(19) Deutsches Patent- und Markenamt

(10) **DE 10 2017 108 129 A1** 2018.10.18

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2017 108 129.1**
(22) Anmeldetag: **13.04.2017**
(43) Offenlegungstag: **18.10.2018**

(51) Int Cl.: ***G06F 21/30*** (2013.01)

(71) Anmelder:
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

(56) Ermittelter Stand der Technik:

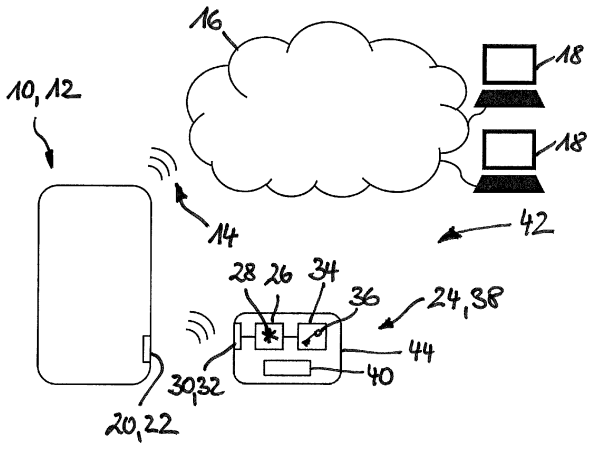
US	**2017 / 0 055 146**	**A1**
WO	**2016/ 177 667**	**A1**

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Hardwarebasiertes Sicherheitsmodul**

(57) Zusammenfassung: Die Erfindung betrifft ein hardwarebasiertes Sicherheitsmodul (24) zur Authentifizierung eines Informations- und/oder Datenverarbeitungsgeräts (12), insbesondere eines mobilen Endgeräts (10), gegenüber zumindest einem weiteren Informations- und/oder Datenverarbeitungsgerät (18), welches mit dem einen Informations- und/oder Datenverarbeitungsgerät (12), insbesondere über ein Netzwerk (16), datenübertragungstechnisch - drahtlos oder drahtgebunden - verbunden ist. Das hardwarebasierte Sicherheitsmodul (24) umfasst:
- ein Rechenwerk (26) zur Durchführung von kryptografischen Operationen zur Authentifizierung des Informations- und/oder Datenverarbeitungsgeräts (12),
- zumindest eine als Luftschnittstelle (30) ausgebildete Schnittstelle (32) zur datenübertragungstechnischen Anbindung des hardwarebasierten Sicherheitsmoduls (24) an das Informations- und/oder Datenverarbeitungsgerät (12) und
- einen Datenspeicher (34), der einen über diese zumindest eine Schnittstelle (32) unzugänglichen Speicherbereich zur Ablage zumindest eines kryptografischen Schlüssels (36) für die kryptografischen Operationen aufweist.
Die Erfindung betrifft weiterhin ein System (42) mit einem Informations- und/oder Datenverarbeitungsgerät (12) und einem derartigen hardwarebasierten Sicherheitsmodul (24).



Beschreibung

[0001] Die Erfindung betrifft ein hardwarebasiertes Sicherheitsmodul zur Authentifizierung eines Informations- und/oder Datenverarbeitungsgeräts gegenüber zumindest einem weiteren Informations- und/oder Datenverarbeitungsgerät welches mit dem einen Informations- und/oder Datenverarbeitungsgerät datenübertragungstechnisch drahtlos oder drahtgebunden verbunden ist.

[0002] Die Erfindung betrifft weiterhin ein System mit einem Informations- und/oder Datenverarbeitungsgerät und einem derartigen hardwarebasierten Sicherheitsmodul.

[0003] Bekannt sind seit langem hardwarebasierte Sicherheitsmodule (HSM: Hardware Security Modules). 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. Mittels derartiger hardwarebasierter Sicherheitsmodule ist eine Authentifizierung möglich. Diese hardwarebasierte Sicherheitsmodule sind dabei gewöhnlich in Form einer Plug-in-Karte oder eines externen Geräts ausgestaltet, das direkt an einen Computer, Netzwerk-Server, oder einem anderen Informations- und/oder Datenverarbeitungsgerät angeschlossen ist.

[0004] Die Nutzung von innerhalb eines Netzwerkes installierten Rechnern und auch der Zugriff von außen via Internet kann sicher via hardwarebasierter Sicherheitsmodule erfolgen. Dies bedeutet jedoch zumeist, dass zusätzliche Hardware verwendet werden muss. So ist die Verwendung von USB-Token, welche gegebenenfalls via Fingerabdruck aktiviert werden können, durchaus üblich. Problematisch ist allerdings die Verwendung von mobilen Devices, wie z.B. von Smartphones und Tablets innerhalb eines solchen Netzwerkes. Die verfügbaren Softwarelösungen sind als nicht sicher einzuschätzen, da die zur Verschlüsselung notwendigen Schlüssel auf dem Smartphone gespeichert sein werden und gefunden werden können. Token für mobile Endgeräte sind nicht bekannt, sodass man gegenwärtig nur auf eine unbefriedigende Lösung mittels App, also Software, zurückgreifen kann.

[0005] Es ist die Aufgabe der Erfindung Maßnahmen zur einfachen Realisierung einer Authentifizierung eines Informations- und/oder Datenverarbeitungsgeräts gegenüber zumindest einem weiteren Informations- und/oder Datenverarbeitungsgerät bereitzustellen.

[0006] Die Lösung der Aufgabe erfolgt erfindungsgemäß durch die Merkmale der unabhängigen Ansprüche. Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben.

[0007] Das erfindungsgemäße hardwarebasierte Sicherheitsmodul zur Authentifizierung eines Informations- und/oder Datenverarbeitungsgeräts gegenüber zumindest einem weiteren Informations- und/oder Datenverarbeitungsgerät, welches mit dem einen Informations- und/oder Datenverarbeitungsgerät datenübertragungstechnisch drahtlos oder drahtgebunden verbunden ist, weist die folgenden Komponenten auf:

(i) ein Rechenwerk zur Durchführung von kryptografischen Operationen zur Authentifizierung des Informations- und/oder Datenverarbeitungsgeräts,

(ii) zumindest eine als Luftschnittstelle ausgebildeten Schnittstelle zur datenübertragungstechnischen Anbindung des hardwarebasierten Sicherheitsmoduls an das Informations- und/oder Datenverarbeitungsgerät und

(iii) einen Datenspeicher, der einen über diese zumindest eine Schnittstelle unzugänglichen Speicherbereich zur Ablage zumindest eines kryptografischen Schlüssels für die kryptografischen Operationen aufweist.

[0008] Ein solches Sicherheitsmodul ist einfach bedienbar und ermöglicht eine Authentifizierung von üblichen Informations- und/oder Datenverarbeitungsgeräten, wie etwa mobilen Endgeräten, ohne diese modifizieren zu müssen.

[0009] Gemäß einer bevorzugten Ausgestaltung der Erfindung ist das Rechenwerk weiterhin zur Durchführung von kryptografischen Operationen zur Ver- und/oder Entschlüsselung von Daten bei der Datenübertragung zwischen dem Informations- und/oder Datenverarbeitungsgerät und dem zumindest einen weiteren Informations- und/oder Datenverarbeitungsgerät eingerichtet. Auch für die Ver- und/oder Entschlüsselung wird der kryptographische Schlüssel genutzt.

[0010] Gemäß einer weiteren bevorzugten Ausgestaltung der Erfindung ist die Luftschnittstelle als Luftschnittstelle für drahtlose Datenkommunikation und/oder für drahtlose Netzwerke, insbesondere auch drahtlose Sensornetzwerke, bevorzugt

- Bluetooth und/oder
- WLAN und/oder
- Nahfeldkommunikation und/oder
- Zigbee und/oder
- proprietäre Datenübertragungssysteme

ausgebildet.

[0011] Gemäß noch einer weiteren bevorzugten Ausgestaltung der Erfindung ist das hardwarebasierte Sicherheitsmodul mobil ausgestaltet, also ein mobiles Sicherheitsmodul.

[0012] Dabei ist bevorzugt vorgesehen, dass das mobile Sicherheitsmodul eine eigene Stromversorgung, insbesondere einen Akkumulator, aufweist.

[0013] Gemäß einer bevorzugten Ausführungsform der Erfindung ist das hardwarebasierte Sicherheitsmodul in einem vom Informations- und/oder Datenverarbeitungsgerät) separaten anderen Gerät integriert. Dieses Gerät ist beispielsweise eine Uhr, ein KFZ-Funkschlüssel oder ein anderes mobiles Gerät.

[0014] Bei dem erfindungsgemäßen System mit einem Informations- und/oder Datenverarbeitungsgerät und einem hardwarebasierten Sicherheitsmodul ist vorgesehen, dass das hardwarebasierte Sicherheitsmodul als vorstehend genanntes Modul ausgebildet ist.

[0015] Gemäß einer bevorzugten Ausgestaltung des erfindungsgemäßen Systems weist dieses weiterhin ein Identifikationsmodul zur Identifikation des Nutzers des Informations- und/oder Datenverarbeitungsgeräts auf. Das Identifikationsmodul ist datenübertragungstechnisch an das Informations- und/oder Datenverarbeitungsgerät und/oder an das hardwarebasierte Sicherheitsmodul angebunden.

[0016] Dabei ist bevorzug vorgesehen, dass das Identifikationsmodul ein Modul zur Erfassung biometrischer Merkmale, insbesondere passive Merkmale wie Fingerabdruck, Gesicht, Retina, Iris und Handgeometrie und/oder ein Modul zur Erfassung aktive Merkmale: Stimme und/oder Sprechverhalten sowie einer Tastatur zur Eingabe einer Zahlenkombination/ eines PINs ist.

[0017] 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 System mit einem in ein Telefon- und Datennetz eingebundenen mobilen Endgerät und ein hardwarebasierte Sicherheitsmodul zur Authentifizierung des Endgerätes im Netz gemäß einer ersten bevorzugten Ausführungsform der Erfindung und

Fig. 2 ein System mit einem in ein Telefon- und Datennetz eingebundenen mobilen Endgerät und ein hardwarebasierte Sicherheitsmodul zur Authentifizierung des Endgerätes im Netz gemäß einer zweiten bevorzugten Ausführungsform der Erfindung.

[0018] Die **Fig. 1** zeigt ein als mobiles Endgerät **10** ausgebildetes Informations- und/oder Datenverarbeitungsgerät **12**, das über eine Mobilfunkverbindung **14** in ein als Telefon- und/oder Datennetz ausgebildetes Netzwerk **16** eingebunden ist, welches eine Vielzahl von weiteren Informations- und/oder Datenverarbeitungsgeräten **18** umfasst. Das mobile Endgerät **10** ist beispielsweise ein Smartphone. Es weist eine als Luftschnittstelle **20** ausgebildete Schnittstelle **22** auf, über die das mobile Endgerät **10** mit einem hardwarebasierten Sicherheitsmodul **24** verbunden ist. Das hardwarebasierte Sicherheitsmodul **24** weist ein Rechenwerk **26** zur Durchführung kryptografischer Operationen mit zumindest einem Prozessor **28**, eine als Luftschnittstelle **30** zur drahtlosen Kommunikation ausgebildete Schnittstelle **32** und einen Datenspeicher **34** auf, der seinerseits einen über die Schnittstelle **32** unzugänglichen Speicherbereich aufweist, in dem ein kryptografischer Schlüssel **36** für die kryptografischen Operationen abgelegt ist.

[0019] Das gezeigte hardwarebasierte Sicherheitsmodul **24** ist als hardwarebasiertes mobiles Sicherheitsmodul **38** (HMD: hardwarebasiertes, mobiles Device) ausgebildet und weist eine eigene Stromversorgungseinheit **40** auf, die die weiteren Komponenten **26**, **32**, **34** des hardwarebasierten mobilen Sicherheitsmoduls **38** mit elektrischer Energie versorgt. Die Stromversorgungseinheit **40** ist im gezeigten Beispiel ein Akkumulator.

[0020] Die Verbindung zwischen den Luftschnittstellen **20**, **30** (des Gerätes 10,12 und des hardwarebasieren Sicherheitsmoduls **24**) ist im gezeigten Beispiel eine Verbindung mittels drahtloser Datenkommunikation. Die Luftschnittstellen **20**, **30** sind dementsprechend Luftschnittstellen **20**, **30** für drahtlose Datenkommunikation. Neben der Luftschnittstellen **20** weist das mobile Endgerät **10** selbstverständlich auch eine (hier nicht explizit gezeigte) Luftschnittstelle für die Funkverbindung **14** auf. Die kryptografischen Operationen des Rechenwerks **26** sind für die Authentifizierung typische Operationen. Entscheidend ist hier, dass der kryptografische Schlüssel weder über die Schnittstelle **32**, hier also die Luftschnittstelle **30**, in den Speicher **34** geschrieben, noch aus ihm ausgelesen werden kann.

[0021] Das im Beispiel gezeigte Rechenwerk **26** ist zur Durchführung von kryptografischen Operationen (a) zur Authentifizierung des Informations- und/ oder Datenverarbeitungsgeräts **12** gegenüber dem zumindest einen weiteren Informations- und/oder Datenverarbeitungsgerät **18** und andererseits (b) zur Durchführung von kryptografischen Operationen zur

Ver- und/oder Entschlüsselung von Daten bei der Datenübertragung zwischen dem Informations- und/oder Datenverarbeitungsgerät **12** und dem zumindest einen weiteren Informations- und/oder Datenverarbeitungsgerät **18** eingerichtet.

[0022] Die Verwendung eines solchen Sicherheitsmoduls **24** ermöglicht beziehungsweise gewährleistet eine sichere Authentifikation und eine damit verbundene sichere, verschlüsselte Kommunikation von Geräten **10** **12**, wie z.B. Smartphones oder Tablets, in einem Netzwerk **16**, wie z.B. dem Internet. Das hardwarebasierte Sicherheitsmodul und das entsprechende Gerät **10**, **12** bilden ein System **42**. Im Zeitalter von IoT (Internet of Things) und vernetzter Industrieproduktion (Smart Factories), vernetzter Kraftfahrzeuge sowie Smart Home-Anwendungen besteht ein besonderer Bedarf an sicherer Kommunikation über das Internet. Das Sicherheitsmodul **24** ermöglicht es durch die drahtlose Anbindung auf bauliche Veränderungen des Geräts **10**, **12** verzichten zu können und gewährleistet gleichzeitig einen sehr hohen (um nicht zu sagen: den höchsten) Sicherheitsstandard. Das Sicherheitsmodul **24** ist auch geeignet zur sicheren Authentifikation von anderen Informations- und/oder Datenverarbeitungsgeräten **12**, wie etwa Geräten für Kraftfahrzeuge (KFZ) oder Maschinen in einem Netzwerk, wie etwa dem Internet.

[0023] Im Folgenden werden die wichtigsten Eigenschaften und Vorteile diverser Ausgestaltungen des hardwarebasierten Sicherheitsmoduls **24** und des Systems **42** mit Sicherheitsmodul **24** und entsprechendem Gerät **10**, **12** noch einmal mit anderen Worten beschrieben:

[0024] Das Sicherheitsmodul **24** dient der bidirektionalen, drahtlosen, optional auch drahtgebundenen, Kommunikation mit stationären und mobilen Geräten **10**, **12**. Es ist für die Authentifizierung und Datenverschlüsselung von heterogener Hardware, wie z.B. von Smartphones, unterschiedlicher Hersteller unabhängig von den verwendeten Betriebssystemen dieser Geräte **12** nutzbar.

[0025] Zur Sicherung der Kommunikation (z.B. in Unternehmen) im Internet werden sogenannte VPNs (virtuelle private Netzwerke) eingesetzt. Sogenannte „Remote User“ können sich via Internet unter Verwendung von VPNs mit dem Head-office verbinden. Dies geschieht zumeist durch Eingabe eines Kennwortes. Allgemein gilt die Verwendung von VPNs jedoch als nicht wirklich sicher. Firmen bezahlen für VPN-Services, da ihnen der Aufwand zu hoch ist, selber einen VPN-Server zu betreiben. Der Betreiber des VPN-Servers hat gegebenenfalls Zugriff auf die übertragenen Daten und hat Informationen über die Kommunikationspartner. Da es mittlerweile üblich ist, Firmendaten in Clouds zu speichern, muss dem Betreiber dieser Cloud in Bezug auf Datensicherheit besonderes Vertrauen entgegengebracht werden. Bezüglich des Firmen-IP (Intellectual Property) bestehen bei Verwendung von VPN und Clouds deutliche Risiken. Alleine die Kenntnis des Kennwortes, welches z.B. durch Schadsoftware ausgespäht werden kann, ermöglicht einen Zugriff auf die Daten des entsprechenden Mitarbeiters und kann das Firmen Know-How gefährden.

[0026] Heutige Verschlüsselungsverfahren sind in Abhängigkeit des gewählten Verfahrens und einer spezifizierten Schlüssellänge als sicher zu betrachten. Lediglich die zur Verschlüsselung von Daten verwendeten Schlüssel (Keys) **36** ermöglichen eine Dechiffrierung. Demnach werden Hacker oder andere Cyber-Kriminelle versuchen, eben jene Schlüssel zu erlangen. Diese liegen üblicherweise auf den Geräten **10**, **12** der Nutzer. Programme zur Datenverschlüsselung verwenden unterschiedliche Verfahren, um diese Schlüssel zu chiffrieren und zu verstecken. Es ist aber möglich und bereits vorgekommen, dass diese Schlüssel gefunden und dechiffriert wurden. Daher ist die Verschlüsselung von Daten mittels Software als nicht absolut sicher anzusehen.

[0027] Die Nutzung von mobilen Endgeräten **10**, wie z.B. Smartphones, Tablets bzw. Notebooks und Smartwatches mit Zugang zum Internet ist heute üblich. Anders als die meisten Privatanwender setzen Firmen für Firmenrechner und Kommunikationstechnik auf VPNs. Diese Kommunikation ist, wie oben beschrieben, unsicher. Eine deutlichere Verbesserung wird durch das hardwarebasierte Sicherheitsmoduls **24** erreicht. Dieses kommuniziert drahtlos mit mobilen und drahtlosen Geräten **10**, wie z.B. Smartphones, etc.

[0028] Das hardwarebasierte Sicherheitsmoduls **24** weist bevorzugt folgende Komponenten auf:

(i) ein Gehäuse **44**, gegebenenfalls einer Armbanduhr mit integrierten Modulkomponenten **26**, **32**, **34** oder einem Halsband mit Anhänger mit integriertem integrierten Modulkomponenten **26**, **32**, **34** oder einem Namensschild (o. ä.) mit integrierten Modulkomponenten **26**, **32**, **34** oder einem Ring mit integrierten Modulkomponenten **26**, **32**, **34**,

(ii) eine oder mehrere drahtlose, optional auch drahtgebundene Kommunikationsschnittstellen **30**, **32**,

(iii) ein Rechenwerk **26** mit einem oder mehreren Prozessoren **28**, insbesondere zur Verschlüsselung und Steuerung einer Sicherheitsschaltung, die das Auslesen des kryptographischen

Schlüssels **36** (Keys) unmöglich macht bzw. sicher verhindert und

(iv) mechanische und/oder elektronische Vorkehrungen zur Manipulationssicherheit (tamper resistance).

[0029] Das hardwarebasierte Sicherheitsmoduls **24** ermöglicht eine zertifikatlose, optional auch zertifikatsgebundene, Authentifizierung und Datenverschlüsselung in Hardware und Software mit extrem hoher Sicherheit, da der kryptographische Schlüssel **26** im hardwarebasierte Sicherheitsmoduls **24** nicht ausgelesen werden kann und somit eine Dechiffrierung durch Fremde (Hacker) nicht möglich ist.

[0030] Die Verschlüsselung kann in dem Informations- und/oder Datenverarbeitungsgerät **12** oder dem hardwarebasierten Sicherheitsmoduls **24** erfolgen. Dies ist dabei unabhängig vom verwendeten Betriebssystem.

[0031] Die Stromversorgung des hardwarebasierten Sicherheitsmoduls **24** erfolgt mittels Batterie/Akkumulator oder Energieautark unter Ausnutzung zumindest einer der folgenden Techniken: Solarzelle, Wärme(-unterschied), Bewegung wie Vibration, etc. Die Aufladung eines Akkumulators bei Verwendung als Energiequelle erfolgt induktiv, über USB-Stecker oder mechanischer und/oder elektrischer Verbindung. Die Verwendung externer Spannungsquelle ist ebenfalls vorgesehen.

[0032] Um das Verfahren der Authentifizierung sicherer zu machen, kann optional eine Zweiwege-Authentifizierung vorgenommen werden. Die **Fig. 2** zeigt ein entsprechendes System **42**. Die optionale, zusätzliche Freigabe des hardwarebasierte Sicherheitsmoduls **24** erfordert die Implementierung von einem Modul **46** zur Erfassung biometrischer Merkmale, insbesondere passive Merkmale wie Fingerabdruck, Gesicht, Retina, Iris und Handgeometrie und/oder aktive Merkmale: Stimme und/oder Sprechverhalten sowie einer Tastatur zur Eingabe einer Zahlenkombination/eines PINs. Das Modul ist also ein Identifikationsmodul **46** zur Identifikation eines Nutzers des Geräts **10**, **12**. Das in **Fig. 2** gezeigte Identifikationsmodul **46** ist ein Fingerabdruck-Scanner. Das Identifikationsmodul **46** weist eine Schnittstelle **48** auf, die mit einer weiteren Schnittstelle **50** des Informations- und/oder Datenverarbeitungsgeräts **12** datenübertragungstechnisch verbunden ist. Das Modul **46** zur Erfassung biometrischer Merkmale ist alternativ direkt in das Informations- und/oder Datenverarbeitungsgerät **12** und/oder in das hardwarebasierte Sicherheitsmodul **24** integriert.

[0033] Mobile und stationäre Geräte **10**, **12**, welche sich über eine Luftschnittstelle/hardwaregebundene Schnittstelle mit dem hardwarebasierten Sicherheitsmodul **24** verbinden können, können mit höchster Sicherheit in Netzwerke eingebunden werden. Der Austausch gesicherter Daten kann durch den Nutzer des hardwarebasierten Sicherheitsmoduls **24** auch in Gruppen erfolgen. Auf Basis einer Software (App) können andere Nutzer, welche gegebenenfalls auch ein hardwarebasiertes Sicherheitsmodul **24** verwenden, in eine Gruppe aufgenommen werden. Die Kommunikation kann im Funk- und Empfangsbereich des oder der hardwarebasierten Sicherheitsmodule **24** erfolgen. Ein entsprechendes Vorgehen ist beispielsweise aus dem Dokument EP 2 937 802 A bekannt. Im Gegensatz zu dem in diesem Dokument beschriebenen Ansatz müssen die mobilen Endgeräte **10** Zwecks sicherem Datenaustausch dabei aber nicht aufeinandergelegt werden.

[0034] Zusätzlich können die Nutzer des hardwarebasierte Sicherheitsmoduls **24** einer Gruppe sicheren Datenaustausch über das Netzwerk **16** vornehmen. Dabei spielt der Standort der Gruppenmitglieder keine Rolle, solange ein Netzwerkzugriff möglich ist.

[0035] Durch die Funkanbindung des hardwarebasierte Sicherheitsmoduls **24** an das Informations- und/oder Datenverarbeitungsgerät **12** wird die Haptik des verwendeten mobilen und stationären Geräts **10**, **12** nicht geändert. Der Nutzer merkt von dem hardwarebasierten Sicherheitsmodul **24** nichts, ist aber umfassend geschützt. Das hardwarebasierte Sicherheitsmodul **24** (HMD) kann man in der Tasche tragen oder in eine Uhr implementieren. Das Gerät **10**, **12**, bei welchem eine sichere Kommunikation und/oder ein sicherer Datentransfer, beispielsweise per Email, etc., durch das hardwarebasierte Sicherheitsmodul **24** ermöglicht wird, wird in seiner Form, Gewicht und Bedienung nicht verändert.

Bezugszeichenliste

10	mobiles Endgerät
12	Informations- und/oder Datenverarbeitungsgerät
14	Mobilfunkverbindung
16	Netzwerk
18	anderes Informations- und/oder Datenverarbeitungsgerät
20	Luftschnittstelle
22	Schnittstelle (Gerät)
24	hardwarebasiertes Sicherheitsmodul
26	Rechenwerk
28	Prozessoreinheit
30	Luftschnittstelle
32	Schnittstelle
34	Datenspeicher

36 kryptografischer Schlüssel

38 mobiles Sicherheitsmodul

40 Stromversorgungseinheit

42 System

44 Gehäuse

46 Identifikationsmodul

48 Schnittstelle

50 Schnittstelle

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- EP 2937802 A [0033]

Patentansprüche

1. Hardwarebasiertes Sicherheitsmodul (24) zur Authentifizierung eines Informations- und/oder Datenverarbeitungsgeräts (12), insbesondere eines mobilen Endgeräts (10), gegenüber zumindest einem weiteren Informations- und/oder Datenverarbeitungsgerät (18), welches mit dem einen Informations- und/oder Datenverarbeitungsgerät (12), insbesondere über ein Netzwerk (16), datenübertragungstechnisch - drahtlos oder drahtgebunden - verbunden ist, mit
- einem Rechenwerk (26) zur Durchführung von kryptografischen Operationen zur Authentifizierung des Informations- und/oder Datenverarbeitungsgeräts (12),
- zumindest einer als Luftschnittstelle (30) ausgebildeten Schnittstelle (32) zur datenübertragungstechnischen Anbindung des hardwarebasierten Sicherheitsmoduls (24) an das Informations- und/oder Datenverarbeitungsgerät (12) und
- einem Datenspeicher (34), der einen über diese zumindest eine Schnittstelle (32) unzugänglichen Speicherbereich zur Ablage zumindest eines kryptografischen Schlüssels (36) für die kryptografischen Operationen aufweist.

2. Sicherheitsmodul nach Anspruch 1, **dadurch gekennzeichnet**, dass das Rechenwerk (26) weiterhin zur Durchführung von kryptografischen Operationen zur Ver- und/oder Entschlüsselung von Daten bei der Datenübertragung zwischen dem Informations- und/oder Datenverarbeitungsgerät (12) und dem zumindest einen weiteren Informations- und/oder Datenverarbeitungsgerät eingerichtet ist.

3. Sicherheitsmodul nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass die Luftschnittstelle (30) als Luftschnittstelle (30) für drahtlose Datenkommunikation und/oder für drahtlose Netzwerke, insbesondere auch drahtlose Sensornetzwerke, bevorzugt für
- Bluetooth und/oder
- WLAN und/oder
- Nahfeldkommunikation und/oder
- Zigbee und/oder
- proprietäre Datenübertragungssysteme ausgebildet ist.

4. Sicherheitsmodul nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass das hardwarebasierte Sicherheitsmodul (24) als hardwarebasiertes mobiles Sicherheitsmodul (38) ausgebildet ist.

5. Sicherheitsmodul nach Anspruch 4, **dadurch gekennzeichnet**, dass das mobile Sicherheitsmodul (38) eine eigene Stromversorgungeinheit (40), insbesondere einen Akkumulator, aufweist.

6. Sicherheitsmodul nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, dass das es in einem vom Informations- und/oder Datenverarbeitungsgerät (12) separaten anderen Gerät integriert ist.

7. System (42) mit einem Informations- und/oder Datenverarbeitungsgerät (12), insbesondere einem mobilen Endgerät (10), und einem hardwarebasierten Sicherheitsmodul (22) nach einem der Ansprüche 1 bis 6.

8. System nach Anspruch 7, **gekennzeichnet durch** ein Identifikationsmodul (46) zur Identifikation des Nutzers des Informations- und/oder Datenverarbeitungsgeräts (12).

9. Sicherheitssystem nach Anspruch 8, **dadurch gekennzeichnet**, dass das Identifikationsmodul (46) ein Modul zur Erfassung biometrischer Merkmale, insbesondere passive Merkmale wie Fingerabdruck, Gesicht, Retina, Iris und Handgeometrie und/oder ein Modul zur Erfassung aktive Merkmale: Stimme und/oder Sprechverhalten sowie einer Tastatur zur Eingabe einer Zahlenkombination/eines PINs ist.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen

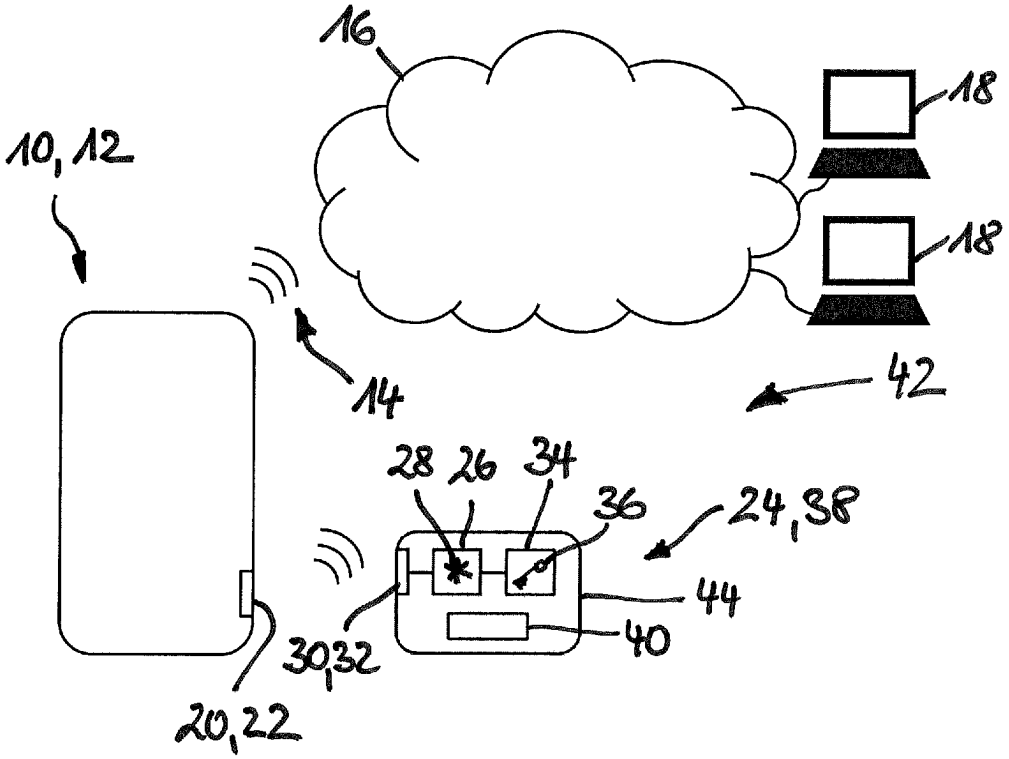


Fig. 1

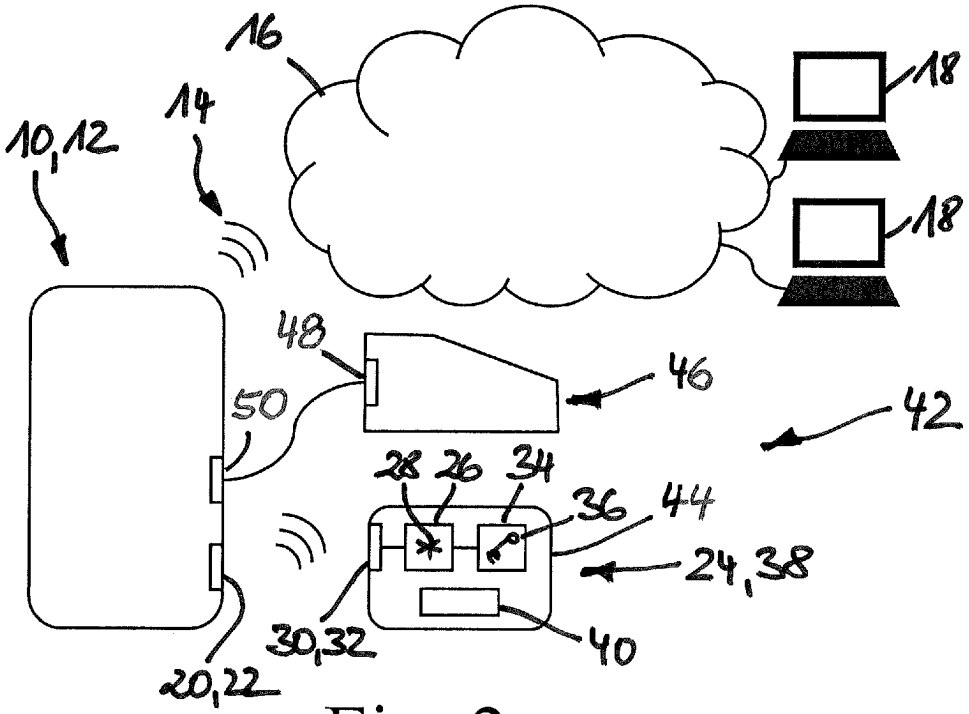


Fig. 2