den Konfigurationseinstellungen in einem Service-Menü des Computers).

Patentansprüche

1. Verfahren zum kryptografischen Schützen von Steuerungskommunikation in und/oder Service-Zugang zu IT-Systemen (ITS), insbesondere im Zusammenhang mit der Diagnose und Konfiguration in einem Automatisierungs-, Steuerungs- oder Kontrollsystem (AMS, STS, KTS), bei dem
a) die Steuerungskommunikation zwischen, vorzugsweise als Feldgerät, Steuergerät, IoT-Gerät, Projektierungs-, Service-, Test- oder Diagnosewerkzeug ausgebildeten, Computern (CPT) innerhalb eines drahtgebundenen oder drahtlosen Lokalen Netzwerkes (LNW), insbesondere eines Ethernet- oder WLAN-basierten Netzwerkes, oder netzwerkübergreifend von dem Lokalen Netzwerk (LNW) zu einem Globalen Netzwerk (GNW), insbesondere dem Internet (IN), stattfindet,
b) der Service-Zugang entweder netzwerkübergreifend von dem Lokalen Netzwerk (LNW) oder direkt in das Globale Netzwerk (GNW, IN) zu mindestens einem Internet-Service (ISV), zu mindestens einem Cloud-Service (CSV), zu mindestens einem Backend-Service (BESV) und/oder zu mindestens einem Blockchain-Service (BCSV) erfolgt,
c) mehrere unterschiedliche, von Kommunikationsprotokollen für die Steuerungskommunikation und/oder den Service-Zugang unterstützte sowie zum kryptografischen Schützen der Steuerungskommunikation und/oder des Service-Zugangs in dem Computer (CPT) benutzte oder aktivierte und benutzbare Cipher Suites und/oder Schlüssellängen, insbesondere für Krypto-Algorithmen erforderliche Mindestschlüssellängen, vorzugsweise in einer Liste, gespeichert werden, **dadurch gekennzeichnet**, dass
d) automatisch und dynamisch, insbesondere regelmäßig oder ereignisgesteuert, oder manuell, insbesondere auf Nutzeraufforderung hin, durch Autokonfiguration ermittelt wird, ob die benutzten oder aktivierten und benutzbaren Cipher Suites und/oder Schlüssellängen für einen aktuellen kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs ausreichend stark sind, indem
d1) im Zuge eines „Internet-Service (ISV)"-Zugangs zu mindestens einem Anbieter von Internet-Diensten jeweils eine erste Kommunikationsverbindung und/oder im Zuge eines „Blockchain-Service (BCSV)"-Zugangs zu mindestens einem Anbieter von Blockchain-Services oder zu mindestens einen eine Blockchain realisierenden Blockchain-Knoten eine zweite Kommunikationsverbindung, vorzugsweise jeweils probeweise, aufgebaut wird,
d2) von dem Internet-Dienst des Internet-Anbieters verfügbare „Cipher Suite"-bezogene/-spezifische, insbesondere den Internet-Dienst des Internet-Anbieters unterstützende Cipher Suites, Informationen, insbesondere auf der aufgebauten ersten Kommunikationsverbindung, abgefragt werden, um für den kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs angemessene, vorzugsweise in einer Referenz-Liste gespeicherte, Referenz-Cipher Suites zu ermitteln und/oder zu den Blockchain-Services des Blockchain-Anbieters oder zu den Blockchains der diese realisierenden Blockchain-Knoten verfügbare Blockchain-Informationen mit als „Proof of Work" bezeichneten Datensätzen zur Lösung von komplexen Rechenaufgaben, insbesondere auf der aufgebauten zweiten Kommunikationsverbindung, abgefragt oder ermittelt werden, um für den kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs aus den Blockchain-Informationen durch die Ermittlung von Blockchain-Difficulty-Parameter als Schlüssellängen-Abschätzparameter angemessene, vorzugsweise in einer Referenz-Liste gespeicherte, Referenz-Schlüssellängen, insbesondere für Krypto-Algorithmen erforderliche Referenz-Mindestschlüssellängen, zu ermitteln,
d3) die ermittelten Referenz-Cipher Suites und/oder die durch die Schlüssellängen-Abschätzparameter ermittelten Referenz-Schlüssellängen mit den gespeicherten, benutzten oder aktivierten und benutzbaren Cipher Suites und/oder Schlüssellängen, vorzugsweise listenweise, abgeglichen werden.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass eine „Cipher Suite"-mäßig zumindest eingeschränkte Liste von aktivierten Cipher Suites oder die aktuell benutzte oder aktivierte und benutzbare Cipher Suite und/oder Schlüssellänge durch manuelle Konfiguration aktiviert wird.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass wenn der Abgleich einer aktuell benutzten oder aktivierten und benutzbaren Cipher Suite und/oder Schlüssellänge der gespeicherten Cipher Suites und/oder Schlüssellängen mit den ermittelten Referenz-Cipher Suites und/oder den bestimmten Referenz-Schlüssellängen ergibt, dass die aktuell benutzte oder aktivierte und benutzbare Cipher Suite und/oder Schlüssellänge nicht unter den ermittelten Referenz-Cipher Suites und/oder den bestimmten Referenz-Schlüssellängen ist, dass dann
(i) ein an den Benutzer des Computers (CPT) adressierter Warnhinweis erzeugt und ausgegeben wird,
(ii) die aktuell benutzte oder aktivierte und benutzbare Cipher Suite und/oder Schlüssellänge unverzüglich gesperrt wird, und/oder
(iii) die aktuell benutzte oder aktivierte und benutzbare Cipher Suite und/oder Schlüssellänge nach einer Karenzzeit des ausgegebenen Warnhinweises gesperrt wird.

4. Verfahren nach Anspruch 1, 2 oder 3, **dadurch gekennzeichnet**, dass die automatisch und dynamisch, insbesondere regelmäßig oder ereignisgesteuert, durchgeführte Ermittlung in einem dedi-

zierten Betriebsmodus des Computers (CPT), z.B. im Wartungsmodus, erfolgt.

5. Verfahren nach Anspruch 3, **dadurch gekennzeichnet**, dass die Referenz-Cipher Suite und/oder Referenz-Schlüssellänge, die zur Sperrung der aktuell benutzten oder aktivierten und benutzbaren Cipher Suite und/oder Schlüssellänge geführt hat, automatisch nach einer Wartezeit oder nach Bestätigung durch einen Servicetechniker übernommen wird/werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, dass die von den Internet-Dienstanbietern abgefragten Informationen für die Ermittlung der angemessenen Referenz-Cipher Suites gewichtet werden.

7. Computer (CPT) zum kryptografischen Schützen von Steuerungskommunikation in und/oder Service-Zugang zu IT-Systemen (ITS), insbesondere im Zusammenhang mit der Diagnose und Konfiguration in einem Automatisierungs-, Steuerungs- oder Kontrollsystem (AMS, STS, KTS), der, vorzugsweise als Feldgerät, Steuergerät, IoT-Gerät, Projektierungs-, Service-, Test- oder Diagnosewerkzeug ausgestaltet,
a) eine Netzwerkschnittstelle (NWSS) sowie einen Konfigurationsspeicher (KSP) aufweist, die derart ausgebildet sind, dass
a1) über die Netzwerkschnittstelle (NWSS) die Steuerungskommunikation mit weiteren Computern (CPT) innerhalb eines drahtgebundenen oder drahtlosen Lokalen Netzwerkes (LNW), insbesondere eines Ethernet- oder WLAN-basierten Netzwerkes, oder netzwerkübergreifend über einen mit der Netzwerkschnittstelle (NWSS) verbindbaren Netzwerkknoten (NWK) des Lokalen Netzwerkes (LNW) von dem Lokalen Netzwerk (LNW) zu einem Globalen Netzwerk (GNW), insbesondere dem Internet (TCP/IP), stattfindet,
a2) über die Netzwerkschnittstelle (NWSS) der Service-Zugang entweder netzwerkübergreifend, über den mit der Netzwerkschnittstelle (NWSS) verbindbaren Netzwerkknoten (NWK) des Lokalen Netzwerkes (LNW), oder direkt in das Globale Netzwerk (GNW, TCP/IP) zu mindestens einem Internet-Service (ISV), zu mindestens einem Cloud-Service (CSV), zu mindestens einem Backend-Service (BESV) und/oder zu mindestens einem Blockchain-Service (BCSV) erfolgt,
a3) in dem Konfigurationsspeicher (KSP) mehrere unterschiedliche, von Kommunikationsprotokollen für die Steuerungskommunikation und/oder den Service-Zugang unterstützte sowie zum kryptografischen Schützen der Steuerungskommunikation und/oder des Service-Zugangs im Computer (CPT) benutzte oder aktivierte und benutzbare Cipher Suites und/oder Schlüssellängen, insbesondere für Krypto-Algorithmen erforderliche Mindestschlüssellängen, vorzugsweise in einer Liste, gespeichert werden, **gekennzeichnet durch**
b) einen nicht-flüchtigen, lesbaren Speicher (SP), in dem prozessorlesbare Steuerprogrammbefehle eines den kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs steuernden Programm-Moduls (PGM) gespeichert sind, und einen mit dem Speicher (SP) verbundenen Prozessor (PZ), der die Steuerprogrammbefehle des Programm-Moduls (PGM) ausführt, mit der Netzwerkschnittstelle (NWSS) und dem Konfigurationsspeicher (KSP) verbunden ist und zur Steuerung des kryptografischen Schutzes der Steuerungskommunikation und/oder des Service-Zugangs mit der Netzwerkschnittstelle (NWSS) und dem Konfigurationsspeicher (KSP) als Funktionseinheit derart ausgebildet ist, dass
b1) automatisch und dynamisch, insbesondere regelmäßig oder ereignisgesteuert, oder manuell, insbesondere auf Nutzeraufforderung über eine Eingabeschnittstelle (ESS) hin, die mit dem Prozessor (PZ) verbunden ist, durch Autokonfiguration ermittelt wird, ob die benutzten oder aktivierten und benutzbaren Cipher Suites und/oder Schlüssellängen für einen aktuellen kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs ausreichend stark sind, indem
b2) im Zuge eines „Internet-Service (ISV)“-Zugangs zu mindestens einem Anbieter von Internet-Diensten jeweils eine erste Kommunikationsverbindung und/oder im Zuge eines „Blockchain-Service (BCSV)“-Zugangs zu mindestens einem Anbieter von Blockchain-Services eine zweite Kommunikationsverbindung, vorzugsweise jeweils probeweise, aufgebaut wird,
b3) von dem Internet-Dienst des Internet-Anbieters verfügbare Informationen, insbesondere auf der aufgebauten ersten Kommunikationsverbindung, abgefragt werden, um für den kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs angemessene, vorzugsweise in einer Referenz-Liste gespeicherte, Referenz-Cipher Suites zu ermitteln und/oder zu den Blockchain-Services des Blockchain-Anbieters oder zu den Blockchains der diese realisierenden Blockchain-Knoten verfügbare Blockchain-Informationen mit als „Proof of Work“ bezeichneten Datensätzen zur Lösung von komplexen Rechenaufgaben, insbesondere auf der aufgebauten zweiten Kommunikationsverbindung, abgefragt oder ermittelt werden, um für den kryptografischen Schutz der Steuerungskommunikation und/oder des Service-Zugangs aus den Blockchain-Informationen durch die Ermittlung von Blockchain-Difficulty-Parameter als Schlüssellängen-Abschätzparameter angemessene, vorzugsweise in einer Referenz-Liste gespeicherte, Referenz-Schlüssellängen, insbesondere für Krypto-Algorithmen erforderliche Referenz-Mindestschlüssellängen, zu ermitteln,
b4) die ermittelten Referenz-Cipher Suites und/oder die durch die Schlüssellängen-Abschätzpara-

meter ermittelten Referenz-Schlüssellängen mit den in dem Konfigurationsspeicher (KSP) gespeicherten, benutzten oder aktivierten und benutzbaren Cipher Suites und/oder Schlüssellängen, vorzugsweise listenweise, abgeglichen werden.

8. Computer (CPT) nach Anspruch 7, **dadurch gekennzeichnet**, dass eine Eingabeschnittstelle (ESS) enthalten ist, die mit dem Prozessor (PZ) verbunden ist und durch die Verbindung eine erste Funktionseinheit bildet, die derart ausgestaltet ist, dass eine „Cipher Suite"-mäßig zumindest eingeschränkte Liste von aktivierten Cipher Suites oder die aktuell benutzte oder aktivierte und benutzbare Cipher Suite und/oder Schlüssellänge durch manuelle Konfiguration aktiviert wird.

9. Computer (CPT) nach Anspruch 7 oder 8, **dadurch gekennzeichnet**, dass eine Ausgabeschnittstelle (ASS) enthalten ist, die mit dem Prozessor (PZ) verbunden ist und durch diese Verbindung zusammen mit dem vom Prozessor (PZ) ausgeführten Progamm-Modul (PGM) und dem Konfigurationsspeicher () eine zweite Funktionseinheit bildet, die derart ausgestaltet ist, dass, wenn der Abgleich einer aktuell benutzten oder aktivierten und benutzbaren Cipher Suite und/oder Schlüssellänge der in dem Konfigurationsspeicher (KSP) gespeicherten Cipher Suites und/oder Schlüssellängen mit den ermittelten Referenz-Cipher Suites und/oder den bestimmten Referenz-Schlüssellängen ergibt, dass die aktuell benutzte oder aktivierte und benutzbare Cipher Suite und/oder Schlüssellänge nicht unter den ermittelten Referenz-Cipher Suites und/oder den bestimmten Referenz-Schlüssellängen ist, dass dann
(i) ein an den Benutzer des Computers (CPT) adressierter Warnhinweis erzeugt und über die Ausgabeschnittstelle (ASS) ausgegeben wird,
(ii) die aktuell benutzte Cipher Suite und/oder Schlüssellänge unverzüglich gesperrt wird, und/oder
(iii) die aktuell benutzte Cipher Suite und/oder Schlüssellänge nach einer Karenzzeit des ausgegebenen Warnhinweises gesperrt wird.

10. Computer (CPT) nach Anspruch 7, 8 oder 9, **dadurch gekennzeichnet**, dass der Prozessor (PZ) und das Programm-Modul (PGM) derart ausgebildet sind, dass die automatisch und dynamisch, insbesondere regelmäßig oder ereignisgesteuert, durchgeführte Ermittlung in einem dedizierten Betriebsmodus des Computers (CPT), z.B. im Wartungsmodus, erfolgt.

11. Computer (CPT) nach Anspruch 9, **dadurch gekennzeichnet**, dass der Prozessor (PZ) und das Programm-Modul (PGM) derart ausgebildet sind, dass die Referenz-Cipher Suite und/oder Referenz-Schlüssellänge die zur Sperrung der aktuell benutzten oder aktivierten und benutzbaren Cipher Suite und/oder Schlüssellänge geführt hat, automatisch nach einer Wartezeit oder nach Bestätigung durch einen Servicetechniker über die Eingabeschnittstelle (ESS) übernommen wird/werden.

12. Computer (CPT) nach einem der Ansprüche 7 bis 11, **dadurch gekennzeichnet**, dass der Prozessor (PZ) und das Programm-Modul (PGM) derart ausgebildet sind, dass die von den Internet-Dienstanbietern abgefragten Informationen für die Ermittlung der angemessenen Referenz-Cipher Suites gewichtet werden.

Es folgen 4 Seiten Zeichnungen

Anhängende Zeichnungen

FIG 1

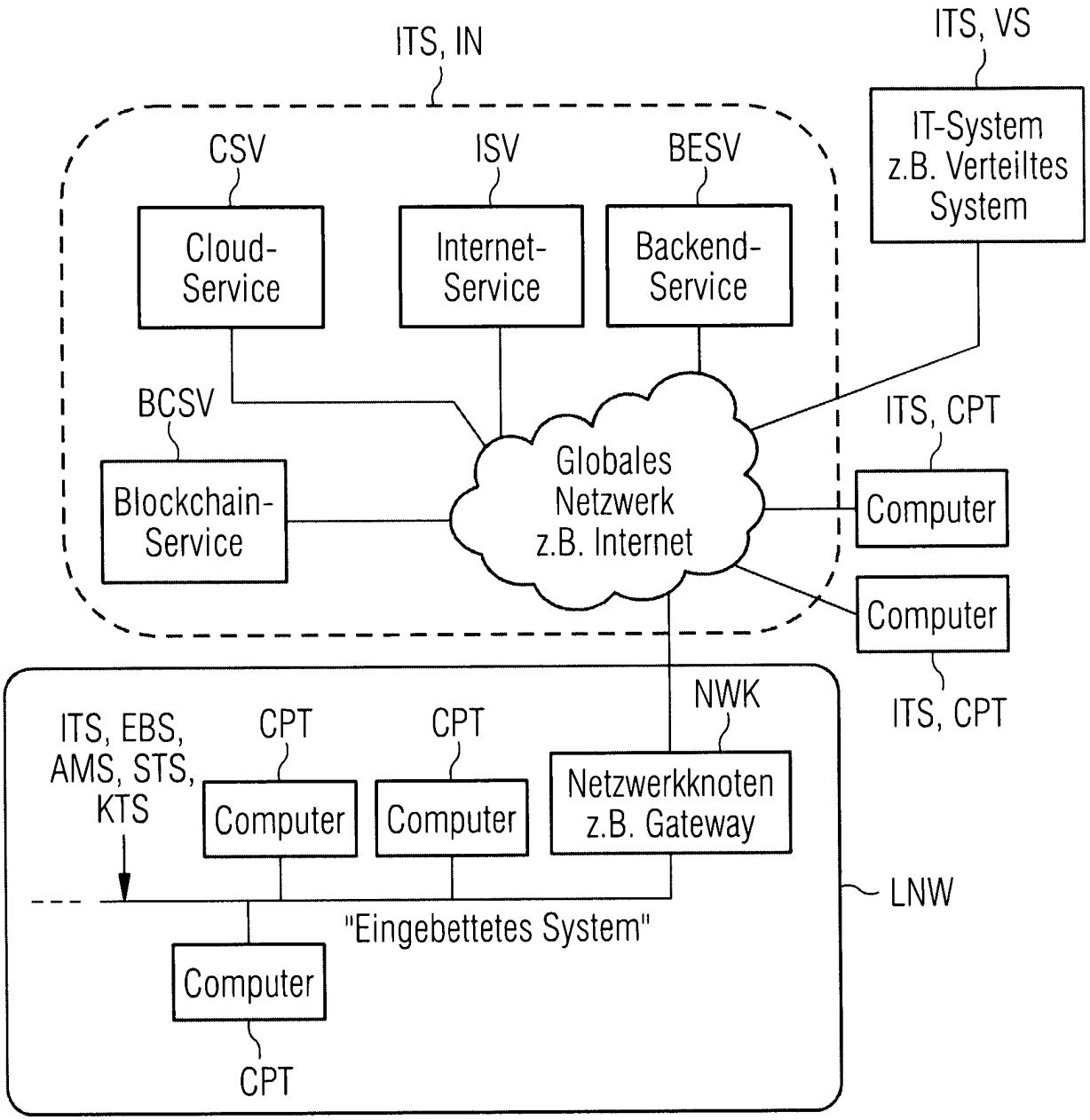


FIG 2

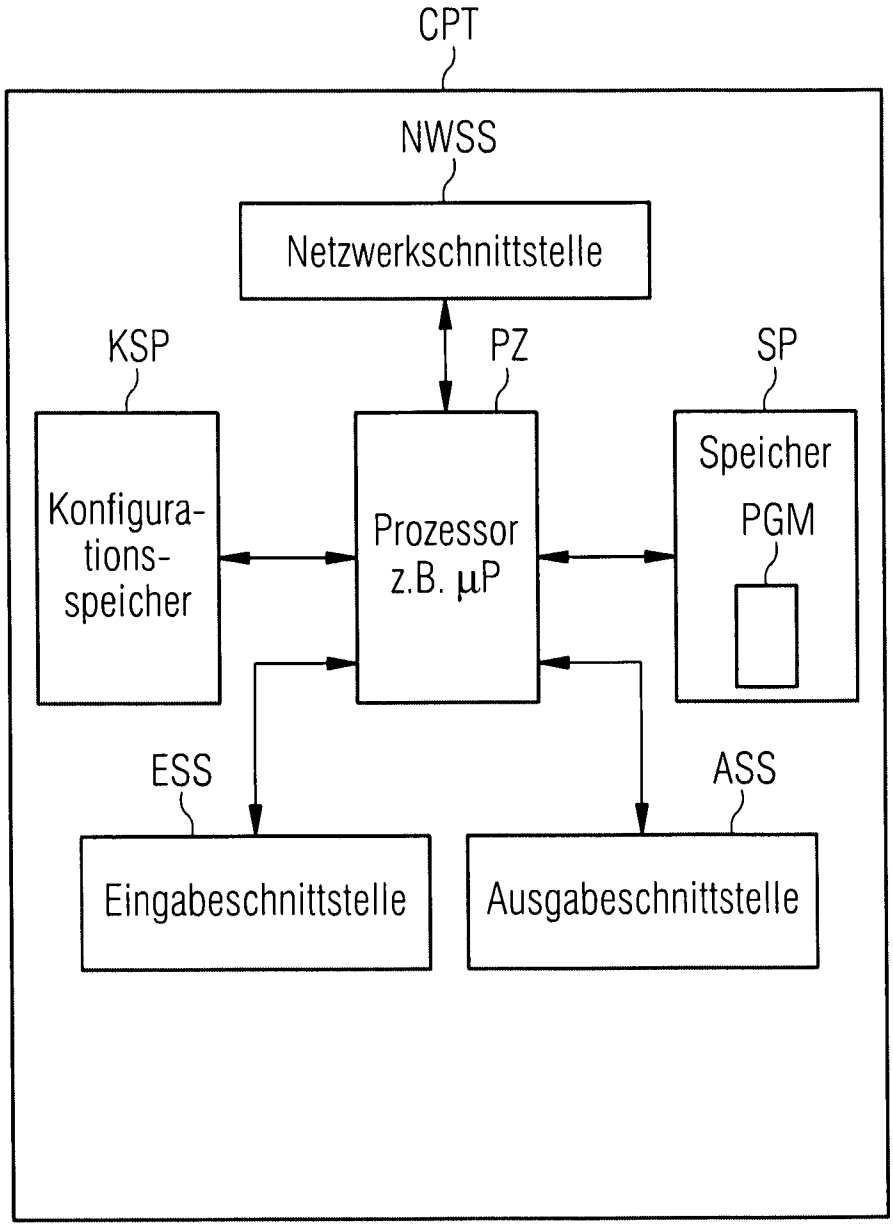

CPT
NWSS
Netzwerkschnittstelle
KSP
PZ
SP
Konfigura-
tions-
speicher
Prozessor
z.B. µP
Speicher
PGM
ESS
ASS
Eingabeschnittstelle
Ausgabeschnittstelle

FIG 3

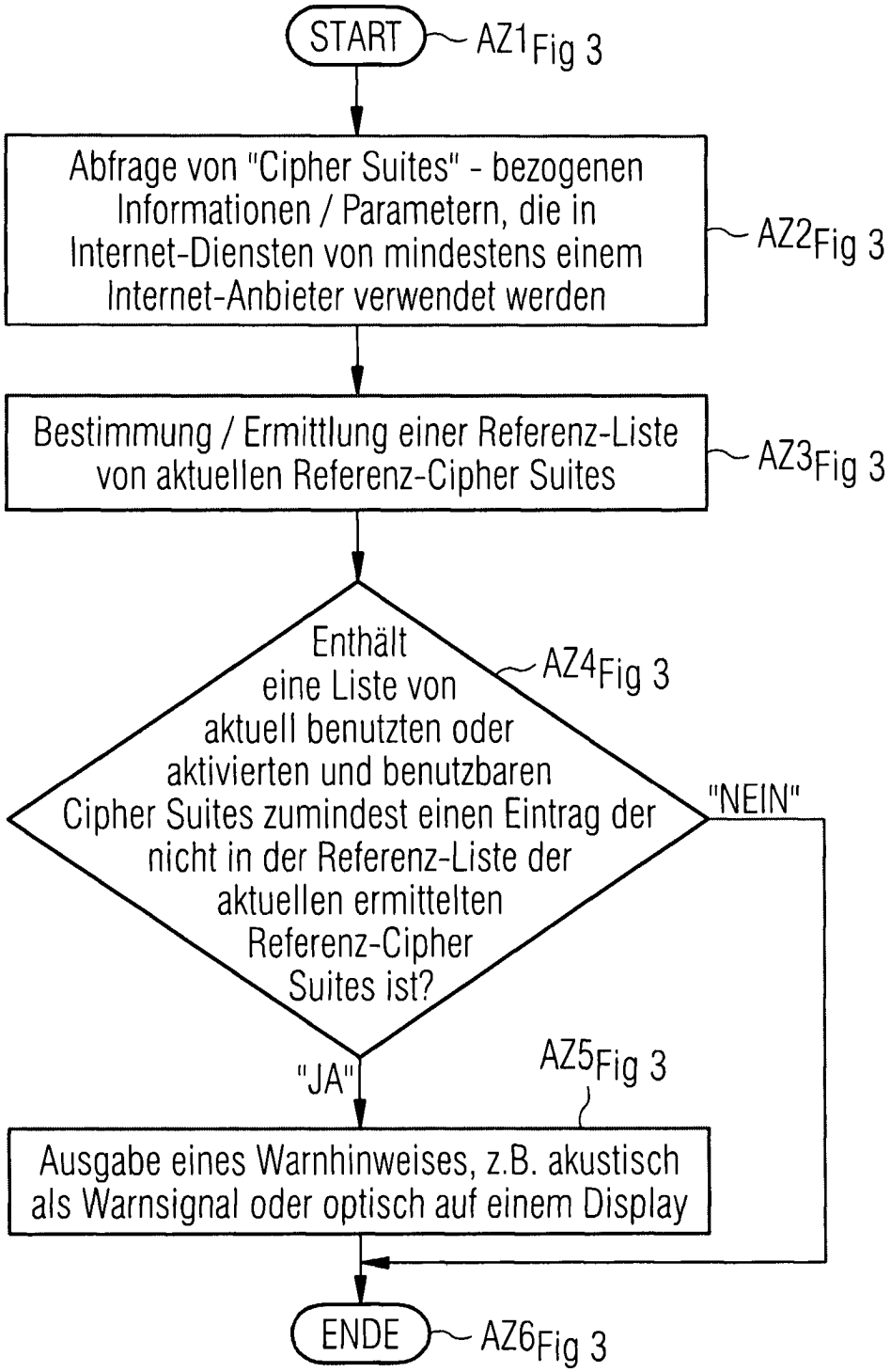
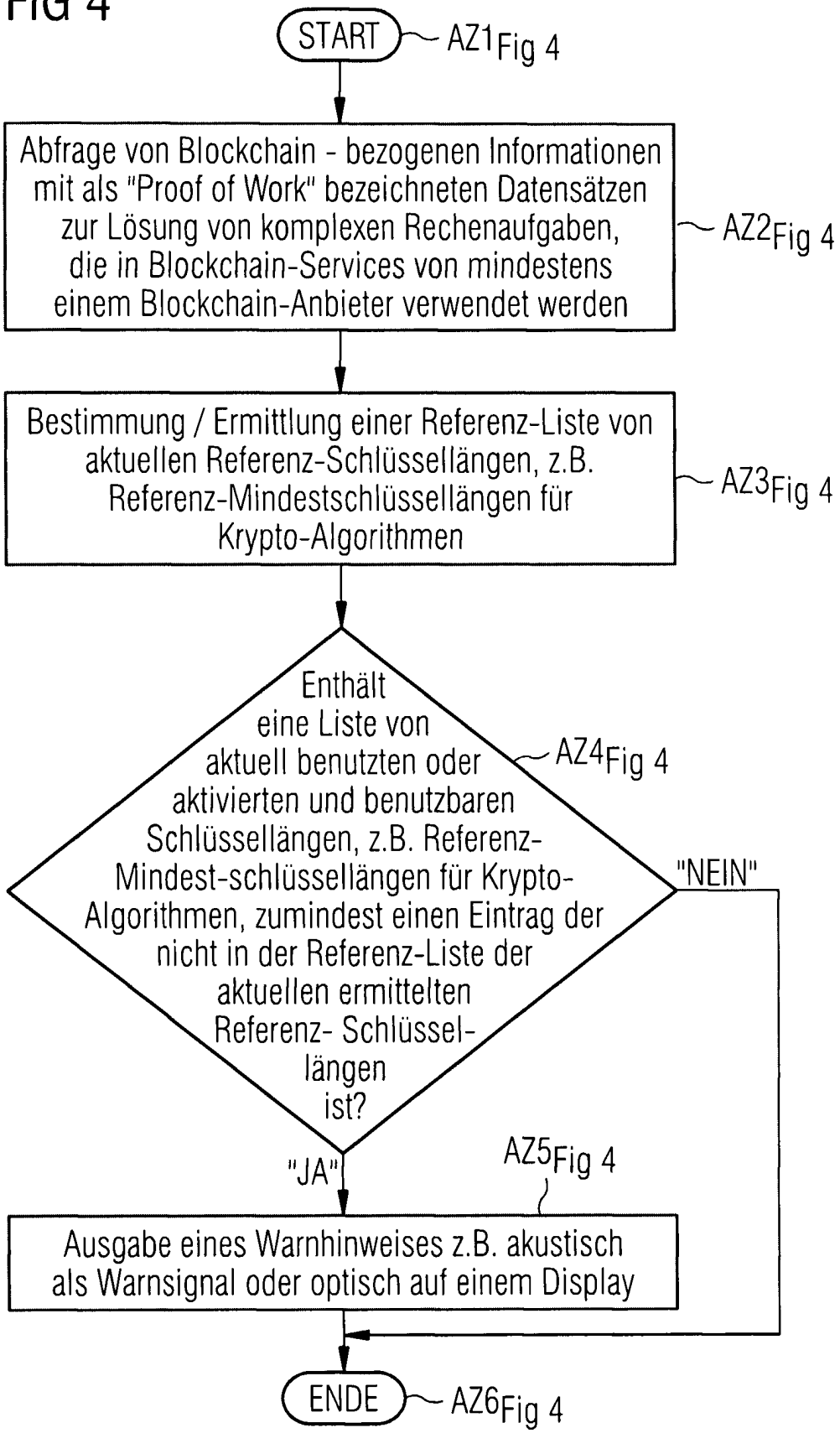

START
AZ1 Fig 3
Abfrage von "Cipher Suites" - bezogenen Informationen / Parametern, die in Internet-Diensten von mindestens einem Internet-Anbieter verwendet werden
AZ2 Fig 3
Bestimmung / Ermittlung einer Referenz-Liste von aktuellen Referenz-Cipher Suites
AZ3 Fig 3
Enthält eine Liste von aktuell benutzten oder aktivierten und benutzbaren Cipher Suites zumindest einen Eintrag der nicht in der Referenz-Liste der aktuellen ermittelten Referenz-Cipher Suites ist?
AZ4 Fig 3
"NEIN"
"JA"
AZ5 Fig 3
Ausgabe eines Warnhinweises, z.B. akustisch als Warnsignal oder optisch auf einem Display
ENDE
AZ6 Fig 3

FIG 4


START
AZ1 Fig 4
Abfrage von Blockchain - bezogenen Informationen mit als "Proof of Work" bezeichneten Datensätzen zur Lösung von komplexen Rechenaufgaben, die in Blockchain-Services von mindestens einem Blockchain-Anbieter verwendet werden
AZ2 Fig 4
Bestimmung / Ermittlung einer Referenz-Liste von aktuellen Referenz-Schlüssellängen, z.B. Referenz-Mindestschlüssellängen für Krypto-Algorithmen
AZ3 Fig 4
Enthält eine Liste von aktuell benutzten oder aktivierten und benutzbaren Schlüssellängen, z.B. Referenz-Mindest-schlüssellängen für Krypto-Algorithmen, zumindest einen Eintrag der nicht in der Referenz-Liste der aktuellen ermittelten Referenz- Schlüssel-längen ist?
AZ4 Fig 4
"NEIN"
"JA"
AZ5 Fig 4
Ausgabe eines Warnhinweises z.B. akustisch als Warnsignal oder optisch auf einem Display
ENDE
AZ6 Fig 4