(19) Deutsches Patent- und Markenamt

(10) **DE 10 2017 108 128 B4** 2021.02.25

(12) # Patentschrift

(21) Aktenzeichen: **10 2017 108 128.3**
(22) Anmeldetag: **13.04.2017**
(43) Offenlegungstag: **18.10.2018**
(45) Veröffentlichungstag der Patenterteilung: **25.02.2021**

(51) Int Cl.: ***H04L 9/00*** (2006.01)
G09C 1/00 (2006.01)
G06F 21/72 (2013.01)
G06F 21/85 (2013.01)
H04L 9/10 (2006.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(73) Patentinhaber:
Westfälische Hochschule Gelsenkirchen Bocholt Recklinghausen, 45879 Gelsenkirchen, DE

(74) Vertreter:
Michalski Hüttermann & Partner Patentanwälte mbB, 40221 Düsseldorf, DE

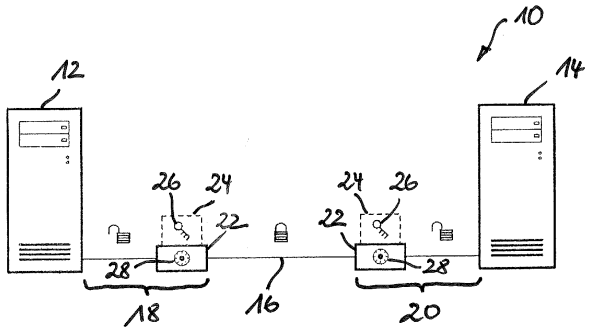
(72) Erfinder:
Jorczyk, Udo, 45657 Recklinghausen, DE; Ridder, Philip, B. Eng., 45663 Recklinghausen, DE

(56) Ermittelter Stand der Technik:

DE	**693 32 543**	**T2**
US	**2005 / 0 114 663**	**A1**
US	**2015 / 0 310 232**	**A1**

(54) Bezeichnung: **Hardwarebasiertes Sicherheitsmodul**

(57) Hauptanspruch: Hardwarebasiertes Sicherheitsmodul (18, 20) zur Ver- und/oder Entschlüsselung von Daten bei der Datenübertragung auf einem Datenübertragungsweg (16) zwischen Netzwerkknoten bildenden Informations- und/oder Datenverarbeitungsgeräten (12, 14), mit
- einem Rechenwerk (22) zur Durchführung kryptografischer Operationen,
- zumindest einer ersten Schnittstelle (30) zur datenübertragungstechnischen Integration des hardwarebasierten Sicherheitsmoduls (18, 20) in den Übertragungsweg (16),
- einem Speicher (24), der eine über diese zumindest eine erste Schnittstelle (30) unzugänglichen Speicherbereich zur Ablage zumindest eines kryptografischen Schlüssels (26) für die kryptografischen Operationen aufweist,
- einer zweiten Schnittstelle (32), über die der Speicher (24) zur Ablage des kryptografischen Schlüssels (26) in dem Speicherbereich unidirektional konfigurierbar ist, und
- einer dem Speicher (24) vorgeschalteten Sicherheitsschaltung (36) zur Überwachung des modulinternen Datenstroms zwischen dem Speicher (24) und den anderen Komponenten, unter anderem dem Rechenwerk (22), der ersten Schnittstelle (30) und der zweiten Schnittstelle (32) des hardwarebasierten Sicherheitsmoduls (18, 20), wobei die Sicherheitsschaltung (36) eingerichtet ist, die Zugriffsrechte auf den Speicherbereich des Speichers (24) zur Ablage des kryptographischen Schlüssels (26) derart zu vergeben, dass die eine erste Schnittstelle (30) keinerlei Zugriffsrechte hat, dass das Rechenwerk (22) ...



Beschreibung

[0001] Die Erfindung betrifft ein hardwarebasiertes Sicherheitsmodul zur Ver- und/oder Entschlüsselung von Daten bei der Datenübertragung auf einem Übertragungsweg zwischen Netzwerkknoten.

[0002] Die Erfindung betrifft weiterhin ein Hardwaresicherheitssystem mit zumindest einem derartigen hardwarebasierten Sicherheitsmodul und einer Programmiereinrichtung und schließlich auch ein entsprechendes Datenübertragungssystem mit derartigen hardwarebasierten Sicherheitsmodulen.

[0003] Bekannt sind einerseits diverse Verschlüsselungslösungen zur Ver- und/oder Entschlüsselung von Daten bei der Datenübertragung auf einem Übertragungsweg zwischen Netzwerkknoten, bei denen ein für die Ver- und Entschlüsselung benötigter kryptografischer Schlüssel in einer Software hinterlegt ist. Dies bietet potentiellen Angreifern jedoch die Möglichkeit, sich diesen Schlüssel über eine Vielzahl von Angriffsstrategien anzueignen.

[0004] Andererseits sind hardwarebasierte Sicherheitsmodule (HSM: Hardware Security Modules) seit langem bekannt. Der englischsprachige Wikipedia-Eintrag zum Thema „Hardware Security Module“ beschreibt ein solches Modul als eine Datenverarbeitungseinrichtung, die digitale Schlüssel für eine starke Authentifizierung sichert und verwaltet sowie kryptographische Prozessierung bietet. Derartige hardwarebasierte Sicherheitsmodule sind gewöhnlich in Form einer Plug-in-Karte oder eines externen Geräts ausgestaltet, das direkt an einen Computer oder Netzwerk-Server angeschlossen ist.

[0005] Die Druckschrift US 2005/ 0 114 663 A1 beschreibt ein Hardwarebasiertes Sicherheitsmodul zur Ver- und/oder Entschlüsselung von Daten bei der Datenübertragung auf einem Datenübertragungsweg zwischen Netzwerkknoten bildenden Informations- und/oder Datenverarbeitungsgeräten, mit einem Rechenwerk zur Durchführung kryptografischer Operationen, zumindest einer ersten Schnittstelle zur datenübertragungstechnischen Integration des hardwarebasierten Sicherheitsmoduls in den Übertragungsweg, einem Speicher, der eine über diese zumindest eine erste Schnittstelle unzugänglichen Speicherbereich zur Ablage zumindest eines kryptografischen Schlüssels für die kryptografischen Operationen aufweist und einer zweiten Schnittstelle, über die der Speicher zur Ablage des kryptografischen Schlüssels in dem Speicherbereich konfigurierbar ist.

[0006] Die Druckschrift US 2015/ 0 310 232 A1 zeigt eine Vorrichtung zur Verschlüsselung in einem Ethernet-Kabel.

[0007] Es ist die Aufgabe der Erfindung Maßnahmen zur einfachen Realisierung einer verschlüsselten Datenübertragung auf einem Übertragungsweg zwischen Netzwerkknoten bildenden Informations- und/oder Datenverarbeitungsgeräten bereitzustellen.

[0008] Die Lösung der Aufgabe erfolgt erfindungsgemäß durch die Merkmale der unabhängigen Ansprüche. Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben.

[0009] Bei dem erfindungsgemäßen hardwarebasierten Sicherheitsmodul zur Ver- und/oder Entschlüsselung von Daten bei der Datenübertragung auf einem Übertragungsweg zwischen Netzwerkknoten bildenden Informations- und/oder Datenverarbeitungsgeräten ist vorgesehen, dass dieses die folgenden Komponenten umfasst: (a) ein Rechenwerk zur Durchführung kryptografischer Operationen, (b) zumindest eine erste Schnittstelle zur datenübertragungstechnischen Integration des Moduls in den Übertragungsweg, (c) ein Speicher mit einem über diese zumindest eine erste Schnittstelle unzugänglichen Speicherbereich zur Ablage zumindest eines kryptografischen Schlüssels für die kryptografischen Operationen und (d) eine zweite Schnittstelle, über die der Speicher zur Ablage des kryptografischen Schlüssels in dem Speicherbereich unidirektional konfigurierbar ist. Der kryptografische Schlüssel kann dabei weder über den Datenstrom auf dem Übertragungsweg in den Speicher geschrieben, noch gelesen werden. Um das hardwarebasierte Sicherheitsmodul mit dem kryptografischen Schlüssel zu versehen, muss der kryptografische Schlüssel über die zweite Schnittstelle auf dem Speicher abgelegt, also in den entsprechenden Speicherbereich des Speichers geschrieben, werden.

[0010] Ein solches hardwarebasiertes Sicherheitsmodul ist einfach bedienbar und ermöglicht eine verschlüsselte Datenübertragung, die sehr sicher ist.

[0011] Erfindungsgemäß ist weiterhin vorgesehen, dass das Modul eine dem Speicher vorgeschaltete Sicherheitsschaltung zur Überwachung des modulinternen Datenstroms zwischen dem Speicher und den anderen Komponenten des Moduls, also zumindest dem Rechenwerk und den Schnittstellen, aufweist. Die Sicherheitsschaltung vergibt insbesondere die Zugriffsrechte auf den Speicherbereich des Speichers zur Ablage zumindest eines kryptografischen Schlüssels. Die zumindest eine erste Schnittstelle hat keinerlei Zugriffsrechte, das Rechenwerk kann den Schlüssel im Rahmen seiner kryptografischen Operationen auslesen, jedoch nicht überschreiben und über zweite Schnittstelle kann der Schlüssel abgelegt, jedoch nicht ausgelesen werden.

[0012] Gemäß einer weiteren bevorzugten Ausführungsform der Erfindung ist das Modul zur Authen-

tifizierung einer den kryptographischen Schlüssel über die zweite Schnittstelle bereitstellenden Programmiereinrichtung (kurz: Programmer) eingerichtet. Diese Authentifizierung der Programmiereinrichtung erfolgt insbesondere mittels der Sicherheitsschaltung.

[0013] Gemäß noch einer weiteren bevorzugten Ausgestaltung der Erfindung ist die erste Schnittstelle oder zumindest eine der ersten Schnittstellen für ein Aufstecken auf eine entsprechende Schnittstelle eines der Informations- und/oder Datenverarbeitungsgeräte eingerichtet. Die erste Schnittstelle ist mit einem entsprechenden Stecker, insbesondere einem RJ-Stecker, versehen.

[0014] Dabei ist insbesondere vorgesehen, dass das hardwarebasierte Sicherheitsmodul als dongleartiges Sicherheitsmodul, insbesondere als dongleartiges Ethernet-Sicherheitsmodul ausgebildet ist. Diese Ausgestaltung des Moduls kann auch als „Ethernet Security Dongle“ bezeichnet werden. Die erste Schnittstelle ist mit einem entsprechenden Stecker, insbesondere einem RJ45-Stecker, versehen.

[0015] Gemäß einer bevorzugten Ausgestaltung der Erfindung ist die zweite Schnittstelle für einen unidirektionalen Zugang zu dem Speicherbereich zur Ablage zumindest eines kryptografischen Schlüssels eingerichtet, der nur ein Ablegen von Daten in diesem Speicherbereich erlaubt. Bei dieser Ausgestaltung ist die zweite Schnittstelle so eingerichtet und/oder mit dem Speicher verschaltet, dass sich ein unidirektionaler Zugang zu dem Speicherbereich, der nur ein Ablegen von Daten in diesem Speicherbereich erlaubt.

[0016] Gemäß noch einer weiteren bevorzugten Ausgestaltung der Erfindung weist das Modul weiterhin eine Überwachungsschaltung auf, die bei Erkennen einer unerlaubter Manipulation des Moduls ein Entfernen des kryptografischen Schlüssels aus dem Speicherbereich des Speichers bewirkt.

[0017] Mit Vorteil ist weiterhin vorgesehen, dass die unerlaubte Manipulation (i) ein Abziehen der ersten Schnittstelle von der entsprechenden Schnittstelle des Informations- und/oder Datenverarbeitungsgeräts ist und/oder (ii) ein Öffnen eines den Speicher und das Rechenwerk einhausenden Gehäuses des Moduls ist.

[0018] Bei dem erfindungsgemäßen Hardwaresicherheitssystem ist vorgesehen, dass dieses zumindest ein vorstehend genanntes hardwarebasiertes Sicherheitsmodul und eine Programmiereinrichtung und mit einer Programmiereinrichtung zum Ablegen des kryptografischen Schlüssels in den Speicher des hardwarebasierten Sicherheitsmoduls über dessen zweite Schnittstelle.

[0019] Bei dem erfindungsgemäßen Datenübertragungssystem mit mehreren Netzwerkknoten bildenden Informations- und/oder Datenverarbeitungsgeräten und zumindest einem die Netzwerkknoten verbindenden Datenübertragungsweg, der einen individuellen Anschlussabschnitt für jeden der Netzwerkknoten bereithält, ist vorgesehen, dass jeder der Anschlussabschnitte als vorstehend genanntes hardwarebasiertes Sicherheitsmodul ausgebildet ist oder zumindest ein solches hardwarebasiertes Sicherheitsmodul aufweist.

[0020] Nachfolgend wird die Erfindung unter Bezugnahme auf die anliegenden Zeichnungen anhand von bevorzugten Ausführungsbeispielen exemplarisch erläutert, wobei die nachfolgend dargestellten Merkmale sowohl jeweils einzeln als auch in Kombination einen Aspekt der Erfindung darstellen können. Es zeigt:

Fig. 1 ein Datenübertragungssystem mit zwei Datenverarbeitungsgeräten und zumindest einem die Geräte verbindenden Datenübertragungsweg, in dem hardwarebasierte Sicherheitsmodule gemäß einer ersten bevorzugten Ausführungsform der Erfindung verschaltet sind,

Fig. 2 den prinzipiellen Aufbau eines hardwarebasierten Sicherheitsmoduls in einer schematische Darstellung,

Fig. 3 ein Übertragen eines Schlüssels auf eines der hardwarebasierten Sicherheitsmodule bei dem Datenübertragungssystem der **Fig. 1** und

Fig. 4 die äußere Gestalt eines als Ethernet Security Dongle ausgebildeten hardwarebasierten Sicherheitsmoduls.

[0021] Die **Fig. 1** zeigt ein Datenübertragungssystem **10** mit zwei Datenverarbeitungsgeräten **12**, **14** und zumindest einem die beiden Datenverarbeitungsgeräte **12**, **14** verbindenden Datenübertragungsweg **16** (kurz: Übertragungsweg). Dieses Datenübertragungssystem **10** kann dabei Teil eines (in Gänze nicht gezeigten) Netzwerks sein, wobei jeder der Datenverarbeitungsgeräte **12**, **14** einen entsprechenden Netzwerkknoten des Netzwerks bildet. Im Datenübertragungsweg **16** sind zwei hardwarebasierte Sicherheitsmodule **18**, **20** verschaltet, wobei jedes der hardwarebasierten Sicherheitsmodule **18**, **20** einen individuellen Anschlussabschnitt des Datenübertragungswegs **16** zum jeweiligen Anschluss je eines der Datenverarbeitungsgeräte **12**, **14** bildet. Mit anderen Worten ist jedes der Datenverarbeitungsgeräte **12**, **14** über ein ihm zugeordnetes hardwarebasiertes Sicherheitsmodul **18**, **20** im Datenübertragungssystem **10** verschaltet. Die hardwarebasierten Sicherheitsmodule **18**, **20** sind dazu jeweils als Security Dongle ausgebildet. Jedes der hardwarebasierten Sicherheitsmodule **18**, **20** ist zur Ver- und/

oder Entschlüsselung von Daten bei der Datenübertragung auf dem Übertragungsweg **16** zwischen den Netzwerkknoten bildenden Datenverarbeitungsgeräten **12**, **14** eingerichtet. Dazu weist jedes der Module **18**, **20** ein Rechenwerk **22** zur Durchführung kryptografischer Operationen und einen Speicher **24** (genauer: einen Datenspeicher) auf, in dem ein kryptografischer Schlüssel **26** für kryptografische Operationen abgelegt ist. Herzstück des Rechenwerks **22** ist eine Prozessoreinheit **28** mit einem oder mehreren Prozessoren. Die Kommunikation bzw. der Datenstrom zwischen Datenverarbeitungsgerät **12**, **14** und zugeordnetem hardwarebasierten Sicherheitsmodul **18**, **20** ist unverschlüsselt und auf dem Rest des Datenübertragungswegs **16**, also zwischen den hardwarebasierten Sicherheitsmodulen **18**, **20**, verschlüsselt.

[0022] Die **Fig. 2** zeigt nun den prinzipiellen Aufbau eines hardwarebasierten Sicherheitsmoduls **18**, **20** zur Ver- und/oder Entschlüsselung von Daten in einer schematische Darstellung. Das Modul **18**, **20** umfasst neben dem Rechenwerk **22** zur Durchführung der kryptografischen Operationen und dem Speicher **24**, der einen Speicherbereich für den Schlüssel **24** bereitstellt, weiterhin eine erste Schnittstelle **30** zur datenübertragungstechnischen Integration des Moduls **18**, **20** in den Übertragungsweg **16**, eine zweite Schnittstelle **32**, über die der Speicher **24** zur Ablage des kryptografischen Schlüssels **26** unidirektional konfigurierbar ist, eine Überwachungsschaltung **34**, die bei Erkennen einer unerlaubter Manipulation des Moduls **18**, **20** ein automatisches Entfernen des kryptografischen Schlüssels **26** aus dem Speicherbereich des Speichers **24** bewirkt, sowie eine zentrale Sicherheitsschaltung **36**. Die Sicherheitsschaltung **36** ist dem Speicher **24** vorgeschaltet und dient zur Überwachung des modulinternen Datenstroms zwischen dem Speicher **24** und den anderen Komponenten **22**, **30**, **32**, **34** des Moduls **18**, **20**. Die Sicherheitsschaltung **36** vergibt insbesondere die Zugriffsrechte auf den Speicherbereich des Speichers **24** zur Ablage zumindest des kryptografischen Schlüssels **26**. Über die erste Schnittstelle **30** ergibt sich keinerlei Zugriffsrechte auf den Speicher **24**, das Rechenwerk **22** kann den Schlüssel **26** im Rahmen seiner kryptografischen Operationen auslesen, jedoch nicht überschreiben und über die zweite Schnittstelle **32** kann der Schlüssel **26** im Speicher **24** abgelegt, jedoch nicht ausgelesen werden. Die zweite Schnittstelle **32** ist im gezeigten Beispiel eine Luftschnittstelle für eine Nahfeldkommunikation (NFC: Near Field Communication).

[0023] Die Überwachungsschaltung **34** dient - wie gesagt - der Erkennung von unerlaubten Manipulationen des Moduls **10** und bewirkt über die Sicherheitsschaltung **36** bei einer erkannten Manipulationen des Moduls **10** ein Entfernen des kryptografischen Schlüssels **26** aus dem Speicherbereich des Speichers **24**. Derartige unerlaubte Manipulation sind beispielsweise ein Abziehen der ersten Schnittstelle **30** von der entsprechenden Schnittstelle des entsprechenden Datenverarbeitungsgeräts **12**, **14** oder ein Öffnen des den Speicher **24** und das Rechenwerk **22** einhausenden Gehäuses **40** des Moduls **18**, **20**.

[0024] Die **Fig. 3** zeigt ein Übertragen des Schlüssels **26** auf eines der hardwarebasierten Sicherheitsmodule **18** bei dem Datenübertragungssystem **10** der **Fig. 1**. Der kryptografische Schlüssel **26** wird mittels einer Programmiereinrichtung (auch Programmer genannt) 38, die über einen Masterschlüssel verfügt, über die als Luftschnittstelle für NFC ausgebildete zweite Schnittstelle **32** des hardwarebasierten Sicherheitsmoduls **18**, **20** in den dafür vorgesehenen Speicherbereich des Speichers **24** geschrieben bzw. dort abgelegt.

[0025] Sowohl die Module **18**, **20** wie auch die Programmiereinrichtung (der Programmer) 38 verfügen über Sicherheitsschaltungen **36**, welche es ermöglichen, dass das jeweilige Modul **18**, **20** nur von Programmern **38** beschrieben werden kann, welche eine korrekte Authentifizierung in sich tragen. Dadurch wird gewährleistet, dass kein fremder Schlüssel in die Module **18**, **20** eingetragen werden kann und somit dritte Stellen die verschlüsselte Kommunikation wieder entschlüsseln können.

[0026] Bei der Programmierung, also der Übertragen des Schlüssels **26** auf das hardwarebasierte Sicherheitsmodul **18**, handelt es sich um eine unidirektionale Kommunikation. Das heißt, es können nur Daten vom Programmer **38** auf das jeweilige Modul **18**, **20** übertragen werden und es gibt keine Reaktion seitens des Moduls **18**, **20** darauf. Somit können keine Rückschlüsse darauf gezogen werden, wenn die Authentifizierung fehlerhaft war und verhindert dadurch eine brute force Attacke auf das Modul **18**, **20**.

[0027] Die **Fig. 4** zeigt schließlich die äußere Gestalt eines als Ethernet Security Dongle ausgebildeten hardwarebasierten Sicherheitsmoduls **18**, **20**. Das Modul **18**, **20** weist ein Gehäuse **40** auf, welches den Speicher **24**, das Rechenwerk **22** mit seiner Prozessoreinheit **28**, die als Luftschnittstelle ausgebildete zweite Schnittstelle **32**, die Sicherheitsschaltung **34** und die Überwachungsschaltung **36** vollständig einhaust und lediglich die als RJ45 Stecker bzw. RJ45 Buchse ausgebildeten ersten Schnittstellen **30** an einander gegenüberliegenden Enden des Gehäuses **40** erkennen lässt.

[0028] Es ergeben sich die folgenden Vorteile der Erfindung:

- Informations- und/oder Datenverarbeitungsgeräte **12**, **14** können ganz einfach mit einem solchen Modul **18**, **20** nachgerüstet werden,

- Nutzer können innerhalb von Minuten für die Installation und Inbetriebnahme der Module **18**, **20** geschult werden,

- die Module **18**, **20** bieten eine Sicherheit, welche in dieser Form noch nicht existiert,

- die Module **18**, **20** sind einfach und günstig herzustellen,

- die Module **18**, **20** sind manipulationssicherer ist als alle bisherigen Lösungen,

- die Verschlüsselung kann auf Kundenwunsch angepasst werden

- die Module **18**, **20** können zusammen mit der jeweils aktuell als sicher geltenden Verschlüsselung genutzt werden und

- die Module **18**, **20** sind protokollunabhängig anwendbar.

Bezugszeichenliste

10	Datenübertragungssystem
12	Datenverarbeitungsgerät (Knoten)
14	Datenverarbeitungsgerät (Knoten)
16	Datenübertragungsweg
18	hardwarebasiertes Sicherheitsmodul
20	hardwarebasiertes Sicherheitsmodul
22	Rechenwerk
24	Speicher
26	kryptografischer Schlüssel
28	Prozessoreinheit
30	erste Schnittstelle
32	zweite Schnittstelle
34	Überwachungsschaltung
36	Sicherheitsschaltung
38	Programmiereinrichtung
40	Gehäuse

Patentansprüche

1. Hardwarebasiertes Sicherheitsmodul (18, 20) zur Ver- und/oder Entschlüsselung von Daten bei der Datenübertragung auf einem Datenübertragungsweg (16) zwischen Netzwerkknoten bildenden Informations- und/oder Datenverarbeitungsgeräten (12, 14), mit
- einem Rechenwerk (22) zur Durchführung kryptografischer Operationen,
- zumindest einer ersten Schnittstelle (30) zur datenübertragungstechnischen Integration des hardwarebasierten Sicherheitsmoduls (18, 20) in den Übertragungsweg (16),
- einem Speicher (24), der eine über diese zumindest eine erste Schnittstelle (30) unzugänglichen Speicherbereich zur Ablage zumindest eines kryptografischen Schlüssels (26) für die kryptografischen Operationen aufweist,
- einer zweiten Schnittstelle (32), über die der Speicher (24) zur Ablage des kryptografischen Schlüssels (26) in dem Speicherbereich unidirektional konfigurierbar ist, und
- einer dem Speicher (24) vorgeschalteten Sicherheitsschaltung (36) zur Überwachung des modulinternen Datenstroms zwischen dem Speicher (24) und den anderen Komponenten, unter anderem dem Rechenwerk (22), der ersten Schnittstelle (30) und der zweiten Schnittstelle (32) des hardwarebasierten Sicherheitsmoduls (18, 20), wobei die Sicherheitsschaltung (36) eingerichtet ist, die Zugriffsrechte auf den Speicherbereich des Speichers (24) zur Ablage des kryptographischen Schlüssels (26) derart zu vergeben, dass die eine erste Schnittstelle (30) keinerlei Zugriffsrechte hat, dass das Rechenwerk (22) den Schlüssel (26) auslesen, jedoch nicht überschreiben kann und dass die zweite Schnittstelle (32) den Schlüssel (26) ablegen, jedoch nicht auslesen kann.

2. Sicherheitsmodul nach Anspruch 1, **dadurch gekennzeichnet**, dass das hardwarebasierte Sicherheitsmodul (18, 20) für eine Authentifizierung einer den kryptographischen Schlüssel (26) über die zweite Schnittstelle (32) bereitstellenden Programmiereinrichtung (38) eingerichtet ist.

3. Sicherheitsmodul nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass die erste Schnittstelle (30) oder zumindest eine der ersten Schnittstellen (30) für ein Aufstecken auf eine entsprechende Schnittstelle eines der Informations- und/oder Datenverarbeitungsgeräte (12, 14) eingerichtet ist.

4. Sicherheitsmodul nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass das hardwarebasierte Sicherheitsmodul (18, 20) als dongleartiges Ethernet Hardwaresicherheitsmodul ausgebildet ist.

5. Sicherheitsmodul nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass die zweite Schnittstelle (32) für einen unidirektionalen Zugang zu dem Speicherbereich zur Ablage zumindest eines kryptografischen Schlüssels eingerichtet ist, der nur ein Ablegen von Daten in diesem Speicherbereich erlaubt.

6. Sicherheitsmodul nach einem der vorherigen Ansprüche, **gekennzeichnet durch** eine Überwachungsschaltung (34), die bei Erkennen einer uner-

laubter Manipulation des hardwarebasierten Sicherheitsmoduls (18, 20) ein Entfernen des kryptografischen Schlüssels aus dem Speicherbereich des Speichers bewirkt.

7. Sicherheitsmodul nach Anspruch 6, **dadurch gekennzeichnet**, dass die unerlaubte Manipulation
- ein Abziehen der ersten Schnittstelle (30) von der entsprechenden Schnittstelle des Informations- und/oder Datenverarbeitungsgeräts (12, 14) ist und/oder
- ein Öffnen eines den Speicher (24) und das Rechenwerk (22) einhausenden Gehäuses (40) des hardwarebasierten Sicherheitsmoduls (18, 20) ist.

8. Hardwaresicherheitssystem mit zumindest einem hardwarebasierten Sicherheitsmodul (18, 20) nach einem der vorherigen Ansprüche und mit einer Programmiereinrichtung (38) zum Ablegen des kryptografischen Schlüssels (26) in den Speicher (24) des hardwarebasierten Sicherheitsmoduls (18, 20) über dessen zweite Schnittstelle (32).

9. Datenübertragungssystem (10) mit mehreren Netzwerkknoten bildenden Informations- und/oder Datenverarbeitungsgeräten (12, 14) und zumindest einem die Netzwerkknoten verbindenden Datenübertragungsweg (16), der einen individuellen Anschlussabschnitt für jeden der Netzwerkknoten bereithält, wobei jeder der Anschlussabschnitte als hardwarebasiertes Sicherheitsmodul (18, 20) nach einem der Ansprüche 1 bis 7 ausgebildet ist oder zumindest aufweist.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

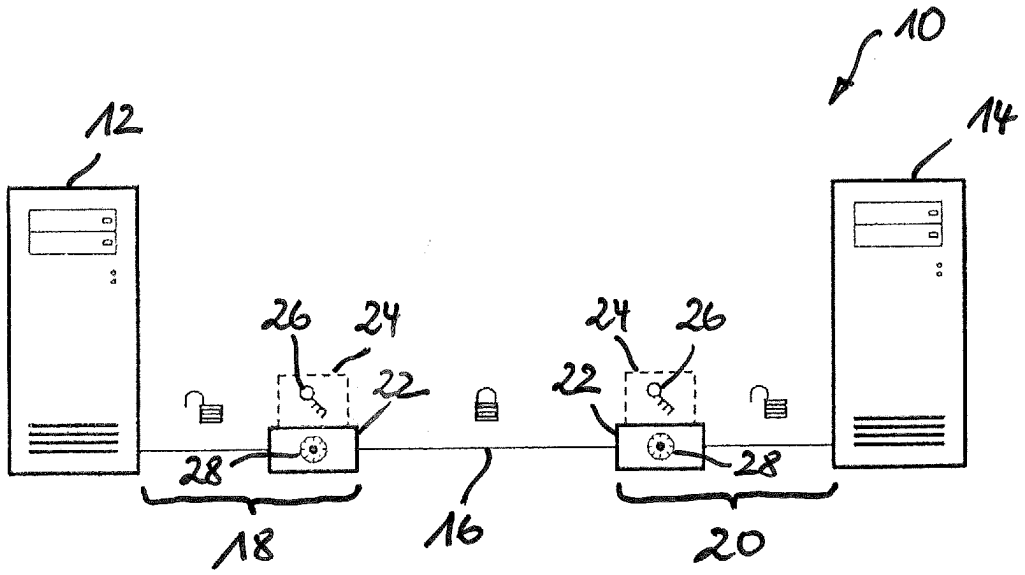


Fig. 1

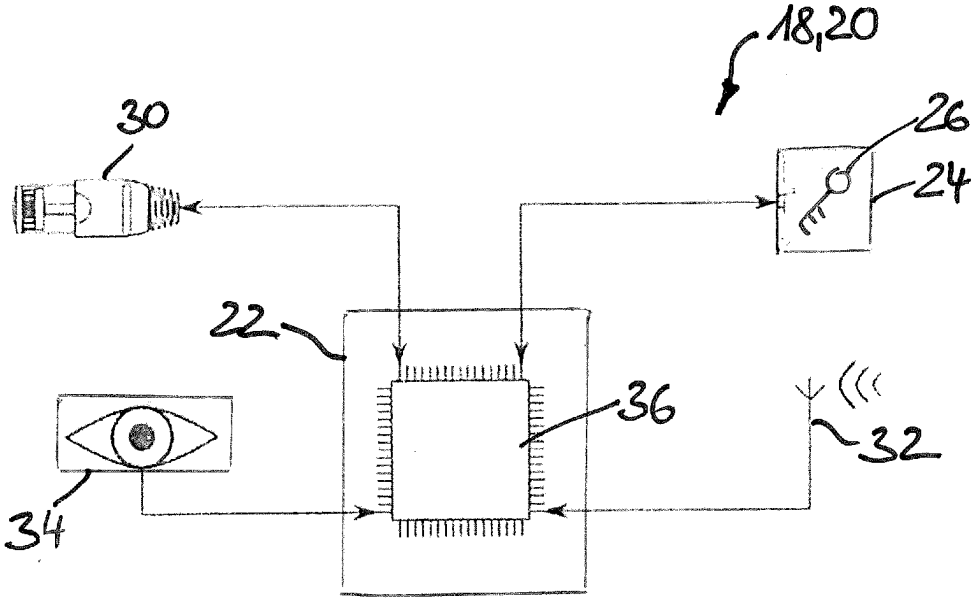


Fig. 2

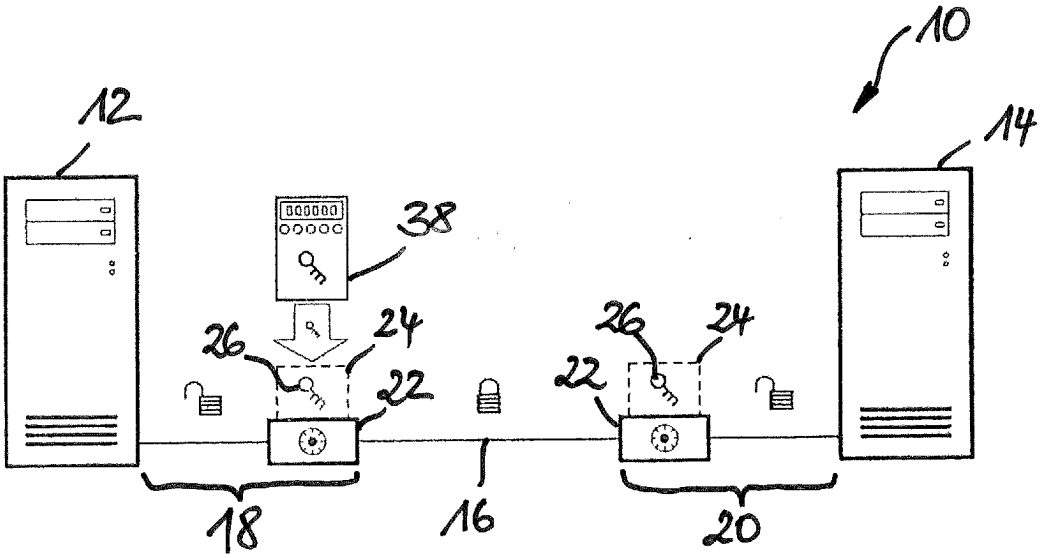


Fig. 3

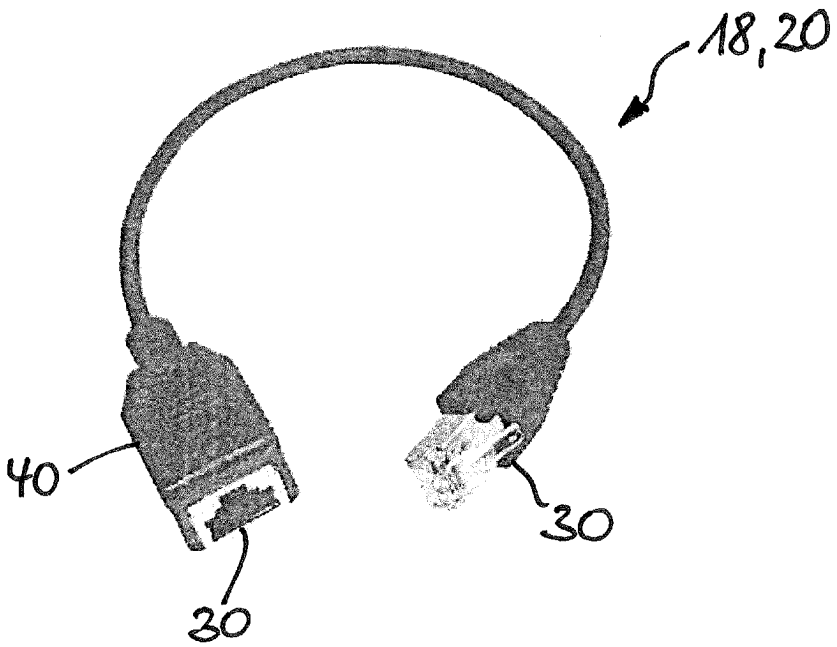


Fig. 4

Das Dokument wurde durch die Firma Jouve erstellt.