(19) Deutsches Patent- und Markenamt

(10) **DE 10 2016 221 699 A1** 2018.05.09

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2016 221 699.6**
(22) Anmeldetag: **04.11.2016**
(43) Offenlegungstag: **09.05.2018**

(51) Int Cl.: ***G06F 21/64*** (2013.01)
G06Q 50/10 (2012.01)

(71) Anmelder:
Bundesdruckerei GmbH, 10969 Berlin, DE

(74) Vertreter:
Richardt Patentanwälte PartG mbB, 65185 Wiesbaden, DE

(72) Erfinder:
Dietrich, Frank, 12437 Berlin, DE; Fritze, Frank, 12437 Berlin, DE

(56) Ermittelter Stand der Technik:

US	**2003 / 0 028 494**	**A1**
US	**2015 / 0 071 486**	**A1**
US	**2016 / 0 306 982**	**A1**
WO	**2016/ 179 334**	**A1**

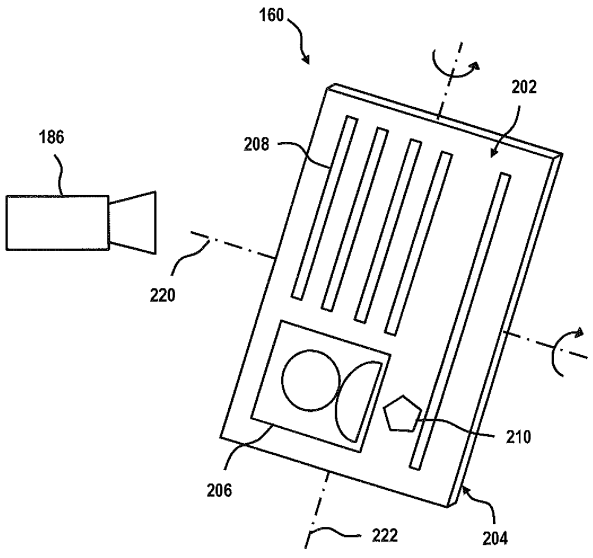
AMATI, Franco: Using the blockchain as a digital signature scheme. In: Signatura Blog, 1. Januar 2016. URL: https://blog.signatura.co/using-the-blockchain-as-a-digital-signature-scheme-f584278ae826 [abgerufen am 30. August 2017]

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren zum Ausstellen einer virtuellen Version eines Dokuments**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Ausstellen einer virtuellen Version (164, 408) eines Dokuments (160) durch ein erstes Computersystem (100) eines ID-Providers, wobei das Dokument (160) eine visuelle Widergabe eines Datensatzes aufweist. Das Verfahren umfasst:
Erstellen des virtuellen Dokuments (164, 408) als virtueller Version des Dokuments (160), welches eine elektronische Kopie des Datensatzes des Dokuments (160) umfasst,
Berechnen eines Hashwerts des virtuellen Dokuments (164, 408),
Signieren des Hashwerts mit einem privaten Schlüssel (106) eines dem Austeller des virtuellen Dokuments (164, 408) zugeordneten asymmetrischen Schlüsselpaars,
Speichern des signierten Hashwerts in einem Eintrag in einer kryptographisch gesicherten Datenbank (110) zur Ausstellung des virtuellen Dokuments (164, 408),
Senden des virtuellen Dokuments (164, 408) an einen Besitzer (150) des Dokuments (160) zusammen mit einer Speicher-ID des virtuellen Dokuments (164, 408), wobei die Speicher-ID den Eintrag der Datenbank (110) mit dem signierten Hashwert des virtuellen Dokuments (164, 408) identifiziert.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Ausstellen einer virtuellen Version eines Dokuments sowie ein Computerprogrammprodukt und ein Computersystem zur Ausführung des Verfahrens.

[0002] Eine Echtheitsprüfung eines elektronischen Dokuments, insbesondere eines hoheitlichen Ausweisdokuments wie etwa eines elektronischen Personalausweises oder eines elektronischen Reisepasses, erfolgt üblicher Weise mittels zentraler Serversysteme die über eine Internetverbindung erreichbar sind.

[0003] Heutige eID-Systeme basieren im Allgemeinen auf dem Ansatz eines 3-Parteien-Systems: Eine erste Partei, welche eine Identifikation einer zweiten Partei fordert, eine zu identifizierende zweite Partei und eine die Identifizierung ausführende dritte Partei, der ID-Provider.

[0004] Die sogenannte eID-Funktion dient insbesondere dem sicheren Identitätsnachweis per Internet. Die eID-Funktion wird von Dienstanbietern in ihre Web-Angebote, d.h. ihre Dienste, integriert und kann dann je nach Bedarf beispielsweise von Ausweisinhabern, deren Ausweis die eID-Funktion unterstützt, genutzt werden. So lassen sich beispielsweise Behördengänge, bei welchen eine sichere Identitätsfeststellung per Sichtprüfung eines Ausweisdokumentes wie z. B. dem Personalausweis realisiert wird, durch die eID-Funktion ersetzen. Die Verwendung dieser Systeme setzt jedoch eine bestehende Internetverbindung voraus.

[0005] Eine Onlineverbindung zu solchen zentralen Serversystemen ist allerdings nicht immer gegeben. Insbesondere bei einer Echtheitsprüfung mittels mobiler Geräte, wie sie etwa bei einer Verkehrskontrolle notwendig ist, kann es zu Störungen oder gar einem völligen Fehlen einer Verbindung zu einem entsprechenden mobilen Netzwerk kommen.

[0006] Ferner ist es bei elektronischen Dokumenten mit hohen Anforderungen an deren Authentizitätssicherung, wie etwa bei hoheitlichen Ausweisdokuments, üblich diese Dokumente eigenständige physische Körper mit entsprechender Elektronik zum Auslesen von Daten bereitzustellen. Dies macht es jedoch notwendig, dass man unter Umständen eine Vielzahl unterschiedlicher physischer Dokumente mit sich führen muss. Eine solche Vielzahl physischer Dokumente ist aber zum einen unhandlich und zum anderen besteht eine hohe Wahrscheinlichkeit, dass einzelne oder alle Dokumente zu Hause liegengelassen werden und damit nicht zur Hand sind, wenn man sie benötigt.

[0007] Der Erfindung liegt demgegenüber die Aufgabe zugrunde, ein effizientes und sicheres Verfahren zum Ausstellen einer virtuellen Version eines Dokuments zu schaffen, welche insbesondere eine Offline-Echtheitsprüfung des Dokuments ermöglicht.

[0008] Die der Erfindung zugrundeliegende Aufgabe wird jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Ausführungsformen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

[0009] Ausführungsformen umfassen ein Verfahren zum Ausstellen einer virtuellen Version eines Dokuments durch ein erstes Computersystem eines ID-Providers. Das Dokument weist eine visuelle Widergabe eines Datensatzes auf. Das Verfahren umfasst:

- Erstellen des virtuellen Dokuments als virtueller Version des Dokuments, welches eine elektronische Kopie des Datensatzes des Dokuments umfasst,
- Berechnen eines Hashwerts des virtuellen Dokuments,
- Signieren des Hashwerts mit einem privaten Schlüssel eines dem Austeller des virtuellen Dokuments zugeordneten asymmetrischen Schlüsselpaars,
- Speichern des signierten Hashwerts in einem Eintrag in einer kryptographisch gesicherten Datenbank zur Ausstellung des virtuellen Dokuments,
- Senden des virtuellen Dokuments an einen Besitzer des Dokuments zusammen mit einer Speicher-ID des virtuellen Dokuments, wobei die Speicher-ID den Eintrag der Datenbank mit dem signierten Hashwert des virtuellen Dokuments identifiziert.

[0010] Ausführungsformen können den Vorteil haben, dass ein sicheres und effizientes Verfahren zum Ausstellen eines virtuellen Dokuments auf Basis eines physischen Dokuments bereitgestellt wird. Dabei umfasst das virtuelle Dokument den gleichen Datensatz wie das zugrundeliegende physische Dokument. Die Authentizität des entsprechenden Datensatzes und damit des virtuellen Dokuments wird durch das zuvor definierte Verfahren sichergestellt und beruht damit auf der Authentizität des zugrundeliegenden physischen Dokuments. Ist das virtuelle Dokument erst einmal erstellt und seine Authentizität von dem Computersystem des ID-Providers durch Eintrag in die kryptographisch gesicherte Datenbank bestätigt, so besitzt das virtuelle Dokument unabhängig von dem physischen Dokument Gültigkeit. Mit anderen Worten ist für eine Echtheitsprüfung des virtuellen Dokuments lediglich eine Prüfung des in der kryptographischen Datenbank eingetragenen Hashwerts notwendig. Es ist insbesondere keine zusätzli-

che Prüfung des physischen Dokuments ist notwendig.

[0011] Ausführungsformen können den Vorteil haben, dass durch die Verwendung eines virtuellen Dokuments die Bindung an einen spezifischen physischen Dokumentenkörper entfällt. Die Echtheit des virtuellen Dokuments ergibt sich alleine aus der Übereinstimmung seines Hashwerts mit dem in der Datenbank als authentisch hinterlegten und gesicherten Hashwert. Somit ist es nach Ausführungsformen möglich eine Mehrzahl von Dokumenten in virtueller Form auf einem einzigen elektronischen Gerät, insbesondere einem handlichen und tragbaren Gerät wie etwa einem Smartphone, zu speichern.

[0012] Bei dem zweiten Computersystem handelt es sich um ein stationäres oder mobiles, insbesondere ein tragbares, Gerät. Bei einem solchen Computersystem kann es sich beispielsweise um ein mobiles Telekommunikationsgerät, insbesondere ein Smartphone, einen tragbaren Computer, wie zum Beispiel einen Laptop oder Palmtop-Computer, einen Personal Digital Assistant oder dergleichen handeln. Ferner kann es sich um ein stationäres Computersystem, wie beispielsweise einen Personalcomputer. Bei dem ersten Computersystem handelt es sich vorzugsweise um ein stationäres Computersystem, beispielsweise um einen Server.

[0013] Ein Computer bzw. Computersystem kann eine Schnittstelle zur Verbindung mit einem Netzwerk umfassen, wobei es sich bei dem Netzwerk um ein privates oder öffentliches Netzwerk handeln kann, insbesondere das Internet. Je nach Ausführungsform kann diese Verbindung auch über ein Mobilfunknetz hergestellt werden.

[0014] Unter einer „Datenbank“ wird hier allgemein eine Zusammenstellung von Daten in Form von Datenbankeinträgen gemäß einer festgelegten Organisationsstruktur der Datenbank verstanden. Eine Datenbank kann zudem ein Verwaltungsprogramm zum Verwalten der Datenbank umfassen. Unter einer kryptographisch gesicherten Datenbank wird eine Datenbank verstanden, deren Einträge kryptographisch gesichert sind. Beispielsweise umfasst die Datenbank verschlüsselte und/oder signierte Daten. Unter einer kryptographisch gesicherten Datenbank wird hier insbesondere eine Blockchain verstanden.

[0015] Unter einem „Zertifikat“ wird hier ein digitales Zertifikat verstanden, welches auch als Public-Key-Zertifikat bezeichnet wird. Im Folgenden werden „digitale“ Objekte auch als „virtuelle“ Objekte bezeichnet, d.h. Datenkonstrukte zur elektronischen Datenverarbeitung. Durch solche Zertifikate basierend auf asymmetrischen Schlüsselpaaren wird eine so genannte Public Key Infrastructure (PKI) realisiert. Bei einem solchen Zertifikat handelt es sich um strukturierte Daten, die dazu dienen, einen öffentlichen Schlüssel eines asymmetrischen Kryptosystems einer Identität, wie zum Beispiel einer Person oder einer Vorrichtung, zuzuordnen. Ein Zertifikat kann beispielsweise einen öffentlichen Schlüssel beinhalten und signiert sein. Alternativ sind auch Zertifikate basierend auf zero-knowledge Kryptosystemen möglich. Beispielsweise kann das Zertifikat dem Standard X.509 oder einem anderen Standard entsprechen. Beispielsweise handelt es sich bei dem Zertifikat um ein CV-Zertifikat oder auch Card Verifiable Certificate (CVC). Eine Implementierung von solchen CVCs ist beispielsweise in der ISO/IEC 7816-8 spezifiziert.

[0016] Die PKI stellt ein System zum Ausstellen, Verteilen und Prüfen digitaler Zertifikate. Ein digitales Zertifikat dient in einem asymmetrischen Kryptosystem dazu die Authentizität eines öffentlichen Schlüssels und seinen zulässigen Anwendungs- und Geltungsbereich zu bestätigen. Das digitale Zertifikat ist selbst durch eine digitale Signatur geschützt, deren Echtheit mit dem öffentlichen Schlüssel des Ausstellers des Zertifikates geprüft werden kann. Um die Authentizität des Ausstellerschlüssels zu prüfen, wird wiederum ein digitales Zertifikat verwendet. Auf diese Weise lässt sich eine Kette von digitalen Zertifikaten aufbauen, die jeweils die Authentizität des öffentlichen Schlüssels bestätigen, mit dem das vorhergehende Zertifikat geprüft werden kann. Eine solche Kette von Zertifikaten bildet einen sogenannten Validierungspfad oder Zertifizierungspfad. Auf die Echtheit des letzten Zertifikats, des sogenannten Wurzelzertifikats, und des durch dieses Zertifikat zertifizierten Schlüssels, müssen sich die Teilnehmer der PKI ohne ein weiteres Zertifikat verlassen können. Das Wurzelzertifikat wird von einer sogenannten Wurzelzertifizierungsinstanz verwaltet, auf deren als gesichert vorausgesetzten Authentizität die Authentizität aller Zertifikate der PKI zurückgeht.

[0017] Digitale Zertifikate sind bei der Absicherung elektronischer Kommunikation durch asymmetrische kryptographische Verfahren ein bewährtes Mittel um Berechtigungen nachzuweisen. Zertifikate sind strukturierte Daten, die die Authentizität und/oder weitere Eigenschaften/Berechtigungen des Eigentümers eines öffentlichen Schlüssels (Signaturprüfschlüssel) dokumentieren und durch eine unabhängige, glaubwürdige Instanz (Zertifizierungsdienstanbieter/ZDA), im Allgemeinen die das Zertifikat zuteilende Zertifizierungsstelle, bestätigen. Zertifikate werden in der Regel einem breiten Personenkreis zur Verfügung gestellt um diesem eine Prüfung elektronischer Signaturen auf Authentizität und Gültigkeit zu ermöglichen.

[0018] Ein Zertifikat kann einer elektronischen Signatur zugeordnet sein, wenn der zu dem öffentlichen Schlüssel gehörende private Schlüssel zur Generierung der zu prüfenden elektronischen Signatur verwendet wurde. Dadurch, dass ein ZDA ein Zertifikat in

Assoziation mit einem öffentlichen Schlüssel der Allgemeinheit zur Verfügung stellt, ermöglicht ein ZDA den Nutzern asymmetrischer Kryptosysteme den öffentlichen Schlüssel einer Identität, beispielsweise einer Person, einer Organisation oder Computersystem, zuzuordnen.

[0019] Asymmetrische Schlüsselpaare werden für eine Vielzahl von Kryptosystemen eingesetzt und spielen auch bei der Signatur elektronischer Dokumente eine wichtige Rolle. Ein asymmetrisches Schlüsselpaar besteht aus einem öffentlichen Schlüssel, welcher zur Ver- und/oder Entschlüsselung von Daten verwendet wird und an Dritte, beispielsweise an einen Dienstanbieter und/oder einen ZDA, weitergegeben werden darf sowie einem privaten Schlüssel, welcher zur Ver- und/oder Entschlüsselung von Daten verwendet wird und im Regelfall geheim gehalten werden muss. Der öffentliche Schlüssel ermöglicht es jedermann, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln, digitale Signaturen von dessen Dokumenten zu prüfen oder ihn zu authentifizieren. Ein privater Schlüssel ermöglicht es seinem Inhaber, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln oder digitale Signaturen für elektronische Dokumente zu erstellen. Eine mit einem privaten Schlüssel erstellte Signatur kann mit dem zugehörigen öffentlichen Schlüssel verifiziert werden.

[0020] Digitale Signaturen werden zum sicheren elektronischen Datenaustausch, beispielsweise im Internet, eingesetzt und ermöglichen die Prüfung von Identitäten und/oder Berechtigungen und der Unverfälschtheit der ausgetauschten Daten. Um dies zu gewährleisten, ist in der Regel eine Public-Key-Infrastruktur notwendig, die die Gültigkeit der verwendeten Schlüssel durch Zertifikate bestätigt.

[0021] Die Erstellung einer digitalen Signatur, im Folgenden auch lediglich als „Signatur“ bezeichnet, ist ein kryptographisches Verfahren, bei dem zu beliebigen Daten, zum Beispiel einem elektronischen Dokument, ein weiterer Datenwert, welcher als „Signatur“ bezeichnet wird, berechnet wird. Die Signatur kann zum Beispiel ein verschlüsselter Hashwert des elektronischen Dokumentes sein, insbesondere ein mit einem privaten Schlüssel eines einem Zertifikat zugeordneten kryptographischen Schlüsselpaares verschlüsselter Hashwert. Ein entsprechendes Verschlüsseln eines Hashwerts wird mithin als Signieren des Hashwerts bezeichnet. Die Besonderheit einer solchen Signatur besteht darin, dass deren Urheberschaft und Zugehörigkeit zu einer bestimmten Person oder Instanz durch jeden Dritten geprüft werden kann.

[0022] Unter einer digitalen Signatur wird hier auch ein digitales Siegel verstanden, welches nicht einer natürlichen Person, sondern einer juristischen Person zugeordnet ist. Ein digitales Siegel dient somit nicht der Abgabe einer Willenserklärung einer einzelnen Person, sondern einer Institution als Herkunftsnachweis. Es kann somit den Ursprung und die Unversehrtheit virtueller Dokumente sicherstellen und nachweisen, dass diese von einer bestimmten juristischen Person stammen.

[0023] Unter einem „Speicher“ werden hier sowohl flüchtige als auch nicht flüchtige elektronische Speicher bzw. digitale Speichermedien verstanden.

[0024] Unter einem „nichtflüchtigen Speicher“ wird hier ein elektronischer Speicher zur dauerhaften Speicherung von Daten verstanden. Ein nichtflüchtiger Speicher kann als nichtänderbarere Speicher konfiguriert sein, der auch als Read-Only Memory (ROM) bezeichnet wird, oder als änderbarer Speicher, der auch als Non-Volatile Memory (NVM) bezeichnet wird. Insbesondere kann es sich hierbei um ein EEPROM, beispielsweise ein Flash-EEPROM, kurz als Flash bezeichnet, handeln. Ein nichtflüchtiger Speicher zeichnet sich dadurch aus, dass die darauf gespeicherten Daten auch nach Abschalten der Energieversorgung erhalten bleiben.

[0025] Unter einem „flüchtigen elektronischen Speicher“ wird hier ein Speicher zur vorübergehenden Speicherung von Daten, welcher dadurch gekennzeichnet ist, dass alle Daten nach dem Abschalten der Energieversorgung verloren gehe. Insbesondere kann es sich hierbei um einen flüchtigen Direktzugriffsspeicher, der auch als Random-Access Memory (RAM) bezeichnet wird, oder einen flüchtigen Arbeitsspeicher des Prozessors handeln.

[0026] Unter einem „geschützten Speicherbereich“ wird hier ein Bereich eines elektronischen Speichers verstanden, auf den ein Zugriff, das heißt ein Lesezugriff oder ein Schreibzugriff, nur über einen Prozessor des entsprechenden elektronischen Geräts möglich ist. Nach Ausführungsformen ist der Zugriff von dem mit dem Speicher gekoppelten Prozessor nur dann möglich, wenn eine hierzu erforderliche Bedingung erfüllt ist. Hierbei kann es sich zum Beispiel um eine kryptografische Bedingung, insbesondere eine erfolgreiche Authentisierung und/oder eine erfolgreiche Berechtigungsprüfung, handeln.

[0027] Unter einem „Prozessor“ wird hier und im Folgenden eine Logikschaltung verstanden, die zur Ausführung von Programminstruktionen dient. Die Logikschaltung kann auf einem oder mehreren diskreten Bauelementen implementiert sein, insbesondere auf einem Chip. Insbesondere wird unter einem „Prozessor“ ein Mikroprozessor oder ein Mikroprozessorsystem aus mehreren Prozessorkernen und/oder mehreren Mikroprozessoren verstanden.

[0028] Unter einer „Schnittstelle“ wird hier eine Schnittstelle verstanden, über die Daten empfangen und gesendet werden können, wobei die Kommunikationsschnittstelle kontaktbehaftet oder kontaktlos konfiguriert sein kann. Bei der Kommunikationsschnittstelle kann es sich um eine interne Schnittstelle oder um eine externe Schnittstelle handeln, welche beispielsweise mittels eines Kabels oder kabellos mit einem zugeordneten Gerät verbunden ist.

[0029] Eine Kommunikation kann beispielsweise über ein Netzwerk erfolgen. Unter einem „Netzwerk“ wird hier jedes Übertragungsmedium mit einer Anbindung zur Kommunikation verstanden, insbesondere eine lokale Verbindung oder ein lokales Netzwerk, insbesondere ein Local Area Network (LAN), ein privates Netzwerk, insbesondere ein Intranet, und ein virtuelles privates Netzwerk (Virtual Private Network - VPN). Beispielsweise kann ein Computersystem eine Standardfunkschnittstelle zur Anbindung an ein WLAN aufweisen. Ferner kann es sich um ein öffentliches Netzwerk, wie beispielsweise das Internet handeln. Je nach Ausführungsform kann diese Verbindung auch über ein Mobilfunknetz hergestellt werden.

[0030] Unter einem „Dokument“ wird insbesondere ein Ausweis-, Wert- oder Sicherheitsdokument, insbesondere ein hoheitliches Dokument, insbesondere ein papierbasiertes und/oder kunststoffbasiertes Dokument, wie zum Beispiel ein elektronisches Ausweisdokument, insbesondere Reisepass, Personalausweis, Visum, Führerschein, Fahrzeugschein, Fahrzeugbrief, Gesundheitskarte, oder einen Firmenausweis, oder eine anderes ID-Dokument, eine Chipkarte, Zahlungsmittel, insbesondere Banknote, Bankkarte oder Kreditkarte, Frachtbrief oder ein sonstiger Berechtigungsnachweis verstanden. Insbesondere kann es sich bei dem Dokument um ein Machine-Readable Travel Document, wie beispielsweise von der Internationalen Luftfahrtbehörde (ICAO) und/oder dem BSI standardisiert, handeln.

[0031] Unter einem „virtuellen“ Dokument wird ein Datenkonstrukt zur elektronischen Datenverarbeitung verstanden, welches dieselben Daten wie ein zuvor definiertes Dokument, jedoch keinen fest zugeordneten physischen Dokumentenkörper umfasst. Insbesondere ist die Gültigkeit eines solchen Dokuments unabhängig von dem Vorhandensein eines fest zugeordneten Dokumentenkörpers. Bei einem „virtuellen“ Dokument kann es sich um eine elektronische Datei eines beliebigen Dateiformats handeln, insbesondere eine nicht ausführbare Text- oder Tabellendatei.

[0032] Unter einem „Programm“ bzw. „Programminstruktionen“ wird hier ohne Einschränkung jede Art von Computerprogramm verstanden, weiches maschinenlesbare Instruktionen zur Steuerung einer Funktionalität des Computers umfasst.

[0033] Ein „Sicherheitsmodul“ stellt kryptographische Kernroutinen in Form von kryptographischen Programminstruktionen mit kryptographischen Algorithmen für Signaturerstellung und -prüfung, Schlüsselgenerierung, Schlüsselaushandlung, Verschlüsselung und Entschlüsselung von Daten sowie Zufallszahlengenerierung bereit und dient als sicherer Speicher für kryptographisches Schlüsselmaterial.

[0034] Bei dem Sicherheitsmodul kann es sich beispielsweise um einen geschützten Mikrocontroller handeln, d.h. einen Mikrocontroller mit physikalisch beschränkten Zugriffsmöglichkeiten. Zudem kann das Sicherheitsmodul zusätzliche Maßnahmen gegen Missbrauch aufweisen, insbesondere gegen unberechtigte Zugriffe auf Daten im Speicher des Sicherheitsmoduls. Beispielsweise umfasst ein Sicherheitsmodul Sensoren zur Überwachung des Zustands des Sicherheitsmoduls sowie von dessen Umgebung, um Abweichungen vom Normalbetrieb zu erkennen, welche auf Manipulationsversuche hinweisen können. Entsprechende Sensortypen umfassen beispielweise einen Taktfrequenzsensor, einen Temperatursensor, einen Spannungssensor, und/oder einen Lichtsensor. Taktfrequenzsensoren, Temperatursensoren und Spannungssensoren erfassen beispielweise Abweichungen der Taktfrequenz, Temperatur und/oder Spannung nach oben oder unten von einem vordefinierten Normalbereich. Insbesondere kann ein Sicherheitsmodul nichtflüchtige Speicher mit einem geschützten Speicherbereich umfassen.

[0035] Durch die Mittel zum Schutz gegen unbefugte Manipulationen wird durch technische Maßnahmen die Vertrauenswürdigkeit des Sicherheitsmoduls, das heißt seine Funktion als „Vertrauensanker“, gewährleistet. Beispielsweise wird das Sicherheitsmodul von einer vertrauenswürdigen Institution, wie z.B. durch ein Trust-Center (Trust Service Provider), konfiguriert und mit dem benötigten kryptografischen Schlüsselmaterial versehen. Durch die Mittel zum Schutz gegen unbefugte Manipulationen kann sichergestellt werden, dass sicherheitsrelevante Funktionalitäten des Sicherheitsmoduls nicht modifiziert werden.

[0036] Beispielsweise sind zumindest Teile des Sicherheitsmoduls signiert, wie z.B. Programmkomponenten und/oder Hardwarekomponenten, die eine digitale Signatur tragen können. Insbesondere können das Betriebssystem, das Binary Input Output System (BIOS), eine Konfigurationsdatei und/oder ein Speicher des Sicherheitsmoduls digital signiert sein. Vor einer Nutzung des Sicherheitsmoduls wird geprüft, ob die Signatur bzw. die Signaturen, valide sind. Wenn eine der Signaturen nicht valide ist, wird die Nutzung des Sicherheitsmoduls und/oder des durch das Si-

cherheitsmodul gesicherten elektronischen Systems gesperrt.

[0037] Nach Ausführungsformen beinhalten die Mittel zum Schutz des Sicherheitsmoduls gegen unbefugte Manipulationen mechanische Mittel, die z.B. das Öffnen des Sicherheitsmoduls oder seiner Teile verhindern sollen, oder die bei dem Versuch eines Eingriffs in das Sicherheitsmodul dieses unbrauchbar machen, beispielsweise indem ein Datenverlust eintritt. Beispielsweise können hierzu sicherheitskritische Teile des Sicherheitsmoduls in Epoxidharz eingegossen sein, wobei ein Versuch, eine betreffende Komponente aus dem Epoxidharz zu entfernen, zu einer unvermeidlichen Zerstörung dieser Komponente führt.

[0038] Des Weiteren kann ein Sicherheitsmodul Mittel zur kryptographischen Datensicherung umfassen, insbesondere in dem geschützten Speicherbereich, wie beispielsweise einen Zufallszahlengenerator, einen Generator für kryptographische Schlüssel, einen Hashgenerator, ein Ver-/Entschlüsselungsmodul, ein Signaturmodul, Zertifikate, und/oder einen oder mehrere nicht migrierbare kryptographische Schlüssel.

[0039] Nach Ausführungsformen weisen das erste und/oder das zweite Computersystem ein Sicherheitsmodul auf. Ausführungsformen können den Vorteil haben, dass das Sicherheitsmodul Mittel zur effizienten kryptographischen Datensicherung, insbesondere zur Sicherung der Datenübertragung zwischen den beiden elektronischen Geräten, bereitstellt.

[0040] Nach Ausführungsformen handelt es sich bei der kryptographisch gesicherten Datenbank um eine auf einer Mehrzahl von Knoten eines Netzwerks redundant gespeicherte Datenbank. Somit liegt die kryptographisch gesicherte Datenbank redundant und dezentral auf einer Mehrzahl von Computersystemen vor. Eine Änderung der kryptographisch gesicherten Datenbank durch das Computersystem eines ID-Providers wird an die anderen Computersysteme des Netzwerks übertragen. Das Netzwerk kann beispielsweise als ein Peer-to-Peer-Netzwerk ausgestaltet sein oder auf einer Client-Server-Struktur beruhen, wobei das Computersystem eines ID-Providers als Server konfiguriert ist. Durch die redundante und dezentrale Speicherung der kryptographisch gesicherten Datenbank kann selbst bei einer Unterbrechung der Netzwerkverbindung sichergestellt werden, dass alle Netzwerkknoten Zugriff auf die kryptographisch gesicherte Datenbank besitzen. Dies gilt insbesondere auch im Falle eines zentralisierten Netzwerks mit Client-Server-Struktur, da bei einer redundanten Speicherung der Datenbank auf allen Clients jeder der Clients über eine Kopie der kryptographisch gesicherten Datenbank verfügen.

[0041] Ausführungsformen können den Vorteil haben, dass während einer Prüfung der Echtheit des virtuellen Dokuments durch ein drittes Computersystem, auf welchem eine redundante Kopie der kryptographisch gesicherten Datenbank gespeichert ist, keine Netzwerkverbindung zu dem Computersystem des ID-Providers als einem entfernten zentralen Serversystem bestehen muss. Die Echtheitsprüfung erfolgt vielmehr unter Verwendung der lokal auf dem dritten Computersystem gespeicherten Datenbank. Da die Datenbank zur Echtheitsprüfung virtueller Dokument nur deren als authentisch anerkannten Hashwerte umfasst, kann die Datenbank selbst im Falle einer großen Anzahl virtueller Dokumente eine kompakte Größe aufweisen, sodass nach Ausführungsformen weder spezielle Speichermedien zum Speichern großer Datenmengen noch aufwendige Datenbanksoftwarelösungen zur effizienten Handhabung großer Datenbanken notwendig sind.

[0042] Da in der Datenbank nur Hashwerte der virtuellen Dokumente gespeichert sind, lassen sich der Datenbank keine in den Dokumenten enthaltenen Informationen entnehmen. Insbesondere können den Hashwerten keine Informationen entnommen werden, welche die Inhaber der entsprechenden virtuellen Dokumente identifizierend könnten. Somit ist es sicher, die Datenbank dezentral zu speichern. Kein hochgesichertes zentrales Serversystem ist zum Schutz der Integrität der von den virtuellen Dokumenten umfassten Daten notwendig. Bereits die kryptographische Sicherung der Datenbank durch die Speicherung von Informationen in Form von Hashwerten kann ein hohes Maß an Sicherheit gewährleisten. Darüber hinaus ist es möglich, dass es sich bei der Datenbank um eine öffentliche Datenbank handelt, auf welche jedermann zugreifen kann.

[0043] Ausführungsformen können den Vorteil haben, dass allein der Besitzer des virtuellen Dokuments, über das virtuelle Dokument verfügt. Der Besitzer hat somit die volle Verfügungshoheit über die in dem virtuellen Dokument enthaltenen Daten inne. Allein der Besitzer entscheidet, wem er das virtuelle nach Erhalt zugänglich macht

[0044] Nach Ausführungsformen handelt es sich bei der kryptographisch gesicherten Datenbank um eine Blockchain und der Hashwert des virtuellen Dokuments ist als Transaktion in einem Block der Blockchain gespeichert.

[0045] Unter einer „Blockchain“ wird hier und im Folgenden eine geordnete Datenstruktur verstanden, wobei jeder Block der Blockchain durch einen Hash-Wert identifiziert wird und einen Vorgängerblock in der Blockchain referenziert, für Beispiele einer Blockchain vergleiche https://en.wikipedia.org/wiki/Block_chain_(database) und „Mastering Bitcoin“, Chapter 7, The Blockchain, Seite 161 ff. Das Konzept der Block-

chains wurde im Jahre 2008 in einem White Paper unter dem Pseudonym Satoshi Nakamoto zu Bitcoin beschrieben („Bitcoin: Peer-to-Peer Electronic Cash System“ (https://bitcoin.org/bitcoin.pdf)). Die Blockchain besteht aus einer Reihe von Datenblöcken, in denen jeweils eine oder mehrere Transaktionen zusammengefasst und mit einer Prüfsumme in Form eines Hashwerts versehen sind. Neue Blöcke der Blockchain werden in einem üblicher Weise rechenintensiven Prozess erzeugt, der auch als sogenanntes Mining bezeichnet wird. Diese neu erzeugten Blöcke werden anschließend der Blockchain hinzugefügt und über ein Netzwerk an alle Teilnehmer, bzw. Knoten des Netzwerks, verbreitet.

[0046] Ausführungsformen können den Vorteil haben, dass die Blockchain durch die Speicherung kryptografischer Prüfsumme, d.h. Haschwerten, des vorangehenden Blocks im jeweils nachfolgenden Block ein hohes Maß an Sicherheit gegenüber nachträglichen Manipulationen bietet. Bei einer Blockchain werden die Transaktionen eines Blocks beispielsweise durch einen Merkle-Baum paarweise miteinander gehasht und nur der letzte auf diese Weise erhaltene Hashwert des Blocks, der sogenannte Root-Hashwert bzw. Wurzelhashwert, als Prüfsumme im Header des Blocks vermerkt. Das Verketten der Blöcke kann dann unter Verwendung dieser Root-Hashwerte. Jeder Block der Blockchain enthält in seinem Header den Hash des gesamten vorherigen Blockheaders. Somit wird die Reihenfolge der Blöcke eindeutig festgelegt und es entsteht eine Kettenstruktur. Durch die so implementierte Verkettung der einzelnen Blöcke miteinander wird erreicht, dass ein nachträgliches Modifizieren vorangegangener Blöcke bzw. einzelner von diesen umfasst und über den Root-Hashwert gesicherten Transaktionen praktisch ausgeschlossen ist, da hierfür die Hashwerte aller nachfolgenden Blöcke in kurzer Zeit ebenfalls neu berechnet werden müssten.

[0047] Der erste Block in der Blockkette ist vorgegeben und wird Genesisblock genannt. Nach Ausführungsformen sind die öffentlichen kryptographischen Schlüssel eines oder mehrerer Aussteller der virtuellen Dokumente, deren Hashwerte in den Transaktionen gespeichert sind in dem Genesisblock gespeichert. Der Genesisblock ist aufgrund der zuvor beschriebenen Kettenstruktur, derjenige Block, dessen Einträge das höchste Maß an Sicherheit aufweisen, da zu seiner Änderung die gesamte Blockchain durch eine neue Blockchain ersetzt werden müsste. Mithin kann der Eintrag des öffentlichen kryptographischen Schlüssels in den Genesisblock einen Vertrauensanker mit einem ausreichenden Maß an Sicherheit darstellen, sodass beispielsweise keine zusätzliche PKI-Prüfung notwendig ist, um der Authentizität des öffentlichen kryptographischen Schlüssels zu vertrauen. Dadurch kann die Sicherheit des Systems im Offline Modus weiter erhöht werden. Nach weiteren Ausführungsformen kann der Genesisblock die PKI des öffentlichen kryptographischen Schlüssels enthalten.

[0048] Zudem kann durch eine Anpassung der notwendigen Rechenintensität für die Erstellung jeweils neuer Blöcke die Sicherheit zusätzlich erhöht werden. Die für die Erstellung neuer Blöcke notwenige Rechenintensität lässt sich über Anforderungen an den Hashwert des zu erstellenden neuen Blocks steuern. Der resultierende Hash-Wert ist nicht vorhersagbar, vielmehr handelt es sich um eine zufallsverteilte Zahl. Es lässt sich aber berechnen, wieviel Zeit in Abhängigkeit von der aufgewendeten Rechenleistung im statistischen Mittel zum Auffinden eines gültigen neuen Blocks notwendig ist. Der Hashwert eines Blocks lässt sich beispielsweise durch Hinzufügen und Variieren eines Nounce variieren. Aufgrund der Kettenstruktur können Daten, die einmal in einer Blockchain gespeichert sind, nicht mehr geändert oder entfernt werden, ohne große Teile der Blockchain zu ersetzen. Eine solche Ersetzung scheidet jedoch als Folge einer ausreichend rechenintensiven Generierung neuer Blöcke aus. Bekannte Ausführungsformen einer Blockchain, wie etwa im Fall der Kryptowährung Bitcoin, basieren auf einer Anonymität der an den Transaktionen beteiligten Partner. Demgegenüber kann durch oben beschriebene Signatur der in die Transaktionen eingetragenen Hashwerte, deren Authentizität belegt und ihr Ursprung nachgewiesen werden. Hierdurch kann die Fälschungssicherheit verbessert werden.

[0049] Eine Anforderung an einen gültigen Block kann beispielsweise darin bestehen, dass der Hashwert des Headers des Blocks kleiner gleich einem Grenzwert ist. Die Hashwertberechnung kann beispielsweise mit dem Secure Hash Algorithm (SHA) SHA 256 erfolgen. Der resultierende Hash-Wert ist in diesem Fall eine Zufallszahl zwischen 0 und 2^{256}-1. Die Wahrscheinlichkeit, dass beim Anwenden des Hashalgorithmus einen bestimmten Hash herauskommt, ist somit (maximaler Hash-Wert +1)$^{-1}$, im Falle des SHA 256-Algorithums also 2^{-256}. Die Wahrscheinlichkeit, dass der resultierende Hash-Wert kleiner gleich einem Grenzwert bzw. Zielwert (engl. target) ist, beträgt daher (target)/(max. Hash-Wert). Für einen beispielhaften maximalen Grenzwert von $(2^{16}-1)\cdot 2^{208}$ beträgt die Wahrscheinlichkeit $[(2^{16}-1)\cdot 2^{208}]/\cdot 2^{256} \approx 2^{-32}$. Die Schwierigkeit S eine Hash-Wert zu erhalten, welcher kleiner gleich einem gewählten Grenzwert bzw. target ist, kann in Abhängigkeit eines maximalen Grenzwerts bzw. max. target wie folgt angegeben werden: S = (max. target)/target. Mithin ist die Wahrscheinlichkeit einen Hash-Wert zu erhalten, weicher kleiner gleich dem gewählten Grenzwert ist, für das zuvor gegebene Beispiel: 2^{-32}/S. Als Beispiel sei ein Computersystem mit einer bestimmten Hashrate betrachtet, welches im Durchschnitt alle x·Sek. einen Hash-Wert findet, welcher kleiner gleich dem gewählten Grenzwert ist. Soll

das Computersystem anstelle aller x·Sek. im Durchschnitt alle y·Sek. einen Treffer erzielen, so kann die Schwierigkeit entsprechend angepasst werden: $S_y = (x/y)\cdot S$. Entsprechende Anpassungen der Schwierigkeit können auch dazu verwendet werden die Trefferrate bei Veränderungen des Computersystems, z.B. Veränderungen der Rechenleistung durch Erhöhen oder Verringern der Anzahl an Blockchainservern, konstant zu halten. Wird die Schwierigkeit so angepasst, dass alle y·Sek. ein Treffer erzielt wird, kann die Hashrate R des Computersystems wie folgt parametrisiert werden: $R = (2^{32}.S)/(y\cdot Sek.)$.

[0050] Werden gültige Blöcke durch ein rechenintensive Verfahren, wie das zuvor Beschriebene erzeugt, so vertrauen die Teilnehmer des Blockchain-Netzwerks der längsten gültigen Blockchain, da hinter dieser die meiste Rechenleistung steht und somit angenommen werden kann, dass diese von der Mehrheit der Teilnehmer als gültig anerkannt wird. Kommt es beispielsweise dazu, dass ein Fork, d.h. eine Verzweigung, in der Blockchain entsteht, setzt sich irgendwann der Fork mit der größeren Kettenlänge durch, da anzunehmen ist, dass hinter diesem die Mehrheit der Teilnehmer steht.

[0051] Eine Blockchain kann beispielsweise auch in Form einer privaten Blockchain implementiert werden, wobei nur eine ausgewählte Gruppe von Teilnehmern eine Berechtigung zum Hinzufügen gültiger Blöcke besitzt. Eine entsprechende Berechtigung kann beispielsweise mittels einer Signatur unter Verwendung eines privaten kryptographischen Schlüssels nachgewiesen werden. Der private kryptographische Schlüssel kann zu einem asymmetrischen Schlüsselpaar gehören, zu welchem auch ein öffentlicher kryptographischer Schlüssel gehört, mit dem die Signatur geprüft werden kann. Dem asymmetrischen Schlüsselpaar kann zudem beispielsweise ein Zertifikat zugeordnet sein, weiches die Berechtigung zum Erzeugen eines gültigen Blocks der Blockchain belegt. Dieses Zertifikat kann ferner einer PKI zugeordnet sein, welche die Authentizität des Zertifikats belegt. Nach einer weiteren Ausführungsform kann beispielsweise für jeden Teilnehmer aus der ausgewählte Gruppe ein öffentlicher Schlüssel in der Blockchain hinterlegt sein, beispielsweise in einem Genesisblock. Anhand dieser öffentlichen Schlüssel kann geprüft werden, ob Signaturen von Blöcken und damit die entsprechenden Blöcke selbst gültig sind.

[0052] Ein Konsens kann auch auf andere Weise in einer Blockchain implementiert werden. So kann etwa ein Konsens erreicht werden, indem über eine Aufnahme vorgeschlagener Einträge in die Blockchain abgestimmt wird. Beispielsweise führt jeder Teilnehmer eine eindeutige Liste anderer Teilnehmer, welchen er als Gruppe vertraut. Jeder Teilnehmer kann neue Einträge vorschlagen, die in einen neuen Block der Blockchain aufgenommen werden sollen. Über die Aufnahme und damit die Anerkennung der Gültigkeit der vorgeschlagenen Einträge wird abgestimmt. So stimmt beispielsweise jeder Teilnehmer nur über diejenigen Vorschläge ab, welche von Teilnehmer seiner Liste stammen. Mit anderen Worten werden für die Entscheidung, ob ein Vorschlag für einen neuen Eintrag als gültig anerkannt wird, d.h. ob bezüglich der Gültigkeit dieses Eintrages ein Konsens zwischen den Teilnehmern besteht, nur die Stimmen derjenigen Teilnehmer berücksichtig, die von der Liste desjenigen Teilnehmers umfasst sind, der den entsprechenden Vorschlag macht. Damit ein Vorschlag für einen Eintrag als gültig angenommen wird, muss ein bestimmter Minimumanteil an stimmberechtigten Teilnehmern mit Ja stimmen, beispielsweise 80%. Alle vorgeschlagenen Einträge, die dieses Kriterium erfüllen werden in die Blockchain aufgenommen. Eine solche Abstimmung kann mehrere Runden umfassen. Alle anderen Vorschläge, die das zuvor genannte Kriterium nicht erfüllen, werden verworfen oder bei der Abstimmung über den nächsten Block der Blockchain erneut zur Abstimmung gestellt. Die zuvor genannten Listen stellen Untergruppen des Blockchain-Netzwerks dar, denen der Teilnehmer, welcher die jeweilige Liste führt, als Gruppe insgesamt traut, ohne dass dies erfordert, dass er jedem einzelnen Teilnehmer der Liste traut. Ein Beispiel für ein solches Konsensverfahren bietet der Ripple Protokoll Konsens Algorithmus (David Schwartz et al.: „The Ripple Protocol Consensus Algorithm“, Ripple Labs Inc, 2014, https://ripple.com/files/ripple_consensus_whitepaper.pdf).

[0053] Beispielsweise kann es sich bei der Blockchain um eine private oder öffentliche Blockchain handeln. Beispielsweise handelt es sich um eine Bitcoin-, Litecoin- oder Ethereum-Blockchain.

[0054] Ferner können Ausführungsformen den Vorteil haben, dass die Blockchain darauf ausgelegt ist als dezentralen Datenbank in einem dezentralen Netzwerk implementiert zu werden, wobei sie redundant und dezentral auf allen Knoten des entsprechenden Netzwerks gespeichert wird. Wird die Verbindung eines Knotens zum Rest des Netzwerks unterbrochen, so steht diesem nach wie vor die vollständige Blockchain zur Verfügung. Selbst wenn die Unterbrechung längere Zeit andauern sollte, so steht dem Knoten dennoch die vollständige Blockchain bis zu der Unterbrechung zur Verfügung und allenfalls neuste Einträge, welche nach diesem Zeitpunkt erfolgt sind fehlen. Somit kann die Blockchain auch im Offline-Betrieb einen effizienten Zugriff auf die in ihr enthaltenen Daten sicherstellen. Durch ein regelmäßiges Update der verteilt gespeicherten redundanten Versionen der Blockchain kann zudem sichergestellt werden, dass die entsprechenden Versionen Blockchain im Offlinebetrieb zwischen den Updates auf einem ausreichend aktuellen Stand sind.

[0055] Nach Ausführungsformen handelt es sich bei der Speicher-ID um eine Transaktions-ID der Transaktion, welche den signierten Hashwert des virtuellen Dokuments umfasst. Ausführungsformen können den Vorteil haben, dass sie eine einfache Identifizierung der Transaktion ermöglichen, welche den Hashwert des zu prüfenden virtuellen Dokuments umfasst.

[0056] Nach Ausführungsformen umfasst das virtuelle Dokument einen öffentlichen kryptographischen Schlüssel eines dem Inhaber des virtuellen Dokuments zugeordneten asymmetrischen Schlüsselpaars. Ausführungsformen können den Vorteil haben, dass somit die Authentizität des öffentlichen Schlüssels und dessen Zuordnung zu dem Inhaber des virtuellen Dokuments durch das virtuelle Dokument selbst bzw. den Aussteller des virtuellen Dokuments bestätigt wird. Ausführungsformen können den Vorteil haben, dass durch das virtuelle Dokument die Authentizität des entsprechenden öffentlichen Schlüssels bestätigt wird. Beispielsweise wird der öffentliche kryptographische Schlüssel des Inhabers bzw. zukünftigen Inhabers durch den Aussteller des virtuellen Dokuments geprüft. Beispielsweise wird die Authentizität des öffentlichen kryptographischen Schlüssels unter Verwendung eines Zertifikats, insbesondere eines Zertifikats einer PKI, überprüft. Somit bestätigt der Aussteller des virtuellen Dokuments durch die Aufnahme des öffentlichen kryptographischen Schlüssels in das virtuelle Dokument dessen Authentizität. Mithin erfüllt das resultierende virtuelle Dokument also zudem die Funktion eines Zertifikats, welches die Authentizität des öffentlichen kryptographischen Schlüssels bestätigt und durch die Signatur mit dem privaten kryptographischen Schlüssel des Ausstellers vor Fälschungen schützt. Dabei kann es vorteilhaft sein, dass ein Nachweis der Authentizität des öffentlichen Schlüssels anhand der Datenbank mit dem signierten Hashwert des virtuellen Dokuments auch offline möglich ist, solange die Datenbank zur Verfügung steht. Dies kann beispielsweise bei einer Blockchain der Fall sein.

[0057] Bei dem Inhaber des virtuellen Dokuments handelt es sich beispielsweise um den Besitzer des Dokuments, welcher anhand des Dokuments als Inhaber des Dokuments und damit auch als Inhaber des zu erstellenden virtuellen Dokuments authentifiziert wurde.

[0058] Nach Ausführungsformen umfasst die Datenbank den öffentlichen kryptographischen Schlüssel des Inhabers des virtuellen Dokuments zusätzlich zu dem entsprechenden Dokument. Beispielsweise kann die Datenbank einen weiteren mit dem privaten kryptographischen Schlüssel des Ausstellers signierten Eintrag umfassen, in welchem der öffentlichen kryptographischen Schlüssel des Inhabers des virtuellen Dokuments hinterlegt ist. Beispielsweise kann die Datenbank den öffentlichen kryptographischen Schlüssel des Inhabers des virtuellen Dokuments als eine Adresse umfassen, welcher das virtuelle Dokument zugeordnet ist. Nach Ausführungsformen kann die Datenbank ein Zertifikat umfassen, welches dem asymmetrischen Schlüsselpaar des Inhabers des virtuellen Dokuments zugeordnet ist, den öffentlichen kryptographischen Schlüssel des Inhabers umfasst und dessen Authentizität bestätigt. Nach Ausführungsformen wird die Authentizität des entsprechenden Zertifikats durch eine PKI belegt, welche beispielsweise von der Datenbank umfasst ist.

[0059] Nach Ausführungsformen umfasst das Verfahren ferner:

- Empfangen einer Anfrage zum Ausstellen des virtuellen Dokuments von einem zweiten Computersystem durch den Besitzer des Dokuments, wobei das zweite Computersystem eine Digitalkamera umfasst,
- Senden einer Abfrage von Daten des Dokuments an das zweite Computersystem,
- Empfang der abgefragten Daten durch das zweite Computersystem,
- Verifizieren der abgefragten Daten,
- Erstellen der virtuellen Kopie des Datensatzes des Dokuments unter Verwendung der verifizierten Daten.

[0060] Ausführungsformen können den Vorteil haben, dass eine Ausstellung eines virtuellen Dokuments von einem entfernten zweiten Computersystem über ein Netzwerk erfolgen kann, ohne dass der Besitzer des Dokuments mit diesem beim ID-Provider persönlich zugegen sein muss. Somit wird ein sicheres und effizientes Verfahren bereitgestellt, um auf Basis eines physischen Dokuments ein virtuelles Dokument zu erhalten. Nach Ausführungsformen erfolgt die Kommunikation zwischen dem ersten Computersystem des ID-Providers und dem zweiten Computer des Besitzers des Dokuments. Nach Ausführungsformen handelt es sich bei dem zweiten Computersystem um ein mobiles Computersystem, wie ein Laptop oder Smartphone oder ein stationäres Computersystem, wie etwa einen PC.

[0061] Nach Ausführungsformen umfasst das Verfahren ferner: Authentisieren des zweiten Computersystems gegenüber dem ersten Computersystem. Ausführungsformen können den Vorteil haben, dass dadurch die Sicherheit des Verfahrens erhöht wird und der zweite Computersystem sicherstellen kann, dass es die Daten des Dokuments an eine vertrauenswürdige Instanz sendet. Dabei erfolgt die Kommunikation zwischen dem ersten und zweiten Computersystem und insbesondere das Übersenden der Daten des Dokuments in verschlüsselter Form. Nach Ausführungsformen können die Daten des Doku-

ments mit einem vom ersten Computersystem an das zweite Computersystem gesendeten öffentlichen kryptographischen Schlüssel des ID-Providers verschlüsselt sein. Nach Ausführungsformen erfolgt die Kommunikation zwischen dem ersten und zweiten Computersystem über einen mittels Ende-zu-Ende-Verschlüsselung gesicherten Kommunikationskanal.

[0062] Unter einer „verschlüsselten Ende-zu-Ende-Verbindung“ bzw. einem „verschlüsselten Ende-zu-Ende-Übertragungskanal“ wird hier eine Verbindung zwischen einem Sender und einem Empfänger mit einer Ende-zu-Ende-Verschlüsslung verstanden, bei der zu übertragende Daten vom Sender verschlüsselt und erst vom Empfänger wieder entschlüsselt werden. Die Verschlüsselung übertragener Daten erfolgt somit über alle Übertragungsstationen hinweg, sodass Zwischenstationen aufgrund der Verschlüsslung keine Kenntnis vom Inhalt der übertragenen Daten erlagen können. Die Verbindung wird durch die Verschlüsselung kryptografisch abgesichert, um ein Ausspähen und/oder eine Manipulation der Übertragung zu verhindern, wobei hierzu ein sogenanntes Secure-Messaging-Verfahren eingesetzt werden kann. Eine Ende-zu-Ende-Verschlüsslung beruht beispielsweise auf zwei symmetrischen kryptographischen Schlüsseln, wobei ein erster der symmetrischen Schlüssel zum Verschlüsseln von Nachrichten und ein zweite der symmetrischen Schlüssel zum Authentifizieren des Senders der Nachricht dient.

[0063] Der Schlüssel zum Authentifizieren des Senders der Nachricht kann beispielsweise zum Erstellen eines Nachrichtenauthentifizierungscodes (Message Authentication Code, MAC) dienen. Mittels eines MAC lässt sich Gewissheit über den Ursprung der Nachrichten erhalten und deren Integrität verifizieren. MAC-Algorithmen erfordern zwei Eingabeparameter, erstens die zu schützenden Daten und zweitens einen geheimen Schlüssel. Aus diesen beiden wird ein Nachrichtenauthentifizierungscode in Form einer Prüfsumme berechnet. Der Sender einer Nachricht berechnet für die zu übermittelnden Daten der Nachricht einen MAC und sendet die Nachricht zusammen mit dem MAC an den Empfänger. Der Empfänger berechnet den MAC zu der empfangenen Nachricht mit seinem Schlüssel und vergleicht den berechneten MAC mit dem empfangenen MAC. Aus einer Übereinstimmung beider Werte folgt, dass die Nachricht von einer Partei abgeschickt wurde, welche Zugriff auf den geheimen Schlüssel besitzt und die Nachricht wurde während der Übertragung nicht verändert.

[0064] Nach Ausführungsformen umfasst die Abfrage der Daten eine Abfrage virtueller Bildaufnahmen des Dokuments unter verschiedenen Blickwinkeln. Ausführungsformen können den Vorteil haben, dass mittels der Bildaufnahmen zum einen auf dem Dokument wiedergegebene Daten gewonnen werden können und zum anderen die Authentizität des Dokuments anhand von Sicherheitsmerkmalen geprüft werden kann, deren Erscheinungsbild beispielsweise in abhängig vom Blickwinkel variiert.

[0065] Sicherheitsmerkmale können beispielsweise auf optisch variable Farben (OVI, „Optical Variable Inks“) oder optisch variabler Merkmaler (OVD „Optical Variable Devices“) etwa in Form von Hologrammen oder Kinegrammen beruhen. Bei einem Changeable oder Multiple Laser Image (CLI/MLI) werden beispielsweise mehrere Informationen mit einem Laser in den Dokumentkörper geschrieben, sodass je nach Blickwinkel des Betrachters immer nur eine Information zu sehen ist. Ebenso können Druckelemente mit Kippeffekt berücksichtigt werden.

[0066] Nach Ausführungsformen werden sowohl Bildaufnahmen von einer Vorderseite als auch von einer Rückseite des Dokuments abgefragt.

[0067] Nach Ausführungsformen werden die Bildaufnahme in Form eines Videostreams aufgenommen und dem ersten Computersystem zur Verarbeitung, z.B. Datenextraktion und Verifikation, bereitgestellt.

[0068] Nach Ausführungsformen werden an das zweite Computersystem assistierende Rückmeldungen zur relativen Ausrichtung zwischen dem Dokument und der Digitalkamera gesendet. Hierbei kann der Besitzer des Dokuments angeleitet werden unter welchen Winkeln die Aufnahmen zu erstellen sind und/oder informiert werden, ob eine aktuelle Aufnahme den gesetzten Anforderungen genügt. Insbesondere kann der Besitzer des Dokuments Informationen erhalten, wie eine ungenügende Aufnahme zu verbessern ist. Ausführungsformen können den Vorteil haben, dass der Besitzer des Dokuments möglichst fehlerfrei und einfach durch den Prozess begleitet wird. Insbesondere kann so sichergestellt werden, dass die Aufnahme unter den korrekten Winkeln erfolgen, so dass die Sicherheitsmerkmale des Dokuments klar erkannt werden können.

[0069] Nach Ausführungsformen umfasst das Verifizieren der abgefragten Daten:

- Verifizieren des Dokuments durch Prüfen von visuellen Sicherheitsmerkmalen des Dokuments unter Verwendung der digitalen Bildaufnahmen des Dokuments unter verschiedenen Blickwinkeln,
- Extrahieren von Daten des Dokuments aus den digitalen Bildaufnahmen.

[0070] Ausführungsformen können den Vorteil haben, dass sowohl die Authentizität des zugrundeliegenden Dokuments effizient verifiziert werden als auch Sicherheit darüber gewonnen werden kann,

dass die Daten, die zum Ausstellen des virtuellen Dokuments verwendet werden, tatsächlich den Daten entsprechen, die von dem Dokument widergegeben werden. Eine Datenextraktion kann beispielsweise mittels eines Verfahrens zur optische Zeichenerkennung (OCR, „Optical Character Recognition“) erfolgen.

[0071] Nach Ausführungsformen umfasst das Verifizieren der abgefragten Daten:

- Extrahieren einer Dokumenten-ID aus dem digitalen Bildaufnahmen,
- Verifizieren der Dokumenten-ID.

[0072] Ausführungsformen können den Vorteil haben, dass das die Dokumenten-ID dazu verwendet werden kann, um zu verifizieren, ob das entsprechende Dokument von einem dafür verantwortlichen Aussteller auch tatsächlich ausgestellt wurde. Hierzu kann beispielsweise eine entsprechende Anfrage an ein viertes Computersystem des Austellers gesendet werden. Fall der ID-Provider beispielsweise mit dem Aussteller des Dokuments identisch ist, kann eine entsprechende interne Datenbankabfrage erfolgen.

[0073] Nach Ausführungsformen umfasst die Abfrage der Daten eine Aufforderung zur Eingabe von Daten des Dokuments über das zweite Computersystem. Nach Ausführungsformen umfasst das Verfahren ferner:

- Vergleichen der extrahierten Daten mit den eingegebenen Daten,
- Korrigieren von Fehlern bei den extrahierten Daten.

[0074] Ausführungsformen können den Vorteil haben, die eingegebenen Daten dazu verwendet werden können Fehler beim Extrahieren der Daten, d.h. bei der automatischen Texterkennung, zu identifizieren und zu korrigieren. Bei Abweichungen zwischen den Ergebnissen der automatischen Texterkennung und dem eingegebenen Text kann bestimmt werden, ob die Abweichungen innerhalb eines vordefinierten Fehlerbereichs liegen, so dass es sich mit hoher Wahrscheinlichkeit um einen Fehler bei der Texterkennung handelt. In diesem Fall kann der Fehler der Texterkennung unter Verwendung der eingegebenen Daten korrigiert werden. Liegt die Abweichung außerhalb des vordefinierten Fehlerbereichs, so ist davon auszugehen, dass es sich um keinen Fehler der Texterkennung handelt, sondern um einen Fehler des eingegebenen Textes. In diesem Fall erfolgt keine Fehlerkorrektur. Hierbei kann es sich um einen absichtliche oder einen versehentlichen Fehler handeln.

[0075] Nach Ausführungsformen umfasst das Verfahren ferner: Authentifizieren des Besitzers des Dokuments gegenüber dem ID-Provider. Ausführungsformen können den Vorteil haben, dass die Anfrage zur Ausstellung des virtuellen Dokuments auch tatsächlich von einer dazu berechtigten Person stammt und dass das entsprechende virtuellen Dokument am Ende auch zu einer dazu berechtigten Person gelangt.

[0076] Nach Ausführungsformen umfasst das Authentifizieren des Besitzers des Dokuments eine Abfrage einer digitalen Bildaufnahme des Besitzers des Dokuments. Nach Ausführungsformen umfasst das Authentifizieren des Besitzers des Dokuments: Vergleichen der digitalen Bildaufnahme des Besitzers des Dokuments mit einem von dem Dokument umfassten Bild einer Person, welcher das Dokument zugeordnet ist. Ausführungsformen können den Vorteil haben, dass die Bildaufnahme des Besitzers des Dokuments mit einem von dem Dokument umfassten Bild verglichen werden kann. Stimmen die Bilder überein, so gilt der Besitzer des Dokuments auf Basis des Dokuments beispielsweise als authentifiziert, falls es sich bei dem Dokument um ein Ausweisdokument handelt.

[0077] Nach Ausführungsformen fragt die Abfrage der digitalen Bildaufnahme digitale Bildaufnahmen des Besitzers des Dokuments unter verschiedenen Blickwinkeln ab. Ausführungsformen können den Vorteil haben, dass so sichergestellt werden kann, dass tatsächlich Live-Aufnahmen übermittelt werden und keine alten archivierten Aufnahmen.

[0078] Nach Ausführungsformen werden an das zweite Computersystem assistierende Rückmeldungen zur relativen Ausrichtung zwischen dem Besitzer des Dokuments und der Digitalkamera gesendet. Ausführungsformen können den Vorteil haben, dass zum einen das Erstellen der Bildaufnahmen erleichtert und zum anderen durch Anweisungen, welche von Authentifizierung zu Authentifizierung variieren, sichergestellt werden kann, dass die Bildaufnahmen auch tatsächlich spontan erfolgen. Zudem kann sichergestellt werden, dass die Bildaufnahmen eine ausreichende Qualität aufweisen, sodass der Besitzer des Dokuments auf Basis der Bildaufnahmen authentifiziert werden kann.

[0079] Nach Ausführungsformen umfasst das Authentifizieren des Besitzers des Dokuments eine Abfrage von digitalen Bildaufnahmen eines Ausweisdokuments des Besitzers unter verschiedenen Blickwinkeln. Nach Ausführungsformen werden an das zweite Computersystem assistierende Rückmeldungen zur relativen Ausrichtung zwischen dem Ausdokument und der Digitalkamera gesendet. Nach Ausführungsformen umfasst das Verifizieren des Ausweisdokuments: Verifizieren des Ausweisdokuments durch Prüfen von visuellen Sicherheitsmerkmalen des Ausweisdokuments unter Verwendung der digitalen Bild-

aufnahmen des Ausweisdokuments unter verschiedenen Blickwinkeln. Nach Ausführungsformen umfasst das Authentifizieren des Besitzers des Dokuments: Vergleichen der digitalen Bildaufnahme des Besitzers des Dokuments mit einem von dem Ausweisdokument umfassten Bild einer Person, welcher das Ausweisdokument zugeordnet ist. Ausführungsformen können den Vorteil haben, dass falls es sich bei dem auszustellenden virtuellen Dokument bzw. dessen Ursprungsdokument um kein Ausweisdokument handelt, sich der Besitzer des Dokuments durch ein zusätzliches Ausweisdokument effizient authentifizieren kann. Beispielsweise handelt es sich bei dem virtuellen Dokument um ein Zeugnis ohne Bild des Zeugnisinhabers. In diesem Fall kann die Authentifizierung beispielsweise unter Verwendung eines Personalausweises erfolgen.

[0080] Nach Ausführungsformen umfasst das Verifizieren des Ausweisdokuments:

- Extrahieren einer Ausweisdokumenten-ID aus dem digitalen Bildaufnahmen,
- Verifizieren der Ausweisdokumenten-ID.

[0081] Ausführungsformen können den Vorteil haben, dass durch eine Verifikation der Ausweisdokumenten-ID die Sicherheit bezüglich der Authentizität des Ausweisdokuments zusätzlich erhöht werden kann.

[0082] Nach Ausführungsformen ist ein dem asymmetrischen Schlüsselpaar des Ausstellers zugeordneter öffentlicher kryptographische Schlüssel in der Datenbank gespeichert. Ausführungsformen können den Vorteil haben, dass somit auch im Offline-Modus allein auf Basis der kryptographisch geschützten Datenbank ein Zugriff auf den öffentlichen kryptographischen Schlüssel des Ausstellers ermöglicht wird. Handelt es sich bei der Datenbank zudem um eine Datenbank mit einer Blockchain-Struktur, wobei der öffentliche kryptographische Schlüssel des Ausstellers in einer der Transaktionen gespeichert ist, so wird der öffentliche kryptographische Schlüssel durch die mittels der Prüfsummenspeicherung geschützte Kettenstruktur gegen Manipulationen gesichert. Beispielsweise kann die Datenbank den öffentlichen kryptographischen Schlüssel des Ausstellers als eine Adresse umfassen, welcher das virtuelle Dokument zugeordnet ist. Nach Ausführungsformen umfasst die Datenbank ein dem asymmetrischen Schlüsselpaar des Ausstellers zugeordnetes Zertifikat, welches den öffentlichen kryptographischen Schlüssel des Ausstellers umfasst und dessen Authentizität bestätigt. Nach Ausführungsformen wird die Authentizität des entsprechenden Zertifikats durch eine PKI belegt, welche beispielsweise von der Datenbank bereitgestellt wird.

[0083] Nach Ausführungsformen umfasst das Verfahren ferner: Speichern des öffentlichen kryptographischen Schlüssels des Ausstellers in dem Datenbankeintrag mit dem signierten Hashwert des virtuellen Dokuments. Ausführungsformen können den Vorteil haben, dass sie einen einfachen Zugriff auf den öffentlichen kryptographischen Schlüssel ermöglichen.

[0084] Nach Ausführungsformen umfasst das Senden des virtuellen Dokuments:

- Empfang eines öffentlichen Schlüssels eines dem Besitzer des Dokuments zugeordneten asymmetrischen Schlüsselpaars,
- Verschlüsseln des zu sendenden virtuellen Dokuments mit dem öffentlichen Schlüssel des Besitzers des Dokuments.

[0085] Ausführungsformen können den Vorteil haben, dass eine sichere Übertragung des virtuellen Schlüssels an den Besitzer des Dokuments ermöglicht wird.

[0086] Nach Ausführungsformen umfasst das Verfahren ferner: Verschlüsseln der Speicher-!D mit dem öffentlichen Schlüssel des Besitzers des Dokuments. Ausführungsformen können den Vorteil haben, dass das auch die Speicher-ID geschützt übertragen wird und somit ein Ziehen einer Verbindung zwischen dem Besitzer des Dokuments und einem mit einer bestimmten Speicher-ID identifizierten Datenbankeintrag verhindert wird.

[0087] Nach Ausführungsformen wird die zum Ausstellen des virtuellen Dokuments verwendete virtuelle Kopie des Datensatzes des Dokuments nach dem Ausstellen des virtuellen Dokuments automatisch gelöscht. Ausführungsformen können den Vorteil haben, dass die Daten des Dokuments geschützt bleiben. Es kann auf diese Weise sichergestellt werden, dass am Ende des Verfahrens allein der Besitzer des virtuellen Dokuments die Verfügungshoheit über das virtuelle Dokument sowie der darin enthaltenen Daten besitzt.

[0088] Nach Ausführungsformen umfasst das virtuelle Dokument selbst die Speicher-ID. Ausführungsformen können den Vorteil haben, dass sie ein einfaches Auffinden der Speicher-ID und damit des Datenbankeintrags sicherstellen.

[0089] Nach Ausführungsformen umfasst das virtuelle Dokument ein Ablaufdatum, welches ein Ende der Gültigkeit des virtuellen Dokuments festlegt. Ausführungsformen können den Vorteil haben, dass ein einmal in die kryptographisch gesicherte Datenbank eingetragenes virtuelles Dokument seine Gültigkeit nicht bis in alle Ewigkeit beibehält. Insbesondere kann durch die Anforderung einer Neuaustellung des

virtuellen Dokuments in regelmäßigen Abständen sichergestellt werden, dass dem Besitzer des ersten elektronischen Geräts bzw. dem Inhaber des virtuellen Dokuments nicht zwischenzeitlich die Berechtigung zur Verwendung des virtuellen Dokuments entzogen wurde.

[0090] Nach Ausführungsformen umfasst das Verfahren ferner: bei Ablaufen der Gültigkeit des virtuellen Dokuments Bereitstellen einer neuen virtuellen Version des Dokuments durch Wiederholen des Ausstellverfahrens. Ausführungsformen können den Vorteil haben, dass das virtuelle Dokument immer wieder auf Basis des zugrundliegenden physischen Dokuments erneuert werden muss.

[0091] Ausführungsformen umfassen ferner ein Computerprogrammprodukt, insbesondere ein computerlesbares, nichtflüchtiges Speichermedium, mit ausführbaren Programminstruktionen zum Ausführen eines Verfahrens nach einer der zuvor beschriebenen Ausführungsformen.

[0092] Ausführungsformen umfassen ferner ein Computersystem, welches konfiguriert ist zum Ausführen eines Verfahrens nach einer der zuvor beschriebenen Ausführungsformen.

[0093] Ausführungsformen umfassen ferner ein Verfahren zur Offline-Echtheitsprüfung eines nach einer der Ausführungsformen des zuvor beschriebenen Verfahrens ausgestellten virtuellen Dokuments mittels eines ersten und eines zweiten elektronischen Geräts. Das erste elektronische Gerät umfasst einen ersten Speicher, in welchem das virtuelle Dokument und eine Speicher-ID des virtuellen Dokuments gespeichert sind. Das zweite elektronische Gerät umfasst einen zweiten Speicher, in welchem eine kryptographisch gesicherte Datenbank gespeichert ist, welche Hashwerte von einer Mehrzahl von virtuellen Dokumenten umfasst. Die Speicher-ID des virtuellen Dokuments identifiziert einen Eintrag der Datenbank mit dem Hashwert des virtuellen Dokuments. Das Verfahren umfasst:

- Übertragen des virtuellen Dokuments zusammen mit der Speicher-ID von dem ersten elektronischen Gerät an das zweite elektronische Gerät,
- Berechnen eines Hashwerts des virtuellen Dokuments durch das zweite elektronische Gerät,
- Identifizieren des Datenbankeintrags mit dem Hashwert des virtuellen Dokuments durch das zweite elektronische Gerät unter Verwendung der Speicher-ID des virtuellen Dokuments,
- Vergleichen des berechneten Hashwerts mit dem in dem identifizierten Datenbankeintrag gespeicherten Hashwert des virtuellen Dokuments, wobei die Echtheit des virtuellen Dokuments bestätigt wird, falls beide Hashwerte übereinstimmen.

[0094] Ausführungsformen können den Vorteil haben, dass durch die Verwendung eines virtuellen Dokuments die Bindung an einen spezifischen physischen Dokumentenkörper entfällt. Die Authentizität und Gültigkeit des virtuellen Dokuments ist insbesondere unabhängig vom ersten elektronischen Gerät, auf welchem das virtuelle Dokument gespeichert ist. Bei dem ersten elektronischen Gerät kann es sich somit um ein beliebiges, vorzugsweise mobiles, elektronisches Gerät mit einem Speicher zum Speichern eines virtuellen Dokuments in Form einer digitalen Datei sowie einer Schnittstelle zur Kommunikation mit dem zweiten elektronischen Gerät handeln. Die Echtheit des virtuellen Dokuments ergibt sich alleine aus der Übereinstimmung seines Hashwerts mit dem in der Datenbank als authentisch hinterlegten Hashwert. Somit ist es nach Ausführungsformen möglich eine Mehrzahl von Dokumenten in virtueller Form auf dem ersten elektronischen Gerät zu speichern. Bei dem ersten elektronischen Gerät kann es sich insbesondere um ein handliches, tragbares Gerät, wie etwa ein Smartphone handeln, welches ein Nutzer im Allgemeinen stets mit sich führt.

[0095] Ausführungsformen können den Vorteil haben, dass das zweite elektronische Gerät keine Onlineverbindung zu einem entfernten zentralen Serversystem zur Prüfung der Echtheit des virtuellen Dokuments benötigt. Die Echtheitsprüfung erfolgt vielmehr unter Verwendung der lokal auf dem zweiten elektronischen Gerät gespeicherten Datenbank. Da die Datenbank zur Echtheitsprüfung virtueller Dokument nur deren als authentisch anerkannten Hashwerte umfasst, kann die Datenbank selbst im Falle einer großen Anzahl virtueller Dokumente eine kompakte Größe aufweisen, sodass nach Ausführungsformen weder spezielle Speichermedien zum Speichern großer Datenmengen noch aufwendige Datenbanksoftwarelösungen zur effizienten Handhabung großer Datenbanken notwendig sind.

[0096] Da in der Datenbank nur Hashwerte der virtuellen Dokumente gespeichert sind, lassen sich der Datenbank keine in den Dokumenten enthaltenen Informationen entnehmen. Insbesondere können den Hashwerten keine Informationen entnommen werden, welche die Inhaber der entsprechenden virtuellen Dokumente identifizierend könnten. Somit ist es sicher, die Datenbank auf dem zweiten elektronischen Gerät zu speichern. Hierbei kann das zweite elektronische Gerät ebenfalls als mobiles Gerät ausgestaltet sein. Kein hochgesichertes zentrales Serversystem ist zum Schutz der Integrität der von den virtuellen Dokumenten umfassten Daten notwendig. Bereits die kryptographische Sicherung der Daten-

bank durch die Speicherung von Informationen in Form von Hashwerten kann ein hohes Maß an Sicherheit gewährleisten. Darüber hinaus ist es möglich, dass es sich bei der Datenbank um eine öffentliche Datenbank handelt, auf welche jedermann zugreifen kann.

[0097] Ausführungsformen können den Vorteil haben, dass allein der Besitzer des virtuellen Dokuments, genauer gesagt der Besitzer des ersten elektronischen Geräts, über das virtuelle Dokument verfügt. Der Besitzer hat somit die volle Verfügungshoheit über die in dem virtuellen Dokument enthaltenen Daten inne. Allein der Besitzer entscheidet, wem er das virtuelle Dokument mittels des zuvor beschriebenen Verfahrens zugänglich macht.

[0098] Bei dem ersten elektronischen Gerät handelt es sich vorzugsweise um ein tragbares elektronisches Gerät. Bei dem zweiten elektronischen Gerät handelt es sich um ein stationäres oder mobiles, insbesondere ein tragbares, Gerät.

[0099] Das erste und zweite elektronische Gerät sind jeweils informationstechnisch aufgerüstete und dazu konfiguriert selbst Informationen zu verarbeiten. Insbesondere handelt es sich um Computersysteme. Entsprechende Computersystemen können als stationäre oder mobile, insbesondere tragbare, Computersysteme konfiguriert sein.

[0100] Bei einem solchen Computersystem kann es sich beispielsweise um ein mobiles Telekommunikationsgerät, insbesondere ein Smartphone, einen tragbaren Computer, wie zum Beispiel einen Laptop oder Palmtop-Computer, einen Personal Digital Assistant oder dergleichen handeln. Ferner kann es sich um ein stationäres Computersystem, wie beispielsweise einen Personalcomputer oder einen in einer Client-Server-Umgebung eingebundenen Server handeln.

[0101] Nach Ausführungsformen weisen das erste und/oder das zweite elektronische Gerät ein Sicherheitsmodul auf. Ausführungsformen können den Vorteil haben, dass das Sicherheitsmodul Mittel zur effizienten kryptographischen Datensicherung, insbesondere zur Sicherung der Datenübertragung zwischen den beiden elektronischen Geräten, bereitstellt.

[0102] Nach Ausführungsformen erfolgt die Übertragung des virtuellen Dokuments von dem ersten elektronischen Gerät an das zweite elektronische Gerät in verschlüsselter Form und das Verfahren umfasst dazu ferner:

- Übertragen eines kryptographischen Schlüssels des zweiten elektronischen Geräts von dem zweiten elektronischen Gerät an das erste elektronische Gerät,
- Verschlüsseln des virtuellen Dokuments durch das erste Gerät mit dem kryptographischen Schlüssel des zweiten Geräts vor der Übertragung an das zweite elektronische Gerät,
- Entschlüsseln des verschlüsselten virtuellen Dokuments durch das zweite elektronische Gerät nach der Übertragung.

[0103] Ausführungsformen können den Vorteil haben, dass durch die verschlüsselte Übertragung des virtuellen Dokuments effektiv verhindert werden kann, dass unbefugte Dritte den Datenaustausch ausspähen können. Insbesondere kann vermieden werden, dass ein unbefugter Dritter das virtuellen Dokument abfängt und missbräuchlich verwendet.

[0104] Nach Ausführungsformen umfasst die Übertragung des virtuellen Dokuments von dem ersten elektronischen Gerät an das zweite elektronische Gerät ferner eine Signatur mit einem privaten kryptographischen Schlüssel eines einem Inhaber des virtuellen Dokuments zugeordneten asymmetrischen Schlüsselpaars, wobei die kryptographisch gesicherte Datenbank eines öffentlichen kryptographischen Schlüssels des dem Inhaber zugeordneten asymmetrischen Schlüsselpaars umfasst. Das Verfahren umfasst dazu ferner:

- Berechnen eines Hashwerts aus dem virtuellen Dokument und einer Kennung, welche die Übertragung des virtuellen Dokuments von dem ersten elektronischen Gerät an das zweite elektronische Gerät identifiziert,
- Signieren des Hashwerts mit dem privaten kryptographischen Schlüssel des Inhabers des virtuellen Dokuments vor der Übertragung an das zweite elektronische Gerät,
- Überprüfen der Signatur durch das zweite elektronische Gerät nach der Übertragung unter Verwendung des von der kryptographisch gesicherten Datenbank umfassten öffentlichen kryptographischen Schlüssels des Inhabers.

[0105] Ausführungsformen können den Vorteil haben, dass anhand der Signatur des Hashwerts mit dem privaten kryptographischen Schlüssel des Inhabers des virtuellen Dokuments unter Verwendung des von der Datenbank bereitgestellten öffentlichen kryptographischen Schlüssels des Inhabers von dem zweiten elektronischen Gerät geprüft werden kann, ob der Sender des virtuellen Dokuments auch tatsächlich dessen Inhaber und zu dessen Nutzung berechtigt ist.

[0106] Die Kennung ist dabei ein Datensatz, welcher dazu geeignet ist eine individuelle Übertragung des virtuellen Dokuments von dem ersten elektronischen Gerät an das zweite elektronische Gerät zu identifizieren.

[0107] Bei einer gesicherten Aufbewahrung des privaten kryptographischen Schlüssels des Inhabers des virtuellen Dokuments, wie etwa in einem geschützten Speicherbereich des ersten elektronischen Geräts, verfügt allein der Inhaber des virtuellen Dokuments, der zugleich Besitzer des ersten elektronischen Geräts sein sollte, über den entsprechenden privaten kryptographischen Schlüssel. Somit kann sichergestellt werden, dass eine bestimmte Übertragung des virtuellen Dokuments mit Wissen und Einverständnis des Inhabers des entsprechenden virtuellen Dokuments erfolgt. Dieses Wissen und Einverständnis wird durch die Signatur mit dem entsprechenden privaten kryptographischen Schlüssel bestätigt. Die Authentizität der Signatur wird wiederum durch den in der Datenbank hinterlegten öffentlichen kryptographischen Schlüssel gewährleistet, welcher dem privaten kryptographischen Schlüssel des Inhabers zugeordnet ist. Wenn die Prüfung der Signatur mit dem der Datenbank entnommen öffentlichen kryptographischen Schlüssel erfolgreich ist, wird die Signatur und damit die vorliegende Verwendung des virtuellen Dokuments als zulässig anerkannt.

[0108] Nach Ausführungsformen umfasst das virtuelle Dokument den öffentlichen kryptographischen Schlüssel des dem Inhaber des virtuellen Dokuments zugeordneten asymmetrischen Schlüsselpaars. Nach Ausführungsformen umfasst die Datenbank den öffentlichen kryptographischen Schlüssel des Inhabers des virtuellen Dokuments. Beispielsweise kann die Datenbank einen weiteren mit dem privaten kryptographischen Schlüssel des Ausstellers signierten Eintrag umfassen, in welchem der öffentlichen kryptographischen Schlüssel des Inhabers des virtuellen Dokuments hinterlegt ist. Beispielsweise kann die Datenbank den öffentlichen kryptographischen Schlüssel des Inhabers des virtuellen Dokuments als eine Adresse umfassen, welcher das virtuelle Dokument zugeordnet ist. Nach Ausführungsformen umfasst die Datenbank ein Zertifikat, welches dem asymmetrischen Schlüsselpaar des Inhabers des virtuellen Dokuments zugeordnet ist, den öffentlichen kryptographischen Schlüssel des Inhabers umfasst und dessen Authentizität bestätigt. Nach Ausführungsformen wird die Authentizität des entsprechenden Zertifikats durch eine PKI belegt, welche beispielsweise von der Datenbank umfasst ist.

[0109] Nach Ausführungsformen umfasst die Kennung einen öffentlichen Schlüssel eines dem zweiten elektronischen Gerät zugeordneten asymmetrischen Schlüsselpaars. Ausführungsformen können den Vorteil haben, dass aus der Kennung somit ersichtlich ist, dass das virtuelle Dokument an das zweite elektronische Gerät adressiert ist. Alternative oder zusätzlich kann die Kennung auch ein Datum, eine Zeitangabe, eine Ortsangabe, eine Kennnummer, wie etwa eine Kennnummer der Übertragung, des ersten und/oder des zweiten elektronischen Geräts, ein Passwort, einen symmetrischen kryptographischen Schlüssel und/oder eine Angabe zu einem Verwendungszweck umfassen. Ausführungsformen können den Vorteil haben, dass das virtuelle Dokument anhand der Kennung einer bestimmten Übertragung zugeordnet wird.

[0110] Da der signierte Hashwert aus dem virtuellen Dokument und einer Kennung berechnet wird, kann anhand der Kennung geprüft werden, ob das entsprechende virtuellen Dokument auch tatsächlich von seinem Inhaber für die konkrete Übertragung und damit einen bestimmten Verwendungszweck freigegeben wurde.

[0111] Somit kann beispielsweise verhindert werden, dass der Empfänger des virtuellen Dokuments, z.B. der Besitzer des zweiten elektronischen Geräts, das empfangene virtuelle Dokument missbräuchlich, d.h. ohne Einverständnis des Inhabers, verwendet. Beispielsweise könnte der Besitzer des zweiten elektronischen Geräts behaupten, er handle im Namen des Inhabers des virtuellen Dokuments und als Nachweis das virtuellen Dokument vorweist. Ebenso wäre es möglich, dass der Besitzer des zweiten elektronischen Geräts versucht sich unter Verwendung des virtuellen Dokuments als dessen Inhaber auszugeben. All diese Versuche können effektiv unterbunden durch die Zuordnung zu einer bestimmten Übertragung mittel der Kennung, die durch die Signatur kryptographisch gesichert wird.

[0112] Nach Ausführungsformen wird der signierte Hashwert aus dem virtuellen Dokument und der Kennung zusammen mit dem virtuellen Dokument durch das erste Gerät mit dem kryptographischen Schlüssel des zweiten Geräts verschlüsselt und in verschlüsselter Form an das zweite Gerät gesendet, welches den verschlüsselten Datensatz mithilfe seines privaten Schlüssels entschlüsseln kann.

[0113] Nach Ausführungsformen ist der in der Datenbank gespeicherte Hashwert des virtuellen Dokuments mit einem privaten Schlüssel eines einem Aussteller des virtuellen Dokuments zugeordneten asymmetrischen Schlüsselpaars signiert. Das Verfahren umfasst ferner: Überprüfen der Signatur des in dem identifizierten Datenbankeintrag gespeicherten Hashwerts durch das zweite elektronische Gerät unter Verwendung eines öffentlichen kryptographischen Schlüssels des dem Aussteller zugeordneten asymmetrischen Schlüsselpaars. Ausführungsformen können den Vorteil haben, dass die Authentizität des Datenbankeintrags gesichert ist. Anhand der Signatur kann geprüft werden, dass der Hashwert, welcher die Grundlage für die Bestätigung der Echtheit des virtuellen Dokuments bildet, von einer dazu berechtigten und vertrauenswürdigen Instanz eingetragen wurde.

[0114] Nach Ausführungsformen umfasst die Datenbank zusätzlich den öffentlichen kryptographischen Schlüssel des Ausstellers. Ausführungsformen können den Vorteil haben, dass somit auch im Offline-Modus des zweiten elektronischen Geräts ein Zugriff auf den öffentlichen kryptographischen Schlüssel des Ausstellers ermöglicht wird. Handelt es sich bei der Datenbank zudem um eine Datenbank mit einer Blockchain-Struktur, wobei der öffentliche kryptographische Schlüssel des Ausstellers in einer der Transaktionen gespeichert ist, so wird der öffentliche kryptographische Schlüssel durch die mittels der Prüfsummenspeicherung gesicherten Kettenstruktur der Blockchain vor Manipulationen geschützt.

[0115] Nach Ausführungsformen umfasst der Datenbankeintrag zusätzlich den öffentlichen kryptographischen Schlüssel des Ausstellers. Ausführungsformen können den Vorteil haben, dass sie einen einfachen Zugriff auf den öffentlichen kryptographischen Schlüssel ermöglichen. Beispielsweise kann der Datenbankeintrag den öffentlichen kryptographischen Schlüssel des Ausstellers als eine Adresse umfassen, welcher das virtuelle Dokument zugeordnet ist. Nach Ausführungsformen umfasst der Datenbankeintrag ein dem asymmetrischen Schlüsselpaar des Ausstellers zugeordnetes Zertifikat, welches den öffentlichen kryptographischen Schlüssel des Ausstellers umfasst und dessen Authentizität bestätigt. Nach Ausführungsformen wird die Authentizität des entsprechenden Zertifikats durch eine PKI belegt, welche beispielsweise von der Datenbank bereitgestellt wird.

[0116] Nach Ausführungsformen wird die Speicher-ID zusammen mit dem virtuellen Dokument durch das erste Gerät mit dem kryptographischen Schlüssel des zweiten Geräts verschlüsselt. Ausführungsformen können den Vorteil haben, dass sie die Sicherheit weiter erhöhen.

[0117] Nach Ausführungsformen umfasst das virtuelle Dokument selbst die Speicher-ID. Ausführungsformen können den Vorteil haben, dass sie ein einfaches Auffinden der Speicher-ID und damit des Datenbankeintrags sicherstellen.

[0118] Nach Ausführungsformen ist das virtuelle Dokument in einem geschützten Speicherbereich des ersten Speichers gespeichert. Ausführungsformen können den Vorteil haben, dass das virtuelle Dokument und insbesondere die darin enthaltenen Daten effektiv gegen unerlaubte Zugriffe geschützt werden können und der Besitzer des ersten elektronischen Geräts sich die Verfügungshoheit über das virtuelle Dokument sichern kann.

[0119] Nach Ausführungsformen wird die kryptographisch gesicherte Datenbank auf dem zweiten elektronischen Gerät in einem regelmäßigen Intervall geupdated, wobei das virtuelle Dokument eine Angabe umfasst, welche den Beginn seiner Gültigkeit definiert und der Beginn der Gültigkeit so gewählt ist, dass die Zeitdifferenz zwischen der Eintragung des Hashwerts des virtuellen Dokuments in die Blockchain und dem Beginn der Gültigkeit größer als das Updateintervall ist. Ausführungsformen können den Vorteil haben, dass die auf dem zweiten elektronischen Gerät gespeicherte Blockchain stets die Hashwerte aller gültigen virtuellen Dokumente umfasst.

[0120] Nach Ausführungsformen umfasst das erste elektronische Gerät ein erstes Display und eine erste Digitalkamera. Das zweite elektronische Gerät umfasst ein zweites Display und eine zweite Digitalkamera. Das Übertragen des verschlüsselten virtuellen Dokuments umfasst:

- Anzeigen des verschlüsselten virtuellen Dokuments auf dem ersten Display,
- Aufnehmen des dargestellten verschlüsselten virtuellen Dokuments mit der zweiten Digitalkamera.

[0121] Ausführungsformen können den Vorteil haben, dass die Übertragung des verschlüsselten virtuellen Dokuments über einen optischen Kanal erfolgt. Eine Kommunikation kann über einen optischen Kanal zwischen zwei optischen Schnittstellen erfolgen. Bei den beiden optischen Schnittstellen kann es sich beispielsweise um ein Display zum Anzeigen bzw. Senden optischer Daten und eine Digitalkamera zur Aufnahme bzw. zum Empfang der optischen Daten handeln. Derartige Schnittstellen sind mittlerweile beispielsweise in allen Smartphones verfügbar ist. Ausführungsformen können zudem den Vorteil haben, dass eine gerichtet Übertragung mittels des Displays durch ein entsprechendes Ausrichten des Displays besser gegenüber Ausspähversuchen Dritter gesichert werden kann, als beispielsweise eine ungerichtete Übertragung mittels RFID oder Bluetooth.

[0122] Nach Ausführungsformen wird das verschlüsselte virtuelle Dokument auf dem ersten Display als zeitlich kodierter graphischer Code in Form eines Videostreams angezeigt. Ausführungsformen können den Vorteil haben, dass auch größere Datenmenge übertragen werden können. Dies mag etwa erforderlich sein, wenn das zu übertragende virtuelle Dokument ein Foto des Dokumenteninhabers umfasst. Insbesondere können Datenmengen übertragen werden, welche die Kapazität üblicher zweidimensionaler graphischer Codes, wie etwa von QR-Codes, übersteigen. Dies wird durch die zusätzliche Dimension der Kodierung, d.h. die zeitliche Abfolge einer Mehrzahl zweidimensionaler graphischer Codes, erreicht. Diese zusätzliche Dimension der Kodierung ist insbesondere unabhängig von der Größe des zur Übertragung verwenden Displays. So-

mit kann beispielsweise durch eine Erhöhung der Anzahl zweidimensionaler graphischer Codebilder in der zeitlichen Abfolge eine aufgrund einer beschränkten Bildschirmgröße reduzierten Größe der einzelnen zweidimensionalen graphischen Codebilder des Videostreams kompensiert werden. Nach Ausführungsbeispielen wird der Videostream in einer Endlosschleife angezeigt. Ausführungsformen können den Vorteil haben, dass sie ein vollständiges Erfassen der übertragenen Daten auch ohne aufwendige Abstimmung vom Beginn der Darstellung auf dem ersten Display und dem Beginn der Aufnahme mittels der zweiten Digitalkamera notwendig machen.

[0123] Nach Ausführungsformen handelt es sich bei dem zeitlich kodierten graphischen Code um einen QR-Codestream. Ausführungsformen können den Vorteil haben, dass es sich bei den einzelnen Bildern des Videostreams jeweils um einen QR-code handelt. Somit kann eine effiziente und sichere Datenübertragung ermöglicht werden.

[0124] Nach Ausführungsformen umfasst das Übertragen des dem zweiten elektronischen Gerät zugeordneten kryptographischen Schlüssels:

- Anzeigen des kryptographischen Schlüssels auf dem zweiten Display,
- Aufnehmen des dargestellten kryptographischen Schlüssels mit der ersten Digitalkamera.

[0125] Ausführungsformen können den Vorteil haben, dass das sie eine sichere und effiziente Übertragung des kryptographischen Schlüssels auf Basis von Standardhardware ermöglichen.

[0126] Nach Ausführungsformen wird der dem zweiten elektronischen Gerät zugeordnete kryptographische Schlüssel auf dem zweiten Display als graphischer Code angezeigt. Nach Ausführungsformen handelt es sich bei dem kodierten graphischen Code um einen QR-Code. Ausführungsformen können den Vorteil haben, dass sie eine sichere und effiziente Übertragung des kryptographischen Schlüssels ermöglichen. Der Schlüssel wird hierzu vor dem Senden von dem zweiten elektronischen Gerät graphisch kodiert und von dem empfangenden ersten elektronischen Gerät wieder dekodiert.

[0127] Nach Ausführungsformen handelt es sich bei dem kryptographischen Schlüssel des zweiten elektronischen Geräts um den öffentlichen Schlüssel des dem zweiten elektronischen Gerät zugeordneten asymmetrischen Schlüsselpaars und das Entschlüsseln des verschlüsselten virtuellen Dokuments erfolgt unter Verwendung eines privaten Schlüssels des asymmetrischen Schlüsselpaars, welcher in einem geschützten Speicherbereich des zweiten Speichers gespeichert ist. Ausführungsformen können den Vorteil haben, dass das sie eine sichere Schlüsselübertragung sowie Verschlüsselung des virtuellen Dokuments ermöglichen.

[0128] Nach Ausführungsformen handelt es sich bei dem kryptographischen Schlüssel des zweiten elektronischen Geräts um einen symmetrischen kryptographischen Schlüssel. Ausführungsformen können den Vorteil haben, dass sie eine schnelle Verschlüsselung und Entschlüsselung des virtuellen Dokuments ermöglichen.

[0129] Nach Ausführungsformen handelt es sich bei dem ersten und/oder zweiten elektronischen Gerät um ein Mobilfunkgerät, insbesondere ein Smartphone. Ausführungsformen können den Vorteil haben, dass das Standardhardware zum implementieren des Verfahrens verwendet werden kann. Insbesondere können Ausführungsformen den Vorteil haben, dass Smartphones die für eine optische Übertragung notwendige Hardware, d.h. Display und Digitalkamera, standardmäßig umfassen.

[0130] Nach Ausführungsformen befindet sich das erste und/oder zweite elektronische Gerät in einem Offline-Modus. Ausführungsformen können den Vorteil haben, dass das Verfahren auch im Offline-Modus der Geräte ohne Internetverbindung oder ähnliches ausführbar ist.

[0131] Nach Ausführungsformen wird das virtuelle Dokument nach der Offline-Echtheitsprüfung automatisch von dem zweiten elektronischen Gerät gelöscht. Ausführungsformen können den Vorteil haben, dass sichergestellt werden kann, dass allein der Besitzer des ersten elektronischen Geräts die Verfügungshoheit über das virtuelle Dokument sowie der darin enthaltenen Daten besitzt. Insbesondere kann so sichergestellt werden, dass abgesehen von der Echtheitsprüfung außerhalb des ersten elektronischen Geräts allein der Hashwert des virtuellen Dokuments zur Verfügung steht. So erfolgen beispielsweise zunächst eine Echtheitsprüfung sowie eine Auswertung der von dem virtuellen Dokument umfassten Daten und anschließend wird das virtuelle Dokument gelöscht.

[0132] Ausführungsformen umfassen ferner ein System zur Offline-Echtheitsprüfung eines virtuellen Dokuments. Das System umfasst ein erstes und ein zweites elektronisches Gerät. Das erste elektronische Gerät umfasst einen ersten Speicher, in welchem das virtuelle Dokument und eine Speicher-ID des virtuellen Dokuments gespeichert sind. Das zweite elektronische Gerät umfasst einen zweiten Speicher, in welchem eine kryptographisch gesicherte Datenbank gespeichert ist, welche Hashwerte von einer Mehrzahl von virtuellen Dokumenten umfasst. Die Speicher-ID des virtuellen Dokuments identifiziert einen Eintrag der Datenbank mit dem Hashwert des virtuellen Dokuments. Das System ist dazu konfigu-

riert ein Verfahren nach einer der zuvor beschriebenen Ausführungsformen auszuführen.

[0133] Im Weiteren werden Ausführungsformen der Erfindung mit Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen:

Fig. 1 ein Blockdiagramm einer Ausführungsform eines exemplarischen Systems zum Ausstellen einer virtuellen Version eines Dokuments,

Fig. 2 ein schematisches Diagramm einer Ausführungsform eines exemplarischen Dokuments,

Fig. 3 ein Flussdiagramm einer Ausführungsform eines exemplarischen Verfahrens zum Ausstellen einer virtuellen Version eines Dokuments,

Fig. 4 ein Blockdiagramm einer Ausführungsform eines exemplarischen Systems zur Offline-Echtheitsprüfung eines virtuellen Dokuments,

Fig. 5 ein Flussdiagramm einer ersten Ausführungsform eines exemplarischen Verfahrens zur Offline-Echtheitsprüfung eines virtuellen Dokuments, und

Fig. 6 ein Flussdiagramm einer zweiten Ausführungsform eines exemplarischen Verfahrens zur Offline-Echtheitsprüfung eines virtuellen Dokuments.

[0134] Elemente der nachfolgenden Ausführungsformen, die einander entsprechen, werden mit denselben Bezugszeichen gekennzeichnet.

[0135] **Fig. 1** zeigt ein exemplarisches System zum Ausstellen einer virtuellen Version **164** eines Dokuments **160**. Das System umfasst ein Computersystem **100** mit einem Speicher **102**, einem Prozessor **112** und einer Kommunikationsschnittstelle **120**. In dem Speicher **102** ist ein dem ID-Provider zugeordneter asymmetrisches kryptographisches Schlüsselpaar gespeichert. Das asymmetrisches kryptographisches Schlüsselpaar umfasst einen privaten kryptographischen Schlüssel **106**, welcher in dem geschützten Speicherbereich **104** gespeichert ist, sowie einen öffentlichen kryptographischen Schlüssel **108**. Auf den geschützten Speicherbereich **104** ist ein Zugriff nur über eines Prozessors **112** des Computersystems **100** möglich ist. Der private kryptographische Schlüssel **106** dient zum Ausstellen digitaler Signaturen, einschließlich digitaler Siegel, durch den ID-Provider. Beispielsweise wird mit dem privaten kryptographischen Schlüssel **106** ein für das virtuelle Dokument **164** berechneter Hashwert signiert.

[0136] Eine kryptographisch gesicherte Datenübertragung von dem Computersystem **170** des Besitzers **150** des Dokuments **160** an das Computersystem **100** des ID-Providers kann beispielsweise implementiert werden, indem das Computersystem **100** dem Computersystem **170** den öffentlichen kryptographischen Schlüssel **108** zur Verschlüsselung zur Verfügung stellt. Mit dem öffentlichen kryptographischen Schlüssel **108** verschlüsselte Daten, welche das Computersystem **100** von dem Computersystem **170** empfängt, können mit dem sicher gespeicherten privaten Schlüssel **106** entschlüsselt werden. Nach Ausführungsformen ist in dem Speicher **102** ein weiteres asymmetrisches Schlüsselpaar gespeichert, dessen öffentlicher kryptographischer Schlüssel dem Computersystem **170** zur Verschlüsselung der Datenübertragung an das Computersystem **100** zur Verfügung gestellt wird. In diesem Fall dient der private kryptographische Schlüssel **106** allein dem Signieren des berechneten Hashwerts des virtuellen Dokuments **164**.

[0137] Ferner ist in dem Speicher **102** eine kryptographische Datenbank in Form einer Blockchain **110** gespeichert. Wenn das Computersystem **100** ein virtuelles Dokument **164** ausstellt, trägt es einen signierten Hashwert des virtuelles Dokument **164** in die Blockchain **110**. Hierzu erzeugt das Computersystem **100** entweder selbst einen neuen Block der Blockchain **110**, welcher eine Transaktion mit dem signierten Hashwert des virtuelles Dokument **164** umfasst. Die Blockchain110 ist auf einer Mehrzahl von Knoten eines Netzwerks redundant gespeichert. Das Computersystem **100** verbreitet den neu generierten Block an die anderen Teilnehmer, bzw. Knoten eines Netzwerks. Nach einer weiteren Ausführungsform wird die Transaktion von dem Computersystem **100** in ein Mining-Netzwerk, welches die redundanten Versionen der Blockchain umfasst, übertragen. Die Knoten des Netzwerks, welche die neuen Transaktion empfangen verifizieren die Signatur und prüfen, ob die Transaktion gültig ist. Anschließend beginnen die Knoten des Mining-Netzwerks die Transaktion zu verarbeiten, indem sie durch Mining einen neuen Block der Blockchain **100** erzeugen, in dem die Transaktion enthalten ist. Der neue Block wird dann über das Netzwerk verbreitet, sodass auch der Computer **100** den neuen Block empfangen, diesen prüfen und der Blockchain **110** hinzufügen kann.

[0138] Der Prozessor **112** ist dazu konfiguriert kryptographische Programminstruktionen **114** auszuführen, welche ein kryptographisches Protokoll implementieren. Das kryptographische Protokoll ist insbesondere zur Sicherung des Datenaustauschs mit dem Computersystem **170** sowie zur Erzeugung von Hashwerten und/oder Signaturen konfiguriert. Beispielsweise dient das kryptographischen Protokoll dazu an das Computersystem **170** zu sendende Daten zu verschlüsseln und von dem Computersystem **170** empfangene Daten zu entschlüsseln. Ferner dient das kryptographischen Protokoll beispielsweise dazu einen Hashwert des virtuellen Dokuments **164**

zu berechnen und diesen mit dem privaten Schlüssel **106** zu signieren. Der Prozessor **112** ist ferner konfiguriert Programminstruktionen **116** auszuführen, welche ein Blockchain-Protokoll implementieren, durch dessen Ausführung der Prozessor **112** das Computersystem **100** so steuert, dass neue Transaktionen für die Blockchain generiert und in diese eingetragen werden. Schließlich ist der Prozessor **112** dazu konfiguriert Programminstruktionen **118** auszuführen, welche ein Protokoll zur Ausstellung des virtuellen Dokuments **164** implementieren. Durch Ausführung der Programminstruktionen **118** wird das Computersystem **100** so von dem Prozessor **112** derart gesteuert, dass es das virtuelle Dokument **164** ausstellt, welches eine virtuelle Kopie des Dokuments **160** ist.

[0139] Die Kommunikationsschnittstelle **120** ist zur Kommunikation mit dem Computersystem **170** über ein Netzwerk **140** konfiguriert. Die Kommunikation kann kabellos oder über ein Kabel erfolgen. Bei einer kabellosen Verbindung kann es sich insbesondere um beispielsweise um eine WLAN-Verbindung handeln. Beispielsweise kann es sich bei dem Netzwerk **140** um ein öffentliches Computernetzwerk, wie etwa das Internet, oder ein Intranet handeln.

[0140] Das Computersystem **170** des Besitzers **150** des Dokuments **160** ist dazu konfiguriert dem Computersystem **100** Daten zum Ausstellen einer virtuellen Version, d.h. eines virtuellen Dokuments **164**, des physischen Dokuments **160** bereitzustellen. Bei dem Computersystem **170** kann es sich beispielsweise um ein mobiles Computersystem, wie etwa ein Laptop oder Smartphone, oder ein stationäres Computersystem, wie etwa einen PC, handeln. Das Dokument **160** umfasst einen Dokumentenkörper, auf welchem ein Satz Daten wiedergeben ist. Das Computersystem **170** umfasst einen Speicher **172** mit einem geschützten Speicherbereich **174**. Auf den geschützten Speicherbereich **104** ist ein Zugriff nur über eines Prozessors **180** des Computersystems **170** möglich ist. In dem Speicher **172** ist ein dem Besitzer **150** des Dokuments **160** zugeordneter asymmetrisches kryptographisches Schlüsselpaar gespeichert. Das asymmetrisches kryptographisches Schlüsselpaar umfasst einen privaten kryptographischen Schlüssel **176**, welcher in dem geschützten Speicherbereich **174**, gespeichert ist sowie einen öffentlichen kryptographischen Schlüssel **178**. Indem das Computersystem **170** dem Computersystem **100** den öffentlichen kryptographischen Schlüssel **178** zur Verschlüsselung von an das Computersystem **170** gesendeten Daten zur Verfügung stellt, kann eine sichere Datenübertragung von dem Computersystem **100** an das Computersystem **170** implementiert werden. Die mit dem öffentlichen kryptographischen Schlüssel **178** verschlüsselten Daten können von dem Computersystem **170** mit dem sicher gespeicherten privaten Schlüssel **176** entschlüsselt werden. Zudem kann das Computersystem **100** den öffentlichen kryptographischen Schlüssel **178** in das virtuelle Dokument **164** als dem Inhaber **150** des virtuellen Dokuments **164** zugeordneten öffentlichen kryptographischen Schlüssel aufnehmen.

[0141] Ferner umfasst das Computersystem **170** einen Prozessor **180** mit kryptographischen Programminstruktionen **182**, welche ein kryptographischen Protokoll implementieren. Das kryptographische Protokoll ist insbesondere zur Sicherung des Datenaustauschs mit dem Computersystem **100** konfiguriert. Beispielsweise dient das kryptographischen Protokoll dazu an das Computersystem **100** zu sendende Daten zu verschlüsseln und von dem Computersystem **100** empfangene Daten zu entschlüsseln. Zudem umfasst das Computersystem **170** ein Display **190** und ein Eingabeinterface **184** zur Steuerung des Computersystems **170** durch den Besitzer **150** des Dokuments **160**. Beispielsweise kann das Eingabeinterface **184** in das Display 122 integriert sein, falls dieses als Touchscreen konfiguriert ist. Ferner umfasst das Computersystem **170** eine Digitalkamera **186** zum Aufnehmen von Bildern von dem Dokument **160** und dessen Besitzer **150**, wobei die Bandaufnahmen vorzugsweise unter verschiedenen Blickwinkeln erfolgen, beispielsweise in Form einer Mehrzahl von Einzelaufnahmen oder in Form einer Videosequenz. Schließlich umfasst das Computersystem **170** noch eine Kommunikationsschnittstelle **190** zur Kommunikation mit dem Computersystem **100** über das Netzwerk **140**. Die Kommunikation kann kabellos oder über ein Kabel erfolgen. Bei einer kabellosen Verbindung kann es sich insbesondere um beispielsweise um eine WLAN-Verbindung handeln.

[0142] Das Computersystem **170** sendet die mittels der Digitalkamera **186** gemachten Bildaufnahmen **162** kryptographisch gesichert über das Netzwerk **140** an das Computersystem **100**. Das Computersystem **100** wertet die empfangenen Bildaufnahmen **162** aus, extrahiert Daten und erzeugt, falls die Bildaufnahmen **162**, das Dokument **160** und der Besitzer **150** authentisch sind, ein virtuelles Dokument **164** unter Verwendung der extrahierten Daten. Das so erzeugte virtuelles Dokument **164** wird als signierter Hashwert in die Blockchain **110** eingetragen und zusammen mit dem öffentlichen Schlüssel **108** kryptographisch gesichert über das Netzwerk **140** an das Computersystem **170** gesendet.

[0143] **Fig. 2** zeigt ein Dokument **160**, welches zumindest ein visuellen Sicherheitsmerkmal **210** umfasst, dessen Aussehen mit dem Blickwinkel, unter dem es betrachtet wird, variiert. Somit ist das Aussehen des Sicherheitsmerkmal **210** in digitalen Bildaufnahmen des Dokuments **160**, welcher von der Digitalkamera **186** aufgenommen werden, abhängig von der relativen Ausrichtung zwischen dem Dokument **160** und der Digitalkamera **186**. Zur Authentifizierung des Dokuments **160** wird dieses mit der Digitalkame-

ra **186** unter verschieden Blickwinkel aufgenommen, indem das Dokument **160** beispielsweise um seine Längsachse **222** und/oder seine Querachse **220** rotiert wird. Handelt es sich bei dem Sicherheitsmerkmal **210** um ein authentisches Sicherheitsmerkmal, ändert sich dessen Aussehen in einer festgelegten Weise in Abhängigkeit von dem Blickwinkel unter welchem die Digitalkamera **186** das Dokument **160**, insbesondere in Form einer Videosequenz, aufnimmt. Die Aufnahme des Dokuments **160** erfolgt beispielsweise in Form eines assistierten Verfahrens, bei welchem dem Besitzer des Dokuments **160** Anweisungen und/oder Rückmeldungen zur Verfügung gestellt werden zur korrekten relativen Ausrichtung zwischen dem Dokument **160** und der Digitalkamera **186**. Diese Anweisung können neben dem Blickwinkel beispielsweise auch den Abstand, die laterale Ausrichtung in der Bildebene und/oder die Beleuchtung des Dokuments **160** betreffen.

[0144] Bei dem Dokument **160** kann es sich beispielsweise um ein Ausweisdokument handeln, welches visuell Daten **206**, **208** des Inhabers des Dokuments **160** wiedergibt. Diese Daten **208** können beispielsweise in Textform Attribute des Inhabers umfassen, wie etwa dessen Namen, Wohnort, Nationalität etc. sowie Attribute des Dokuments **160**, wie etwa eine Dokumenten-ID, ein Ausstellungsdatum, ein Gültigkeitsdatum, die ausstellende Institution etc. Beispielsweise umfassen die Daten **208** einen maschinenlesbaren Bereich („Machine Readable Zone“, abgekürzt MRZ), beispielsweise nach dem Standard ICAO Dokument 9303. Im Falle eines Führerscheins kann das Dokument **160** beispielsweise zusätzlich Attribute des Inhabers enthalten, welche die Fahrzeugklassen angeben, für welche der Inhaber des Führerscheins eine Berechtigung zum Führen von Fahrzeugen besitzt. Die Daten **206** können ferner ein Bild des Inhabers des Dokuments **160** umfassen.

[0145] Das Dokument kann relevante Daten sowohl auf seiner Vorderseite **202** als auch auf seiner Rückseite **204** umfassen. Vorzugsweise werden mit der Digitalkamera **186** Bildaufnahmen daher sowohl der Vorderseite **202** als auch auf der Rückseite **204** des Dokuments **160** unter verschieden Blickwinkeln gemacht.

[0146] Fig. 3 zeigt ein Flussdiagramm einer Ausführungsform eines exemplarischen Verfahrens zum Ausstellen einer virtuellen Version eines Dokuments durch ein Computersystem eines ID-Providers. Das Verfahren zur Ausstellung eines virtuellen Dokuments wird im Folgenden am Beispiel eines Führerscheindokumentes beschrieben. In Block 300 empfängt das Computersystem eines ID-Provider eine Anfrage zum Ausstellen des virtuellen Dokuments von einem Computersystem des Besitzers eines physischen Originaldokuments, d.h. eines herkömmlichen Führerescheins. In Block 302 erfolgt eine Authentifizierung des Computersystems des ID-Providers durch das Computersystem des Besitzers. Beispielsweise überträgt das Computersystem des ID-Providers ein Zertifikat mit einem öffentlichen Schlüssel eines dem ID-Provider zugeordneten asymmetrischen Schlüsselpaars an das Computersystem des Besitzers. Durch Ausführen eines kryptographischen Protokolls wird sodann durch das Computersystem des Besitzers eine so genannte Challenge generiert, d.h. beispielsweise eine Zufallszahl. Diese Zufallszahl wird mit dem in dem empfangenen Zertifikat enthaltenen öffentlichen Schlüssel verschlüsselt. Das resultierende Chiffrat wird von dem Computersystem des Besitzers an das Computersystem des ID-Providers gesendet. Durch Ausführen eines kryptographischen Protokolls entschlüsselt das Computersystem des ID-Providers das Chiffrat mit Hilfe eines privaten Schlüssels, welcher dem zuvor mit dem Zertifikat an das Computersystem des Besitzers gesendeten öffentlichen Schlüssel zugeordnet ist, und erhält so die Zufallszahl. Die Zufallszahl sendet das Computersystem des ID-Providers an das Computersystem des Besitzers zurück. Durch Ausführung des kryptographischen Protokolls wird dort geprüft, ob die von dem Computersystem des ID-Providers empfangene Zufallszahl mit der ursprünglich generierten Zufallszahl, d.h. der Challenge, übereinstimmt. Ist dies der Fall, so gilt das Computersystem des ID-Providers als gegenüber dem Computersystem des Besitzers authentifiziert. In analoger Weise kann zusätzlich eine Authentifizierung des Computersystems des Besitzers durch das Computersystem des ID-Providers erfolgen unter Verwendung eines Zertifikats mit einem öffentlichen Schlüssel des Computersystems des Besitzers. In Block 304 wird ein sicherer Kommunikationskanal zwischen dem Computersystem des ID-Providers erfolgen und dem Computersystem des Besitzers aufgebaut, beispielsweise mittels eine Ende-zu-Ende Verschlüsselung. Für die Ende-zu-Ende Verschlüsselung kann beispielsweise die zuvor brechente Zufallszahl als symmetrischer Schlüssel verwendet werden.

[0147] In Block 306 wird eine Abfrage von Daten des Führerscheins an das Computersystem des Besitzers gesendet. Die Datenabfrage umfasst dabei beispielsweise eine Aufforderung Bildaufnahmen des Führerscheins, vorzugsweise als Videosequenz, unter verschieden Blickwinkel anzufertigen, sodass sowohl Sicherheitsmerkmale identifiziert als auch von dem Führerschein Daten gelesen werden können. Hierzu können in einem assistierten Prozess sowohl Informationen zur korrekten relativen Ausrichtung zwischen dem Dokument und der Digitalkamera zur Verfügung stellt als auch Rückmeldungen, ob die resultierende Aufnahmen die Voraussetzungen für eine erfolgreiche Auswertung durch das Computersystem des ID-Providers erfüllen. Ferner kann die Abfrage von Daten eine Aufforderung zum Erstellen von Bildaufnahmen des Besitzers des Füh-

rerscheins zu erstellen und/oder Daten des Führerscheins in ein mit der Abfrage bereitgestelltes Formular einzutragen. In Block 308 werden die abgefragten Daten, d.h. die Bildaufnahmen von Dokument und/oder Besitzer sowie ggf. das ausgefüllte Formular, empfangen. In Block 310 wird der Besitzer des Dokuments anhand der in Block 308 empfangen Daten authentifiziert. Hierzu wird beispielsweise die Bildaufnahme des Besitzers des Führerscheins mit dem auf dem Führerschein abgedruckten Bild des Führerscheininhabers abgeglichen. Stimmen beide Bilder in einem ausreichenden Maß überein, wird der Besitzer des Führerscheins als der Inhaber des Führerscheins identifiziert. Im Falle eines Dokuments ohne integriertes Foto des Inhabers, kann eine Authentifizierung des Besitzers des Dokuments eine Datenabfrage eines Ausweisdokuments des Besitzers, wie etwa eines Personalausweises, umfassen. Hierzu können in analoger Weise Bildaufnahmen des Ausweisdokuments empfangen werden und die Authentifizierung anhand des von dem Ausweisdokument bereitstellten Bildes des Ausweisinhabers sowie von Attributen zu dem Ausweisinhaber erfolgen. Die Attribute umfassen beispielsweise Namen, Geburtsdatum und Geburtsort des Ausweisinhabers. Umfasst auch das Dokument, von welchem eine virtuelle Kopie erstellt werden soll, diese Attribute, so kann der Besitzer des Dokuments diesem als legitimer Besitzer und Antragssteller zugeordnet werden. In Block 312 werden die abgefragten Daten verifiziert, wobei anhand der Bildaufnahmen des Führerscheins insbesondere geprüft wird, ob dieser die Sicherheitsmerkmale aufweist, welche ihn als ein authentisches Originaldokument kennzeichnen. Ist den Bildaufnahmen zu entnehmen, dass der Führerschein die korrekten Sicherheitsmerkmale aufweist, ist dieser authentifiziert und damit seine Daten verifiziert. Ferner werden beispielsweise die auf dem Führerschein wiedergegebene Daten in Textform mittels optische Zeichenerkennung extrahiert. Falls zusätzliche Texteingaben des Besitzers übermittelt wurden, können die mittels optische Zeichenerkennung extrahierten Daten unter Verwendung der eingegebenen Daten auf ihre Korrektheit überprüft und ggf. korrigiert werden.

[0148] In Block 314 wird aus den extrahierten Daten das virtuelle Dokument als virtuelle Kopie des Führerscheins erstellt, welche einen elektronischen Datensatz umfasst. Dieser Datensatz umfasst neben den mittels optischer Zeichenerkennung extrahierten Daten auch das auf dem Führerschein abgebildeten Bildes des Inhabers. Nach Ausführungsformen umfasst das virtuelle Dokument zudem einen öffentlichen kryptographischen Schlüssel eines dem Inhaber des virtuellen Dokuments zugeordneten asymmetrischen Schlüsselpaars. Nach Ausführungsformen wird vor der Aufnahme des öffentlichen kryptographischen Schlüssels in das virtuelle Dokument, die Authentizität des entsprechenden Schlüssels unter Verwendung eines dem Schlüssel zugeordneten Zertifikats überprüft. In Block 316 wird ein Hashwert des ausgestellten virtuellen Führerscheins berechnet und in Block 318 mit einem privaten kryptographischen Schlüssel des ID-providers signiert. In Block 320 wird eine Transaktion für die Blockchain erzeugt, welche den signierten Hashwert des virtuellen Führerscheins umfasst. In Block 322 wird die Transaktion in einen neuen Block der Blockchain eingetragen, welcher in einem entsprechenden Mining-Prozess erzeugt wird. Das Erzeugen des neuen Blocks mit der darin eingetragenen Transaktion erfolgt beispielsweise durch das Computersystem des ID-Providers. Nach weiteren Ausführungsformen erfolgt das Erzeugen des neuen Blocks durch ein weiteres Computersystem eines Miningnetzwerks zum Erzeugen neuer Blöcke der Blockchain. In Block 324 wird das virtuelle Führerscheindokument zusammen mit der Transaktions-ID der Transaktion, welche den signierten Hashwert des virtuellen Führerscheins umfasst, über den sicheren Kanal an das Computersystem des Besitzers des originalen Führerscheins gesendet. Nach Ausführungsformen werden das virtuelle Führerscheindokument sowie die Transaktions-ID vor dem Senden von dem Computersystem des ID-Providers zusätzlich mit einem öffentlichen Schlüssel des Besitzers des originalen Führerscheins verschlüsselt.

[0149] Die **Fig. 4** zeigt ein Blockdiagramm einer Ausführungsform eines exemplarischen Systems zur Offline-Echtheitsprüfung eines virtuellen Dokuments **408**, wobei das System ein erstes und ein zweites elektronische Gerät **402**, **452** umfasst. Bei dem ersten elektronischen Gerät **402** des Nutzer **400** handelt es sich um ein tragbares Computersystem, beispielsweise ein Smartphone. Das Smartphone **402** umfasst einen Speicher **404** mit einem geschützten Speicherbereich **406** auf den ein Zugriff nur über einen Prozessor **412** des Smartphone **402** möglich ist. In dem geschützten Speicherbereich **406** ist ein virtuelles Dokument **408** gespeichert. Ferner kann in dem geschützten Speicherbereich **406** ein privater kryptographischer Schlüssel **407** eines dem Inhaber des virtuellen Dokuments zugeordneten asymmetrischen Schlüsselpaars gespeichert sein. Zudem ist in dem Speicher **404** eine Transaktions-ID **410** gespeichert, welche diejenige Transaktion in der Blockchain **462** identifiziert, in der ein signierter Hashwert des virtuellen Dokuments **408** gespeichert ist. Ferner kann in dem Speicher **404** ein öffentlicher kryptographischer Schlüssel **409** des dem Inhaber des virtuellen Dokuments zugeordneten asymmetrischen Schlüsselpaars gespeichert sein. Nach Ausführungsformen umfasst das virtuelle Dokument **408** den öffentlichen Schlüssel **409**. Nach Ausführungsformen ist das asymmetrische Schlüsselpaar aus privatem Schlüssel **407** und öffentlichem Schlüssel **409** identisch mit dem asymmetrischen Schlüsselpaar aus privatem Schlüssel **176** und öffentlichem Schlüssel **178** aus **Fig. 1**.

[0150] Ferner umfasst das Smartphone **402** einen Prozessor **412** mit kryptographischen Programminstruktionen **414**, welche ein kryptographischen Protokoll implementieren. Das kryptographische Protokoll ist insbesondere dazu konfiguriert das virtuelles Dokument **408** mit einem von dem zweiten elektronischen Gerät bereitgestellten öffentlichen Schlüssel **460** eines dem zweiten elektronischen Geräts **452** zugeordneten asymmetrischen Schlüsselpaar zu verschlüsseln. Zudem führt der Prozessor **412** Programminstruktionen **416** aus, welche dazu konfiguriert sind, eine graphische Kodierung von Daten zur Anzeige auf dem Display **422** des Smartphones **402** zu erzeugen sowie mittels Digitalkamera **420** aufgenommene graphisch kodierte Daten zu dekodieren.

[0151] Schließlich umfasst das Smartphone **402** noch ein Eingabeinterface **418**, welches beispielsweise in das Display **422** integriert sein kann, falls dieses als Touchscreen konfiguriert ist. Das Eingabeinterface **418** dient zur Steuerung des Smartphone **402** durch den Nutzer **400**. Das Display **422** ist zur Anzeige eines graphischen Codes, wie etwa eines QR-Codes geeignet. Insbesondere ist das Display **422** auch zur Anzeige eines zusätzlich zeitlich kodierten graphischen Codes geeignet, welcher als Videostream in einer Endlosschleife angezeigt wird. Beispielsweise handelt es sich bei dem Display **422** um ein bistabiles Display, E-Paper, LCD-Display („Liquid Crystal Display“), OLED-Display („Organic Light-Emitting Diode dis-play“), oder ein AMOLED-Display („Active Matrix Organic Light-Emitting Diode dis-play“). Zudem ist in das Smartphone **402** eine Digitalkamera **420** zur Aufnahme von Bildern und Videosequenzen integriert.

[0152] Bei dem zweiten elektronischen Gerät **452** des Verifizierers **450** handelt es sich beispielsweise ebenfalls um ein tragbares Computersystem, wie etwa ein Smartphone. Ebenso könnte es sich bei dem zweiten elektronischen Gerät **452** aber auch um ein speziell konfiguriertes Verifikationsgerät oder ein stationäres Computersystem handeln. Das Smartphone **452** umfasst einen Speicher **454** mit einem geschützten Speicherbereich **456** auf den ein Zugriff nur über einen Prozessor **464** des Smartphone **452** möglich ist. In dem geschützten Speicherbereich **456** ist ein privater Schlüssel **458** eines dem zweiten elektronischen Gerät **452** zugeordneten asymmetrischen Schlüsselpaars gespeichert. Zudem ist in dem Speicher **454** ein dem privaten Schlüssel **458** zugeordneter öffentlicher Schlüssel **460** gespeichert. Ferner ist in dem Speicher **454** eine kryptographische gesicherte Datenbank in Form einer Blockchain **462** gespeichert. In den Blöcken der Blockchain **462** sind signierte Hashwerte von einer Mehrzahl von virtuellen Dokumenten als Transaktionen gespeichert, wobei die Blockchain **462** auch eine Transaktion mit einem signierten Hashwert des virtuellen Dokuments **408** umfasst. Die Transaktion mit dem signierten Hashwert des virtuellen Dokuments **408** wird durch die Transaktions-ID **410** identifiziert.

[0153] Ferner umfasst das Smartphone **452** einen Prozessor **464** mit kryptographischen Programminstruktionen **466**, welche ein kryptographischen Protokoll implementieren. Das kryptographische Protokoll ist insbesondere dazu konfiguriert das mit dem öffentlichen kryptographischen Schlüssel **460** verschlüsselte virtuelles Dokument **408** mit dem privaten Schlüssel **458** zu entschlüsseln. Zudem führt der Prozessor Programminstruktionen **468** aus, welche dazu konfiguriert sind, eine graphische Kodierung von Daten zur Anzeige auf dem Display **474** des Smartphones **452** zu erzeugen sowie mittels Digitalkamera **472** aufgenommene graphisch kodierte Daten zu dekodieren.

[0154] Schließlich umfasst das Smartphone **452** noch ein Eingabeinterface **470**, welches beispielsweise in das Display **474** integriert sein kann, falls dieses als Touchscreen konfiguriert ist. Das Eingabeinterface **470** dient zur Steuerung des Smartphone **452** durch den Verifizierer **450**. Das Display **474** ist zur Anzeige eines graphischen Codes, wie etwa eines QR-Codes geeignet. Beispielsweise handelt es sich bei dem Display **474** um ein bistabiles Display, E-Paper, LCD-Display („Liquid Crystal Display“), OLED-Display („Organic Light-Emitting Diode display“), oder ein AMOLED-Display („Active Matrix Organic Light-Emitting Diode display“). Zudem ist in das Smartphone **452** eine Digitalkamera **472** zur Aufnahme von Bildern und Videosequenzen integriert.

[0155] Mittels des Displays **422** des Smartphones **402** und der Digitalkamera **472** des Smartphones **452** sowie mittels des Displays **474** des Smartphones **452** und der Digitalkamera **420** des Smartphones **402** kann ein bidirektionaler optischer Kommunikationskanal **480** zum Datenaustausch zwischen den beiden Smartphones **402** und **452** implementiert werden.

[0156] **Fig. 5** zeigt ein Flussdiagramm einer ersten Ausführungsform eines exemplarischen Verfahrens zur Offline-Echtheitsprüfung eines virtuellen Dokuments. Beispielsweise handelt es sich bei dem virtuellen Dokument um eine virtuelle Version eines Führerscheins. Im Fall einer Verkehrskontrolle, bei welche ein Polizist (Verifizierer) den Führerschein eines Fahrzeugführers (Besitzer) überprüfen möchte, überträgt der Fahrzeugführer das virtuelle Dokument beispielsweise von seinem Smartphone an ein Verifikationsgerät des Polizisten zu einer Offline-Echtheitsprüfung. Bei dem Verifikationsgerät kann es sich entweder ebenfalls um ein Smartphone handeln, auf welchem eine kryptographisch gesicherte Datenbank beispielsweise in Form einer Blockchain gespeichert ist, oder ein speziell für diese Zwecke konfiguriertes Gerät.

[0157] In Block 500 zeigt der Verifizierer seinen öffentlichen Schlüssel auf einem Display seines Verifikationsgeräts beispielsweise kodiert in Form eines QR-Codes an. In Block 502 scannt der Besitzer des virtuellen Dokuments den angezeigten öffentlichen Schlüssel des Verifizierers mit einer Digitalkamera seines Smartphones vom Display des Verifizierers ab und dekodiert diesen gegebenenfalls. In Block 504 verschlüsselt der Besitzer das virtuelle Dokument auf seinem Smartphone mit dem öffentlichen Schlüssel des Verifizierers. Das virtuelle Dokument ist in einer Blockchain registriert, auf welche der Verifizierer auch offline mit seinem Verifikationsgerät Zugriff hat, d.h. die Blockchain ist beispielsweise auf dem Verifikationsgerät gespeichert. Zusammen mit dem virtuellen Dokument wird auch die Transaktions-ID, unter der das virtuelle Dokument bzw. dessen Hashwert in der Blockchain registriert wurde, verschlüsselt. In Block 506 wird der verschlüsselte Datensatz aus virtuellem Dokument und Transaktions-ID in einem Videostream, beispielsweise einem QR-Codestream kodiert und in Block 508 von dem Besitzer in einer Endlosschleife auf dessen Display abgespielt.

[0158] In Block 510 scannt bzw. filmt der Verifizierer den angezeigten Videostream mit einer Digitalkamera seines Verifikationsgerätes vom Display des Smartphones des Besitzers ab. In Block 512 wird der gescannte Datensatz dekodiert, sobald dieser vollständig empfangen wurde. In Block 514 wird der dekodierte Datensatz mit dem privaten Schlüssel des Verifizierers entschlüsseln. In Block 516 berechnet der Verifizierer den Hashwert des empfangenen virtuellen Dokuments. In Block 518 wird die Signatur des in der Blockchain unter der Transaktions-ID gespeicherten Hashwerts mit dem öffentlichen Schlüssel des Ausstellers des virtuellen Dokuments geprüft. Dieser öffentlichen Schlüssel des Ausstellers wird beispielsweise zusammen mit dem virtuellen Dokument von dem Smartphone des Besitzers des virtuellen Dokuments bereitgestellt oder der öffentlichen Schlüssel ist in der Blockchain gespeichert. Ist die Signatur gültig, so wird in Block 520 der berechnete Hashwert mit dem in der Blockchain gespeicherten Hashwert verglichen. Wenn der berechnete Hashwert mit dem in der Blockchain unter der Transaktions-ID gespeicherten Hashwert übereinstimmt, ist die Echtheitsprüfung erfolgreich und damit das von dem Besitzer übertragene virtuelle Dokument gültig. Mit dem gültigen virtuellen Dokument, beispielsweise einer virtuellen Version eines Führerscheines, kann nun vom Polizisten anhand des Führerscheinfotos überprüft werden, ob es sich bei dem virtuellen Dokument auch tatsächlich um den Führerschein des Fahrzeugführers, der kontrolliert wird, handelt. Zudem kann der Verifizierer dem übertragenen virtuellen Dokument Informationen über den Besitzer entnehmen, deren Authentizität durch die erfolgreiche Echtheitsprüfung belegt wird. Er kann beispielsweise anhand der Führerscheindaten prüfen, ob der Fahrzeugführer zum Führen des Fahrzeugs, in dem er unterwegs ist, auch tatsächlich berechtigt ist.

[0159] **Fig. 6** zeigt ein Flussdiagramm einer zweiten Ausführungsform eines exemplarischen Verfahrens zur Offline-Echtheitsprüfung eines virtuellen Dokuments. Beispielsweise handelt es sich bei dem virtuellen Dokument um eine virtuelle Version eines Führerscheins wie in **Fig. 5**. Nach Ausführungsformen umfasst das virtuelle Dokument zudem einen öffentlichen kryptographischen Schlüssel, welcher dem Inhaber des Dokuments zugeordnet ist.

[0160] In Block 600 zeigt der Verifizierer seinen öffentlichen Schlüssel auf einem Display seines Verifikationsgeräts beispielsweise kodiert in Form eines QR-Codes an.

[0161] In Block 602 scannt der Besitzer des virtuellen Dokuments den angezeigten öffentlichen Schlüssel des Verifizierers mit einer Digitalkamera seines Smartphones vom Display des Verifizierers ab und dekodiert diesen gegebenenfalls. In Block 604 signiert der Besitzer das virtuelle Dokument zusammen mit einer Kennung auf seinem Smartphone, wobei die Kennung die auszuführende Übertragung an den Verifizierer, d.h. den aktuellen Verifizierungsvorgang, identifiziert. Die Kennung umfasst beispielsweise einen Zeitstempel und den öffentlichen Schlüssel des Verifizierers. Hierdurch werden der Vorgang an sich durch den Zeitstempel und der bestimmungsgemäße Empfänger anhand des öffentlichen Schlüssel identifiziert. Nach Ausführungsbeispielen kann die Kennung ergänzend und/oder alternativ auch andere Angaben umfassen, welche dazu geeignet sind den entsprechenden Übertragungsvorgang zu identifizieren. Zum Signieren verwendet der Besitzer des Smartphones beispielsweise einen auf dem Smartphone gespeicherten privaten kryptographischen Schlüssel, welcher dem Inhaber des Dokuments zugeordnet ist, d.h. im vorliegenden Fall dem Besitzer des Smartphones. Dieser private kryptographische Schlüssel ist beispielsweise dem von dem virtuellen Dokument umfassten öffentlichen kryptographischen Schlüssel zugeordnet. Das virtuelle Dokument ist zudem in einer Blockchain registriert, auf weiche der Verifizierer auch offline mit seinem Verifikationsgerät Zugriff hat, d.h. die Blockchain ist beispielsweise auf dem Verifikationsgerät gespeichert. Zusammen mit dem virtuellen Dokument wird beispielsweise auch die Transaktions-ID, unter der das virtuelle Dokument bzw. dessen Hashwert in der Blockchain registriert wurde, signiert. In Block 606 wird der signierte Datensatz aus virtuellem Dokument, Kennung und Transaktions-ID in einem Videostream, beispielsweise einem QR-Codestream kodiert und in Block 608 von dem Besitzer in einer Endlosschleife auf dessen Display abgespielt. Nach Ausführungsformen kann der Datensatz zudem verschlüsselt sein.

[0162] In Block 610 scannt bzw. filmt der Verifizierer den angezeigten Videostream mit einer Digitalkamera seines Verifikationsgerätes vom Display des Smartphones des Besitzers ab. In Block 612 wird der gescannte Datensatz dekodiert, sobald dieser vollständig empfangen wurde. In Block 614 wird die Signatur des Datensatzes mit dem von dem virtuellen Dokument umfassten öffentlichen Schlüssel des Inhabers des virtuellen Dokuments geprüft. In Block 616 berechnet der Verifizierer den Hashwert des empfangenen virtuellen Dokuments. In Block 618 wird die Signatur des in der Blockchain unter der Transaktions-ID gespeicherten Hashwerts mit dem öffentlichen Schlüssel des Ausstellers des virtuellen Dokuments geprüft. Dieser öffentlichen Schlüssel des Ausstellers wird beispielsweise zusammen mit dem virtuellen Dokument von dem Smartphone des Besitzers des virtuellen Dokuments bereitgestellt oder der öffentlichen Schlüssel ist in der Blockchain gespeichert. Ist die Signatur gültig, so wird in Block 620 der berechnete Hashwert mit dem in der Blockchain gespeicherten Hashwert verglichen. Wenn der berechnete Hashwert mit dem in der Blockchain unter der Transaktions-ID gespeicherten Hashwert übereinstimmt, ist die Echtheitsprüfung erfolgreich und damit das von dem Besitzer übertragene virtuelle Dokument gültig. Zudem bestätigt eine Übereinstimmung der Hashwerte auch, dass der zur Signaturprüfung des übertragenen Datensatzes aus virtuellem Dokument, Kennung und Transaktions-ID verwendete öffentliche Schlüssel des Inhabers des virtuellen Dokuments authentisch ist. Sollten Abweichungen zwischen dem durch das übertragene virtuelle Dokument bereitgestellten öffentlichen Schlüssel des Inhabers und dem öffentlichen Schlüssel, welcher in die Berechnung des in der Blockchain hinterlegten Hashwerts eingegangen ist, bestehen, so wird diese Abweichung beim oben beschriebenen Vergleich der Hashwerte offensichtlich. Diese Bestätigung kann somit insbesondere auch offline sichergestellt werden.

Bezugszeichenliste

100	erster Computer
102	Speicher
104	geschützter Speicherbereich
106	privater Schlüssel
108	öffentlicher Schlüssel
110	Blockchain
112	Prozessor
114	kryptographisches Protokoll
116	Blockchain-Protokoll
118	Protokoll zum Ausstellen eines virtuellen Dokuments
120	Kommunikationsschnittstelle
140	Netzwerk
150	Besitzer Dokument
160	Dokument
162	Bildaufnahmen
164	virtuelles Dokument
170	zweiter Computer
172	Speicher
174	geschützter Bereich
176	privater Schlüssel
178	öffentlicher Schlüssel
180	Prozessor
182	kryptographisches Protokoll
184	Eingabeinterface
186	Digitalkamera
188	Display
190	Kommunikationsschnittstelle
202	Vorderseite
204	Rückseite
206	Bild
208	Daten
210	Sicherheitsmerkmal
220	erste Achse
222	zweite Achse
400	Besitzer virtuelles Dokument
402	erstes elektronisches Gerät
404	Speicher
406	geschützter Speicherbereich
407	privater Schlüssel
408	virtuelles Dokument
409	öffentlicher Schlüssel
410	Transaktions-ID
412	Prozessor
414	kryptographisches Protokoll
416	Kodierungsprotokoll
418	Eingabeinterface
420	Digitalkamera
422	Display
450	Verifizierer
452	zweites elektronisches Gerät
454	Speicher

456 geschützter Speicherbereich

458 privater Schlüssel

460 öffentlicher Schlüssel

462 Blockchain

464 Prozessor

466 kryptographisches Protokoll

468 Kodierungsprotokoll

470 Eingabeinterface

472 Digitalkamera

474 Display

480 optischer Kommunikationskanal

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 Nicht-Patentliteratur

- ISO/IEC 7816-8 [0015]

Patentansprüche

1. Verfahren zum Ausstellen einer virtuellen Version (164, 408) eines Dokuments (160) durch ein erstes Computersystem (100) eines ID-Providers, wobei das Dokument (160) eine visuelle Widergabe eines Datensatzes aufweist, wobei das Verfahren umfasst:
• Erstellen des virtuellen Dokuments (164, 408) als virtueller Version des Dokuments (160), welches eine elektronische Kopie des Datensatzes des Dokuments (160) umfasst,
• Berechnen eines Hashwerts des virtuellen Dokuments (164, 408),
• Signieren des Hashwerts mit einem privaten Schlüssel (106) eines dem Austeller des virtuellen Dokuments (164, 408) zugeordneten asymmetrischen Schlüsselpaars,
• Speichern des signierten Hashwerts in einem Eintrag in einer kryptographisch gesicherten Datenbank (110) zur Ausstellung des virtuellen Dokuments (164, 408),
• Senden des virtuellen Dokuments (164, 408) an einen Besitzer (150) des Dokuments (160) zusammen mit einer Speicher-ID des virtuellen Dokuments (164, 408), wobei die Speicher-ID den Eintrag der Datenbank (110) mit dem signierten Hashwert des virtuellen Dokuments (164, 408) identifiziert.

2. Verfahren nach Anspruch 1, wobei es sich bei der kryptographisch gesicherten Datenbank (110) um eine auf einer Mehrzahl von Knoten eines Netzwerks redundant gespeicherte Datenbank (110, 462) handelt.

3. Verfahren nach einem der vorhergehenden Ansprüche, wobei es sich bei der kryptographisch gesicherten Datenbank um eine Blockchain (110) handelt und der Hashwert des virtuellen Dokuments (164, 408) als Transaktion in einem Block der Blockchain (110) gespeichert ist.

4. Verfahren nach Anspruch 3, wobei es sich bei der Speicher-ID um eine Transaktions-ID der Transaktion handelt, welche den signierten Hashwert des virtuellen Dokuments (164, 408) umfasst.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei das virtuelle Dokument einen öffentlichen Schlüssel eines dem Inhaber des virtuellen Dokuments (164, 408) zugeordneten asymmetrischen Schlüsselpaars umfasst.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Verfahren ferner umfasst:
• Empfangen einer Anfrage zum Ausstellen des virtuellen Dokuments (164, 408) von einem zweiten Computersystem (170) durch den Besitzer (150) des Dokuments (160), wobei das zweite Computersystem (170) eine Digitalkamera (186) umfasst,
• Senden einer Abfrage von Daten des Dokuments (160) an das zweite Computersystem (170),
• Empfang der abgefragten Daten durch das zweite Computersystem (170),
• Verifizieren der abgefragten Daten,
• Erstellen der virtuellen Kopie des Datensatzes des Dokuments (160) unter Verwendung der verifizierten Daten.

7. Verfahren nach Anspruch 6, wobei das Verfahren ferner umfasst:
Authentisieren des zweiten Computersystems (170) gegenüber dem ersten Computersystem (100).

8. Verfahren nach einem der Ansprüche 6 bis 7, wobei die Abfrage der Daten eine Abfrage digitaler Bildaufnahmen (162) des Dokuments (160) unter verschiedenen Blickwinkeln umfasst.

9. Verfahren nach Anspruch 8, wobei an das zweite Computersystem (170) assistierende Rückmeldungen zur relativen Ausrichtung zwischen dem Dokument (160) und der Digitalkamera (186) gesendet werden.

10. Verfahren nach einem der Ansprüche 6 bis 9, wobei das Verifizieren der abgefragten Daten umfasst:
• Verifizieren des Dokuments (160) durch Prüfen von visuellen Sicherheitsmerkmalen (210) des Dokuments (160) unter Verwendung der digitalen Bildaufnahmen (162) des Dokuments (160) unter verschiedenen Blickwinkeln,
• Extrahieren von Daten (208) des Dokuments (160) aus den digitalen Bildaufnahmen (162).

11. Verfahren nach einem Anspruch 10, wobei das Verifizieren der abgefragten Daten ferner umfasst:
• Extrahieren einer Dokumenten-ID aus dem digitalen Bildaufnahmen (162),
• Verifizieren der Dokumenten-ID.

12. Verfahren nach einem der Ansprüche 6 bis 11, wobei die Abfrage der Daten eine Aufforderung zur Eingabe von Daten des Dokuments (160) an dem zweiten Computersystem (170) umfasst.

13. Verfahren nach Anspruch 12, wobei das Verfahren ferner umfasst:
• Vergleichen der extrahierten Daten mit den eingegebenen Daten,
• Korrigieren von Fehlern bei den extrahierten Daten.

14. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Verfahren ferner umfasst:
Authentifizieren des Besitzers (150) des Dokuments (160) gegenüber dem ID-Provider.

15. Verfahren nach Anspruch 14, wobei das Authentifizieren des Besitzers (150) des Dokuments

(160) eine Abfrage einer digitalen Bildaufnahme des Besitzers (150) des Dokuments (160) umfasst.

16. Verfahren nach Anspruch 15, wobei die Abfrage der digitalen Bildaufnahme digitale Bildaufnahmen des Besitzers (150) des Dokuments (160) unter verschiedenen Blickwinkeln abfragt.

17. Verfahren nach Anspruch 16, wobei an das zweite Computersystem (170) assistierende Rückmeldungen zur relativen Ausrichtung zwischen dem Besitzer (150) des Dokuments (160) und der Digitalkamera (186) gesendet werden.

18. Verfahren nach einem der Ansprüche 15 bis 17, wobei das Authentifizieren des Besitzers (150) des Dokuments (160) umfasst:
Vergleichen der digitalen Bildaufnahme des Besitzers (150) des Dokuments (160) mit einem von dem Dokument (160) umfassten Bild (206) einer Person, welcher das Dokument (160) zugeordnet ist.

19. Verfahren nach einem der Ansprüche 14 bis 18, wobei das Authentifizieren des Besitzers (150) des Dokuments (160) eine Abfrage von digitalen Bildaufnahmen eines Ausweisdokuments des Besitzers (150) unter verschiedenen Blickwinkeln umfasst.

20. Verfahren nach Anspruch 19, wobei an das zweite Computersystem (170) assistierende Rückmeldungen zur relativen Ausrichtung zwischen dem Ausdokument und der Digitalkamera (186) gesendet werden.

21. Verfahren nach einem der Ansprüche 19 bis 20, wobei das Verifizieren des Ausweisdokuments umfasst:
Verifizieren des Ausweisdokuments durch Prüfen von visuellen Sicherheitsmerkmalen des Ausweisdokuments unter Verwendung der digitalen Bildaufnahmen des Ausweisdokuments unter verschiedenen Blickwinkeln.

22. Verfahren nach einem Anspruch 21, wobei das Verifizieren des Ausweisdokuments umfasst:
• Extrahieren einer Ausweisdokumenten-ID aus dem digitalen Bildaufnahmen,
• Verifizieren der Ausweisdokumenten-ID.

23. Verfahren nach einem der Ansprüche 19 bis 22, wobei das Authentifizieren des Besitzers (150) des Dokuments (160) umfasst:
Vergleichen der digitalen Bildaufnahme des Besitzers (150) des Dokuments (160) mit einem von dem Ausweisdokument umfassten Bild einer Person, welcher das Ausweisdokument zugeordnet ist.

24. Verfahren nach einem der vorhergehenden Ansprüche, wobei ein dem asymmetrischen Schlüsselpaar des Ausstellers zugeordneter öffentlicher kryptographische Schlüssel (108) in der Datenbank (110) gespeichert ist.

25. Verfahren nach Anspruch 1 bis 24, wobei das Verfahren ferner umfasst:
Speichern des öffentlichen kryptographischen Schlüssels (108) des Ausstellers in dem Datenbankeintrag mit dem signierten Hashwert des virtuellen Dokuments (164, 408).

26. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Senden des virtuellen Dokuments (164, 408) umfasst:
• Empfang eines öffentlichen Schlüssels (178) eines dem Besitzer (150) des Dokuments (160) zugeordneten asymmetrischen Schlüsselpaars,
• Verschlüsseln des zu sendenden virtuellen Dokuments (164, 408) mit dem öffentlichen Schlüssel (178) des Besitzers (150) des Dokuments (160).

27. Verfahren nach Anspruch 26, wobei das Verfahren ferner umfasst:
Verschlüsseln der Speicher-ID mit dem öffentlichen Schlüssel (178) des Besitzers (150) des Dokuments (160).

28. Verfahren nach einem der vorhergehenden Ansprüche, bei die zum Ausstellen des virtuellen Dokuments (164, 408) verwendete virtuelle Kopie des Datensatzes des Dokuments (160) nach dem Ausstellen des virtuellen Dokuments (164, 408) automatisch gelöscht wird.

29. Verfahren nach einem der vorhergehenden Ansprüche, wobei das virtuelle Dokument (164, 408) selbst die Speicher-ID umfasst.

30. Verfahren nach einem der vorhergehenden Ansprüche, wobei das virtuelle Dokument (164, 408) ein Ablaufdatum umfasst, welches ein Ende der Gültigkeit des virtuellen Dokuments (164, 408) festlegt.

31. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Verfahren ferner umfasst:
bei Ablaufen der Gültigkeit des virtuellen Dokuments (164, 408) Bereitstellen einer neuen virtuellen Version des Dokuments durch Wiederholen des Ausstellverfahrens.

32. Verfahren zur Offline-Echtheitsprüfung eines nach einem der Verfahren 1 bis 31 ausgestellten virtuellen Dokuments (408) mittels eines ersten und eines zweiten elektronischen Geräts (402, 452), wobei das erste elektronische Gerät (402) einen ersten Speicher (404) umfasst, in welchem das virtuelle Dokument (408) und eine Speicher-ID (410) des virtuellen Dokuments (408) gespeichert sind, wobei das zweite elektronische Gerät (452) einen zweiten Speicher (454) umfasst, in welchem eine kryptographisch gesicherte Datenbank (462) gespeichert ist,

welche Hashwerte von einer Mehrzahl von virtuellen Dokumenten umfasst, wobei die Speicher-ID (410) des virtuellen Dokuments (408) einen Eintrag der Datenbank (462) mit dem Hashwert des virtuellen Dokuments (408) identifiziert, wobei das Verfahren umfasst:

• Übertragen des virtuellen Dokuments (408) zusammen mit der Speicher-ID (410) von dem ersten elektronischen Gerät (402) an das zweite elektronische Gerät (452),

• Berechnen eines Hashwerts des virtuellen Dokuments (408) durch das zweite elektronische Gerät (452),

• Identifizieren des Datenbankeintrags mit dem Hashwert des virtuellen Dokuments (408) durch das zweite elektronische Gerät (452) unter Verwendung der Speicher-ID (410) des virtuellen Dokuments (408),

• Vergleichen des berechneten Hashwerts mit dem in dem identifizierten Datenbankeintrag gespeicherten Hashwert des virtuellen Dokuments (408), wobei die Echtheit des virtuellen Dokuments (408) bestätigt wird, falls beide Hashwerte übereinstimmen.

33. Computerprogrammprodukt, insbesondere ein computerlesbares, nichtflüchtiges Speichermedium, mit ausführbaren Programminstruktionen zum Ausführen eines Verfahrens nach einem der Ansprüche 1 bis 31.

34. Computersystem (100), welches konfiguriert ist zum Ausführen eines Verfahrens nach einem der Ansprüche 1 bis 31.

35. System zur Offline-Echtheitsprüfung eines nach einem der Verfahren 1 bis 31 ausgestellten virtuellen Dokuments (408), wobei das System ein erstes und ein zweites elektronisches Gerät (402, 452) umfasst,
wobei das erste elektronische Gerät (402) einen ersten Speicher (404) umfasst, in welchem das virtuelle Dokument (408) und eine Speicher-ID (410) des virtuellen Dokuments (408) gespeichert sind,
wobei das zweite elektronische Gerät (452) einen zweiten Speicher (454) umfasst, in welchem eine kryptographisch gesicherte Datenbank (462) gespeichert ist, welche Hashwerte von einer Mehrzahl von virtuellen Dokumenten umfasst, wobei die Speicher-ID (410) des virtuellen Dokuments (408) einen Eintrag der Datenbank (462) mit dem Hashwert des virtuellen Dokuments (408) identifiziert,
wobei das System dazu konfiguriert ist das Verfahren nach Anspruch 32 auszuführen.

Es folgen 7 Seiten Zeichnungen

Anhängende Zeichnungen

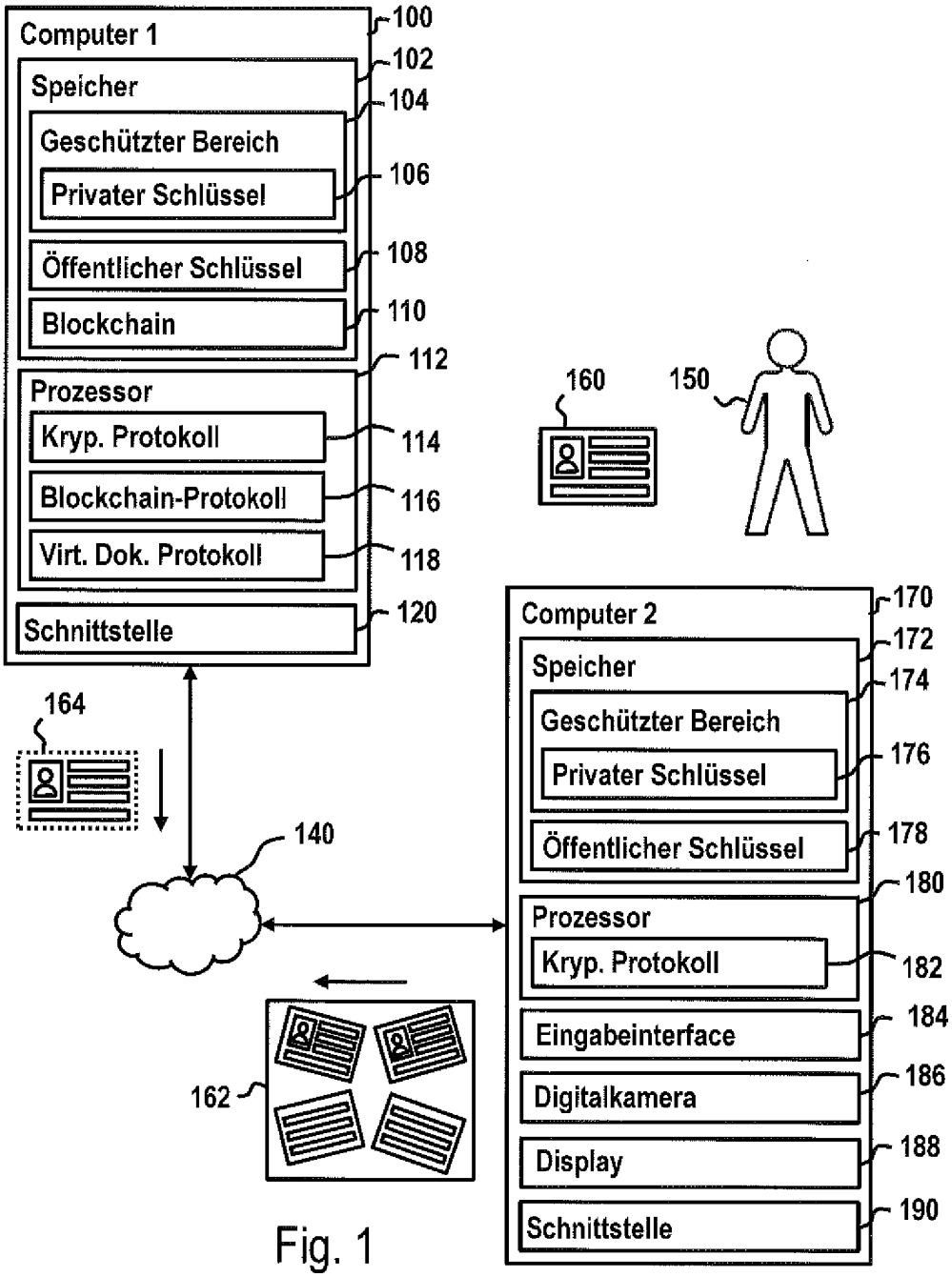


Fig. 1

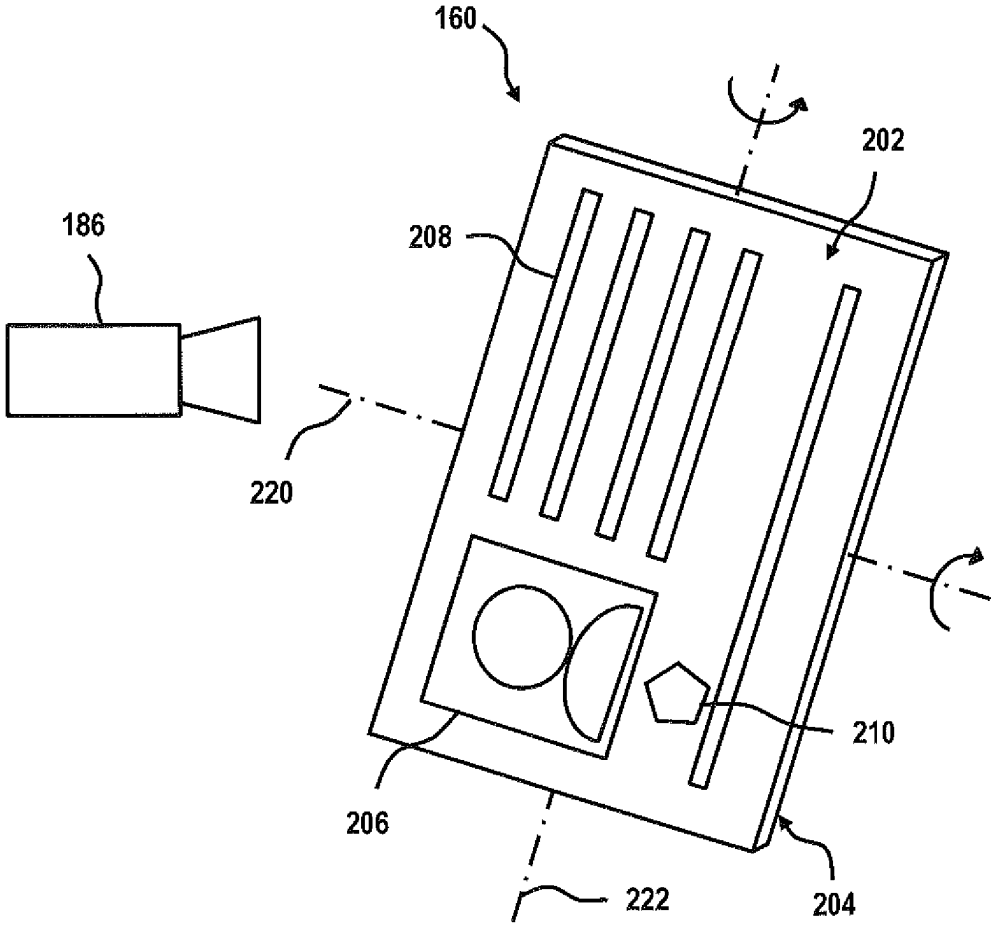


Fig. 2

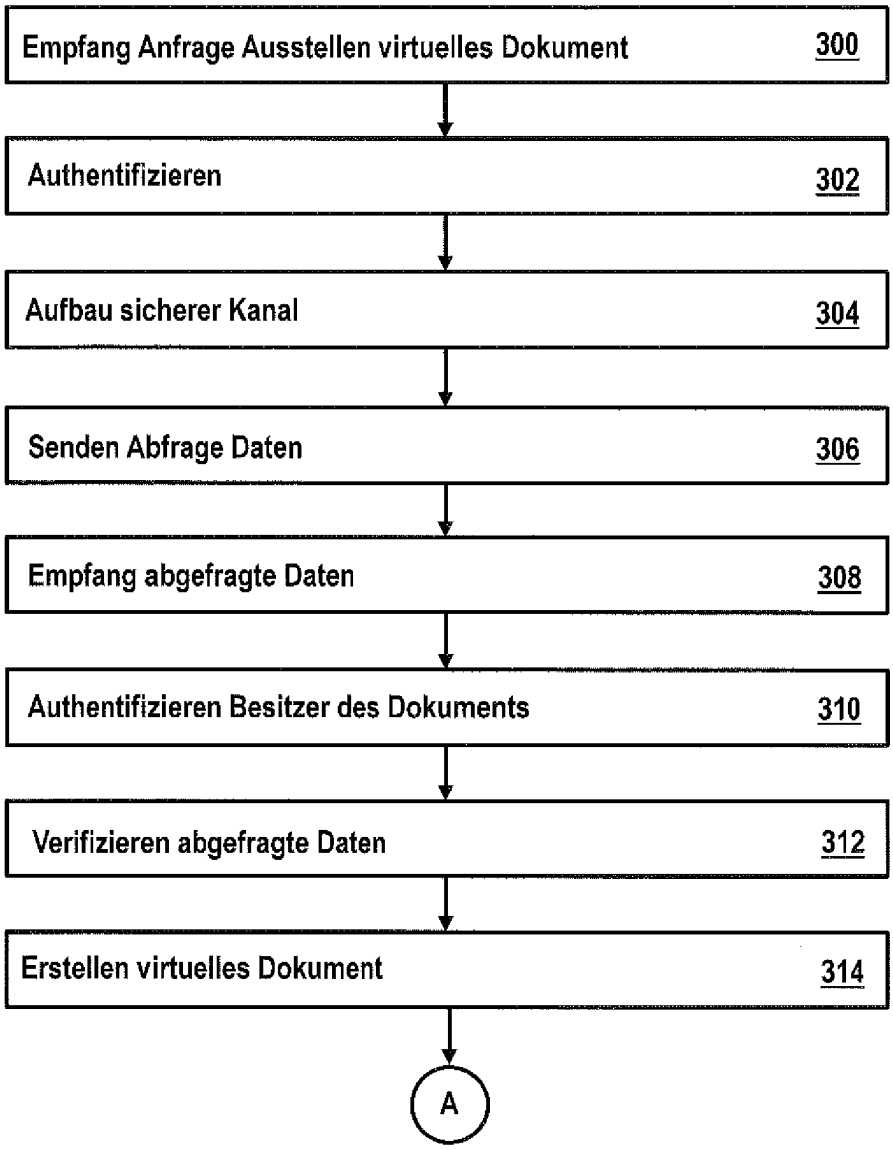

Empfang Anfrage Ausstellen virtuelles Dokument
300
Authentifizieren
302
Aufbau sicherer Kanal
304
Senden Abfrage Daten
306
Empfang abgefragte Daten
308
Authentifizieren Besitzer des Dokuments
310
Verifizieren abgefragte Daten
312
Erstellen virtuelles Dokument
314
A

Fig. 3A

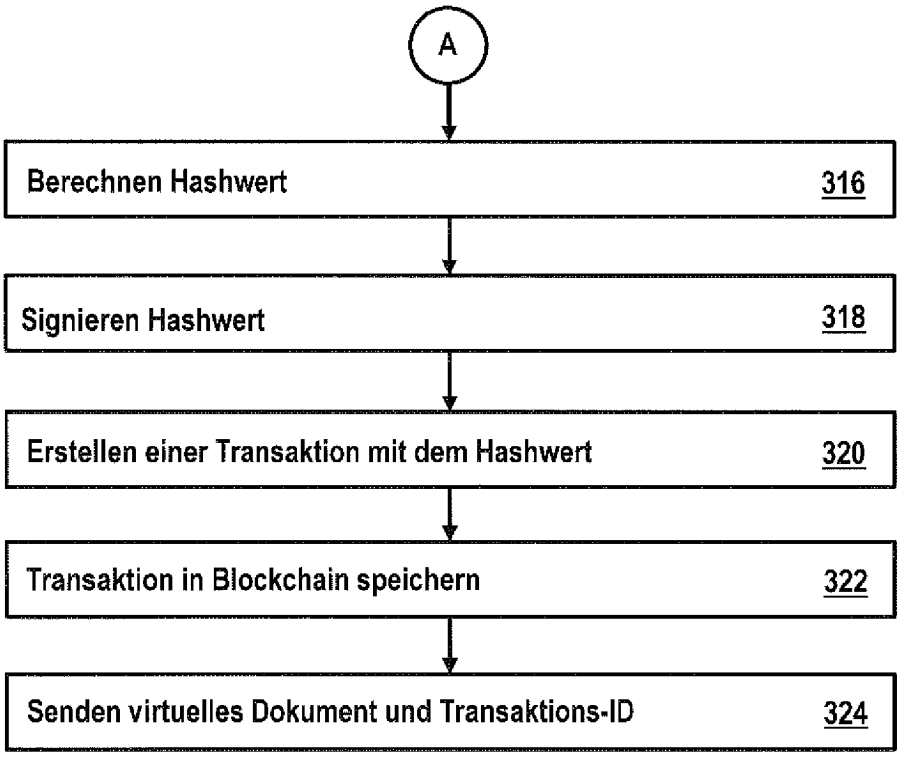

A
Berechnen Hashwert 316
Signieren Hashwert 318
Erstellen einer Transaktion mit dem Hashwert 320
Transaktion in Blockchain speichern 322
Senden virtuelles Dokument und Transaktions-ID 324

Fig. 3B

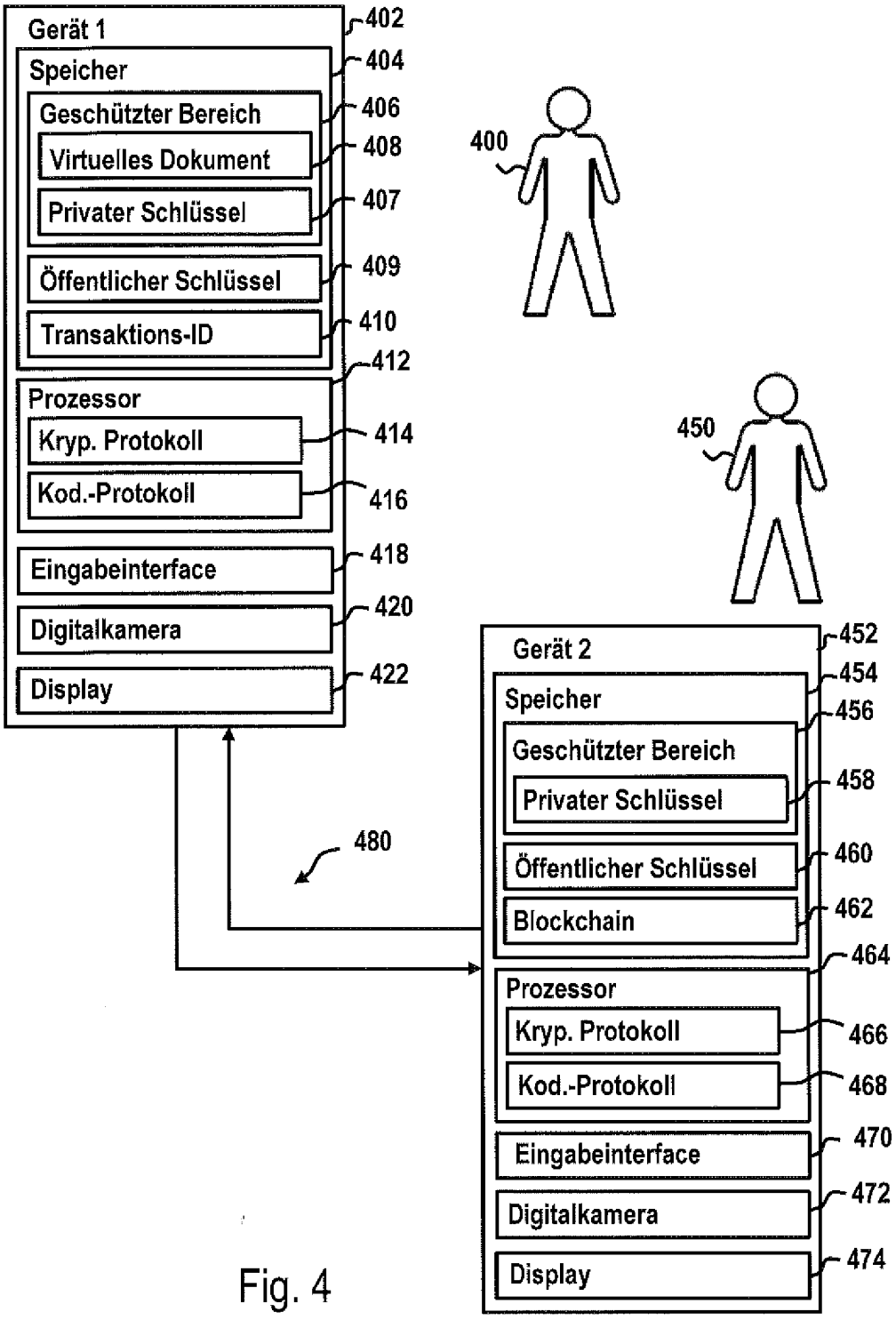

Gerät 1
402
Speicher
404
Geschützter Bereich
406
Virtuelles Dokument
408
Privater Schlüssel
407
Öffentlicher Schlüssel
409
Transaktions-ID
410
Prozessor
412
Kryp. Protokoll
414
Kod.-Protokoll
416
Eingabeinterface
418
Digitalkamera
420
Display
422
400
450
480
Gerät 2
452
Speicher
454
Geschützter Bereich
456
Privater Schlüssel
458
Öffentlicher Schlüssel
460
Blockchain
462
Prozessor
464
Kryp. Protokoll
466
Kod.-Protokoll
468
Eingabeinterface
470
Digitalkamera
472
Display
474

Fig. 4

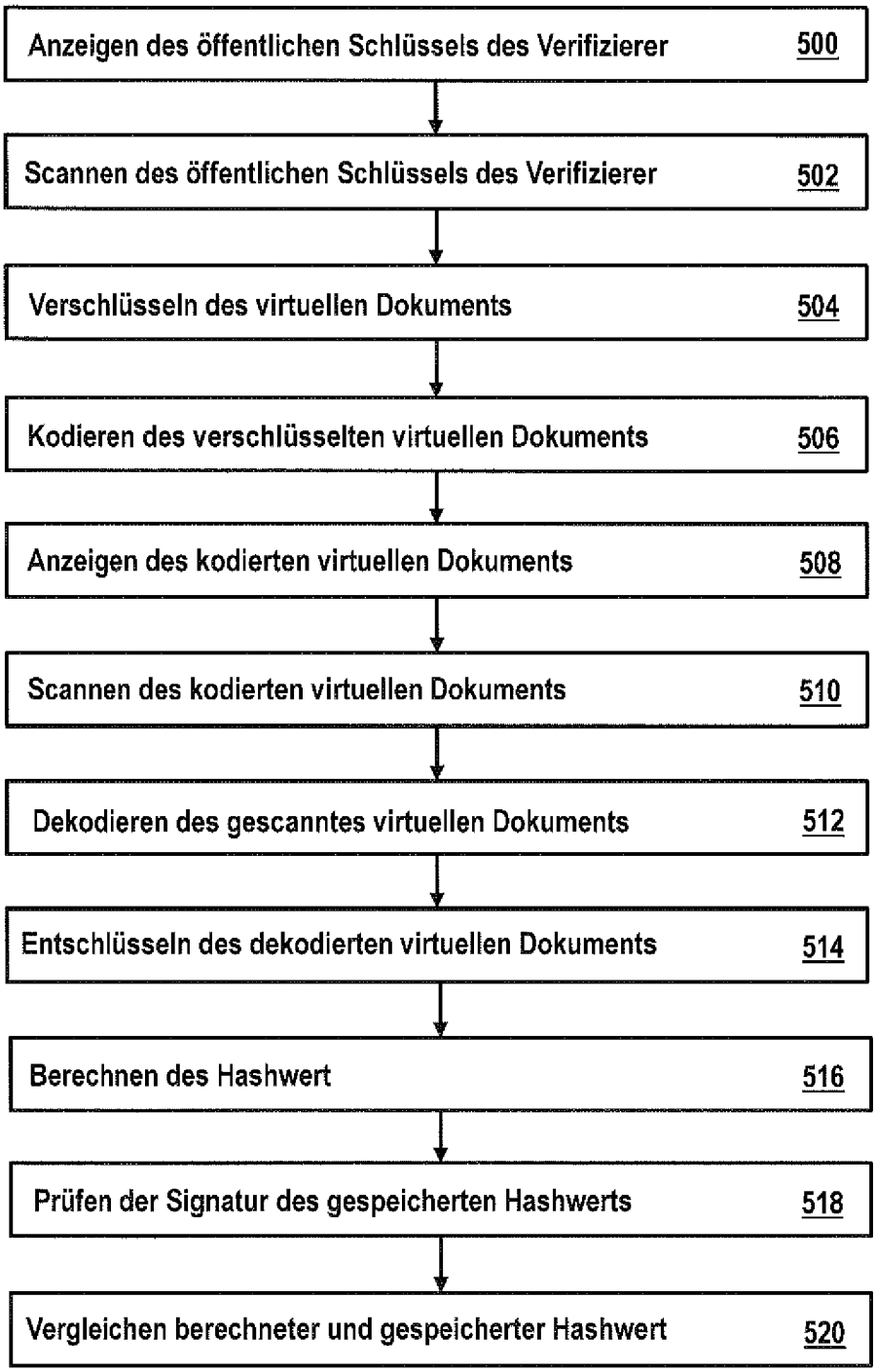

Anzeigen des öffentlichen Schlüssels des Verifizierer 500
Scannen des öffentlichen Schlüssels des Verifizierer 502
Verschlüsseln des virtuellen Dokuments 504
Kodieren des verschlüsselten virtuellen Dokuments 506
Anzeigen des kodierten virtuellen Dokuments 508
Scannen des kodierten virtuellen Dokuments 510
Dekodieren des gescanntes virtuellen Dokuments 512
Entschlüsseln des dekodierten virtuellen Dokuments 514
Berechnen des Hashwert 516
Prüfen der Signatur des gespeicherten Hashwerts 518
Vergleichen berechneter und gespeicherter Hashwert 520

Fig. 5

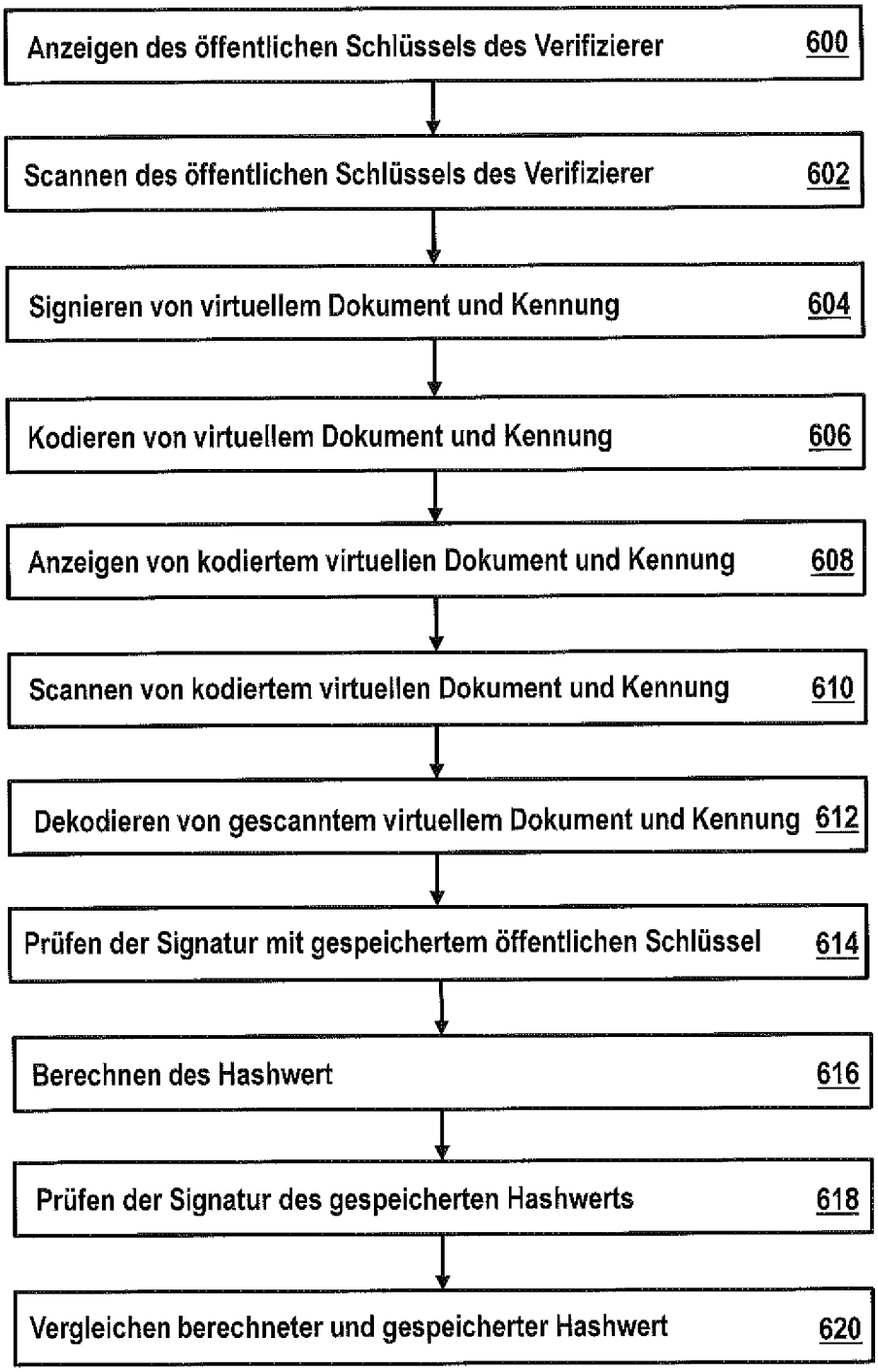

Anzeigen des öffentlichen Schlüssels des Verifizierer 600
Scannen des öffentlichen Schlüssels des Verifizierer 602
Signieren von virtuellem Dokument und Kennung 604
Kodieren von virtuellem Dokument und Kennung 606
Anzeigen von kodiertem virtuellen Dokument und Kennung 608
Scannen von kodiertem virtuellen Dokument und Kennung 610
Dekodieren von gescanntem virtuellem Dokument und Kennung 612
Prüfen der Signatur mit gespeichertem öffentlichen Schlüssel 614
Berechnen des Hashwert 616
Prüfen der Signatur des gespeicherten Hashwerts 618
Vergleichen berechneter und gespeicherter Hashwert 620

Fig. 6