(19) Deutsches Patent- und Markenamt

(10) **DE 10 2022 203 797 A1** 2023.10.19

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2022 203 797.9**
(22) Anmeldetag: **14.04.2022**
(43) Offenlegungstag: **19.10.2023**

(51) Int Cl.: ***H04L 9/08*** (2006.01)

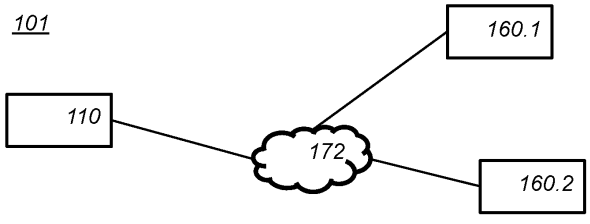
(71) Anmelder:
Robert Bosch Gesellschaft mit beschränkter Haftung, 70469 Stuttgart, DE

(72) Erfinder:
Bartelt, Andreas, 70435 Stuttgart, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Netzvorrichtung, ausgelegt für eine kryptografisch geschützte Kommunikation mit Unterstützung mehrerer Ausführungsumgebungen**

(57) Zusammenfassung: Einige Ausführungsformen richten sich auf eine Netzvorrichtung, die für eine kryptografisch geschützte Kommunikation mit einer zweiten Netzvorrichtung ausgelegt ist. Die kryptografisch geschützte Kommunikation umfasst wenigstens ein Handshake-Protokoll, ein Protokoll für den kryptografischen Schutz von Massendaten und ein Wiederaufnahmeprotokoll. Ein Sitzungshandhabungssystem erhält von dem Handshake-Protokoll einen ersten kryptografischen Massenschutzschlüssel und einen Wiederaufnahmeschlüssel. Der erste kryptografisch Schutzschlüssel wird an das Host-System weitergeleitet, nicht jedoch der Wiederaufnahmeschlüssel.



Beschreibung

Gebiet der Technik

[0001] Der hier offenbarte Erfindungsgegenstand betrifft eine erste Netzvorrichtung, die für eine kryptografisch geschützte Kommunikation mit einer zweiten Netzvorrichtung ausgelegt ist, ein Verfahren für eine kryptografisch geschützte Kommunikation zwischen einer ersten Netzvorrichtung und einer zweiten Netzvorrichtung, ein computerlesbares Medium.

Stand der Technik

[0002] Eine geschützte Kommunikation zwischen zwei computergestützten Vorrichtungen ist in Computernetzen, wie etwa dem Internet, gängig. Beispielsweise kann das Schützen von Daten durch Verschlüsseln der Daten, Authentifizieren der Daten oder beides erfolgen. Ein bestens bekanntes System zum Schützen der Kommunikation in einem Computernetz ist TLS, oder DTLS.

[0003] Das anfängliche TLS- oder DTLS-Handshake zwischen zwei Endpunkten steht für ein vollständiges Handshake, bei dem langfristige geheime Schlüssel für das Einrichten einer Endpunkt-Authentifizierung verwendet werden, z. B. einer Authentifizierung des Server-Endpunkts oder, alternativ, eine gegenseitige Authentifizierung von Client- und Server-Endpunkten. Mehrere Varianten für eine solche Endpunkt-Authentifizierung über langfristige geheime Schlüssel sind IETF-standardisiert; beispielsweise asymmetrische private Schlüssel, die den öffentlichen Schlüsseln von X509v3-Zertifikaten entsprechen, asymmetrische private Schlüssel, die sogenannten rohen öffentlichen Schlüsseln entsprechen, oder ein symmetrischer vorab vereinbarter geheimer Schlüssel, der zuvor über irgendein Außerbandmittel an beide Endpunkte verteilt worden ist. Während eines vollständigen Handshakes wird ein authentifiziertes Schlüsseleinrichtungsverfahren verwendet, um ephemeres Schlüsselmaterial kryptografisch abzuleiten, z. B. kurzfristige Schlüssel, welche dann die Basis für das Ableiten von Schlüsseln zur Massenverschlüsselung sowie für sogenannte Wiederaufnahmemechanismen sein können, die abgekürzte Handshakes für zukünftige TLS- oder DTLS-Verbindungen zwischen denselben Endpunkten ermöglichen. Abgekürzte Handshakes ermöglichen leistungsbezogene Einsparungen, z. B. einen reduzierten Netzlatenz-Overhead aufgrund weniger erforderlicher Handshake-Nachrichten sowie einen geringeren Rechenaufwand im Hinblick auf die Kryptographie.

[0004] Mehrere versionsspezifische Wiederaufnahmemechanismen sind für die Protokolle TLS, RFC5246, RFC8446 und DTLS, RFC6347 IETF-standardisiert worden. Beispielsweise wird in Versionen <=1.2 eine Sitzungswiederaufnahme über Sitzungs-IDs von RFC 5246 verwendet, Sitzungstickets von RFC5077 werden in Versionen <=1.2 verwendet, und eine Wiederaufnahme von RFC8446 über vorab vereinbarte Schlüssel wie für Version 1.3 spezifiziert. Die genannten RFCs werden hier durch Verweis aufgenommen.

[0005] Die bekannten Wiederaufnahmevarianten nutzen effektiv einen ephemeren Wiederaufnahmeschlüssel, der dann effektiv die explizite Endpunkt-Authentifizierung über langfristige geheime Schlüssel von dem anfänglichen vollständigen Handshake ersetzt. Der Begriff Wiederaufnahmeschlüssel wird hier verwendet, da die TLS-RFCs keine einheitliche Benennung in dieser Hinsicht bereitstellen. Wiederaufnahmeschlüssel sind kurzfristige Schlüssel, da sie mit einer konfigurierbaren Lebensdauer verknüpft sind, die typischerweise 24 Stunden nicht überschreitet. In dem spezifischen Fall von TLS 1.3 hat diese Lebensdauer auch einen festen oberen Grenzwert von höchstens 7 Tagen. Ein abgekürztes Wiederaufnahme-Handshake ist, aufgrund seiner kryptografischen Bindung an das authentifizierte Schlüsseleinrichtungsverfahren von dem anfänglichen vollständigen Handshake, nur implizit endpunkt-authentifiziert.

[0006] Ein typischerweise vorgefundenes Problem, z. B. bei IoT-Vorrichtungen, besteht darin, dass ephemere Schlüssel im Rahmen der Wiederaufnahme effektiv viel weniger vor Angreifern geschützt sind als die langfristigen geheimen Schlüssel für eine Endpunkt-Authentifizierung. Ein Angreifer, der sich Zugriff zu einem Wiederaufnahmeschlüssel verschafft, wäre in der Lage, die entsprechende TLS-(oder DTLS-)Sitzung wiederaufzunehmen, ohne tatsächlich irgendeinen Zugriff auf die langfristigen geheimen Schlüssel zu benötigen, was für eine explizite Endpunkt-Authentifizierung während des anfänglichen vollständigen Handshakes erforderlich wäre. Einmal im Besitz eines durchgesickerten Wiederaufnahmeschlüssels, könnte die entsprechende TLS-(oder DTLS-) Sitzung potenziell sogar mehrfach und von unterschiedlichen Endpunkten aus wiederaufgenommen werden. Dies würde typischerweise die Sicherheitsziele des Systems verletzen.

[0007] Darüber hinaus nutzen, insbesondere an serverseitigen TLS- (oder DTLS-) Endpunkten, die auf Sitzungstickets basierenden Wiederaufnahmevarianten einen sogenannten Sitzungsticket-Verschlüsselungsschlüssel (Session Ticket Encryption Key, STEK), der typischerweise, wie das gesamte andere ephemere Schlüsselmaterial, auch dem Host-System zugänglich gemacht wird. Ein Angreifer, der auf irgendeine Weise, wie etwa durch Ausnutzen einer Informationsleck-Schwachstelle am Host-System, Kenntnis vom STEK erlangt, wäre effektiv in der Lage, das Wiederaufnahmeschlüsselmaterial zu ent-

schlüsseln, welches in (STEK-verschlüsselten) Sitzungstickets enthalten ist, und diese könnten aus zuvor aufgezeichneten TLS- (oder DTLS-)Sitzungen erfasst werden. Zusätzlich dazu, dass dem Angreifer, bei TLS-Versionen <1.3, ermöglicht wird, die entsprechenden Sitzungen wiederaufzunehmen, ermöglicht diese Art von Angriff außerdem eine Entschlüsselung des entsprechenden Massenverkehrs, was die Sicherheitsvorteile einer vorwärtsgerichteten Geheimhaltung effektiv zunichte macht. Es sei dringend darauf hingewiesen, dass diese Art von Angriff eine groß angelegte Überwachung effektiv erleichtert.

Kurzdarstellung

[0008] Vorteilhaft wäre eine verbesserte Kommunikation zwischen einer ersten Netzvorrichtung und einer zweiten Netzvorrichtung.

[0009] In einer Ausführungsform wird ein verbesserter Schutz von ephemerem Schlüsselmaterial zur Laufzeit bereitgestellt. Beispielsweise handelt es sich in einer Ausführungsform bei dem einzigen ephemeren Schlüsselmaterial, welches einem Host-System der Netzvorrichtung direkt zugänglich gemacht werden könnte, um die symmetrischen Schlüssel, die im spezifischen Rahmen eines Massenschutzes, z. B. Verschlüsselung etc., verwendet werden; beispielsweise kann eine Ausführungsform den kryptografisch abgeleiteten Schlüsselblock (key_block) eines TLS-Protokolls für das Host-System zugänglich machen. Selbst wenn ein Angreifer sich Zugriff zu diesen Schlüsseln verschafft, dann wird er nur in der Lage sein, die jeweilige TLS- (oder DTLS-)Verbindung zu entschlüsseln oder zu manipulieren. Allerdings wird der Angreifer effektiv daran gehindert, den Wiederaufnahmeschlüssel und anderes ephemeres Schlüsselmaterial, wie z. B. zur Wiederaufnahme verwendetes Material, zu stehlen.

[0010] Beispielsweise kann eine erste Netzvorrichtung für eine kryptografisch geschützte Kommunikation mit einer zweiten Netzvorrichtung ausgelegt sein. Die kryptografisch geschützte Kommunikation umfasst wenigstens ein Handshake-Protokoll, ein Protokoll für den kryptografischen Schutz von Massendaten und ein Wiederaufnahmeprotokoll. Beispielsweise können die erste und die zweite Netzvorrichtung für ein TLS- oder DTLS-Protokoll ausgelegt sein.

[0011] Interessanterweise ist die erste Netzvorrichtung dafür ausgelegt, mehrere getrennte Ausführungsumgebungen in der ersten Netzvorrichtung anzuordnen, was ein Host-System und ein Sitzungshandhabungssystem beinhaltet. Die Protokolle, die an der kryptografischen Kommunikation beteiligt sind, werden auf wenigstens zwei dieser Ausführungsumgebungen aufgeteilt.

[0012] Das Sitzungshandhabungssystem kann dafür ausgelegt sein, eine kryptografische Antwort in Abhängigkeit von dem langfristigen Geheimnis zu erhalten und eine sichere Sitzung zwischen der ersten Netzvorrichtung und der zweiten Netzvorrichtung einzurichten. Ein oder mehrere Schlüssel, die auf diese Weise für den kryptografischen Schutz von Massendaten erhalten werden, werden an das Host-System weitergeleitet, nicht jedoch anderes ephemeres Schlüsselmaterial, insbesondere Wiederaufnahmeschlüssel.

[0013] Der kryptografische Schutz von Massendaten kann jetzt vom Host-System durchgeführt werden, aber ein Angriff auf das Host-System führt nicht zu einem Leck des anderen ephemeren Schlüsselmaterials. Darüber hinaus werden die langfristigen geheimen Schlüssel ferner aus dem Host-System entfernt; in einer Ausführungsform sind die langfristigen geheimen Schlüssel in einem Sicherheitssystem gespeichert, welches für das Host-System nicht zugänglich ist, während der Sitzungshandler nur Zugriff über eine Schnittstelle hat, z. B. über eine vordefinierte API.

[0014] Im Einsatz erfolgen die meisten Aktivitäten typischerweise im Host-System. Bei dem Host-System kann es sich auch um die Ausführungsumgebung handeln, in der eine Benutzeranwendung läuft. Ein potenzieller Angriff auf die erste Netzvorrichtung erfolgt daher mit größerer Wahrscheinlichkeit auf dem Host-System, da das Host-System eine größere Angriffsfläche bietet und/oder mehr externe Netzverbindungen aufweist. Tatsächlich muss, in einer Ausführungsform, das Sitzungshandhabungssystem keinerlei Verbindung zu externen Computern aufweisen, da beispielsweise jegliche erforderliche Kommunikation, etwa für das Einrichten eines kryptografischen Kanals, durch das Host-System weitergeleitet wird.

[0015] Schlüsselmaterial, das nicht für das Bereitstellen von Massenschutzdiensten benötigt wird, z. B. für eine Benutzeranwendung, die auf dem Host-System läuft, wird dem Host-System nicht zugänglich gemacht. Interessanterweise ist das erste Netzwerk wiederaufnahmefähig und somit in der Lage, mit geringer Verzögerung an einer kryptografischen Kommunikation teilzunehmen, da das Sitzungshandhabungssystem Zugriff auf die hierfür verwendeten ephemeren Schlüssel hat.

[0016] In einer Ausführungsform umfasst die erste Netzvorrichtung ein Sicherheitssystem, wobei das Sicherheitssystem dafür ausgelegt ist, ein langfristiges Geheimnis zu speichern, und das Sitzungshandhabungssystem dafür ausgelegt die kryptografische

Antwort von dem Sicherheitssystem zu erhalten. Vorzugsweise handelt es sich bei dem Sicherheitssystem um ein hardwaremäßig abgeschirmtes Modul, z. B. ein sicheres Modul, einen sicheren Kryptoprozessor, ein sogenanntes vertrauenswürdiges Plattformmodul (Trusted Platform Module, TPM), einen dedizierten Mikrocontroller etc., die dafür ausgelegt sind, kryptografische Schlüssel zu speichern und abzuschirmen.

[0017] In einer Ausführungsform haben weder die Ausführungsumgebung des Host-Systems noch die Ausführungsumgebung des Sitzungshandhabungssystems Zugriff auf das langfristige Geheimnis, und die Ausführungsumgebung des Host-Systems hat keinen Zugriff auf den Wiederaufnahmeschlüssel.

[0018] Ein weiterer Aspekt ist ein Kommunikationsverfahren. Eine Ausführungsform des Verfahrens kann auf einem Computer als ein computerimplementiertes Verfahren oder in dedizierter Hardware oder in einer Kombination von beiden implementiert sein. Ausführbarer Code für eine Ausführungsform des Verfahrens kann auf einem Computerprogrammprodukt gespeichert sein. Beispiele für Computerprogrammprodukte beinhalten Speichervorrichtungen, optische Datenspeichervorrichtungen, integrierte Schaltungen, Server, Online-Software etc. Vorzugsweise umfassen die Computerprogrammprodukte nicht-transitorischen Programmcode, der auf einem computerlesbaren Medium gespeichert ist, um eine Ausführungsform des Verfahrens durchzuführen, wenn das besagte Programmprodukt auf einem Computer ausgeführt wird.

[0019] In einer Ausführungsform umfasst das Computerprogramm Computerprogrammcode, der dafür angepasst ist, alle oder einen Teil der Schritte einer Ausführungsform des Verfahrens durchzuführen, wenn das Computerprogramm auf einem Computer ausgeführt wird. Vorzugsweise liegt das Computerprogramm auf einem computerlesbaren Medium vor.

Kurze Beschreibung der Zeichnungen

[0020] Weitere Einzelheiten, Aspekte und Ausführungsformen werden, lediglich beispielhaft, unter Bezugnahme auf die Zeichnungen beschrieben. Elemente in den Figuren werden im Hinblick auf Einfachheit und Übersichtlichkeit veranschaulicht und sind nicht notwendigerweise maßstabsgetreu gezeichnet. In den Figuren können Elemente, welche Elementen entsprechen, die bereits beschrieben wurden, dieselben Bezugszeichen aufweisen. In den Zeichnungen gilt:

Fig. 1a zeigt schematisch eine beispielhafte Ausführungsform einer ersten Netzvorrichtung, die für eine kryptografisch geschützte Kommunikation ausgelegt ist.

Fig. 1b zeigt schematisch eine beispielhafte Ausführungsform einer zweiten Netzvorrichtung.

Fig. 1c zeigt schematisch eine beispielhafte Ausführungsform eines Kommunikationssystems.

Fig. 2 zeigt schematisch eine beispielhafte Ausführungsform einer ersten Netzvorrichtung, die für eine kryptografisch geschützte Kommunikation ausgelegt ist.

Fig. 3 zeigt schematisch eine beispielhafte Ausführungsform eines Verfahrens für eine kryptografisch geschützte Kommunikation.

Fig. 4a zeigt schematisch ein computerlesbares Medium mit einem beschreibbaren Teil, der ein Computerprogramm gemäß einer Ausführungsform umfasst.

Fig. 4b zeigt schematisch eine Darstellung eines Prozessorsystems gemäß einer Ausführungsform.

Liste der Bezugszeichen

[0021] Die nachfolgende Liste mit Verweisen und Abkürzungen entspricht den **Fig.** 1a-2, **Fig.** 4a und **Fig.** 4b und wird bereitgestellt, um die Interpretation der Zeichnungen zu erleichtern; die Liste ist nicht dahingehend auszulegen, dass sie die Ansprüche einschränkt.

100, 101	ein Kommunikationssystem
110	eine erste Netzvorrichtung
130	ein Prozessorsystem
140	Datenspeicher
150	Kommunikationsschnittstelle
160, 160.1, 160.2	eine zweite Netzvorrichtung
170	ein Prozessorsystem
180	ein Datenspeicher
190	eine Kommunikationsschnittstelle
172	ein Computernetzwerk
200	eine erste Netzvorrichtung
211	kryptografisch geschützte Kommunikation
210	ein Host-System

220	ein Sitzungshandhabungssystem
230	ein Sicherheitssystem,
231	eine kryptographische Schnittstelle
221	ein erster Kommunikationskanal
222	ein zweiter Kommunikationskanal
1000	ein computerlesbares Medium
1010	ein beschreibbarer Teil
1020	ein Computerprogramm
1110	integrierte Schaltung (en)
1120	eine Verarbeitungseinheit
1122	ein Speicher
1124	eine dedizierte integrierte Schaltung
1126	ein Kommunikationselement
1130	eine Zwischenverbindung
1140	ein Prozessorsystem

Beschreibung der Ausführungsformen

[0022] Auch wenn der hier offenbarte Erfindungsgegenstand in vielen unterschiedlichen Formen ausführbar ist, werden in den Zeichnungen eine oder mehrere spezifische Ausführungsformen gezeigt und hier ausführlich beschrieben, in dem Verständnis, dass die vorliegende Offenbarung als beispielhaft für die Prinzipien des hier offenbarten Erfindungsgegenstands zu verstehen ist und nicht dazu gedacht ist, diese auf die spezifischen, hier gezeigten und beschriebenen Ausführungsformen zu beschränken.

[0023] Im Folgenden werden, zum besseren Verständnis, Elemente von Ausführungsformen im Betrieb beschrieben. Allerdings ist offensichtlich, dass die jeweiligen Elemente angeordnet sind, um die Funktionen durchzuführen, die als von ihnen durchgeführte Funktionen beschrieben werden. Ferner ist der Erfindungsgegenstand, der hier offenbart wird, nicht nur auf die Ausführungsformen beschränkt, sondern beinhaltet auch jede andere Kombination von Merkmalen, die hier beschrieben oder in voneinander unterschiedlichen Ansprüchen aufgeführt sind.

[0024] Herkömmlicherweise nutzen Netzvorrichtungen, wie etwa IoT-Vorrichtungen, Desktop-Vorrichtungen, Server und so weiter, das TLS- (oder DTLS-)Protokoll, um einen kryptografisch geschützten sicheren Ende-zu-Ende-Tunnel zwischen TCP-fähiger (oder UDP-fähiger) Software, die auf der Vorrichtung ausgeführt wird, und den entsprechenden Diensten, die auf dem Backend der Vorrichtung ausgeführt werden, zu ermöglichen. Kryptografisch geschützte Daten werden bei digitaler Kommunikation jeder Art verwendet, z. B. um digitale Daten zu senden oder zu empfangen, z. B. Sensordaten, Computeranweisungen, Medien und so weiter.

[0025] Bei vielen TLS- (oder DTLS-)Implementierungen ist das ephemere Schlüsselmaterial, z. B. insbesondere Schlüsselmaterial zur Wiederaufnahme, viel weniger geschützt als die langfristigen geheimen Schlüssel. Der Einfachheit halber wird Schlüsselmaterial mit einem davon abgeleiteten Schlüssel gleichgesetzt.

[0026] Beispielsweise sind asymmetrische langfristiges geheime Schlüssel typischerweise in einem dedizierten Sicherheitssystem geschützt, das speziell dafür konzipiert ist, diese Art von geheimem Schlüsselmaterial davor zu schützen, dass es „im Ruhezustand“ durchsickert, wenn die Vorrichtung ausgeschaltet ist, und auch „zur Laufzeit“. Diese Arten von Sicherheitssystemen werden typischerweise handelsüblich als Hardware-Sicherheitsmodul (Hardware Security Module, HSM), vertrauenswürdiges Plattformmodul (Trusted Platform Module, TPM), PKCS#11-basiertes Sicherheitssystem oder als eine andere Art von spezialisierten Krypto-Subsystemen bereitgestellt. Diese Subsysteme machen typischerweise nur APIs für generische Kryptoschemata zugänglich (z. B. APIs für das Erstellen von ECDSA-Signaturen, RSA-basierte Verschlüsselung und Signaturen etc.). Allerdings stellen solche Sicherheitssysteme keine APIs bereit, die speziell auf das TLS- (oder DTLS-)Handshake zugeschnitten sind, was erforderlich wäre, um in der Lage zu sein, ephemeres Schlüsselmaterial in dem Sicherheitssystem zu halten, z. B. das sogenannte Master-Geheimnis (Master Secret), das auch dem Wiederaufnahmeschlüssel in TLS-Versionen <1.3 etc. entspricht. Im Folgenden wird weiterhin Sicherheitssystem als Oberbegriff für diese Art von spezialisierten, handelsüblichen Krypto-Subsystemen verwendet. Das Sicherheitssystem ist typischerweise Teil einer Netzvorrichtung.

[0027] Die eigentliche Verschlüsselung und Authentifizierung von Massenverkehr erfolgt oft direkt auf dem Host-System. Dieser Ansatz hat den Vorteil, dass Latenzen eingespart werden, da Massendaten

nicht durch das Sicherheitssystem durchgeschleift werden müssen. Herkömmlicherweise wird ephemeres Schlüsselmaterial im Rahmen der Wiederaufnahme somit typischerweise direkt dem Host-System zugänglich gemacht, wo der Schutz vor einem Durchsickern viel schwächer ist als für die langfristigen Schlüssel im Sicherheitssystem.

[0028] Hier beschriebene Ausführungsformen können mit allen aktuellen TLS- und DTLS-Protokollversionen, z. B. IETF-standardisierten Versionen, angewendet werden. Beispielsweise ist, in einer Ausführungsform, ein zusätzliches Subsystem, das Sitzungshandhabungssystem, zwischen dem Host-System und dem Sicherheitssystem integriert. Das Sitzungshandhabungssystem kann gewählt werden, um zur Laufzeit robustere Schutzgarantien bereitzustellen als das Host-System; beispielsweise kann das Sitzungshandhabungssystem eine robustere Trennung aufweisen, die durch einen Typ-1-Hypervisor oder eine Variante einer vertrauenswürdigen Ausführungsumgebung (Trusted Execution Environment, TEE) bereitgestellt wird. Beispielsweise kann das Sitzungshandhabungssystem dafür ausgelegt sein, die TLS- (oder DTLS-)Subprotokolle handshake (Handshake), alert (Alarm) und change_cipher_spec (Chiffrenspezifikation ändern) auszuführen und ephemeres Schlüsselmaterial (z. B. Wiederaufnahmeschlüssel, den STEK im Fall von serverseitigen Endpunkten etc.) geschützt zu halten. Die abgeleiteten Schlüssel für den Massenschutz, z. B. Massenverschlüsselung (z. B. key_block) werden für das Host-System bereitgestellt, das die gesamte Massenverschlüsselung handhabt (z. B. Datensätze des Typs application_data (Anwendungsdaten) im Rahmen des TLS-(oder DTLS-)-Protokolls).

[0029] TLS, RFC5246, RFC8446 und DTLS, RFC6347 sind die IETF-standardisierten kryptografischen Protokolle, welche vielfach verwendet werden, um einen kryptografisch geschützten und sicheren Ende-zu-Ende-Tunnel zwischen Software auf IoT-Vorrichtungen und Diensten am IoT-Backend bereitzustellen; diese werden hier durch Verweis aufgenommen. Das TLS-Handshake ist auch auf das neuere QUIC-Protokoll RFC9001 angewendet worden, hier durch Verweis aufgenommen.

[0030] Die IETF-standardisierten Mechanismen zur Wiederaufnahme RFC5246, RFC8446, RFC5077 ermöglichen leistungsbezogene Vorteile wie etwa einen reduzierten Netzlatenz-Overhead und einen geringeren Rechenaufwand im Hinblick auf die Kryptographie; diese sind hier durch Verweis aufgenommen. Allerdings haben ohne einen geeigneten Laufzeitschutz von ephemerem Schlüsselmaterial in diesem Rahmen (z. B. Wiederaufnahmeschlüssel, den STEK im Fall von serverseitigen TLS/DTLS-Endpunkten etc.) all diese Wiederaufnahmeverfahren potenziell gravierende Nachteile hinsichtlich der Sicherheit. Das hier ausführlich beschriebene Verfahren reduziert das Risiko, dass ephemeres Schlüsselmaterial von der Vorrichtung angriffsbedingt durchsickert. Die Ausführungsform kann mit bestehenden handelsüblichen Sicherheitssystemen kombiniert werden, insbesondere solchen, die keine TLS-(oder DTLS-)spezifischen APIs bereitstellen. Das Verfahren kann auf clientseitige sowie serverseitige TLS- (oder DTLS-) Endpunkte angewendet werden. Darüber hinaus funktioniert eine Integration mit dem Sicherheitssystem zur Endpunkt-Authentifizierung während des vollständigen Handshakes für eine clientseitige sowie eine serverseitige Endpunkt-Authentifizierung, je nach sitzungsspezifischen Anforderungen und dem spezifischen Anwendungsfall.

[0031] Die IETF-standardisierten TLS- und DTLS-Versionen ermöglichen verschiedene Endpunkt-Authentifizierung- und Schlüsselaustauschverfahren, und einige davon sind außerdem an spezifische Protokollversionen gebunden. Die kryptografischen Schemata und Konventionen zum Ableiten von ephemerem Schlüsselmaterial, z. B. der Schlüssel, der tatsächlich in Wiederaufnahmemechanismen verwendet wird, können außerdem ziemlich heterogen sein.

[0032] Beispielsweise können Operationen im Rahmen von Datensätzen des Typs application_data (Anwendungsdaten) durch das Host-System gehandhabt werden, z. B. bei der Handhabung einer Massenverschlüsselung, während andere Subprotokolle, z. B. handshake (Handshake), alert (Alarm) und change_cipher_spec (Chiffrenspezifikation ändern), an das Sitzungshandhabungssystem delegiert werden. Das Sitzungshandhabungssystem kann die Kontrolle, sogar die exklusive Kontrolle über das gesamte ephemere Schlüsselmaterial haben, was z. B. Wiederaufnahmeschlüssel, den STEK im Fall von serverseitigen TLS/DTLS-Endpunkten etc. einschließt. Wechsel zwischen application_data (Anwendungsdaten) und den anderen Datensatztypen können durch eine explizite Übergabe von Zustand und Steuerung zwischen dem Host-System und dem TLS/DTLS-Sitzungshandhabungssystem abgewickelt werden.

[0033] **Fig.** 1a zeigt schematisch eine beispielhafte Ausführungsform einer ersten Netzvorrichtung 110. **Fig.** 1b zeigt schematisch eine beispielhafte Ausführungsform einer zweiten Netzvorrichtung 160. Die erste Netzvorrichtung 110 und die zweite Netzvorrichtung 160 können Teil eines Kommunikationssystems 100 sein.

[0034] Die erste Netzvorrichtung 110 ist dafür ausgelegt, eine kryptografisch geschützte Kommunika-

tion an die/von der zweite(n) Netzvorrichtung 160 zu senden und/oder zu empfangen.

[0035] Die zweite Netzvorrichtung 160 ist in gleicher Weise dafür ausgelegt, die kryptografisch geschützte Kommunikation von der/an die erste(n) Netzvorrichtung 110 zu empfangen und/oder zu senden. Die Beziehung zwischen der ersten und der zweiten Netzvorrichtung muss keine Eins-zu-Eins-Beziehung sein. Beispielsweise kann die erste Netzvorrichtung 110 dafür ausgelegt sein, an einer kryptografisch geschützten Kommunikation mit mehreren zweiten Netzvorrichtungen oder mit einer einzelnen zweiten Netzvorrichtung teilzunehmen. Die erste Netzvorrichtung 110 kann als Server-Vorrichtung ausgeführt sein, oder als Client-Vorrichtung. Bei der zweiten Netzvorrichtung kann es sich um eine Vorrichtung gemäß einer Ausführungsform handeln, z. B. wie es die erste Netzvorrichtung ist, aber dies ist nicht notwendig. Die zweite Netzvorrichtung kann herkömmlich ausgeführt sein.

[0036] Die kryptografisch geschützte Kommunikation umfasst unterschiedliche Protokolle, was wenigstens ein Handshake-Protokoll, ein Protokoll für den kryptografischen Schutz von Massendaten und ein Wiederaufnahmeprotokoll beinhaltet. Diese Protokolle werden hier ausführlicher erläutert. Ausführungsformen können einem von mehreren Standards folgen, was hier als Implementieren dieser Protokolle bezeichnet wird; allerdings sind auch Ausführungsformen möglich, die nicht diesen Standards folgen.

[0037] Beispielsweise kann das Kommunikationssystem 100 verwendet werden, um andere Kommunikationsbedürfnisse zu schützen, z. B. sichere Nachrichtenübermittlung, E-Mails, Banking, Cloud-Computing und so weiter.

[0038] Die erste Netzvorrichtung 110 kann ein Prozessorsystem 130, einen Datenspeicher 140 und eine Kommunikationsschnittstelle 150 umfassen. Die zweite Netzvorrichtung 160 kann ein Prozessorsystem 170, einen Datenspeicher 180 und eine Kommunikationsschnittstelle 190 umfassen. Bei dem Datenspeicher 140 und 180 kann es sich z. B. um elektronischen Datenspeicher, magnetischen Datenspeicher etc. handeln. Der Datenspeicher kann lokalen Datenspeicher umfassen, z. B. ein lokales Festplattenlaufwerk oder elektronischen Speicher. Der Datenspeicher 140 und 180 kann nicht-lokalen Datenspeicher umfassen, z. B. Cloud-Datenspeicher. Im letzteren Fall kann der Datenspeicher 140 und 180 eine Datenspeicherschnittstelle zu dem nicht-lokalen Datenspeicher umfassen. Der Datenspeicher kann mehrere diskrete Unterdatenspeicher umfassen, die zusammen den Datenspeicher 140, 180 ausmachen. Der Datenspeicher kann einen flüchtigen beschreibbaren Teil, wie etwa ein RAM, einen nichtflüchtigen beschreibbaren Teil, z. B. Flash, einen nichtflüchtigen nicht beschreibbaren Teil, z. B. ROM, umfassen.

[0039] Bei dem Datenspeicher 140 und 180 kann es sich um nicht-transitorischen Datenspeicher handeln. Beispielsweise kann der Datenspeicher 140 und 180 Daten bei Anliegen von Strom speichern, wie etwa eine flüchtige Speichervorrichtung, z. B. ein Direktzugriffsspeicher (Random Access Memory, RAM). Beispielsweise kann der Datenspeicher 140 und 180 Daten bei Anliegen von Strom sowie bei Nicht-Anliegen von Strom speichern, wie etwa eine nichtflüchtige Speichervorrichtung, z. B. Flash-Speicher.

[0040] Die Vorrichtungen 110 und 160 können intern, miteinander, mit anderen Vorrichtungen, externem Speicher, Eingabevorrichtungen, Ausgabevorrichtungen und/oder einem oder mehreren Sensoren über ein Computernetz kommunizieren. Das Computernetz kann ein Intranet, ein LAN, ein WLAN etc. sein. Bei dem Computernetz kann es sich um das Internet handeln. Die Vorrichtungen 110 und 160 umfassen eine Verbindungsschnittstelle, die dafür ausgelegt ist, je nach Bedarf innerhalb eines Kommunikationssystems 100 oder außerhalb eines Kommunikationssystems 100 zu kommunizieren. Beispielsweise kann die Verbindungsschnittstelle einen Verbinder umfassen, z. B. einen drahtgebundenen Verbinder, z. B. einen Ethernet-Verbinder, einen optischen Verbinder etc., oder einen drahtlosen Verbinder, z. B. eine Antenne, z. B. eine Wi-Fi-, 4G- oder 5G-Antenne.

[0041] Die Kommunikationsschnittstelle 150 kann verwendet werden, um digitale Daten zu senden oder zu empfangen, z. B. die Kommunikation, insbesondere kryptografisch geschützte Kommunikation. Die Kommunikationsschnittstelle 190 kann verwendet werden, um digitale Daten zu senden oder zu empfangen, z. B. die Kommunikation, insbesondere kryptografisch geschützte Kommunikation.

[0042] Die Ausführung der Vorrichtungen 110 und 160 kann in einem Prozessorsystem implementiert sein. Die Vorrichtungen 110 und 160 können Funktionseinheiten umfassen, um Aspekte von Ausführungsformen zu implementieren. Die Funktionseinheiten können Teil des Prozessorsystems sein. Beispielsweise können die hier gezeigten Funktionseinheiten ganz oder teilweise in Computeranweisungen implementiert sein, die in einem Datenspeicher der Vorrichtung gespeichert sind und von dem Prozessorsystem ausgeführt werden können.

[0043] Das Prozessorsystem kann eine oder mehrere Prozessorschaltungen umfassen, z. B. Mikroprozessoren, CPUs, GPUs etc. Die Vorrichtungen 110 und 160 können mehrere Prozessoren umfas-

sen. Eine Prozessorschaltung kann in einer verteilten Weise implementiert sein, z. B. als mehrere Subprozessorschaltungen. Beispielsweise können die Vorrichtungen 110 und 160 Cloud-Computing verwenden.

[0044] Typischerweise umfassen die erste Netzvorrichtung 110 und die zweite Netzvorrichtung 160 jeweils einen Mikroprozessor, welcher geeignete Software ausführt, die auf der Vorrichtung gespeichert ist; beispielsweise kann diese Software heruntergeladen worden sein und/oder in einem entsprechenden Speicher gespeichert sein, z. B. einem flüchten Speicher, wie etwa RAM, oder in einem nichtflüchtigem Speicher, wie etwa Flash.

[0045] Anstatt Software zu verwenden, um eine Funktion zu implementieren, können die Vorrichtungen 110 und/oder 160, ganz oder teilweise, in programmierbarer Logik implementiert sein, z. B. als feldprogrammierte Gatteranordnung (Field-Programmable Gate Array, FPGA). Die Vorrichtungen können, ganz oder teilweise, als eine sogenannte anwendungsspezifische integrierte Schaltung (Application-Specific Integrated Circuit, ASIC) implementiert sein, z. B. als integrierte Schaltung (Integrated Circuit, IC), die für ihre jeweilige Verwendung individuell angepasst wurde. Beispielsweise können die Schaltungen im CMOS implementiert sein, z. B. unter Verwendung einer Hardware-Beschreibungssprache wie etwa Verilog, VHDL etc. Insbesondere können die erste Netzvorrichtung 110 und die zweite Netzvorrichtung 160 Schaltungen umfassen, z. B. für eine kryptografische Verarbeitung und/oder eine arithmetische Verarbeitung.

[0046] Die erste Netzvorrichtung 110 und/oder die zweite Netzvorrichtung 160 können ein Sicherheitssystem umfassen. Das Sicherheitssystem ist dafür ausgelegt, ein langfristiges Geheimnis zu speichern. Beispielsweise kann das Sicherheitssystem ein vertrauenswürdiges Plattformmodul (Trusted Platform Module, TPM) umfassen, z. B. gemäß ISO/IEC 11889, einen sicheren Kryptoprozessor, einen dedizierten Mikrocontroller, der dafür konzipiert ist, einen oder mehrere kryptografische Schlüssel sicher zu speichern und/oder zu isolieren. Das Sicherheitssystem kann einen Hypervisor umfassen, um die getrennte Ausführungsumgebung zu erstellen und/oder durchzusetzen. Das Sicherheitssystem wird vorzugsweise durch eine sichere Hardware unterstützt, könnte aber auch in Software erstellt werden. Beispielsweise kann ein Kernel, der auf der Vorrichtung ausgeführt wird, das Sicherheitssystem implementieren. Ein Sicherheitssystem, insbesondere eines mit hardwarebasierter Sicherheit, wird bevorzugt, auch wenn dies nicht notwendig ist; notfalls kann der Sitzungshandler die Speicherung, den Schutz und die Verarbeitung langfristiger Schlüssel handhaben. Auch wenn die letztgenannte keine bevorzugte Anordnung ist, ist diese immer noch besser als eine, in der das Host-System die langfristigen Geheimnisse handhaben müsste.

[0047] Diese Arten von Sicherheitssystemen werden typischerweise handelsüblich als Hardware-Sicherheitsmodul (Hardware Security Module, HSM), vertrauenswürdiges Plattformmodul (Trusted Platform Module, TPM), PKCS#11-basiertes Sicherheitssystem oder als eine andere Art von spezialisierten Krypto-Subsystemen bereitgestellt. Diese Subsysteme machen typischerweise nur APIs für generische Kryptoschemata zugänglich (z. B. APIs für das Erstellen von ECDSA-Signaturen, RSA-basierte Verschlüsselung und Signaturen etc.).

[0048] Die erste Netzvorrichtung 110 und/oder die zweite Netzvorrichtung 160 können dafür ausgelegt sein, mehrere getrennte Ausführungsumgebungen anzuordnen. Beispielsweise kann die Vorrichtung einen Ausführungsumgebungsmechanismus umfassen. Beispielsweise kann die Vorrichtung einen OS-Kernel und/oder einen Hypervisor etc. umfassen, um eine getrennte Ausführungsumgebung zu erstellen und/oder durchzusetzen.

[0049] In hybriden Ausführungsformen sind Funktionseinheiten teilweise in Hardware implementiert, z. B. als Coprozessoren, z. B. kryptografisch Coprozessoren, und teilweise in Software, die auf der Vorrichtung gespeichert und ausgeführt wird.

[0050] Fig. 1c zeigt schematisch eine beispielhafte Ausführungsform des Kommunikationssystems 101. Das Kommunikationssystem 101 kann mehrere zweite Netzvorrichtungen umfassen; gezeigt werden die zweiten Netzvorrichtungen 160.1 und 160.2. Das Kommunikationssystem 100 kann mehrere erste Netzvorrichtungen umfassen; eine erste Netzvorrichtung 110 wird gezeigt. Die Vorrichtungen sind durch ein Computernetz 172, z. B. das Internet, verbunden. Die Client- und die Server-Vorrichtung können gemäß einer Ausführungsform ausgeführt sein.

[0051] Fig. 2 zeigt schematisch eine beispielhafte Ausführungsform einer ersten Netzvorrichtung, die für eine kryptografisch geschützte Kommunikation ausgelegt ist. Die erste Netzvorrichtung 200 ist für eine kryptografisch geschützte Kommunikation 211 mit einer zweiten Netzvorrichtung ausgelegt. Die zweite Netzvorrichtung wird in **Fig.** 2 nicht gezeigt. Die erste und die zweite Netzvorrichtung, und möglicherweise weitere erste und/oder zweite Netzvorrichtungen, können Teil eines Kommunikationssystems für das Austauschen von kryptografisch geschützten Daten sein.

[0052] In einer Ausführungsform ist die erste Netzvorrichtung 200 kompatibel mit bestehenden Standards, sodass die zweite Netzvorrichtung eine her-

kömmliche Netzvorrichtung sein kann. Dies ist nicht notwendig; die zweite Netzvorrichtung kann gemäß einer Ausführungsform ausgeführt sein. Das Letztgenannte ist vorteilhaft, da Daten, die über ein Netzwerk ausgetauscht werden, sicherer sind, falls beide Endpunkte sicherer sind. Das zweite Digitalnetz könnte jedoch auch oder stattdessen eine höhere Sicherheit durch herkömmliche Mittel aufweisen.

[0053] Fig. 2 zeigt eine kryptografisch geschützte Kommunikation 211 mit der zweiten Netzvorrichtung. Die kryptografisch geschützte Kommunikation 211 umfasst wenigstens drei Teile: ein Handshake-Protokoll, ein Protokoll für den kryptografischen Schutz von Massendaten und ein Wiederaufnahmeprotokoll. Das Handshake-Protokoll richtet ephemere Schlüssel für kryptografische Schutzmaßnahmen ein und ordnet ein Mittel an, um die Kommunikation bei Bedarf wiederaufzunehmen, ohne eine vollständige Iteration des Handshake-Protokolls ausführen zu müssen. Das Letztgenannte kommt in einem späteren Wiederaufnahmeprotokoll zum Einsatz. Da das Handshake-Protokoll Zeit benötigt und die Kommunikation verzögert, ist dies vorteilhaft. Ein Entfernen oder Reduzieren des Handshake-Protokolls reduziert Latenzen.

[0054] Beispielsweise können die erste Netzvorrichtung 200 und/oder die zweite Netzvorrichtung eine kryptografische Anwendung ausführen, die eine wechselseitige Kommunikation beinhaltet. Durch Schützen der Kommunikation zwischen der ersten und der zweiten Vorrichtung wird die Sicherheit der Anwendung erhöht.

[0055] Ausführungsformen können auf der Server-Seite nutzbringend eingesetzt werden. Beispielsweise kann es sich, in einer Ausführungsform, bei der ersten Netzvorrichtung 200 um eine Server-Vorrichtung oder eine loT-Backend-Vorrichtung handeln.

[0056] Ausführungsformen können auf der Verbraucherseite nutzbringend eingesetzt werden. Beispielsweise kann es sich, in einer Ausführungsform, bei der ersten Netzvorrichtung 200 um eine Verbrauchervorrichtung oder eine loT-Client handeln.

Sicherheitssystem 230

[0057] Eine erste Netzvorrichtung 200 ist mit einem Sicherheitssystem 230 ausgeführt. Das Sicherheitssystem 230 ist dafür ausgelegt, ein langfristiges Geheimnis zu speichern. Typischerweise umfasst das Sicherheitssystem 230 hardwarebasierte Sicherheit, um das langfristige Geheimnis zu schützen. Das Sicherheitssystem kann dafür ausgelegt sein, das langfristige Geheimnis vom Rest der Netzvorrichtung 200 abzuschirmen. Beispielsweise kann das langfristige Geheimnis den privaten Schlüssel eines asymmetrischen Schlüsselpaares, z. B. eines öffentlich-privaten Schlüsselpaares, umfassen. Beispielsweise kann das langfristige Geheimnis einen privaten RSA-Schlüssel, eine privaten ECDSA-Schlüssel, umfassen. Der öffentliche Schlüssel, welcher dem privaten Schlüssel entspricht, kann mit der zweiten Netzvorrichtung geteilt werden. Beispielsweise kann das langfristige Geheimnis einen symmetrischen Schlüssel umfassen, der, z. B. über einen Außerbandkanal, mit der zweiten Netzvorrichtung geteilt wird.

[0058] Das langfristige Geheimnis ermöglicht das Generieren eines mit einer anderen Vorrichtung geteilten ephemeren Geheimnisses. Der Zugriff auf das langfristige Geheimnis bietet im Allgemeinen die Möglichkeit, die gesamte Kommunikation zu lesen und/oder Authentizitätstoken zu erstellen. Ein Durchsickern des langfristigen Geheimnisses sollte daher vermieden werden.

[0059] Das Sicherheitssystem ist derart ausgelegt, dass der Rest der Vorrichtung 200, außerhalb des Sicherheitssystems 230, keinen direkten Zugriff auf das langfristige Geheimnis hat. Um nach wie vor die Verwendung des langfristigen Geheimnisses zu erlauben, exportiert das Sicherheitssystem 230 eine kryptografische Schnittstelle 231, die es erlaubt, dass einige Operationen mit dem langfristigen Geheimnis durchgeführt werden. Bei dem Sicherheitssystem kann es sich um ein hardwarebasiertes Modul handeln, das ein oder mehrere langfristige Geheimnisse speichert, die nur über eine kryptografische Schnittstelle zugänglich sind. Beispielsweise kann die Schnittstelle 231 eine Operation zum Entschlüsseln von Daten unter Verwendung des langfristigen Geheimnisses umfassen. Beispielsweise kann die Schnittstelle 231 eine Operation zum Berechnen eines Authentifizierungstokens für Daten unter Verwendung des langfristigen Geheimnisses umfassen, z. B. eine Signatur oder einen Nachrichtenauthentifizierungscode. Das Sicherheitssystem kann mehrere langfristige Geheimnisse speichern. Das Sicherheitssystem wird bevorzugt, ist jedoch optional.

[0060] Es wird für eine höhere Sicherheit bevorzugt, dass das Sicherheitssystem hardwarebasiert ist, aber dies ist nicht notwendig. Beispielsweise kann das Sicherheitssystem eine Ausführungsumgebung wie der hier beschriebene Sitzungshandler sein.

Ausführungsumgebungen

[0061] Die erste Netzvorrichtung 200 ist dafür ausgelegt, mehrere getrennte Ausführungsumgebungen in einer ersten Netzvorrichtung 200 anzuordnen. Die mehreren getrennten Ausführungsumgebungen beinhalten ein Host-System 210 und ein Sitzungshandhabungssystem 220.

[0062] Beispielsweise kann, in einer Ausführungsform, bei der (D)TLS verwendet wird, das Host-System als ein (D)TLS-Frontend betrachtet werden. Beispielsweise kann das (D)TLS-Frontend in einer Ausführungsumgebung als Teil des ursprünglichen Anwendungsprozesses unter Verwendung von (D)TLS geladen werden, z. B. durch Importieren einer Bibliothek. Das Host-System, z. B. das (D)TLS-Frontend, handhabt Datensätze des Typs application_data (Anwendungsdaten). Das Sitzungshandhabungssystem kann als ein (D)TLS-Backend betrachtet werden. Beispielsweise können ein oder mehrere Daemons zu diesem Zweck in einem getrennten Prozesskontext ausgeführt werden. Das Frontend und das Backend können nur über dedizierte Kanäle verbunden sein, z. B. über Sitzungs- und Steuerkanäle. Das Sitzungssystem, z. B. das (D)TLS-Backend, handhabt die anderen Subprotokolle von (D)TLS.

[0063] Eine Ausführungsumgebung hat keinen Zugriff auf Daten und/oder Software in einer anderen Ausführungsumgebung in der ersten Netzvorrichtung 200, und auch nicht auf Daten und/oder Software im Sicherheitssystem 230. Insbesondere haben weder die Ausführungsumgebung des Host-Systems 210 noch die Ausführungsumgebung des Sitzungshandhabungssystems 220 Zugriff auf das langfristige Geheimnis, welches im Sicherheitssystem 230 gespeichert ist. Auch wenn zwei Ausführungsumgebungen keinen direkten Lese- oder Schreibzugriff auf den Code der jeweils anderen Umgebung haben, könnten sie mit einer Schnittstelle ausgeführt sein, um Daten zu senden und/oder zu empfangen.

[0064] Der Zugriff auf die Schnittstelle 231 ist typischerweise auf Teile des Systems 200 beschränkt. Beispielsweise kann die Vorrichtung 200 so ausgeführt sein, dass nur der Sitzungshandler 220 Zugriff auf die Schnittstelle 231 hat.

[0065] In einer Ausführungsform führt das Host-System eine kryptografische Anwendung aus, um Daten unter Verwendung des kryptografischen Massenschutzschlüssels kryptografisch zu schützen, wobei die kryptografische Anwendung dafür ausgelegt ist, Daten, die an die zweite Netzvorrichtung gesendet und/oder von der zweiten Netzvorrichtung empfangen werden, mit einem kryptografischen Massenschutzschlüssel zu schützen. Beispielsweise können die kryptografische Operationen von anderen Anwendungsteilen getrennt sein. Beispielsweise führt, in einer Ausführungsform, das Host-System 210 eine kryptografische Anwendung aus, um Daten unter Verwendung eines kryptografischen Massenschutzschlüssels kryptografisch zu schützen, und führt eine Benutzeranwendung aus, wobei die Benutzeranwendung dafür ausgelegt ist, Daten zu verwenden, die von der zweiten Netzvorrichtung empfangen werden, und/oder Daten für die zweite Netzvorrichtung bereitzustellen. Das Senden und Empfangen von Daten durch die Benutzeranwendung kann dann durch die kryptografische Anwendung erfolgen, wobei die besagten Daten, wie hier erörtert, mit einem kryptografischen Massenschutzschlüssel geschützt sind.

[0066] Beispielsweise sind, in einer Ausführungsform, die Ausführungsumgebungen, insbesondere Ausführungsumgebung des Host-Systems und die Ausführungsumgebung des Sitzungshandhabungssystems, durch eine hardwareunterstützte Ausführungstrennung, z. B. einen Hypervisor, z. B. einen Typ-1-Hypervisor, oder irgendeine Variante der vertrauenswürdigen Ausführungsumgebung (Trusted Execution Environment), voneinander getrennt.

[0067] Die Ausführungsumgebung kann unter Verwendung eines beliebigen generischen Trennungsmechanismus durchgesetzt werden. Der Trennungsmechanismus kann eine vertrauenswürdige Datenverarbeitungsbasis (Trusted Computing Base, TCB) verwenden. Die Trennung kann durch die TCB durchgesetzt werden. Die TCB (Trusted Computing Base) beinhaltet z. B. die TCB eines OS-Kernels, z. B. eines Linux- oder BSD-Kernels, die Prozesse verwaltet und trennt, die TCB eines Hypervisors, die virtuelle Maschinen (Virtual Machines, VMs) trennt, oder die TCB einer vertrauenswürdigen Ausführungsumgebung (Trusted Execution Environment, TEE) (z. B. eine ARM TrustZone's Secure World), welche die nicht-sichere Welt von der sicheren Welt trennt. Diese TCBs bieten unterschiedliche Kompromisse hinsichtlich Trennungsstärke, HW-Ressourcenanforderungen, Latenz/Durchsatz etc. Diese TCBs können gestapelt sein.

[0068] Wie hier weiter erörtert, können unterschiedliche Ausführungsumgebungen verwendet werden, um unterschiedliche kryptografische Anwendungen zu unterstützen.

[0069] Insbesondere kann das Host-System verwendet werden, um Massenoperationen, z. B. den kryptografischen Schutz von Massendaten, zu unterstützen. Beispielsweise kann der kryptografische Schutz einen Vertraulichkeitsschutz umfassen, z. B. die Verschlüsselung und/oder Entschlüsselung von Daten. Beispielsweise kann der kryptografische Schutz einen Integritätsschutz umfassen, z. B. die Generierung und/oder Verifizierung von Authentizitätstoken.

[0070] Der Sitzungshandler kann verwendet werden, um Operationen zu unterstützen, die sich nicht auf den Schutz von Massendaten beziehen. Beispielsweise kann der Sitzungshandler Operationen unterstützen, die die Verwendung der Schnittstelle 231 zum Sicherheitssystem umfassen.

[0071] Beispielsweise ist, in einer Ausführungsform, die erste Netzvorrichtung 200 gemäß TLS ausgeführt, z. B. gemäß RFC 8446 (hier durch Verweis aufgenommen), wobei

- das Host-System 210 dafür ausgelegt ist, Datensätze des Protokolltyps application_data (Anwendungsdaten) zu verarbeiten, nicht jedoch Operationen eines anderen Typs, z. B. handshake (Handshake), alert (Alarm) und change_cipher_spec type (Chiffrenspezifikation ändern), und

- das Sitzungshandhabungssystem 220 dafür ausgelegt ist, Operationen der anderen Typen auszuführen.

Handshake-Protokoll

[0072] Das Handshake-Protokoll wird durch den Sitzungshandler gehandhabt. Während des Handshake-Protokolls ist das Sitzungshandhabungssystem 220 dafür ausgelegt, vom Sicherheitssystem 230 eine kryptografische Antwort in Abhängigkeit von dem langfristigen Geheimnis zu erhalten. Beispielsweise kann die Schnittstelle 231 mit einer Anforderung für eine spezifische Antwort in Abhängigkeit von dem langfristigen Geheimnis aufgerufen werden. Bei der Antwort kann es sich z. B. um eine Entschlüsselung, eine Signatur, die Generierung oder Verifizierung eines Nachrichtenauthentifizierungscodes handeln. Beispielsweise kann die Antwort eine Signatur umfassen, die über einen Nonce-Wert etc. berechnet wird.

[0073] Die kryptografische Antwort wird als Teil des Handshake-Protokolls an die zweite Netzvorrichtung gesendet, um eine sichere Sitzung zwischen der ersten Netzvorrichtung 200 und der zweiten Netzvorrichtung einzurichten. Das Sitzungshandhabungssystem 220 erhält von dem Handshake-Protokoll einen ersten kryptografischen Massenschutzschlüssel und einen Wiederaufnahmeschlüssel. De erste kryptografische Massenschutzschlüssel wird an das Host-System 210 weitergeleitet. Der Wiederaufnahmeschlüssel wird nicht an das Host-System 210 weitergeleitet.

[0074] Beispielsweise kann das Sitzungshandhabungssystem einen Schlüsselblock (key_block) erhalten, der einen oder mehrere kryptografische Schlüssel enthalten kann. Beispielsweise kann key_block unterschiedliche Schlüssel für die Client- und die Server-Seite und für Verschlüsselungs-/Authentifizierungszwecke umfassen, wobei die Schlüssel von den verwendeten Chiffrensammlungen abhängen können. Ein typisches Beispiel eines Schlüssels für den Massenschutz ist ein ephemerer Sitzungsschlüssel. Wie hier erörtert, kann sich der Massenschutz auf die Verschlüsselung von Daten, die von der ersten Netzvorrichtung gesendet werden, auf die Entschlüsselung von Daten, die an der ersten Netzvorrichtung empfangen werden, auf die Generierung und Verifizierung von Authentifizierungstoken etc. beziehen.

[0075] Hier zwei Beispiele für das Einrichten eines Schlüssels für den Massenschutz, z. B. von ephemerem Sitzungsschlüsselmaterial: 1) authentifizierte Schlüsselvereinbarung, z. B. basierend auf (EC) DHE und 2) Schlüsseltransport, z. B. von älteren RSA-Chiffrensammlungen in TLS <=1.2. Für Beispiele siehe RFC 8446 Abschnitt 4 (TLS 1.3) und die Abschnitte 7 u. 8 in RFC 5246 (TLS 1.2), die hier durch Verweis aufgenommen sind.

[0076] Der Wiederaufnahmeschlüssel bezieht sich im Allgemeinen auf das gesamte andere ephemere Schlüsselmaterial, das gegebenenfalls verwendet wird, um die kryptografische Kommunikation zwischen der ersten und der zweiten Netzvorrichtung ohne Einbeziehung des langfristigen Geheimnisses wiederaufzunehmen, z. B. ohne ein vollständiges Handshake-Protokoll auszuführen. Beispielsweise kann der Wiederaufnahmeschlüssel ein TLS- oder DTLS-Premaster-Geheimnis, ein Master-Geheimnis, einen Wiederaufnahme-PSK, einen Sitzungsticket-Verschlüsselungsschlüssel (Session Ticket Encryption Key, STEK) und so weiter umfassen.

[0077] Das Sitzungshandhabungssystem 220 kann dafür ausgelegt sein, von dem Handshake-Protokoll ein Master-Geheimnis zu erhalten, das mit der zweiten Netzvorrichtung geteilt wird. Das Master-Geheimnis kann verwendet werden, um einen ersten kryptografischen Massenschutzschlüssel und einen Wiederaufnahmeschlüssel abzuleiten. Insbesondere kann das Master-Geheimnis selbst von einem Premaster-Geheimnis abgeleitet sein, das zwischen der ersten und der zweiten Netzvorrichtung geteilt, z. B. ausgehandelt, wird. Das Premaster-Geheimnis sollte ebenfalls geschützt werden. In TLS <=1.2 kann das Master-Geheimnis als Wiederaufnahmeschlüssel verwendet werden. In TLS 1.3 ist der Wiederaufnahmeschlüssel ein abgeleiteter Schlüssel, der als vorab vereinbarter Schlüssel (Pre-Shared Key, PSK) bezeichnet wird.

[0078] Es sei darauf hingewiesen, dass die Ausführungsumgebung des Host-Systems 210 keinen Zugriff auf den Wiederaufnahmeschlüssel hat. Falls beispielsweise ein Master-Schlüssel und/oder ein Premaster-Schlüssel verwendet werden, dann hat die Ausführungsumgebung des Host-Systems 210 keinen Zugriff auf das Master-Geheimnis oder das Premaster-Geheimnis. Beispielsweise hat die Ausführungsumgebung des Host-Systems 210 unter Umständen nur Zugriff auf das ephemere Schlüsselmaterial im Rahmen des Schutzes von Massendaten, wie etwa einen Schlüsselblock (key_block) oder Verkehrsschlüssel.

[0079] Der kryptografische Massenschutzschlüssel und der Wiederaufnahmeschlüssel sind typischerweise kurzfristige Schlüssel. Beispielsweise können diese ein Gültigkeitsdatum aufweisen, z. B. eine Gültigkeit von höchstens einer Woche, einem Tag oder dergleichen. Das Handshake-Protokoll kann das Authentifizieren der zweiten Netzvorrichtung durch den Sitzungshandler beinhalten.

Protokoll für den kryptografischen Schutz von Massendaten

[0080] Das Host-System 210 ist dafür ausgelegt, Massendaten, die an der zweiten Netzvorrichtung empfangen werden oder an die zweite Netzvorrichtung gesendet werden, kryptografisch zu schützen.

[0081] Kryptografischer Schutz kann Vertraulichkeitsschutz sein. Beispielsweise können empfangene Daten unter Verwendung eines Massenschutzschlüssels, z. B. eines symmetrischen Entschlüsselungsschlüssels, entschlüsselt werden. Beispielsweise können gesendete Daten unter Verwendung eines Massenschutzschlüssels, z. B. eines symmetrischen Verschlüsselungsschlüssels, verschlüsselt werden.

[0082] Kryptografischer Schutz kann Integritätsschutz sein. Beispielsweise können empfangene Daten unter Verwendung eines Massenschutzschlüssels verifiziert werden, z. B. mit einem symmetrischen Verifizierungsschlüssel; beispielsweise kann ein mit den empfangenen Daten verknüpftes Authentifizierungstoken, empfangen z. B. als Teil oder in Verbindung mit den empfangenen Daten, mit dem Massenschutzschlüssel verifiziert werden. Beispielsweise können gesendete Daten mit einem Authentifizierungstoken bereitgestellt werden, generiert mit dem Massenschutzschlüssel. Nicht alle der vorgenannten vier Funktionen müssen vorhanden sein, es können z. B. nur eine oder zwei oder einige etc. sein. Beispielsweise wird, in einer Ausführungsform, der Vertraulichkeitsschutz nicht verwendet, aber die Authentifizierung wird verwendet. Beispielsweise wird, in einer Ausführungsform, der Integritätsschutz nicht verwendet, aber der Vertraulichkeitsschutz wird verwendet. Die vorstehenden vier Funktionen können jeweils einen unterschiedlichen Schlüssel verwenden, oder einige oder alle können denselben Schlüssel verwenden. Aus Leistungsgründen wird ein symmetrischer Schlüssel für jede dieser Funktionen bevorzugt, aber jede dieser Funktionen kann auch mit einem asymmetrischen Schlüssel erfolgen. Beispielsweise durch asymmetrische Verschlüsselung/Entschlüsselung, Signaturgenerierung/-verifizierung etc.

[0083] Beispielsweise kann, auf der Empfangsseite, ein kryptografischer Schutz von Massendaten die Entschlüsselung von Daten und die Verifizierung eines Authentifizierungstokens beinhalten. Beispielsweise kann der Schutz eine authentifizierte Verschlüsselung (Authenticated Encryption, AE) und eine authentifizierte Verschlüsselung mit zugehörigen Daten (Authenticated Encryption with Associated Data, AEAD) umfassen, z. B. Verschlüsselungsformen, die gleichzeitig die Vertraulichkeit und die Authentizität von Daten sicherstellen. Beispielsweise kann eine Ausführungsform eine Chiffrensammlung implementieren, wie etwa TLS <=1.2, die einen reinen Authentifizierungsmodus unterstützt.

[0084] Andere kryptografische Schutzmaßnahmen können wie gewünscht integriert werden. Beispielsweise kann ein Wiedergabeschutz hinzugefügt werden, wodurch z. B. die Aktualität von gesendeten und/oder empfangenen Antworten sichergestellt wird. In einer Ausführungsform wird der Massenschutz ausschließlich in der Ausführungsumgebung des Host-Systems 210 durchgeführt.

Wiederaufnahmeprotokoll

[0085] Das Sitzungshandhabungssystem 220 ist dafür ausgelegt, während des Wiederaufnahmeprotokolls eine kryptografische Antwort von dem Wiederaufnahmeschlüssel zu erhalten. Die kryptografische Antwort wird als Teil des Wiederaufnahmeprotokolls an die zweite Netzvorrichtung gesendet, um eine sichere Sitzung zwischen der ersten Netzvorrichtung 200 und der zweiten Netzvorrichtung wiederherzustellen. Das Sitzungshandhabungssystem 220 erhält von dem Wiederaufnahmeprotokoll einen zweiten kryptografischen Massenschutzschlüssel. Der zweite kryptografische Massenschutzschlüssel wird zur Verwendung beim Schutz von Massendaten an das Host-System 210 weitergeleitet. Typischerweise handelt es sich bei dem ersten und dem zweiten Massenschutzschlüssel um symmetrische Schlüssel, auch wenn dies nicht notwendig ist.

[0086] Während des Wiederaufnahmeprotokolls kann der Wiederaufnahmeschlüssel verarbeitet werden, z. B. um einen weiteren Schlüssel zu erhalten. Beispielsweise kann ein Premaster-Geheimnis oder ein Master-Geheimnis während des Wiederaufnahmeprotokolls verarbeitet werden, um einen weiteren Schlüssel zu erhalten, welcher dann verwendet werden kann, um eine kryptografische Operation durchzuführen. Ein Teil der Verarbeitung im Wiederaufnahmeprotokoll kann vorausberechnet werden.

[0087] In einer Ausführungsform erhält das Sitzungshandhabungssystem 220 von dem Wiederaufnahmeprotokoll einen neuen Schlüsselblock (key_block) oder neue Verkehrsschlüssel, die mehrere Schlüssel umfassen. Die Schlüssel aktualisieren die bestehenden Schlüssel. Beispielsweise kann der erste Massenschutzschlüssel Teil eines ersten Mehr-

fachen von Schutzschlüsseln sein. Das Wiederaufnahmeprotokoll kann ein zweites Mehrfaches von Schutzschlüsseln bereitstellen.

[0088] Der zweite Massenschutzschlüssel kann vom Host-System zum Massenschutz verwendet werden, z. B. als erster Massenschutzschlüssel, z. B. zum Vertraulichkeits- oder Integritätsschutz.

Kommunikation

[0089] In einer Ausführungsform ist die Protokollkommunikation zwischen dem Host-System und dem Sitzungshandler aufgeteilt. In einer Ausführungsform ist das Sicherheitssystem nicht dafür ausgelegt, auf Protokollnachrichten zu antworten oder diese zu generieren. Falls eine Antwort vom Sicherheitssystem benötigt wird, kann der Sitzungshandler die Schnittstelle zum Sicherheitssystem aufrufen.

[0090] Das Host-System und der Sitzungshandler können auf verschiedene Art und Weise zusammenarbeiten. In einer Ausführungsform sind das Host-System 210 und das Sitzungshandhabungssystem 220 beispielsweise mit einem ersten Kommunikationskanal 221 ausgeführt.

[0091] Beispielsweise können das Host-System 210 und das Sitzungshandhabungssystem 220 mit einem Steuerungsmechanismus ausgeführt sein, um die Steuerung der kryptografisch geschützten sicheren Kommunikation 211 anzuzeigen. Der Steuerungsmechanismus zeigt die Steuerung für das Host-System 210 während des Massenschutzes an. Der Steuerungsmechanismus ändert die Steuerung vom Host-System 210 zum Sitzungshandhabungssystem 220 für das Handshake-Protokoll und für das Wiederaufnahmeprotokoll.

[0092] Aufgrund des Steuerungsmechanismus ist es für das Host-System 210 und den Sitzungshandler 220 klar, wer von beiden für die Kommunikation zuständig ist. Der Steuerungsmechanismus kann einen zweiten Kommunikationskanal umfassen, um einen Zustand der kryptografisch geschützten sicheren Kommunikation 211 zwischen dem Host-System 210 und dem Sitzungshandhabungssystem 220 zu übergeben. Falls beispielsweise das Host-System Nachrichten generieren muss, die es nicht generieren kann, weil es keinen Zugriff auf die erforderlichen Schlüssel hierfür hat, kann das System eine Nachricht über den zweiten Kommunikationskanal 222 senden, um die Steuerung zu übergeben. Die Übergabe kann einen beliebigen Zustand beinhalten, der benötigt wird, um neue Nachrichten zu generieren.

[0093] Beispielsweise kann die Kommunikation zwischen der ersten Netzvorrichtung 200 und der zweiten Netzvorrichtung im Host-System 210 ankommen und wird über einen ersten Kommunikationskanal 221 während des Handshake-Protokolls und während des Wiederaufnahmeprotokolls an das Sitzungshandhabungssystem 220 übergeben.

[0094] Falls beispielsweise Nachrichten ankommen, während die Steuerung beim Sitzungshandler liegt, kann die Kommunikation weitergeleitet werden.

[0095] Das Host-System kann auch oder stattdessen dafür ausgelegt sein, eine empfangene Kommunikation an den Sitzungshandler weiterzuleiten, je nachdem, welcher Kommunikationstyp mit der empfangenen Kommunikation verknüpft ist, z. B. darin eingebettet ist.

[0096] In einer Ausführungsform kann die empfangene Kommunikation verschlüsselt sein, auch wenn es sich nicht um Massendaten handelt. Insbesondere kann jede Angabe zur Art der Kommunikation verschlüsselt sein, z. B. kann der Kommunikationstyp verschlüsselt sein. In einer Ausführungsform ist das Host-System dafür ausgelegt, je nach Kommunikationstyp, wenigstens den Kommunikationstyp zu entschlüsseln, bevor die Kommunikation an den Sitzungshandler weitergeleitet wird. Beispielsweise ist, in einer Ausführungsform, das Host-System dafür ausgelegt, die gesamte eingehende Kommunikation zu entschlüsseln und weiterzuleiten, falls die Kommunikation einer weiteren Behandlung durch den Sitzungshandler bedarf.

[0097] Beispielsweise verwenden Ausführungsformen, die DTLS verwenden, ein Inhaltstyp-Feld (ContentType), das den Datensatztyp angibt. Das Feld ContentType kann verwendet werden, um zu entscheiden, ob ein DTLS-Datensatz durch das Host-System oder durch das Sitzungshandhabungssystem gehandhabt wird. Dies entspricht dem verwendeten Subprotokoll von TLS (z. B.: application_data (Anwendungsdaten), handshake (Handshake), alert (Alarm), change_cipher_spec (Chiffrenspezifikation ändern) etc.) Das Host-System kann dafür ausgelegt sein, alle Datensätze, bei denen es sich nicht um Anwendungsdaten (application_data) handelt, an das Sitzungshandhabungssystem durchzuleiten. Dies kann um eine Verschlüsselung des Feldes ContentType erweitert werden, z. B. im Rahmen des Merkmals Record Payload Protection (Schutz der Datensatznutzlast). Falls eine Verschlüsselung gemäß ContentType-Feld verwendet wird, kann das Host-System dafür ausgelegt sein, dieses Feld zu entschlüsseln, bevor der Datensatz selbst verarbeitet oder an den Sitzungshandler weitergeleitet wird.

[0098] Anstatt das Host-System alle TLS (oder DTLS-)Datensätze, bei denen es sich nicht um Anwendungsdaten (application_data) handelt, einfach (z. B. unmodifiziert) an das Sitzungshandhabungssystem weiterleiten zu lassen, ist es als Variante möglich, dem Host-System die Entschlüss-

elung/Authentifizierungsprüfung für alle Arten von geschützten Datensätzen - nicht nur für Datensätze des Typs application_data (Anwendungsdaten), sondern auch für andere Arten von TLS-Datensätzen - nach dem anfänglichen Handshake immer zu überlassen. Dies ist möglich, da das Host-System und das Sitzungshandhabungssystem ihre Zuständigkeiten wie gewünscht aufteilen können, z. B. unter Verwendung des Kommunikationskanals 222.

[0099] Nachstehend werden einige weitere optionale Verfeinerungen, Einzelheiten und Ausführungsformen veranschaulicht.

Beispielhafte Ausführungsform 1

[0100] Im Folgenden wird ein Überblick über den Aufbau und dessen Funktionsweise gegeben. Die Vorrichtung umfasst ein TLS/DTLS-Sitzungshandhabungssystem (Session Handling System). Es sei darauf hingewiesen, dass das beschriebene Verfahren unabhängig davon angewendet werden kann, ob das Host-System als Client oder als Server fungiert. Für jede aktive TLS/DTLS-Sitzung mit einem externen TLS/DTLS-Endpunkt können zwei logische Kommunikationskanäle zwischen dem Host-System und dem TLS/DTLS-Sitzungshandhabungssystem eingerichtet werden. Der Sitzungskanal kann verwendet werden, um alle TLS/DTLS-Protokoll-Datensatztypen immer dann transparent weiterzuleiten, wenn das TLS/DTLS-Sitzungshandhabungssystem die aktive Kontrolle hat. Der Steuerkanal kann verwendet werden, um Zustand und Steuerung zwischen dem Host-System und dem TLS/DTLS-Sitzungshandhabungssystem zu übergeben (z. B. kann zu jedem Zeitpunkt und in Abhängigkeit vom aktuell verarbeiteten Subprotokoll nur eines dieser Systeme der aktive TLS/DTLS-Protokollendpunkt sein). Während eines vollständigen Handshakes interagiert das TLS/DTLS-Sitzungshandhabungssystem mit dem Sicherheitssystem im Rahmen der Endpunkt-Authentifizierung (Endpoint Authentication).

[0101] Beispielsweise kann das Host-System für eine TCP/IP-basierte Anbindung mit externen TLS/DTLS-Endpunkten ausgelegt sein. Das Host-System ist für einen Massenschutz, insbesondere eine Massenverschlüsselung (z. B. die Handhabung des Datensatztyps application_data (Anwendungsdaten)) ausgelegt. Das Host-System hat Zugriff auf symmetrische Schlüssel zur Verschlüsselung und Authentifizierung (key_block), nicht jedoch auf anderes ephemeres Schlüsselmaterial. Der Sitzungskanal (Session) ist dafür ausgelegt, alle anderen Datensatzprotokolltypen transparent an das TLS/DTLS-Sitzungshandhabungssystem weiterzuleiten.

[0102] Das Sitzungshandhabungssystem ist dafür ausgelegt, Handshake und TLS/DTLS-Sitzungszustand und das gesamte ephemere Schlüsselmaterial, z. B. Datensätze des Typs handshake (Handshake), alert (Alarm) und change_cipher_spec (Chiffrenspezifikation ändern), zu verwalten. Das Sitzungshandhabungssystem interagiert mit dem Sicherheitssystem im Rahmen der Endpunkt-Authentifizierung während eines vollständigen Handshakes.

[0103] Schritt 1. Eine neue TCP/IP-Verbindung für TLS (oder DTLS im Fall von UDP) wird zwischen einem externen TLS/DTLS-Endpunkt und dem Host-System initiiert. Um das TLS/DTLS-Handshake zu initiieren, stellt das Host-System einen vorinitialisierten TLS/DTLS-Zustand bereit (z. B. um zu signalisieren, ob TLS oder DTLS angefordert wird) und übergibt dann die Steuerung an das TLS/DTLS-Sitzungshandhabungssystem. Nach Aufgabe der aktiven Kontrolle leitet das Host-System dann alle weiteren Datensätze transparent zwischen dem TLS/DTLS-Sitzungshandhabungssystem und dem externen TLS/DTLS-Endpunkt weiter.

[0104] Schritt 2. In Rahmen der Endpunkt-Authentifizierung während eines anfänglichen vollständigen Handshakes interagiert das TLS/DTLS-Sitzungshandhabungssystem mit dem Sicherheitssystem (z. B. um die ECDSA-Signatur zu erhalten, die für eine Endpunkt-Authentifizierung über langfristige Schlüssel erforderlich ist). Bei serverseitigen TLS/DTLS-Endpunkten ist, für den Fall, dass ein abgekürztes Wiederaufnahme-Handshake angefordert wird und akzeptabel ist, eine Beteiligung des Sicherheitssystems nicht erforderlich. Das Handshake zwischen dem TLS/DTLS-Sitzungshandhabungssystem und dem externen TLS/DTLS-Endpunkt richtet alle erforderlichen Zustandsinformationen und ephemeres Schlüsselmaterial ein (z. B. Schlüsselmaterial zur Wiederaufnahme, Schlüsselblock (key_block) zur Massenverschlüsselung, ein STEK zum Verschlüsseln von Sitzungstickets für den Fall, dass dieser Wiederaufnahmemechanismus an einem serverseitigen Endpunkt verwendet wird, etc.).

[0105] Schritt 3. Nach Abschluss des Handshakes stellt das TLS/DTLS-Sitzungshandhabungssystem alle erforderlichen Zustandsinformationen für die Handhabung von Datensätzen des Typs application_data (Anwendungsdaten) (z.B. key_block (Schlüsselblock), nicht jedoch anderes ephemeres Schlüsselmaterial) für das Host-System über den Steuerkanal bereit und übergibt die Steuerung. Das Host-System übernimmt die Steuerung, bis ein Subprotokoll abweichend vom Datensatztyp application_data (Anwendungsdaten) vorgefunden wird, welches dann einen weiteren Transfer von Zustand und Steuerung an das TLS/DTLS-Sitzungshandhabungssystem auslösen würde. Das TLS/DTLS-Sitzungshandhabungssystem wäre dann der aktive TLS/DTLS-Endpunkt, bis das entspre-

chende Subprotokollereignis (z. B. Umschlüsselung, Neuaushandlung, Wiederaufnahme, Beendigung etc.) abgeschlossen worden ist.

[0106] Schritt 4. Das Host-System übernimmt wieder als aktiver TLS/DTLS-Endpunkt, um eine Massenverschlüsselung (z. B. Datensätze des Typs application_data (Anwendungsdaten) zu verarbeiten. Eine aktive Beteiligung des TLS/DTLS-Sitzungshandhabungssystem ist nicht erforderlich, bis ein anderer Datensatztyp als application_data vorgefunden wird.

Beispielhafte Ausführungsform 2

[0107] In dieser beispielhaften Ausführungsform ist die erste Netzvorrichtung mit einem Trennungsmechanismus ausgestattet, z. B. einer vertrauenswürdige Datenverarbeitungsbasis (Trusted Computing Base, TCB), z. B. einem Hypervisor und einem Sicherheitssystem. Das Sicherheitssystem ist vorzugsweise dafür ausgelegt, eine hardwarebasierte Abschirmung eines langfristigen Geheimnisses bereitzustellen, auch wenn dies nicht notwendig ist. Es wird davon ausgegangen, dass das Sicherheitssystem ein hardwarebasiertes Modul ist, das ein langfristiges Geheimnis oder mehrere langfristige Geheimnisse speichert, auf die nur über eine kryptografische Schnittstelle zugegriffen werden kann. Es sei darauf hingewiesen, dass das Hardwaremodul nicht für das Sicherheitssystem benötigt wird.

[0108] Ohne hardwarebasierten Schutz bietet der Aufbau unter Umständen keinen Schutz vor lokalen, physischen Angriffen auf die Vorrichtung. Dies gilt insbesondere, da das langfristige private Schlüsselmaterial dann nicht durch irgendein Hardwaremittel geschützt wäre, wenn die Vorrichtung ausgeschaltet ist. Allerdings bietet das Trennen des langfristigen Geheimnisses vom Host-System nach wie vor Vorteile in Fällen, in denen nur vom Netzwerk ausgehende Angriffe als relevant angesehen werden.

[0109] Es wird angenommen, dass die Ausführungsform eine TCP/IP-basierte Anbindung und TLS aufweist. Eine Ausführungsvariante kann stattdessen UDP und DTLS verwenden. Noch eine weitere Variante verwendet QUIC von RFC9000. QUIC basiert ebenfalls auf UDP.

[0110] Mehrere Ausführungsumgebungen werden erstellt, z. B. unter Verwendung des Trennungsmechanismus wie etwa einem Hypervisor. Eine erste Ausführungsumgebung wird als „Host-Ausführungsumgebung“ bezeichnet. Sie führt ein Softwarepaket aus, das als „Host-System“ bezeichnet wird. Die erste Ausführungsumgebung kann auch eine Anwendung ausführen, z. B. eine Benutzeranwendung. Eine zweite Ausführungsumgebung wird als „Sitzungshandhabung-Ausführungsumgebung“ bezeichnet. Sie führt ein Softwarepaket aus, das als „Sitzungshandhabungssystem“ bezeichnet wird.

[0111] Beispielsweise kann eine Benutzeranwendung eine TLS-Bibliothek in der Host-Ausführungsumgebung verwenden, was im Wesentlichen bedeutet, dass der Bibliothekscode hinsichtlich TLS in demselben Prozesskontext ausgeführt wird, nur das Subprotokoll application_data (Anwendungsdaten) wird dort gehandhabt.

[0112] Im einfachsten Fall, z. B. bei Trennung von Prozessen nur durch OS-Kernel oder dergleichen, kann das Sitzungshandhabungssystem lediglich ein anderer Prozess sein, getrennt durch die TCB des OS-Kernels, die dann für die Aufgabe der TLS-Sitzungshandhabung, z. B. die Handhabung der Subprotokolle handshake (Handshake), alert (Alarm) und change_cipher_spec (Chiffrenspezifikation ändern), und die Interaktion mit dem Sicherheitssystem dediziert ist. In einer optionalen Variante, die zusätzlich eine stärkere Trennung von einem Hypervisor verwendet, wären das Host-System und das Sitzungshandhabungssystem getrennte Umgebungen, die sich in unterschiedlichen, durch einen Hypervisor getrennten VMs befinden. Als noch eine andere Alternative könnte das Sitzungshandhabungssystem potenziell auch als eine Art von Bare-Metal-Anwendung implementiert werden, z. B. ein Unikernel, das den POSIX-OS-Kernel etc. auslässt. Ein anderes alternatives Einsatzszenario würde das Sitzungshandhabungssystem in eine vertrauenswürdige Ausführungsumgebung (Trusted Execution Environment, TEE) verlagern.

[0113] Ein oder mehrere Kommunikationskanäle werden zwischen dem Host-System und dem aufgerufenen Sitzungshandhabungssystem erstellt. In einer Ausführungsform gibt es wenigstens zwei Kommunikationskanäle: den Sitzungskanal und den Steuerkanal

[0114] In einer Ausführungsform werden nur ein Sitzungskanal und ein Steuerkanal verwendet. Selbst in diesem Fall können mehrere TLS-Sitzungen unterstützt werden, z. B. durch Multiplexen des oder der Kommunikationskanäle. In einer Ausführungsform werden mehrere Kommunikationskanäle erstellt, was die Handhabung mehrerer TLS-Sitzungen vereinfacht.

[0115] In einer Ausführungsform würde jede Anwendung, die TLS verwendet, typischerweise einem dedizierten „Host-System“ entsprechen und würde typischerweise als ein dedizierter Anwendungsprozess ausgeführt - z. B. kann die Vorrichtung mehrere Host-Systeme im Sinne von mehreren TLS-fähigen Prozessen/Anwendungen aufweisen. Jedes der Host-Systeme kann eine eigene Ausführungsumgebung aufweisen. Jedes Host-System könnte dann

über einen oder mehrere Sitzungs- und Steuerkanäle mit einem einzelnen, geteilten Sitzungshandhabungssystem verbunden werden. Alternativ können mehrere, dedizierte Sitzungshandhabungssysteme konfiguriert werden, z. B. eines für jedes Host-System.

[0116] Mehrere TLS-Sitzungen, die von derselben Anwendung (z. B. in derselben Host-Systemumgebung) gehandhabt werden, könnten über ein einzelnes Paar aus Sitzungs- und Steuerkanal gehandhabt werden (z. B. durch Multiplexing oder, alternativ, durch Einrichten von dedizierten Sitzungs- und Steuerkanälen für jede TLS-Sitzung).

Anfängliches Handshake - Nichtwiederaufnahmefall

[0117] Anwendung: Die Benutzeranwendung signalisiert dem Host-System über eine API, dass sie, unter Verwendung von TLS, einen kryptografisch geschützten sicheren Ende-zu-Ende-Tunnel (eine kurzfristige sichere Sitzung) mit einer zweiten Netzvorrichtung initiieren möchte. Anstatt dass die Anwendung die sichere Sitzung initiiert, kann die sichere Sitzung durch die zweite Netzvorrichtung initiiert werden.

[0118] Typischerweise gehören die Benutzeranwendung und das Host-System effektiv zu demselben Prozess, z. B. würde der TLS-Handhabungsteil typischerweise durch eine geladene TLS-Bibliothek erfolgen.

[0119] Host-System:

a. Übergibt die Steuerung über den Steuerkanal. Das Host-System kann zuerst eine Handshake-Nachricht vorinitialisieren und diese über den Steuerkanal an das Sitzungshandhabungssystem weiterleiten, z. B. in Verbindung mit Übergabe der Steuerung.

b. Während die Steuerung beim Sitzungshandhabungssystem liegt, leitet das Host-System alle Nachrichten vom Sitzungshandhabungssystem transparent an die zweite Netzvorrichtung weiter, und umgekehrt.

[0120] Beispielsweise kann die Vorinitialisierung am Host-System wenigstens in einigen Fällen verwendet werden. Wenn die Anwendung beispielsweise als Client fungiert, kann das Host-System an das Sitzungshandhabungssystem signalisieren, falls eine TLS- oder eine DTLS-Sitzung initiiert werden soll, welche SNI initialisiert werden soll, gegebenenfalls auch, welche TLS-Protokollversionen, Chiffrensammlungen etc. Solche Parameter der Kommunikation können in strukturierter Weise über den Steuerkanal statt über den Sitzungskanal übertragen werden. Beide Optionen sind möglich.

[0121] Sitzungshandhabungssystem:

c. Beendet das Handshake-Protokoll, was beinhaltet:

i. Weiteres Ausfüllen der vorinitialisierten Handshake-Nachricht (sofern verwendet)

ii. Interagieren mit dem Sicherheitssystem (z. B. um eine Signatur zu erhalten, die für eine Endpunkt-Authentifizierung über langfristige Schlüssel erforderlich ist).

iii. Erhalten von dem Handshake-Protokoll:

1. Zustand

2. Ephemeres Schlüsselmaterial zur Massenverschlüsselung: key_block (Schlüsselblock)

a. Ein Beispiel für einen key_block findet sich in TLS 1.2 RFC 5246. Ein Beispiel für einen key_block sind die Verkehrsschlüssel in TLS 1.3 RFC 8446.

3. Ephemeres Schlüsselmaterial zur Wiederaufnahme.

d. Überträgt die Steuerung über den Steuerkanal an das Host-System und leitet den key_block über den Steuerkanal an das Host-System weiter.

[0122] Im Allgemeinen handelt es sich bei ephemerem Schlüsselmaterial um Schlüsselmaterial mit einer begrenzten Lebensdauer (z. B. kurzfristige Schlüssel im Gegensatz zu langfristigen Schlüsseln). Beim anfänglichen Handshake unter Verwendung der langfristigen Schlüssel, beinhaltend z. B. DHE oder ECDHE etc., kann ein sogenanntes Premaster-Geheimnis erstellt werden. Das Premaster-Geheimnis wird im Sitzungshandhabungssystem geschützt aufbewahrt, da es kryptografisch mit öffentlich sichtbaren Informationen von dem früheren Handshake kombiniert werden kann, um das Master-Geheimnis zu berechnen. Folglich wird das Master-Geheimnis vom Premaster-Geheimnis abgeleitet und kann auf diese Weise für Wiederaufnahmezwecke in TLS <=1.2 verwendet werden. In TLS 1.3 wird dieser Wiederaufnahmeschlüssel als vorab vereinbarter Schlüssel (Pre-Shared Key, PSK) bezeichnet, und die Protokollspezifikationen sind ebenfalls unterschiedlich.

[0123] Es sei darauf hingewiesen, dass der Schlüsselblock key_block (in TLS 1.3 / RFC8446 Verkehrsschlüssel genannt) vorzugsweise die einzige Art von ephemerem Schlüsselmaterial ist, welches das Sitzungshandhabungssystem mit dem Host-System teilt. Ephemeres Schlüsselmaterial zur Wiederaufnahme kann z. B. das Master-Geheimnis, das Premaster-Geheimnis beinhalten.

[0124] Der Sitzungsticket-Verschlüsselungsschlüssel (Session Ticket Encryption Key, STEK) ist ein

anderes Beispiel für ephemeres Schlüsselmaterial, das im Rahmen einer auf Sitzungstickets basierenden Wiederaufnahme verwendet wird und das nur im Sitzungshandhabungssystem aufbewahrt werden sollte und nicht dem Host-System zur Verfügung gestellt werden sollte. Ein STEK wird in dem Sitzungsticket-Mechanismus (RFC5077) verwendet. Der STEK ist ein Schlüssel mit einer begrenzten Lebensdauer von z. B. 1 Stunde. Er wird verwendet, um Sitzungstickets zu verschlüsseln, die dann an die Clients gesendet werden, um diesen zu ermöglichen, Sitzungen wiederaufzunehmen.

Massenschutz

[0125] Host-System: Empfangen einer TLS-Nachricht des Typs application_data (Anwendungsdaten) mit verschlüsselten Daten. Durchführen einer Massenentschlüsselung unter Verwendung des Schlüsselblocks (key_block), der vom Sitzungshandler empfangen wird. Senden von entschlüsselten Daten an eine Anwendung

e. Ein Beispiel für application_data (Anwendungsdaten) findet sich in TLS 1.2 RFC5246 und TLS 1.3 RFC8446

[0126] Host-System: Empfangen von unverschlüsselten Daten von einer Anwendung. Durchführen einer Massenverschlüsselung unter Verwendung des Schlüsselblocks (key_block) in der sicheren Sitzung. Senden von verschlüsselten Daten in der Anwendungsdatennachricht (application_data) an eine zweite Netzvorrichtung.

[0127] Dieses Beispiel betrachtet Verschlüsselung als Beispiel für einen kryptografischen Schutz von Massenverkehr. Allerdings sind auch andere Beispiele möglich. Beispielsweise kann (je nach verwendeter Chiffrensammlung) ein Schlüsselblock (key_block) mehrere symmetrische Schlüssel umfassen, z. B. 2 zur Verschlüsselung und 2 zur Authentifizierung, z. B. kann es für AES-CBC 4 Schlüssel geben, 2 zur Authentifizierung und 2 zur Verschlüsselung - die vom Client- und vom Server-Endpunkt jeweils zur Kommunikation in einer Richtung verwendet werden. Für AEAD-Chiffren gibt noch andere Optionen, da AEAD eine Verschlüsselung und Authentifizierung mit einer einzelnen Operation erzielt...; für TLS <=1.2 sind auch Chiffrensammlungen mit reiner Authentifizierung möglich, etc.

Handhabung von Verschlüsselungsnachrichten ohne Massenverschlüsselung

[0128] Host-System: Empfangen einer Nachricht eines Typs in der Gruppe {handshake, alert, change_cipher_spec} (Handshake, Alarm, Chiffrenspezifikation ändern).

[0129] Weiterleiten der Nachricht an den Sitzungshandler über den Sitzungskanal und Transfer der Steuerung über den Steuerkanal Sitzungshandhabungssystem:

f. Erstellen einer Antwort auf die Nachricht eines anderen Typs als application_data (Anwendungsdaten) und Senden an die zweite Netzvorrichtung (durch das Host-System unter Verwendung des Sitzungskanals).

g. Rückgabe der Steuerung an das Host-System über den Steuerkanal

Handshake - Wiederaufnahmefall

[0130] Anwendung / Host-System: Initiieren einer wiederhergestellten Sitzung mit der zweiten Netzvorrichtung wie vorstehend.

[0131] Host-System: Übergibt die Steuerung über den Steuerkanal. Das Host-System kann zuerst eine Handshake-Nachricht vorinitialisieren und diese über den Steuerkanal an das Sitzungshandhabungssystem weiterleiten. Andere Optionen, wie vorstehend beschrieben, können hier ebenfalls verwendet werden. Sitzungshandhabungssystem: Beenden des Handshake-Protokolls, jetzt unter Verwendung des Wiederaufnahmeschlüsselmaterials anstelle des langfristigen Geheimnisses. Nach Abschluss wird die Steuerung wieder an das Host-System übergeben.

[0132] Fig. 3 zeigt schematisch eine beispielhafte Ausführungsform eines Verfahrens 300 für eine kryptografisch geschützte Kommunikation zwischen einer ersten Netzvorrichtung und einer zweiten Netzvorrichtung. Die kryptografisch geschützte Kommunikation umfasst wenigstens ein Handshake-Protokoll, ein Protokoll für den kryptografischen Schutz von Massendaten und ein Wiederaufnahmeprotokoll. Das Verfahren umfasst:

- Anordnen (31) mehrerer getrennter Ausführungsumgebungen in der ersten Netzvorrichtung, wobei die mehreren getrennten Ausführungsumgebungen ein Host-System und ein Sitzungshandhabungssystem beinhalten; wobei erfolgt:

- während des Handshake-Protokolls, Erhalten (320), durch das Sitzungshandhabungssystem, einer kryptografischen Antwort in Abhängigkeit von dem langfristigen Geheimnis, wobei die kryptografische Antwort im Rahmen des Handshake-Protokolls an die zweite Netzvorrichtung gesendet wird, um eine sichere Sitzung zwischen der ersten Netzvorrichtung und der zweiten

[0133] Netzvorrichtung einzurichten, wobei das Sitzungshandhabungssystem von dem Handshake-

Protokoll einen ersten kryptografischen Massenschutzschlüssel und einen Wiederaufnahmeschlüssel erhält

- Weiterleiten (330) des ersten kryptografischen Schutzschlüssels an das Host-System

- während des Protokolls für den kryptografischen Schutz von Massendaten, kryptografisches Schützen (340), durch das Host-System, von Massendaten, die in der sicheren Sitzung an die zweite Netzvorrichtung gesendet und/oder von der zweiten Netzvorrichtung empfangen werden, mit einem kryptografischen Massenschutzschlüssel, der von dem Sitzungshandhabungssystem empfangen wird,

- während des Wiederaufnahmeprotokolls, Erhalten (350), durch das Sitzungshandhabungssystem, einer kryptografischen Antwort von dem Wiederaufnahmeschlüssel, wobei die kryptografische Antwort im Rahmen des Wiederaufnahmeprotokolls an die zweite Netzvorrichtung gesendet wird, um eine sichere Sitzung zwischen der ersten Netzvorrichtung und der zweiten Netzvorrichtung wiederherzustellen, wobei das Sitzungshandhabungssystem von dem Wiederaufnahmeprotokoll einen zweiten kryptografischen Massenschutzschlüssel erhält,

- Weiterleiten (360) des zweiten kryptografischen Schutzschlüssels an das Host-System zur Verwendung beim kryptografischen Massenschutz.

[0134] In einer Ausführungsform umfasst die erste Netzvorrichtung ein Sicherheitssystem, wobei das Sicherheitssystem dafür ausgelegt ist, ein langfristiges Geheimnis zu speichern, und das Verfahren das Erhalten, durch das Sitzungshandhabungssystem, der kryptografischen Antwort von dem Sicherheitssystem umfasst.

[0135] Viele unterschiedliche Arten der Ausführung des Verfahrens sind möglich, was für Fachleute offensichtlich ist. Beispielsweise können die Schritte in der gezeigten Reihenfolge durchgeführt werden; die Reihenfolge der Schritte kann jedoch auch variiert werden und einige Schritte können parallel ausgeführt werden. Darüber hinaus können zwischen den Schritten andere Verfahrensschritte eingefügt werden. Die eingefügten Schritte können Verfeinerungen des Verfahrens darstellen, wie vorstehend beschrieben, oder können nichts mit dem Verfahren zu tun haben. Beispielsweise können einige Schritte, wenigstens teilweise, parallel ausgeführt werden. Darüber hinaus kann es vorkommen, dass ein gegebener Schritt noch nicht vollständig beendet ist, bevor ein nächster Schritt begonnen wird.

[0136] Ausführungsformen des Verfahrens können unter Verwendung von Software ausgeführt werden, die Anweisungen umfasst, um ein Prozessorsystem zu veranlassen, das Verfahren 300 durchzuführen. Software kann gegebenenfalls nur solche Schritte beinhalten, die von einer bestimmten Untereinheit (Subentität) des Systems ausgeführt werden. Die Software kann in einem geeigneten Datenspeichermedium gespeichert sein, wie etwa einer Festplatte, einer Floppy, einem Speicher, einer optischen Platte etc. Die Software kann als Signal drahtgebunden oder drahtlos oder unter Verwendung eines Datennetzes, z. B. dem Internet, gesendet werden. Die Software kann zum Herunterladen und/oder zur Fernnutzung auf einem Server verfügbar gemacht werden. Ausführungsformen des Verfahrens können unter Verwendung eines Bitstroms ausgeführt werden, der dafür ausgelegt ist, programmierbare Logik zu konfigurieren, z. B. eine feldprogrammierte Gatteranordnung (Field-Programmable Gate Array, FPGA), um das Verfahren durchzuführen.

[0137] Es versteht sich, dass sich der hier offenbarte Erfindungsgegenstand auch auf Computerprogramme erstreckt, insbesondere Computerprogramme auf oder in einem Träger, die dafür angepasst sind, den hier offenbarten Erfindungsgegenstand in die Praxis umzusetzen. Das Programm kann in Form von Quellcode, Objektcode, einer Codezwischenquelle und Objektcode wie etwa in teilweise kompilierter Form oder in irgendeiner anderen Form vorliegen, die sich zur Verwendung in der Implementierung einer Ausführungsform des Verfahrens eignet. Eine Ausführungsform, die sich auf ein Computerprogrammprodukt bezieht, umfasst computerausführbare Anweisungen entsprechend jedem der Verarbeitungsschritte von wenigstens einem der dargelegten Verfahren. Diese Anweisungen können in Subroutinen unterteilt und/oder in einer oder mehreren Dateien gespeichert sein, die statisch oder dynamisch verknüpft sind. Eine andere Ausführungsform, die sich auf ein Computerprogrammprodukt bezieht, umfasst computerausführbare Anweisungen entsprechend jeder/jedem der Vorrichtungen, Einheiten und/oder der Teile von wenigstens einem der dargelegten Systeme und/oder Produkte.

[0138] Fig. 4a zeigt ein computerlesbares Medium 1000, das einen beschreibbaren Teil 1010 aufweist, und ein computerlesbares Medium 1001, das ebenfalls einen beschreibbaren Teil aufweist. Das computerlesbare Medium 1000 wird als optisch lesbares Medium gezeigt. Das computerlesbare Medium 1001 wird als elektronischer Speicher, in diesem Fall als Speicherkarte, gezeigt. Die computerlesbaren Medien 1000 und 1001 können Daten 1020 speichern, wobei die Daten Anweisungen angeben können, die, wenn sie von einem Prozessorsystem ausgeführt werden, das Prozessorsystem veranlas-

sen, das Kommunikationsverfahren gemäß einer Ausführungsform durchzuführen. Das Computerprogramm 1020 kann auf dem computerlesbaren Medium 1000 als physische Markierungen oder durch Magnetisierung des computerlesbaren Mediums 1000 ausgebildet sein. Allerdings sind auch andere geeignete Ausführungsformen denkbar. Des Weiteren versteht es sich, dass, auch wenn das computerlesbare Medium 1000 hier als optische Platte gezeigt wird, das computerlesbare Medium 1000 irgendein geeignetes computerlesbares Medium sein kann, wie etwa eine Festplatte, ein Festkörperspeicher, ein Flash-Speicher etc., und beschreibbar oder nicht beschreibbar sein kann. Das Computerprogramm 1020 umfasst Anweisungen, die ein Prozessorsystem veranlassen, das besagte Kommunikationsverfahren durchzuführen.

[0139] **Fig.** 4b zeigt in einer schematischen Darstellung ein Prozessorsystem 1140 gemäß einer Ausführungsform der ersten Netzvorrichtung. Das Prozessorsystem umfasst eine oder mehrere integrierte Schaltungen 1110. Die Architektur der ein oder mehreren integrierten Schaltungen 1110 wird schematisch in **Fig.** 4b gezeigt. Die Schaltung 1110 umfasst eine Verarbeitungseinheit 1120, z. B. eine CPU, zum Ausführen von Computerprogrammkomponenten, um ein Verfahren gemäß einer Ausführungsform auszuführen und/oder zugehörige Module oder Einheiten zu implementieren. Die Schaltung 1110 umfasst einen Speicher 1122 zum Speichern von Programmiercode, Daten etc. Ein Teil des Speichers 1122 kann nur lesbar sein. Die Schaltung 1110 kann ein Kommunikationselement 1126, z. B. eine Antenne, Verbinder oder beides, und dergleichen umfassen. Die Schaltung 1110 kann eine dedizierte integrierte Schaltung 1124 zum Durchführen eines Teils oder der gesamten Verarbeitung, die im Verfahren definiert ist, umfassen. Der Prozessor 1120, der Speicher 1122, die dedizierte integrierte Schaltung (IC) 1124 und das Kommunikationselement 1126 können über eine Zwischenverbindung 1130, wie etwa einen Bus, miteinander verbunden sein. Das Prozessorsystem 1110 kann für eine kontaktgebundene bzw. eine kontaktlose Kommunikation unter Verwendung einer Antenne und/oder von Verbindern ausgelegt sein.

[0140] Beispielsweise kann, in einer Ausführungsform, das Prozessorsystem 1140, z. B. die erste Netzvorrichtung, eine Prozessorschaltung und eine Speicherschaltung umfassen, wobei der Prozessor dafür ausgelegt ist, Software auszuführen, die in der Speicherschaltung gespeichert ist. Beispielsweise kann es sich bei der Prozessorschaltung um einen Prozessor des Typs Intel Core i7, einen ARM Cortex-R8 etc. handeln. Bei der Speicherschaltung kann es sich um einen flüchtigen Speicher handeln, z. g. einen SRAM-Speicher. Im letzteren Fall kann die Vorrichtung eine nichtflüchtige Softwareschnittstelle umfassen, z. B. ein Festplattenlaufwerk, eine Netzschnittstelle etc., die für das Bereitstellen der Software ausgelegt ist.

[0141] Es sei darauf hingewiesen, dass die vorgenannten Ausführungsformen den hier offenbarten Erfindungsgegenstand nicht einschränken, sondern nur veranschaulichen, und dass Fachleute auf diesem Gebiet der Technik in der Lage sein werden, viele alternative Ausführungsformen zu konzipieren.

[0142] In den Ansprüchen sollen jegliche Bezugszeichen, die in Klammern gesetzt sind, nicht als den Anspruch einschränkend ausgelegt werden. Die Verwendung des Verbs „umfassen“ und seiner Konjugationsformen schließt das Vorhandensein von anderen Elementen oder Schritten als denen, die in einem Anspruch angegeben sind, nicht aus. Der Artikel „ein/eine/eines“ oder „einen/eine/eines“ vor einem Element schließt das Vorhandensein von einer Mehrzahl solcher Elemente nicht aus. Ausdrücke wie „wenigstens eines von“ vor einer Liste von Elementen stehen für eine Auswahl aller Elemente oder einer beliebigen Untermenge von Elementen aus der Liste. Beispielsweise ist der Ausdruck „wenigstens eines von A, B und C“ so zu verstehen, dass dieser Begriff nur A, nur B, nur C, sowohl A als auch B, sowohl A als auch C, sowohl B als auch C oder alle von A, B und C beinhaltet. Der hier offenbarte Erfindungsgegenstand kann durch Hardware, die mehrere verschiedene Elemente umfasst, und durch einen auf geeignete Weise programmierten Computer implementiert werden. In den Vorrichtungsansprüchen, in denen mehrere Teile durchnummeriert sind, können mehrere dieser Teile durch ein und dieselbe Hardwareposition verkörpert sein. Die bloße Tatsache, dass bestimmte Merkmale in voneinander unterschiedlichen Unteransprüchen aufgeführt sind, ist kein Hinweis darauf, dass eine Kombination dieser Merkmale nicht vorteilhaft genutzt werden kann.

[0143] In den Ansprüchen beziehen sich Verweise in Klammern auf Bezugszeichen in Zeichnungen mit veranschaulichenden Ausführungsformen oder auf Formeln von Ausführungsformen, wodurch sich somit die Lesbarkeit des Anspruchs erhöht. Diese Verweise sollen nicht als den Anspruch einschränkend ausgelegt werden.

Patentansprüche

1. Erste Netzvorrichtung (200), ausgelegt für eine kryptografisch geschützte Kommunikation mit einer zweiten Netzvorrichtung, wobei die kryptografisch geschützte Kommunikation wenigstens ein Handshake-Protokoll, ein Protokoll für den krypto-

grafischen Schutz von Massendaten und ein Wiederaufnahmeprotokoll umfasst, wobei die erste Netzvorrichtung dafür ausgelegt ist, mehrere getrennte Ausführungsumgebungen in der ersten Netzvorrichtung anzuordnen, wobei die mehreren getrennten Ausführungsumgebungen ein Host-System (210) und ein Sitzungshandhabungssystem (220) beinhalten, wobei
- während des Handshake-Protokolls, das Sitzungshandhabungssystem dafür ausgelegt ist, eine kryptografische Antwort in Abhängigkeit von dem langfristigen Geheimnis zu erhalten, wobei die kryptografische Antwort im Rahmen des Handshake-Protokolls an die zweite Netzvorrichtung gesendet wird, um eine sichere Sitzung zwischen der ersten Netzvorrichtung und der zweiten Netzvorrichtung einzurichten, wobei das Sitzungshandhabungssystem von dem Handshake-Protokoll einen ersten kryptografischen Massenschutzschlüssel und einen Wiederaufnahmeschlüssel erhält, wobei der erste kryptografische Schutzschlüssel an das Host-System weitergeleitet wird
- während des Protokolls für den kryptografischen Schutz von Massendaten, das Host-System dafür ausgelegt ist, Massendaten, die in der sicheren Sitzung an die zweite Netzvorrichtung gesendet oder von der zweiten Netzvorrichtung empfangen werden, mit einem kryptografischen Massenschutzschlüssel, der von dem Sitzungshandhabungssystem empfangen wird, kryptografisch zu schützen
- während des Wiederaufnahmeprotokolls, das Sitzungshandhabungssystem dafür ausgelegt ist, eine kryptografische Antwort von dem Wiederaufnahmeschlüssel zu erhalten, wobei die kryptografische Antwort im Rahmen des Wiederaufnahmeprotokolls an die zweite Netzvorrichtung gesendet wird, um eine sichere Sitzung zwischen der ersten Netzvorrichtung und der zweiten Netzvorrichtung wiederherzustellen, wobei das Sitzungshandhabungssystem von dem Wiederaufnahmeprotokoll einen zweiten kryptografischen Massenschutzschlüssel erhält, wobei der zweite kryptografische Schutzschlüssel an das Host-System zur Verwendung beim kryptografischen Massenschutz weitergeleitet wird.

2. Erste Netzvorrichtung nach Anspruch 1, wobei die erste Netzvorrichtung ein Sicherheitssystem (230) umfasst, wobei das Sicherheitssystem dafür ausgelegt ist, ein langfristiges Geheimnis zu speichern und das Sitzungshandhabungssystem dafür ausgelegt ist, die kryptografische Antwort von dem Sicherheitssystem zu erhalten.

3. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei das Protokoll für den kryptografischen Schutz von Massendaten eine Massenverschlüsselung, -entschlüsselung und/oder -authentifizierung umfasst.

4. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei der kryptografische Massenschutz ausschließlich in der Ausführungsumgebung des Host-Systems durchgeführt wird.

5. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei eine Ausführungsumgebung keinen Zugriff auf Daten und/oder Software in einer anderen Ausführungsumgebung in der ersten Netzvorrichtung hat, und auch nicht auf Daten und/oder Software im Sicherheitssystem.

6. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei
- weder die Ausführungsumgebung des Host-Systems noch die Ausführungsumgebung des Sitzungshandhabungssystems Zugriff auf das langfristige Geheimnis hat und
- die Ausführungsumgebung des Host-Systems keinen Zugriff auf den Wiederaufnahmeschlüssel hat.

7. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche , wobei das Host-System eine kryptografische Anwendung ausführt, um Daten unter Verwendung des kryptografischen Massenschutzschlüssels kryptografisch zu schützen, wobei die kryptografische Anwendung dafür ausgelegt ist, Daten zu schützen, die an die zweite Netzvorrichtung gesendet und/oder von der zweiten Netzvorrichtung empfangen werden.

8. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei, während des Handshake-Protokolls, das Sitzungshandhabungssystem dafür ausgelegt ist, von dem Handshake-Protokoll ein Master-Geheimnis zu erhalten, das mit der zweiten Netzvorrichtung geteilt wird, wobei der erste kryptografische Massenschutzschlüssel und der Wiederaufnahmeschlüssel von dem geheimen Master-Schlüssel abgeleitet werden und wobei die Ausführungsumgebung des Host-Systems keinen Zugriff auf das Master-Geheimnis hat.

9. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei der kryptografische Massenschutzschlüssel und der Wiederaufnahmeschlüssel kurzfristige Schlüssel sind.

10. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, ausgelegt für TLS gemäß RFC8446, wobei das Host-System dafür ausgelegt ist, Datensätze des Protokolltyps application_data (Anwendungsdaten) zu verarbeiten, nicht jedoch Operationen eines anderen Typs, z. B. handshake (Handshake), alert (Alarm) und
change_cipher_spec (Chiffrenspezifikation ändern), und das Sitzungshandhabungssystem dafür ausgelegt ist, Operation der anderen Typen auszuführen.

11. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei das Host-System und das Sitzungshandhabungssystem mit einem ersten Kommunikationskanal ausgeführt sind, wobei die Kommunikation zwischen der ersten Netzvorrichtung und der zweiten Netzvorrichtung im Host-System ankommt und während des Handshake-Protokolls und während des Wiederaufnahmeprotokolls über den ersten Kommunikationskanal an das Sitzungshandhabungssystem weitergeleitet wird.

12. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei das Host-System und das Sitzungshandhabungssystem mit einem Steuerungsmechanismus ausgeführt sind, um die Steuerung der kryptografisch geschützten sicheren Kommunikation anzuzeigen, wobei der Steuerungsmechanismus die Steuerung für das Host-System während des kryptografischen Massenschutzes anzeigt und wobei der Steuerungsmechanismus die Steuerung vom Host-System zum Sitzungshandhabungssystem für das Handshake-Protokoll und für das Wiederaufnahmeprotokoll ändert.

13. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei der Steuerungsmechanismus einen zweiten Kommunikationskanal umfasst, um einen Zustand der kryptografisch geschützten sicheren Kommunikation zwischen dem Host-System und dem Sitzungshandhabungssystem zu übergeben.

14. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei eine Kommunikation einen Kommunikationstyp umfasst und das Host-System dafür ausgelegt ist, die Kommunikation je nach Kommunikationstyp an den Sitzungshandler zu übergeben.

15. Erste Netzvorrichtung nach Anspruch 14, wobei der Kommunikationstyp verschlüsselt ist und das Host-System dafür ausgelegt ist, wenigstens den Kommunikationstyp zu entschlüsseln, bevor die Kommunikation je nach Kommunikationstyp an den Sitzungshandler weitergeleitet wird.

16. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei das Host-System dafür ausgelegt ist, einen teilweise initialisierten Zustand für das Sitzungshandhabungssystem bereitzustellen, zum Abschluss durch das Sitzungshandhabungssystem während des Handshake-Protokolls und/oder des Wiederaufnahmeprotokolls.

17. Erste Netzvorrichtung nach einem der vorstehenden Ansprüche, wobei
- die erste Netzvorrichtung eine Verbrauchervorrichtung oder ein IoT-Client ist und/oder
- die erste Netzvorrichtung eine Server-Vorrichtung oder eine IoT-Backend-Vorrichtung ist.

18. Verfahren (300) für eine kryptografisch geschützte Kommunikation zwischen einer ersten Netzvorrichtung und einer zweiten Netzvorrichtung, wobei die kryptografisch geschützte Kommunikation wenigstens ein Handshake-Protokoll, ein Protokoll für den kryptografischen Schutz von Massendaten und ein Wiederaufnahmeprotokoll umfasst, wobei das Verfahren umfasst:
- Anordnen (31) mehrerer getrennter Ausführungsumgebungen in der ersten Netzvorrichtung, wobei die mehreren getrennten Ausführungsumgebungen ein Host-System und ein Sitzungshandhabungssystem beinhalten; wobei erfolgt:
- während des Handshake-Protokolls, Erhalten (320), durch das Sitzungshandhabungssystem, einer kryptografischen Antwort in Abhängigkeit von dem langfristigen Geheimnis, wobei die kryptografische Antwort im Rahmen des Handshake-Protokolls an die zweite Netzvorrichtung gesendet wird, um eine sichere Sitzung zwischen der ersten Netzvorrichtung und der zweiten Netzvorrichtung einzurichten, wobei das Sitzungshandhabungssystem von dem Handshake-Protokoll einen ersten kryptografischen Massenschutzschlüssel und einen Wiederaufnahmeschlüssel erhält,
- Weiterleiten (330) des ersten kryptografischen Schutzschlüssels an das Host-System,
- während des Protokolls für den kryptografischen Schutz von Massendaten, kryptografisches Schützen (340), durch das Host-System, von Massendaten, die in der sicheren Sitzung an die zweite Netzvorrichtung gesendet und/oder von der zweiten Netzvorrichtung empfangen werden, mit einem kryptografischen Massenschutzschlüssel, der von dem Sitzungshandhabungssystem empfangen wird,
- während des Wiederaufnahmeprotokolls, Erhalten (350), durch das Sitzungshandhabungssystem, einer kryptografischen Antwort von dem Wiederaufnahmeschlüssel, wobei die kryptografische Antwort im Rahmen des Wiederaufnahmeprotokolls an die zweite Netzvorrichtung gesendet wird, um eine sichere Sitzung zwischen der ersten Netzvorrichtung und der zweiten Netzvorrichtung wiederherzustellen, wobei das Sitzungshandhabungssystem von dem Wiederaufnahmeprotokoll einen zweiten kryptografischen Massenschutzschlüssel erhält,
- Weiterleiten (360) des zweiten kryptografischen Schutzschlüssels an das Host-System zur Verwendung beim kryptografischen Massenschutz.

19. Transitorisches oder nicht-transitorisches computerlesbares Medium (1000), umfassend Daten (1020), die Anweisungen darstellen, die, wenn sie von einem Prozessorsystem ausgeführt

werden, das Prozessorsystem veranlassen, das Verfahren nach Anspruch 18 durchzuführen.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

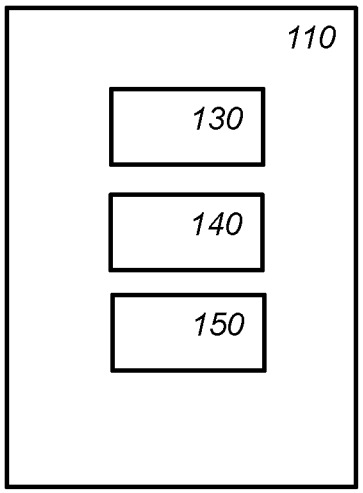


Fig. 1a

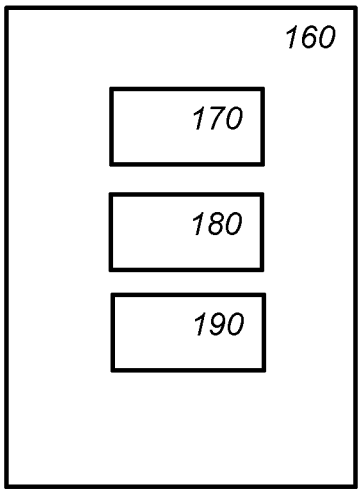


Fig. 1b

100

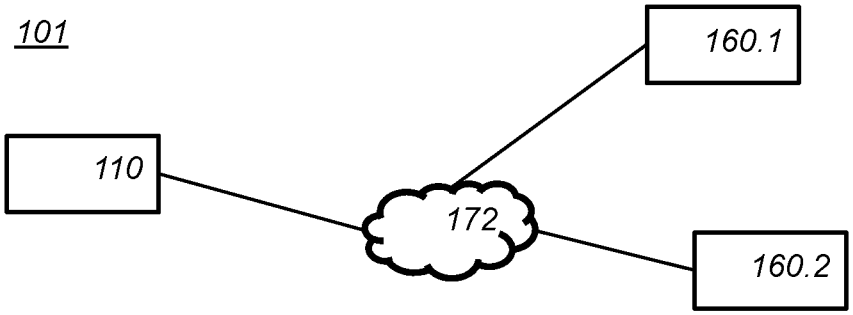


Fig. 1c

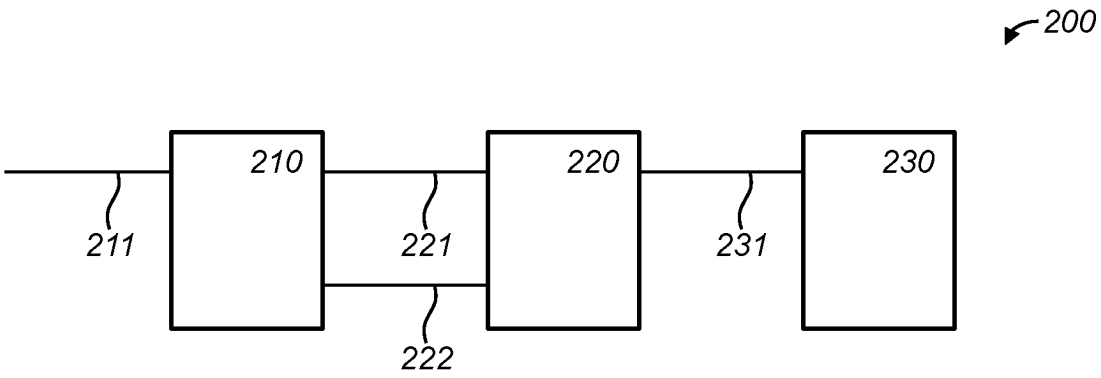


Fig. 2

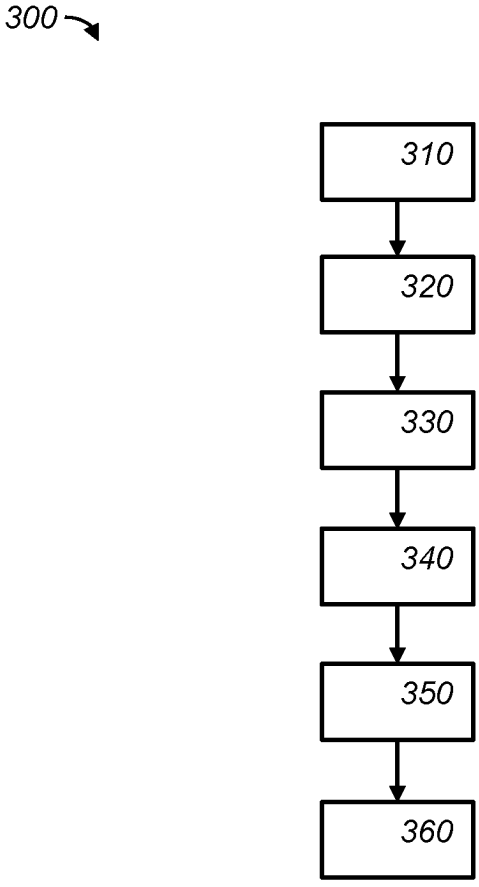


Fig. 3

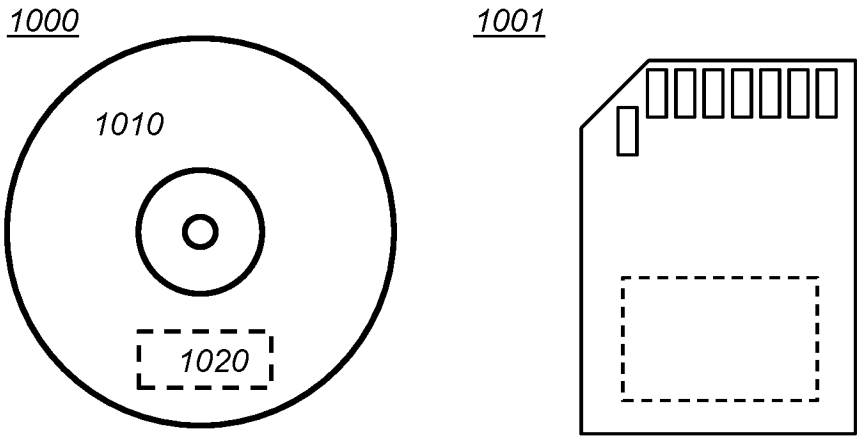


Fig. 4a

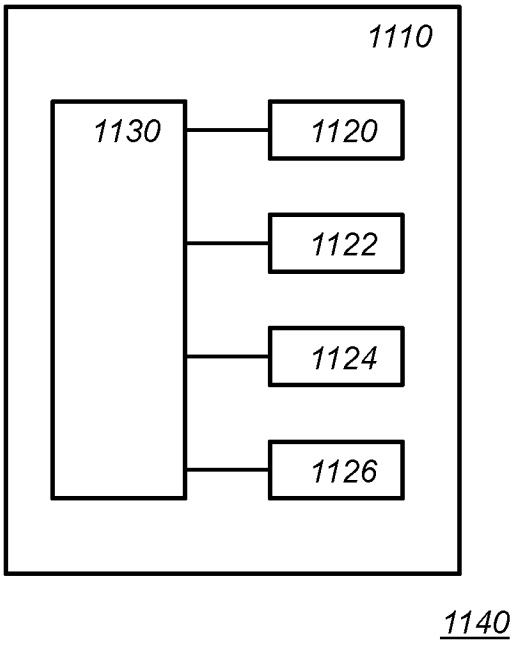


Fig. 4b

