(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2007 016 538 A1** 2008.10.09

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2007 016 538.4**
(22) Anmeldetag: **05.04.2007**
(43) Offenlegungstag: **09.10.2008**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)

(71) Anmelder:
Infineon Technologies AG, 81669 München, DE

(74) Vertreter:
Viering, Jentschura & Partner, 81675 München

(72) Erfinder:
Schmidt, Andreas, 38124 Braunschweig, DE; Schwagmann, Norbert, 26892 Lehe, DE; Luft, Achim, 38120 Braunschweig, DE

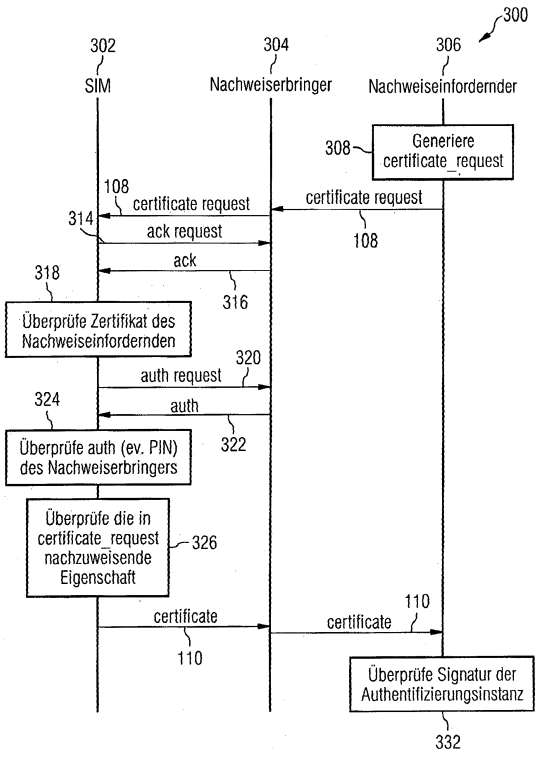
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
US2003/01 72 278 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gemäß § 44 PatG ist gestellt.

(54) Bezeichnung: **Kommunikationsendgerät, Kommunikationseinrichtung, elektronische Karte, Verfahren für ein Kommunikationsendgerät und Verfahren für eine Kommunikationseinrichtung zum Bereitstellen eines Nachweises**

(57) Zusammenfassung: Ein Kommunikationsendgerät zum Bereitstellen eines Nachweises weist auf eine Applikation, eingerichtet zum Empfangen einer ersten Nachricht von einer anfragenden Kommunikationseinrichtung, wobei die erste Nachricht eine Anforderung nach einem Nachweis, eine erste digitale Signatur sowie eine Anfrage nach einer den Nutzer beschreibenden Information enthält. Die Applikation ist ferner eingerichtet, die erste digitale Signatur zu überprüfen und bei erfolgreicher Überprüfung die Anforderung zu bearbeiten und eine Antwortnachricht für die anfordernde Kommunikationseinrichtung zu erstellen, wobei die Antwortnachricht eine Antwort auf die Anfrage in der Anforderung enthält.



Beschreibung

[0001] Die Erfindung betrifft ein Kommunikationsendgerät, eine Kommunikationseinrichtung, eine elektronische Karte, ein Verfahren für ein Kommunikationsendgerät und ein Verfahren für eine Kommunikationseinrichtung zum Bereitstellen eines Nachweises.

[0002] Wünschenswert ist eine Nutzung eines Kommunikationsendgerätes, wie z. B. ein Mobilfunkgerät zur Erbringung eines Nachweises personenbezogener Daten.

[0003] Ausführungsbeispiele der Erfindung sind in den Figuren dargestellt und werden im Folgenden näher erläutert.

[0004] Es zeigen

[0005] Fig. 1 eine Anordnung eines Kommunikationsendgerätes und einer Kommunikationseinrichtung zum Übertragen von Nachrichten, gemäß einem Ausführungsbeispiel der Erfindung;

[0006] Fig. 2A ein eine Nachweis-Nachricht erstellendes Kommunikationsendgerät gemäß einem Ausführungsbeispiel der Erfindung;

[0007] Fig. 2B eine eine Nachweis-Nachricht anfordernde Kommunikationseinrichtung gemäß einem Ausführungsbeispiel der Erfindung;

[0008] Fig. 3 ein Nachrichtenflussdiagramm mit den Nachrichten zwischen den beteiligten Instanzen gemäß einem Ausführungsbeispiel der Erfindung;

[0009] Fig. 4 ein Ablaufdiagramm eines Verfahrens zur Erzeugung einer Nachweis-Nachricht-Anforderungsnachricht gemäß einem Ausführungsbeispiel der Erfindung;

[0010] Fig. 5 ein Ablaufdiagramm, eines Verfahrens zur Überprüfung der digitalen Signatur der die Nachweis-Nachricht anfordernden Kommunikationseinrichtung gemäß einem Ausführungsbeispiel der Erfindung;

[0011] Fig. 6 ein Ablaufdiagramm, eines Verfahrens zur Authentifizierung des Benutzers gemäß einem Ausführungsbeispiel der Erfindung;

[0012] Fig. 7 ein Ablaufdiagramm, eines Verfahrens zur Erstellung der angeforderten Nachweis-Nachricht gemäß einem Ausführungsbeispiel der Erfindung;

[0013] Fig. 8 ein Ablaufdiagramm, eines Verfahrens zur Überprüfung der digitalen Signatur des Kommunikationsendgerätes und zur Überprüfung des angeforderten Nachweises durch die Kommunikationseinrichtung gemäß einem Ausführungsbeispiel der Erfindung;

[0014] Fig. 9 eine Nachricht zur Anforderung eines Nachweises gemäß einem Ausführungsbeispiel der Erfindung;

[0015] Fig. 10 eine Nachricht zur Anforderung einer Bestätigung durch den Benutzer gemäß einem Ausführungsbeispiel der Erfindung;

[0016] Fig. 11 eine Nachricht mit der Benutzerantwort der Bestätigungsanforderung gemäß einem Ausführungsbeispiel der Erfindung;

[0017] Fig. 12 eine Nachricht, die den vom Kommunikationsendgerät erstellten Nachweis enthält, gemäß einem Ausführungsbeispiel der Erfindung;

[0018] Fig. 13A ein Verfahren zum Bereitstellen eines digitalen Nachweises bezüglich eines Kommunikationsendgerätes gemäß einem Ausführungsbeispiel der Erfindung;

[0019] Fig. 13B ein Verfahren zum Bereitstellen eines digitalen Nachweises bezüglich einer Kommunikationseinrichtung gemäß einem Ausführungsbeispiel der Erfindung;

[0020] Fig. 14 die Struktur eines digitalen Zertifikats gemäß dem ITU-T X.509 Standard; und

[0021] Fig. 15 ein Ablaufdiagramm zu digitalen Signaturen.

[0022] Im Rahmen dieser Beschreibung werden die Begriffe "verbunden", "angeschlossen" sowie "gekoppelt" zum Beschreiben sowohl einer direkten als auch einer indirekten Verbindung, eines direkten oder indirekten Anschlusses sowie einer direkten oder indirekten Kopplung verwendet. In den Figuren werden identische oder ähnliche Elemente mit identischen Bezugszeichen versehen, soweit dies zweckmäßig ist.

[0023] Ein Mobilfunkendgerät wird aufgrund seiner hohen Marktdurchdringung und der ständigen Präsenz bei den Teilnehmern zunehmend zum Universal-Werkzeug. So werden schon heute viele Mobilfunkendgeräte als Personal Digital Assistant eingesetzt, und das Mobilfunkendgerät wird verwendet, um Adressen, Termine, Notizen, usw. zu verwalten. Auch der Bereich eCommerce und die damit gegebenen Möglichkeiten, das Mobilfunkendgerät wie eine Geldkarte zu verwenden, werden zur Zeit vielerorts getestet oder sind bereits im Einsatz, um z. B. Fahrkarten für Bus und Bahn zu bezahlen.

[0024] Daher wäre es wünschenswert, wenn eine weitere alltägliche Aufgabe mit Hilfe eines Mobilfun-

kendgerätes besser als bisher gelöst werden könnte. Diese Aufgabe ist die Erbringung eines Nachweises. Die Bandbreite der Anwendungen reicht über den Altersnachweis für den Erwerb von Alkohol, Spielen, Zigaretten oder für den Zutritt zu Spielhallen, Videotheken über den Nachweis des Geschlechtes für Internetforen bis hin zur digitalen Authentifizierung z. B. an Videotheksautomaten.

[0025] Dabei kann man zwischen zwei Arten eines Nachweises unterscheiden, nämlich ob der Nachweis gegenüber einer Person oder Instanz erfolgen soll, zu der der Nachweisende schon eine geschäftliche Beziehung hatte und die einen Datensatz über den Nachweisenden führt, oder ob es sich um einen Nachweis gegenüber einer Person oder Instanz handelt, der der Nachweisende völlig unbekannt ist. Bei der zweiten Art des Nachweises sollte eine dritte Person oder Instanz einbezogen sein, der von beiden anderen Parteien vertraut wird.

[0026] Auch hier erfolgt wieder die Unterscheidung der beiden Nachweistypen:
Handelt es sich um einen Nachweis gegenüber einer Person oder Instanz, zu der der Nachweisende schon eine geschäftliche Beziehung hat, dann erfolgt der Nachweis in der Regel mit einem Dokument, das von der Instanz ausgestellt wurde, die den Nachweis fordert. So stellt z. B. eine Videothek dem Kunden einen Kundenausweis zur Verfügung, mit dessen Hilfe der Kunde zukünftig seine Mitgliedschaft nachweisen kann. Ein Link zwischen der Kundenkarte und dem in der Videothek angelegten Datensatz sorgt für die Bereitstellung der benötigten Daten; z. B. ob das Alter des Kunden zum Ausleihen eines bestimmten Filmes berechtigt. Oft ist eine Kundenkarte mit zusätzlichen Merkmalen ausgestattet, die einen Missbrauch erschweren. So kann sich auf der Karte ein Bild des Kunden befinden oder es erfolgt zusätzlich zum Zeigen des Ausweises die Eingabe einer PIN (Personal Identification Number), die mit dem Kundendatensatz verglichen wird. Diese Maßnahmen sollen verhindern, dass sich jemand mit Hilfe einer gefundenen oder gestohlenen Kundenkarte als jemand anderer ausgibt.

[0027] Somit sammeln sich viele verschiedene Kundenkarten beim Kunden an. Diese sind evtl. mit unterschiedlichen PINs verknüpft. Der Kunde befindet sich in der Situation, entweder mehrere Plastikkarten mit sich zu führen oder die jeweils richtige Karte vorzuhalten.

[0028] Die Sicherheit der unterschiedlichen Kundenkarten variiert sehr stark. Oft sind sie aus Kostengründen niedrig und enthalten in der Regel keine kryptographischen Schutzmechanismen und oft auch keine biometrischen Angaben.

[0029] Die Karten sind physikalisch zugänglich und können somit gestohlen werden oder gehen anderweitig verloren. Als typisches Beispiel sei das Mitwaschen der in der Kleidung vergessenen Karten in der Waschmaschine genannt.

[0030] Die Karten sind leicht von Dritten einsichtig. Sie enthalten neben dem Namen oft zusätzliche Daten, wie z. B. Kontonummer bei einer Kundenkarte einer Bank. Geht eventuell eine ganze Ausweismappe verloren, werden viele Informationen über den Inhaber preisgegeben, die einen Identitätsdiebstahl erleichtern.

[0031] Derartige Karten unterliegen auch Verschleißerscheinungen.

[0032] Eine Datenübertragung zwischen Karte und Kundendatensystem kann mit Hilfe von zusätzlichen Verfahren (z. B. unter Verwendung von Magnetstreifen) implementiert werden. Diese sind in der Regel nicht berührungslos, was dazu führt, dass die Karten zusätzlichem Verschleiß ausgesetzt sind und die Karte aus der Hand gegeben wird. Die Kommunikation ist aus Kostengründen und mangels einer Daten verarbeitenden Einheit auf der Karte oft unverschlüsselt und damit anfällig gegenüber Manipulationen.

[0033] Für die Herstellung der Karten wird zudem Material benötigt.

[0034] Für das erstmalige Anlegen eines oben beschriebenen Kundendatensatzes sowie für jeden Nachweis gegenüber einer Person oder Instanz, zu der man (bis dahin noch) keine geschäftliche Beziehung hat, wird ein Nachweis, der von einer vertrauenswürdigen Instanz ausgestellt wurde, erforderlich. In dem Beispiel der Videothek wird für das Anlegen eines Kundendatensatzes üblicherweise ein Personalausweis gefordert. Dieser von der Bundesregierung ausgestellte Nachweis enthält Name, Wohnort, Geburtsdatum, Geburtsort und einige biometrische Angaben wie Passbild, Größe und Augenfarbe.

[0035] Eine Vermeidung der Preisgabe von vielen Informationen, die für den eigentlichen Nachweis nicht nötig wären, ist erstrebenwert. Es besteht nicht die Notwendigkeit, dass der Kassierer in einem Geschäft beim Verkauf von Zigaretten, wobei lediglich ein Altersnachweis gefordert ist (z. B. älter als 16 Jahre), den Namen, das Geburtsdatum und die Anschrift des Käufers erfährt.

[0036] Wünschenswert gegenüber den herkömmlichen beiden Typen zur Nachweiserbringung ist das Funktionieren über eine Distanz (z. B. das Internet) und die Vermeidung des Mitwirkens eines Menschen, um so einen erheblich geringeren Aufwand und eine vollständige Automatisierung zu erreichen.

[0037] Fig. 1 zeigt eine Anordnung **100** gemäß ei-

nem Ausführungsbeispiel der Erfindung, die ein Kommunikationsendgerät **102** (in anderen Ausführungsbeispielen der Erfindung eine beliebige Anzahl von Kommunikationsendgeräten) und eine Kommunikationseinrichtung **106** (in anderen Ausführungsbeispielen der Erfindung eine beliebige Anzahl von Kommunikationseinrichtungen) aufweist. Die Kommunikationseinrichtung kann z. B. in einen Automaten oder einem anderen Gerät integriert sein. Die Kommunikationseinrichtung **106** enthält gemäß diesem Ausführungsbeispiel eine Nachrichtenerzeugungseinheit **122** zur Erzeugung einer Nachricht **108**, die an das Kommunikationsendgerät **102** gesendet wird. Die von dem Kommunikationsendgerät **102** empfangene Nachricht **108** wird an eine Applikation **124**, die in einer Prozessoreinheit **104**, beispielsweise einem Mikroprozessor oder einer anderen Art einer programmierbaren Logik, ausgeführt wird, weitergegeben und dort ausgewertet. Die Prozessoreinheit **104** kann ein fester Bestandteil des Kommunikationsendgerätes **102** sein oder eine, beispielhaft in Fig. 2A dargestellte, herausnehmbare elektronische Karte **202**, wie z. B. eine SIM-Karte eines Mobilfunkendgerätes **218**.

[0038] Wenn die weiter unten ausgeführten Bedingungen erfüllt werden, generiert die Applikation **124** in der Prozessoreinheit **104**, die zumindest einen Prozessor enthält, eine Antwortnachricht **110**, die wiederum an die Kommunikationseinrichtung **106** gesendet wird und von der dortigen Prozessoreinrichtung **122** ausgewertet wird.

[0039] Die Kommunikationseinrichtung **106** kann z. B. Teil eines Automaten sein, der für eine Aktion eine bestätigte Information über eine persönliche Eigenschaft eines Nutzers benötigt, um die Erlaubnis zu erlangen, diese Aktion ausführen zu dürfen. Beispielsweise ist der Automat ein Zigarettenautomat, der den Nachweis des Alters der Person benötigt, die an dem Zigarettenautomaten eine Schachtel Zigaretten erwerben möchte. Die Kommunikationseinrichtung **106** sendet eine Anfrage über die persönliche Eigenschaft mittels einer Anforderungsnachricht **108** an das Kommunikationsendgerät **102**.

[0040] Der Nachweis wird gemäß einem Ausführungsbeispiel der Erfindung als digitale Nachweis-Nachricht mit der Antwort auf die Anfrage in der Antwortnachricht **110** von dem Kommunikationsendgerät **102** an die Kommunikationseinrichtung **106** gesendet.

[0041] Unter einer digitalen Nachweis-Nachricht werden in dieser Beschreibung beispielsweise strukturierte Daten, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen, verstanden. In einem Ausführungsbeispiel der Erfindung weist die digitale Nachweis-Nachricht ein digitales Zertifikat auf. Durch ein digitales Zertifikat können Nutzer eines asymmetrischen Kryptographiesystems, wie z. B. RSA (Die Abkürzung RSA steht für die Erfinder Ronald L. Rivest, Adi Shamir und Leonard Adleman des Kryptographiesystems), den öffentlichen Schlüssel einer Identität (z. B. einer Person oder einem IT-System) zuordnen und seinen Geltungsbereich bestimmen. Damit ermöglicht das digitale Zertifikat den Schutz der Vertraulichkeit, Authentizität und Integrität von Daten durch die korrekte Anwendung des öffentlichen Schlüssels. Gemäß einem Ausführungsbeispiel der Erfindung enthält ein digitales Zertifikat den öffentlichen Schlüssel eines Nutzers sowie eine digitale Signatur über den öffentlichen Schlüssel.

[0042] So wird z. B. sichergestellt, dass das Alter einer Person von der die Nachweis-Nachricht ausstellenden Einrichtung – z. B. die Applikation in der Prozessoreinrichtung **104** in dem Kommunikationsendgerät **102** – korrekt festgestellt wird. In der Nachweis-Nachricht wird gemäß einem Ausführungsbeispiel der Erfindung eine digitale Signatur verwendet, um zu garantieren, dass die Nachweis-Nachricht und gegebenenfalls das darin enthaltene Zertifikat für z. B. den Altersnachweis unverfälscht und tatsächlich von dem entsprechenden Benutzer stammend an der empfangenden Kommunikationseinrichtung **106** ankommt, bzw. je nachdem, welches Ergebnis die Nachweis-Nachricht beinhaltet (z. B. positiv oder negativ) und der Feststellung, dass die empfangene Nachricht authentisch ist, eine entsprechende Reaktion an z. B. dem Automaten stattfindet. Mit anderen Worten bedeutet dies, dass die Nachricht tatsächlich die Antwort auf die Anforderung nach der Nachweis-Nachricht ist und sie nicht verfälscht wurde, und dass der Sender der Antwort mit der Nachweis-Nachricht auch tatsächlich die dazu autorisierte Einrichtung, wie z. B. die Applikation **124** in der Prozessoreinheit **104** in dem Kommunikationsendgerät **102** ist.

[0043] Aus Fig. 1 sind weiterhin die Nachweis-Nachricht-Anforderungsnachricht **108** und die Antwortnachricht **110** zu ersehen. Die Nachrichten weisen verschiedene Teile auf, in Fig. 1 durch die Blöcke **112**, **114**, **116** bzw. **118**, **120**, **122** repräsentiert, die im Folgenden noch weiter im Detail beschrieben werden.

[0044] Die Kommunikationseinrichtung **106** sendet gemäß einem Ausführungsbeispiel der Erfindung eine Nachricht **108**, die eine Anforderung **112** nach einem Nachweis enthält, an das Kommunikationsendgerät **102**. Die Blöcke **112** bis **122** der Nachrichten **108** und **110** in Fig. 1 sind nur symbolisch zu verstehen. Beispiele möglicher Formate der Nachrichten werden im weiteren Verlauf dieser Beschreibung anhand der Fig. 9 bis Fig. 12 noch ausführlich dargestellt.

[0045] Die Nachricht **108** enthält weiterhin gemäß

einem Ausführungsbeispiel der Erfindung ein Zertifikat des Nachweis-Einfordernden mit beispielsweise einer ersten digitalen Signatur.

[0046] Unter einer digitalen Signatur wird hier beispielsweise ein kryptographisches Verfahren verstanden bzw. eine mittels eines kryptographischen Verfahrens generierte Ziffernfolge, die z. B. mittels eines so genannten privaten Schlüssels aus dem so genannten Hash-Wert einer Nachricht nach einem bestimmten Verschlüsselungsalgorithmus erzeugt wurde und mit einem so genannten öffentlichen Schlüssel wieder entschlüsselt werden kann. Der entschlüsselte Wert kann im Empfänger der Nachricht mit dem Hash-Wert, der aus der empfangenen Nachricht generiert wird, verglichen werden. So kann der Sender der Nachricht verifiziert werden. Ferner wird die Integrität der Nachricht festgestellt. Die Anwendung des Verschlüsselungsalgorithmus erfolgt in einer Hash-Funktion.

[0047] Unter einer Hash-Funktion wird hier beispielsweise eine Funktion verstanden, die zu einer Eingabe aus einer üblicherweise großen Quellmenge eine Ausgabe aus einer im Allgemeinen kleineren Zielmenge erzeugt, z. B. durch Erstellen einer Prüfsumme. Die Prüfsummen werden verwendet, um Änderungen an Daten zu erkennen, die entweder durch technische Störeinflüsse oder absichtliche Manipulation auftreten können. Es können aber auch andere Algorithmen zum Einsatz kommen, die beispielsweise eine Quersumme, eine Parität, eine Prüfziffer, eine Moduln-Funktion oder eine zyklische Redundanzprüfung bilden oder z. B. nach folgenden bekannten Verfahren funktionieren: Adler-32, Hashtabelle, Merkfes Meta-Verfahren oder Salted Hash. Eine Verwendung einer Hash-Funktion hat allerdings eine bessere Sicherheitsgewährleistung zur Folge. Dies ist beispielsweise darin begründet, dass eine Hash-Funktion zusätzliche Sicherheitsanforderungen hat. Beispielsweise stellt eine Hash-Funktion eine geringe Kollision (zwei unterschiedliche Texte sollte nach Möglichkeit nicht zu dem gleichen Hashwert führen) bereit. Ferner wird durch eine Hash-Funktion sichergestellt, dass keine Rückschlüsse auf die ursprünglichen Daten möglich sind und dass eine garantierte Änderung des Hashwertes bei geringster Änderung der zugrunde liegenden Daten erfolgt. Bekannte Hash-Algorithmen in der Kryptographie sind z. B. MD2, MD4, MD5, SHA, RIPEMD-160, Tiger, HAVAL oder Whirlpool.

[0048] Das Verfahren der digitalen Signatur wird in der weiteren Beschreibung noch näher erläutert.

[0049] Das Kommunikationsendgerät **102** enthält gemäß einem Ausführungsbeispiel der Erfindung eine Applikation **124**, die in der Prozessoreinrichtung **104** ausgeführt wird. Die Nachricht **108** mit der Nachweis-Nachricht-Anforderung wird gemäß einem Ausführungsbeispiel von der Prozessoreinrichtung **104** empfangen und von deren Applikation **124** verarbeitet. Wie noch im Weiteren ausführlich beschrieben wird, überprüft die Applikation **124** gemäß einem Ausführungsbeispiel zunächst das Zertifikat des Nachweis-Einfordernden und die erste digitale Signatur, um sicherzustellen, dass der Sender der Nachricht die dazu berechtigte Kommunikationseinrichtung **106** ist und die Nachricht bei der Übertragung nicht verfälscht wurde. Die Anforderungsnachricht **108** kann weitere Felder enthalten, die gemäß den weiter unten beschriebenen Ausführungsbeispielen geprüft werden können.

[0050] Gemäß einem weiteren Ausführungsbeispiel wird nach erfolgreicher Überprüfung der ersten digitalen Signatur die Anfrage nach den Informationen bearbeitet und als Nachweis, der von der Applikation **124** in der Prozessoreinrichtung **104** erstellt wird, in eine Antwortnachricht **110** eingefügt. Das Kommunikationsendgerät **102** sendet daraufhin die Antwortnachricht **110** an die Kommunikationseinrichtung **106**.

[0051] Damit die Kommunikationseinrichtung **106** sicherstellen kann, dass die Antwortnachricht **110** auch tatsächlich von dem Kommunikationsendgerät **102** abgeschickt wurde und unverfälscht empfangen wurde, wird von der Applikation **124** gemäß einem Ausführungsbeispiel der Erfindung vor dem Senden ihrerseits eine zweite digitale Signatur der Nachricht **110** hinzugefügt.

[0052] Fig. 2A zeigt ein Ausführungsbeispiel eines Kommunikationsendgerätes **102**, welches mobil ist, in Fig. 2A beispielsweise als Mobilfunkendgerät **218** ausgeführt, mit einer Antenne **208**, einer Nahfeldkommunikationsschnittstelle **210**, einer optischen Schnittstelle **212**, einer Mensch-Maschine-Schnittstelle, aufweisend ein Display **204**, eine Tastatur **206** und einen Lautsprecher **216**, einer SIM-Karte **202**, und einer darauf implementierten Applikation **124**. Das Kommunikationsendgerät **102** kann gemäß einem Ausführungsbeispiel einen Datenspeicher aufweisen, in dem die Applikation **124** gespeichert ist und einen Prozessor, auf dem die Applikation **124** ausgeführt wird.

[0053] Die Applikation **124** könnte aber zumindest teilweise auch in Hardware realisiert sein.

[0054] Gemäß einem Ausführungsbeispiel kann in das mobile Kommunikationsendgerät **102** eine SIM-Karte eingelegt werden, die einen SIM-Kartenspeicher enthält, in dem die Applikation gespeichert ist.

[0055] Die Applikation **124** kann den Benutzer des Kommunikationsendgerätes **102**, für den ein Nachweis in Form einer Nachweis-Nachricht erstellt werden soll, gemäß einem Ausführungsbeispiel optisch

über das Display **204** oder akustisch über den Lautsprecher **216** auffordern, zu bestätigen, dass die Nachweis-Nachricht erstellt und an die Kommunikationseinrichtung **106** übertragen werden soll.

[0056] Die Nachrichten **108**, **110**, die zwischen dem Kommunikationsendgerät **102** und der Kommunikationseinrichtung **106** ausgetauscht werden, können über die Datenschnittstelle eines Mobilfunkkommunikationsstandards wie z. B. GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System), FPLMTS (Future Public Land Mobile Telecommunication System), CDMA 2000 (Code Division Multiple Access 2000) oder über eine paketorientierte bzw. Internet-Schnittstelle, wie z. B. gemäß GPRS (General Packet Radio Service) als Teil von GSM, oder alternativ unter Verwendung von UMTS, übertragen werden.

[0057] Gemäß einem weiteren Ausführungsbeispiel kann das Kommunikationsendgerät **102** aber auch ein drahtloses Kommunikationsendgerät **102** sein, bei dem die Nachrichten über eine Schnittstelle **210** eines Nahfeldkommunikationsstandards wie z. B. Bluetooth, eines Standards eines Drahtlos-Kommunikationssystem, wie z. B. IEEE 802.11, WiMax (Worldwide Interoperability for Microwave Access), einer optischen Datenschnittstelle **212**, wie z. B. IrDA (Infrared Data Association) oder einen optischen Scanner, wie z. B. einen Barcode-Leser oder eine Kamera oder anderen Drahtlos-Standards übertragen werden. Das Kommunikationsendgerät **102** kann beispielsweise ein PDA (Personal Digital Assistant), ein tragbarer Computer oder auch ein Musikabspielgerät mit digitalen Kommunikationsmöglichkeiten oder ein sonstiges tragbares elektronisches Gerät sein, in das die von der Applikation **124** benötigten Funktionen implementiert sind. Im Falle eines optischen Scanners könnte z. B. ein Barcode von einem Display **220** (siehe **Fig. 2B**) der Kommunikationseinrichtung **106** eingelesen werden.

[0058] Auch eine drahtgebundene Schnittstelle über ein Datenkabel ist in einer alternativen Ausführungsform der Erfindung vorgesehen. Wenn es sich um eine Funkverbindung handelt, erfolgt das Empfangen und Senden über eine Antenne **208**, die in das Kommunikationsendgerät **102** integriert sein kann oder auch aus diesem herausgeführt sein kann.

[0059] Die Applikation **124** kann gemäß einem Ausführungsbeispiel über einen sicheren Übertragungskanal aktualisiert werden. So können z. B. die Datenstruktur, der ausführbare Code oder die Daten flexibel geändert werden. Hierbei kann auch z. B. der Anwendungsbereich verändert werden, beispielsweise durch eine zusätzliche Anforderung von Informationen oder eine Änderung der Abfrage. So könnte im Beispiel des Zigarettenautomaten leicht einer eventuellen Gesetzesänderung bezüglich eines Mindestalters beim Kauf von Zigaretten Rechnung getragen werden. Der sichere Übertragungskanal zum Aktualisieren der Applikation kann ein drahtgebundener Übertragungskanal oder ein drahtloser Übertragungskanal sein. Weiterhin kann der sichere Übertragungskanal zum Aktualisieren der Applikation ein Telekommunikations-Übertragungskanal sein, beispielsweise ein drahtgebundener Telekommunikations-Übertragungskanal oder ein drahtloser Telekommunikations-Übertragungskanal.

[0060] Das hier beschriebene Verfahren gemäß einem Ausführungsbeispiel der Erfindung dient beispielsweise zum einen dazu, eine Kundenkarte durch eine digitale Lösung zu ersetzen und zum zweiten einen Nachweis gegenüber einer Instanz zu erbringen, zu der bis dahin keinerlei Geschäftsbeziehungen bestanden hat.

[0061] Handelt es sich gemäß obigen Ausführungsbeispielen bei dem Kommunikationsendgerät **102** um ein Mobilfunkendgerät **218**, so werden die Nachweise mit Hilfe dieses Mobilfunkendgerätes **218** bewerkstelligt.

[0062] Das Mobilfunkendgerät **218** eines Kunden hat gemäß diesem Ausführungsbeispiel eine Applikation **124** gemäß einem Ausführungsbeispiel der Erfindung installiert. Diese Applikation **124** kann vertrauenswürdig sein, d. h. eine Instanz sorgt nachweislich für das Vorhandensein der Applikation **124** und deren Unveränderheit. Diese Instanz könnte beispielsweise für den Fall, dass sich die Applikation **124** auf dem Terminal, also z. B. dem Mobilfunkendgerät **218** selbst befindet, der Hersteller des Mobilfunkendgerätes **218** sein. Alternativ kann die Instanz auch der Mobilfunkbetreiber selbst sein.

[0063] Die Prozessoreinheit **104** mit einem Prozessor sowie einem Datenspeicher zum Speichern von Informationen und vom Prozessor der Prozessoreinheit ausführbaren Daten, die die Applikation bilden, kann sich gemäß einem Ausführungsbeispiel auf dem Kommunikationsendgerät **102**, welches z. B. das Mobilfunkendgerät **218** sein kann, selbst befinden.

[0064] Die Applikation **124** kann sich gemäß einem Ausführungsbeispiel auf einer elektronischen Karte befinden, die zumindest einen Datenspeicher und/oder einen Prozessor enthält. In einem Ausführungsbeispiel der Erfindung ist der Prozessor ein programmierbarer Prozessor, beispielsweise ein Mikrocontroller. Ein Beispiel einer derartigen elektronischen Karte ist eine SIM-Karte (Subscriber Identity Module) **202** eines Mobilfunkanbieters.

[0065] Die SIM-Karte **202** in der Ausführung einer so genannten Smartcard weist beispielsweise folgende Eigenschaften auf:

- Sie enthält eine verarbeitende Einheit (beispielsweise einen Microcontroller).
- Sie ist gegen Manipulation von außen (anders ausgedrückt von außerhalb der SIM-Karte) geschützt.
- Die Schnittstelle ist definiert und nur nach Autorisation nutzbar.
- Sie stellt, gegenüber einem Mobilfunkendgerät mit eventuell offenem Betriebssystem und Schnittstellen zur Programmierung, ein geschlossenes, Daten verarbeitendes System dar.
- Sie ist personenbezogen und bleibt bei einem Wechsel des Mobilfunkendgerätes erhalten, was ebenfalls der Aufgabe, einen personenbezogenen Nachweis zu liefern, entgegenkommt.

[0066] In dem zweitgenannten Fall ist der Mobilfunkanbieter die vertrauenswürdige Instanz, die ihre Dienste gegenüber Dritten (wie die beispielhafte genannte Videothek) zur Verfügung stellen kann.

[0067] Unter diesen Voraussetzungen erhält die Nachweis-Ausstellende Instanz somit die Möglichkeit, ein selbst erzeugtes digitales Zertifikat in die Applikation **124** der vertrauenswürdigen Instanz zu hinterlegen. Des Weiteren erhält diese Instanz die Möglichkeit, in Form eines vom Mobilfunkanbieter ausgestellten digitalen Zertifikats sich gegenüber der Applikation **124** authentifizieren zu können. Dieses Zertifikat ersetzt in einem Ausführungsbeispiel eine herkömmliche Kundenkarte. Die vertrauenswürdige Instanz kann aber auch selbst Informationen über den Mobilfunkteilnehmer in der Applikation **124** hinterlegen, die zum Nachweis geeignet sind.

[0068] In die von der Kommunikationseinrichtung **106** gesendeten erste Nachricht **108** kann gemäß einem Ausführungsbeispiel der Erfindung zusätzlich eine Zufallszahl **114** eingefügt werden, die auch in die Antwortnachricht **110** eingebunden wird. Das Einbinden einer Zufallszahl **114** dient der Verhinderung einer so genannten Replay-Attacke. Durch die wechselnde Zahlenfolge unterscheidet sich jede Anfrage von vorherigen Anfragen, so dass ein einfaches neues Übertragen einer zuvor generierten Antwortnachricht **110** zum Fehlerfall führt.

[0069] In dem Kommunikationsendgerät **102** kann gemäß einem Ausführungsbeispiel eine Verschlüsselungseinheit vorhanden sein, die die Zufallszahl beispielsweise mit dem öffentlichen Schlüssel des Nachweisenden verschlüsselt, so dass das Kommunikationsendgerät **102** die verschlüsselte Zufallszahl in die Antwortnachricht **110** einfügen kann und damit die Stärke der Authentifizierung erhöht wird.

[0070] In die Antwortnachricht **110** kann gemäß einem Ausführungsbeispiel der Erfindung weiterhin das Datum und/oder die Uhrzeit **116** eingebunden werden, um zu verhindern, dass durch Verstellen der internen Uhr ein falscher Nachweis erzeugt wurde.

[0071] Zur Authentifizierung des Benutzers des Kommunikationsendgerätes **102** kann das Kommunikationsendgerät **102** gemäß einem Ausführungsbeispiel die Eingabe einer Kennzeichnung, wie beispielsweise einer PIN (Personal Identification Number) von dem Nutzer des Kommunikationsendgerätes fordern, die er über die Tastatur **206** eingeben kann. Dadurch wird sichergestellt, dass der Nutzer der tatsächlich berechtigte Nutzer des Kommunikationsendgerätes **102** bzw. des Mobilfunkendgerätes **218** ist. Es können jedoch auch andere Verfahren, wie z. B. biometrische Verfahren, also beispielsweise Fingerabdruck, Scannen von Gesichtsmerkmalen oder der Iris oder Stimmerkennung zur Authentifizierung eingesetzt werden.

[0072] Indem die Applikation **124** von dem Nutzer des Kommunikationsendgerätes eine Bestätigung anfordert, dass das Kommunikationsendgerät eine Nachweis-Nachricht mit der Antwort der Anfrage erstellen und an die Kommunikationseinrichtung übertragen soll, behält der Benutzer die Kontrolle über den Vorgang und darüber, ob die Daten übertragen werden sollen.

[0073] Bei der Anfrage, die durch das Erstellen der Nachweis-Nachricht beantwortet werden soll, kann es sich beispielsweise um Informationen über persönliche Eigenschaften des Nutzers des Mobilfunkgerätes **218** handeln, wie z. B. Alter, bzw. ob ein bestimmtes Alter unterschritten oder überschritten ist, eine Kundennummer oder das Geschlecht, um nur ein paar Beispiele zu nennen.

[0074] Fig. 2B zeigt ein Ausführungsbeispiel für eine zu dem Kommunikationsendgerät **102** korrespondierende Kommunikationseinrichtung **106**.

[0075] Gemäß diesem Ausführungsbeispiel weist die Kommunikationseinrichtung **106** eine Prozessoreinrichtung **224** auf, die die Anforderungsnachricht **108** erstellt und an das Kommunikationsendgerät **102** sendet. Die Anforderungsnachricht **108** enthält zumindest eine Anforderung nach einem Nachweis und eine erste digitale Signatur. Die digitale Signatur in der Anforderungsnachricht gewährleistet, dass nicht jeder einen Nachweis anfordern kann. Es ist jedoch darauf hinzuweisen, dass die erste digitale Signatur optional ist.

[0076] Die Anforderungsnachricht kann aber auch, wie weiter unten anhand der Fig. 9 beschrieben wird, noch weitere Daten, wie beispielsweise eine Zufallszahl, das aktuelle Datum und die Uhrzeit und einen Nachrichtenkopf enthalten. Gemäß einem Ausführungsbeispiel betrifft die Anforderung Informationen über den Benutzer des Kommunikationsendgerätes **102**.

[0077] Gemäß einem Ausführungsbeispiel kann die Kommunikationseinrichtung **106** ferner eine Information über den Typ des angeforderten Nachweises einfügen.

[0078] Die Prozessoreinrichtung **104** empfängt gemäß einem Ausführungsbeispiel auf das Senden der Anforderungsnachricht **108** hin eine Antwortnachricht **110** von dem Kommunikationsendgerät **102** und überprüft deren Inhalt. Diese enthält gemäß einem Ausführungsbeispiel z. B. eine zweite, von dem Kommunikationsendgerät **102** erstellte, digitale Signatur, den angeforderten Nachweis, die zurückgesendete, eventuell verschlüsselte Zufallszahl, Datum und Uhrzeit sowie einen Nachrichtenkopf. Eine beispielhafte Antwortnachricht **110** wird später anhand der Fig. 12 beschrieben.

[0079] Die Kommunikationseinrichtung **106** weist gemäß einem Ausführungsbeispiel ebenfalls eine Mensch-Maschinen-Schnittstelle auf, mit z. B. einem Display **220** und einer mechanischen oder elektronischen Eingabeeinrichtung, wie z. B. einem oder mehreren Bedienknöpfen, einer Tastatur oder einem berührungsempfindlichen Bildschirm. Die Kommunikationseinrichtung **206** besitzt weiterhin eine oder mehrere zu dem Kommunikationsendgerät **102** korrespondierende Schnittstellen **226**, **228**. Diese können dementsprechend beispielsweise eine oder mehrere Mobilfunk-Kommunikationsschnittstellen, Drahtlos-Kommunikationsschnittstellen oder optische Kommunikationsschnittstellen sein. Falls die Nachrichten über eine Funkverbindung übertragen werden, besitzt die Kommunikationseinrichtung gemäß einem Ausführungsbeispiel der Erfindung zumindest eine Antenne. Gemäß einem Ausführungsbeispiel erstellt die Prozessierungseinheit **224** die Anforderungsnachricht **108**, die über eine der Schnittstellen und eventuell die Antenne **230** zu dem Kommunikationsendgerät **102** übertragen werden. In umgekehrter Richtung wird die über eventuell die Antenne **230** und eine der Schnittstellen **226**, **228** übertragene Antwortnachricht **110** zu der Prozessierungseinheit **224** weitergeleitet, die schließlich den Inhalt der Antwortnachricht **110** auswertet und entsprechende Aktionen, wie z. B. das Auswerfen einer Zigarettenschachtel im Beispiel des Zigarettenautomaten veranlasst.

[0080] In dem Diagramm **300** in Fig. 3 ist der folgende Nachrichtenablauf zwischen den Instanzen gemäß einem Ausführungsbeispiel der Erfindung dargestellt, wenn sich ein Nachweis-Erbringer, wie z. B. ein Mobilfunkteilnehmer **304**, gegenüber einer Instanz **306** ausweisen möchte.

[0081] Die Nachrichten, die zwischen den Instanzen **302**, **304**, **306** übertragen werden, werden weiter unten anhand der Fig. 9 bis Fig. 12 detailliert beschrieben.

1. Gemäß einem Ausführungsbeispiel generiert die einen Nachweis einfordernde Instanz **306** in **308** eine Nachweis-Nachricht-Anforderungsnachricht **108** und stellt digital, entweder über Nahfeldkommunikation, z. B. Bluetooth, optische Kommunikation, z. B. über IrDa, oder über ein anderes informationsübertragendes System (z. B. Internet) mittels dieser Nachweis-Nachricht-Anforderungsnachricht **108** eine Anfrage an das Kommunikationsendgerät **102** des Mobilfunkteilnehmers **304**, die dort an die in Fig. 3 eingezeichnete SIM **302** weitergeleitet wird. In alternativen Ausführungsbeispielen sind andere Übertragungswege vorgesehen, wie z. B. eine optische Übertragung, bei der beispielsweise ein am Bildschirm der Nachweis-einfordernden Instanz **306** dargestellter Barcode (z. B. Semacode) gelesen wird, oder eine Übertragung über das Mobilfunknetz selbst. Dabei sind in der Nachweis-Nachricht-Anforderungsnachricht **108** beispielsweise folgende Informationen enthalten:
   - Zertifikat der einfordernden Instanz **306**;
   - Binärcodierte Art des Nachweises (z. B. Übereinstimmung der Kundennummer, „älter als X Jahre?", „männlich?");
   - Zufällige Zahlenfolge.
2. Die Nachweis-Nachricht-Anforderungsnachricht **108** wird gemäß diesem Ausführungsbeispiel an die Applikation **124** in der SIM-Karte **202** geleitet.
3. Der Mobilfunkteilnehmer **304** bestätigt gemäß dem Ausführungsbeispiel mit der Nachricht „ack" **316** auf eine Anfrage ack_request **314** hin an seinem Endgerät **218**, dass er mit Hilfe seines Mobilfunkendgerätes **218** den geforderten Nachweis an die autorisierte Instanz **306** führen möchte.
4. In der Applikation **124** wird gemäß diesem Ausführungsbeispiel in **318** das Zertifikat der anfragenden Stelle **306** überprüft und im Falle eines positiven Nachweises die in der Nachweis-Nachricht-Anforderungsnachricht **108** enthaltene Anfrage weiter bearbeitet. Im negativen Falle wird eine Fehlermeldung ausgegeben und der Vorgang an dieser Stelle abgebrochen.
5. Weiter gemäß diesem Ausführungsbeispiel authentifiziert sich der Mobilfunkteilnehmer **304** nun gegenüber der Applikation **124**. Dies kann beispielsweise mittels des Nachrichtenpaares auth_request **320** und auth **322** durch Eingabe der vom Benutzer gewählten PIN für die SIM-Karte **202** und der nachfolgenden Überprüfung **324** geschehen und dient dazu, dass ein Nachweis nicht von einer Person geführt werden kann, die unrechtmäßig in den Besitz des Mobilfunkendgerätes **218** erlangt ist. Es ist darauf hinzuweisen, dass die Authentifikation optional ist.
6. Die Applikation **124** überprüft in **326** die nachzuweisende Eigenschaft. Wird beispielsweise ein Nachweis gefordert, dass der Mobilfunkteilnehmer **304** gleich öder älter als 16 Jahre alt ist, wird aus dem hinterlegten Geburtsdatum und dem ak-

tuellen Datum eine Ja-oder-Nein-Antwort generiert.

7. Für den Fall, dass der Nachweis positiv ist, stellt die Applikation **124** eine Antwort zusammen, die die in der Nachweis-Nachricht-Anforderungsnachricht „certificate_request" **108** übertragene zufällige Zahlenfolge **114**, das aktuelle Datum und das hinterlegte Zertifikat bzw. die in 6. berechnete Antwort enthält und signiert diese digital mit einer Signatur des Mobilfunkanbieters. Das Prinzip der digitalen Signatur wird weiter unten anhand der Fig. 14 und Fig. 15 erläutert. Die so erzeugte Antwortnachricht **110**, in Fig. 3 als „certificate"-Nachricht **110** bezeichnet, wird an die Nachweis-einfordernde Instanz **306** übertragen. Ist im oben genannten Beispiel der Teilnehmer **304** nicht gleich oder älter als 16 Jahre alt, wird entweder keine Antwort generiert oder zu Gunsten der besseren Nutzbarkeit eine negative Antwort, nämlich eine Antwort, dass die nachzuweisende Eigenschaft nicht erfüllt ist.

8. Die nachfragende Instanz **306** überprüft gemäß einer Weiterführung dieses Ausführungsbeispiels mit Hilfe eines vom Mobilfunkanbieter bereitgestellten öffentlichen Schlüssels, ob die digitale Signatur der Antwortnachricht **110** der Applikation **124** gültig ist. Ist diese gültig, kann dem Nachweis vertraut werden. Kann die Signatur nicht verifiziert werden, führt dies zu einer

[0082] Fehlermeldung. Der Vorgang kann gegebenenfalls wiederholt werden.

[0083] Es könnte auch die Überprüfung des Zertifikats vor der ack_request Nachricht **314** erfolgen. Dies hätte beispielsweise den Effekt, dass der Nachweiserbringer **304** im Fehlerfall nicht erst um Autorisation gebeten wird. Auf der anderen Seite benötigt die Überprüfung des Zertifikats Rechenleistung, so dass mit häufig eingespielten „certificate_request" Nachrichten **108** eine DoS-Attacke (Denial of Service) erfolgen könnte. Da die Autorisation mit Teilnehmer-Präferenzen weitestgehend automatisiert (ohne Beteiligung des Nachweisenden **304**) werden könnte, ist in einem Ausführungsbeispiel die hier angegebene Reihenfolge vorgesehen.

[0084] Die gemäß den Ausführungsbeispielen verwendeten Nachrichten werden in der Beschreibung weiter unten anhand der Fig. 9 bis Fig. 12 genauer beschrieben.

[0085] Im Folgenden werden die im Nachrichtenablauf-Diagramm dargestellten Prozesse detailliert dargestellt:

Fig. 4 zeigt ein Ablaufdiagramm gemäß einem Ausführungsbeispiel zur Generierung **308** der Nachweis-Nachricht-Anforderungsnachricht (certificate_request-Nachricht) **108**. Zunächst wird nach Starten des Prozesses in **400** in **402** eine Zufallszahlenfolge erzeugt, danach in **404** die eigentliche Anfrage, die z. B. Anforderung eines Altersnachweises enthält, in die Nachweis-Nachricht-Anforderungsnachricht **108** eingefügt. Schließlich wird die Nachricht noch in **406** digital signiert. Dies kann z. B. mit einem allgemein bekannten, oben genannten Verfahren geschehen. Dann wird der Prozess in **408** beendet.

[0086] Fig. 5 zeigt in einem Ablaufdiagramm gemäß einem Ausführungsbeispiel die Überprüfung **318** des Zertifikats des Nachweisfordernden **306** durch die Applikation **124** in der Prozessoreinheit **104** (z. B. SIM-Karte **202**) des Kommunikationsendgerätes **102** (z. B. das Mobilfunkendgerät **218**). Hierbei wird nach Starten des Prozesses in **500** in **502** der Hashwert über die empfangene Nachricht **108** bis (ausschließlich) zum Nachrichtenfeld „Message Authentication" **914**, welches weiter unten in Fig. 9 genauer beschrieben wird, gebildet (in Fig. 5 bezeichnet mit **512**). In **504** wird der Hashwert, der in dem Nachrichtenfeld „Message Authentication" **914** (in Fig. 5 bezeichnet mit **514**) verschlüsselt übertragen wurde, entschlüsselt. Die beiden Werte werden in **506** miteinander verglichen. Bei positiver Übereinstimmung ("Ja" in **506**) wird in **508** zur Benutzerauthentifizierung weitergegangen; bei negativer Übereinstimmung ("Nein" in **506**) wird in **510** eine Fehlermeldung generiert und der Prozess wird in **516** abgebrochen.

[0087] Fig. 6 zeigt ein Ablaufdiagramm der Benutzerauthentifizierung **324** gemäß einem Ausführungsbeispiel der Erfindung. Nach Starten des Prozesses in **600** wird in **602** der Benutzer zur Eingabe einer PIN aufgefordert. In **604** wird die eingegebene PIN mit der gespeicherten PIN **610** verglichen. Bei positiver Übereinstimmung ("Ja" in **604**) wird in **606** zum Nachweisprozess weitergegangen; bei negativer Übereinstimmung ("Nein" in **604**) wird in **608** eine Fehlermeldung generiert und der Prozess wird in **612** abgebrochen. Es können jedoch auch andere Verfahren, wie z. B. biometrische Verfahren zur Authentifizierung eingesetzt werden.

[0088] In Fig. 7 ist ein Ablaufdiagramm zum Überprüfen **326** der nachzuweisenden Eigenschaft in dem Kommunikationsendgerät **102** gemäß einem Ausführungsbeispiel der Erfindung dargestellt. Nach Starten des Prozesses in **700** wird in **702** werden die gespeicherten Werte (in Fig. 7 bezeichnet mit **708**) mit dem geforderten Nachweis (in Fig. 7 bezeichnet mit **710**) verglichen. Dies ist z. B. in der Fortführung des Beispiels zur Altersverifizierung die eigentliche Überprüfung, ob der Benutzer das Mindestalter besitzt oder nicht. Bei einem positiven Ergebnis ("Ja" in **702**) wird in **704** die Nachricht „certificate" **110** erstellt, die an die Nachweis-einfordernde Instanz **306** gesendet wird. Bei einem negativen Ergebnis ("Nein" in **702**) wird in **706** eine Fehlermeldung generiert. Dann wird

der Prozess in **712** beendet.

[0089] Fig. 8 zeigt ein Ablaufdiagramm zur Überprüfung **332** der „certificate"-Nachricht **110** gemäß einem Ausführungsbeispiel der Erfindung. Ähnlich der Vorgehensweise für die „certifiate request"-Nachricht **108** wird nach Starten des Prozesses in **800** in **802** zunächst der Hashwert über die Nachricht **110**, die in Fig. 12 weiter unten detailliert erläutert wird, bis (ausschließlich) zum Feld „Message Authentication" **1212** (siehe Fig. 12) gebildet (in Fig. 8 bezeichnet mit **814**) und in **804** der verschlüsselt übertragene Wert in dem Nachrichtenfeld „Message Authentication" **1212** (in Fig. 8 bezeichnet mit **816**) entschlüsselt. Diese beiden Werte werden in **806** miteinander verglichen. Bei negativem Ergebnis ("Nein" in **806**) wird in **812** eine Fehlermeldung generiert und der Prozess wird in **818** beendet. Ist der Vergleich positiv ("Ja" in **806**), wird in **808** der erbrachte Nachweis (in Fig. 8 bezeichnet mit **820**) mit dem geforderten Nachweis (in Fig. 8 bezeichnet mit **822**) verglichen. An dieser Stelle überprüft also z. B. die Nachweis-einfordernde Instanz **306**, ob der Altersnachweis erbracht wurde. Bei positivem Ergebnis ("Ja" in **808**) kann die Nachweis-einfordernde Instanz **306** durch eine Meldung oder ein Signal weitere Aktionen ausführen, wie z. B. die Ausgabe der Meldung oder in dem Beispiel des Zigarettenautomaten der Auswurf einer Schachtel Zigaretten. Anders ausgedrückt, ist bei positivem Ergebnis ("Ja" in **808**) der Nachweis in **810** erfolgt. Bei negativem Ergebnis ("Nein" in **808**) wird in **812** eine Fehlermeldung generiert und der Prozess wird in **818** beendet.

[0090] Im Folgenden werden die Nachrichten gemäß Ausführungsbeispielen der Erfindung näher erläutert:
In Fig. 9 ist die „certificate_request" Nachricht **108**, auch bezeichnet als Nachweis-Nachricht-Anforderungsnachricht **108**, dargestellt, die gemäß einem Ausführungsbeispiel folgende Felder enthält:

- Nachricht-Kopffeld (Message Header) **902**:
  Das Nachricht-Kopffeld **902** enthält gemäß einem Ausführungsbeispiel beispielsweise Adressat, Absender, Nachrichtenart (in diesem Fall die Nachrichtenart „certificate_request") und optional eine „Message ID" (eindeutige Identifikation der Nachricht). Hierfür könnte auch eine Zufallszahlenfolge (RAND) verwendet werden. Durch die Einführung einer „Message ID" im Nachrichten-Kopffeld **902** ist die im Vergleich zur Zufallszahlenfolge kleinere „Message ID" leichter und somit schneller zu bearbeiten.
- Zufallszahlenfolge RAND **904**:
  Die Zufallszahlenfolge **904** bezeichnet die Zufallszahlenfolge, die sowohl zur Zuordnung zwischen einer Nachweis-Nachricht-Anforderungsnachricht (auch bezeichnet als „certificate_request" Nachricht) **108** und einer „certificate" Nachricht **110** als auch zur Authentifizierung des Nachweisenden **304** verwendet wird.
- Datum & Uhrzeit **906**:
  Dieses Feld ist in dieser Nachricht **108** optional. Eine Wirkung in der Einführung dieses Feldes ist darin zu sehen, dass Fehler, die durch Abweichungen zwischen den Uhren des Nachweis-Einfordernden **306** und des Nachweisenden **304** entstehen könnten, vermieden werden. Schließlich sollte für die Berechnung des Nachweises Datum und Uhrzeit des Nachweis-Einfordernden **306** gelten. Würden diese Werte übermittelt und für die Berechnung übernommen, kann somit eine mögliche Fehlerquelle ausgeschlossen werden. Eine weitere Wirkung besteht darin, dass dieses Feld eine Replay-Attacke, in der ein Eingreifer eine zuvor abgefangene und aufgezeichnete Nachricht einem Nachweisenden **304** vorspielt, erschwert.
- Nachweis-Typ **908**:
  Dieses Nachrichtenfeld enthält die Art des Nachweises, der gefordert wird. Es wird beispielsweise festgelegt, ob es sich um einen vorab hinterlegten Nachweis (bereits bestehende Geschäftsbeziehung), oder einen anonym dynamisch erzeugten Nachweis handelt.
- Nachweis-Parameter **910**:
  Die Nachweis-Parameter **910** sind in Abhängigkeit des Feldes „Nachweis-Typ" **908** zu interpretieren. Dieses Feld enthält die je nach Art des geforderten Nachweises zugehörigen Parameter, wie beispielsweise das nachzuweisende Mindestalter.
- X.509 Zertifikat **912**:
  Hierbei handelt es sich um das Zertifikat des Nachweis-Einfordernden **306**. Dies könnte Beispielsweise dem ITU-Standard X.509 folgen oder anderweitig in einer vordefinierten Struktur vorliegen. Der X.509-Standard ist weiter unten näher erläutert.
- Nachricht-Auth **914**:
  Dieses Feld enthält die digitale Signatur der Nachweis-Nachricht-Anforderungsnachricht **108** durch den Nachweis-Einfordernden **306**. Dieses Feld sichert die Integrität der Nachricht **108** zu. Wird ein Feld der Nachricht verändert, passt das „Nachricht-Auth" Feld **914** nicht mehr zu dem Rest der Nachricht **108** und die Nachricht **108** kann ohne weitere Bearbeitung verworfen werden.

[0091] Die Nachricht „certificate_request" **108** könnte gemäß einem Ausführungsbeispiel zur Minimierung der Bandbreite binärcodiert und/oder komprimiert werden.

[0092] Die Nachweis-Nachricht-Anforderungsnachricht **108** kann gemäß weiteren Ausführungsbeispielen auch mehr oder weniger als die in Fig. 9 beispielhaft aufgeführten Felder aufweisen.

[0093] Fig. 10 zeigt die „ack_request" Nachricht **314**, die gemäß einem Ausführungsbeispiel der Erfin-

dung folgende Felder enthält:

• Nachricht-Kopffeld, (Message Header) **1002**:
Das Nachricht-Kopffeld **1002** enthält gemäß einem Ausführungsbeispiel mindestens die Nachrichtenart (in diesem Fall die Nachrichtenart „ack_request").

• Nachweis-Typ **1004**:
Dieses Nachrichtenfeld enthält die Art des Nachweises, der gefordert wird. Es handelt sich inhaltlich um den in „certificate_request" **108** übermittelten Eintrag. Er dient dem Nachweisenden **304** zu entscheiden, ob er dieser Art des Nachweises zustimmen möchte.

• Nachweis-Parameter **1008**:
Ebenfalls für die Autorisation durch den Nachweisenden **304** vorgesehen werden die Parameter des geforderten Nachweises. Es handelt sich inhaltlich um die in „certificate_request" **108** übermittelten Einträge.

[0094] Die Nachricht „ack_request" **314** könnte zur Minimierung der Bandbreite binärcodiert und/oder komprimiert werden.

[0095] Auch die Nachricht ack_request **314** kann gemäß weiteren Ausführungsbeispielen auch mehr oder weniger als die in Fig. 10 beispielhaft aufgeführten Felder aufweisen.

[0096] Fig. 11 zeigt die „ack" Nachricht **316**, die gemäß einem Ausführungsbeispiel der Erfindung folgende Felder enthält:

• Nachricht-Kopffeld **1102**:
Das Nachricht-Kopffeld **1102** enthält gemäß diesem Ausführungsbeispiel mindestens die Nachrichtenart (in diesem Fall die Nachrichtenart „ack").

• Ack Wert **1104**:
Dieses Feld gibt gemäß einem Ausführungsbeispiel die Antwort auf die Autorisationsanfrage in der ack_request Nachricht **314** zurück an die SIM **202**. Das Feld „Ack Wert" enthält mindestens einen booleschen Ausdruck (Wahr/Falsch). Denkbar wären auch Fehlercodes oder Gründe der Ablehnung bis hin zu alternativen Nachweisen, die an Stelle des geforderten geliefert werden könnten.

[0097] Die Nachricht „ack" könnte zur Minimierung der Bandbreite binärcodiert und/oder komprimiert werden.

[0098] In Fig. 12 ist die „certificate" Nachricht **110** dargestellt, die gemäß einem Ausführungsbeispiel der Erfindung folgende Felder enthält:

• Nachricht-Kopffeld (Message Header) **1202**:
Das Nachricht-Kopffeld **1202** enthält beispielsweise Adressat, Absender, Nachrichtenart (in diesem Fall die Nachrichtenart „certificate") und optional die „Message ID". Letztere ist identisch mit der „certificate_request" Nachricht **108** und nur enthalten, wenn es in der „certificate_request" Nachricht **108** eine "Message ID" gab.

• Zufallszahlenfolge (RAND) **1204**:
Die Zufallszahlenfolge **1204** bezeichnet die Zufallszahlenfolge, die in der „certificate_request" Nachricht **108** übermittelt wurde. Sie ist vorgesehen, um eine eindeutige Zuordnung zwischen der „certificate_request" Nachricht **108** und der „certificate" Nachricht **110** zu erreichen. Da die gesamte Nachricht **110** signiert wird („Message Auth" **1212**), dient die Zufallszahlenfolge **1204** der Verhinderung, eine zuvor mitgeschnittene „certificate" Nachricht **110** nochmals als Antwort auf die aktuelle „certificate_request" Nachricht **108** zu einem späteren Zeitpunkt zurückzusenden. Die Zufallszahlenfolge **1204** garantiert somit die Aktualität der Antwort. Die Sicherheit des Verfahrens kann beispielsweise durch starke asymmetrische Verschlüsselung der Zufallszahlenfolge **1204** erhöht werden. In diesem Fall wird die Zufallszahlenfolge **1204** noch mit dem öffentlichen Schlüssel (public-key) des Nachweisenden **304** (für den Fall, dass bereits eine Geschäftsbeziehung zu dem Nachweisenden **304** besteht) oder dem öffentlichen Schlüssel (public-key) der authentifizierenden Instanz (zum Beispiel eines Mobilfunknetzbetreibers) verschlüsselt werden. Wird diese Zufallszahlenfolge dann unverschlüsselt oder mit dem öffentlichen Schlüssel (public-key) des Nachweiseinfordernden **306** übermittelt, ist sichergestellt, das der Nachweisende **304** im Besitz des geheimen Schlüssels (secret-key) ist, was die Stärke der Authentifizierung des Nachweisenden **304** deutlich erhöht.

• Datum & Uhrzeit **1206**:
Dieses Nachrichtenfeld enthält das in der SIM **202** für die Berechnung des Nachweises zu Grunde liegende Datum und die entsprechende Uhrzeit. Dieses könnte Datum und Uhrzeit des Terminals sein, oder die in der „certificate_request" Nachricht **108** übermittelten Werte.

• Nachweis-Typ **1208**:
Dieses Nachrichtenfeld ist optional und enthält die Art des Nachweises, der gefordert wurde. Dieses Feld entspricht, falls vorhanden, dem Feld der entsprechenden „certificate_request" Nachricht **108**. Eine Wirkung des Wiederholens der Art des Nachweises besteht darin, dass sichergestellt werden würde, dass bei der Übermittlung der Nachweisanfordeqrung kein Übertragungsfehler entstanden ist und die Antwort wirklich den geforderten Nachweis enthält und nicht fehlerhaft einen falsch interpretierten Nachweis. Es ist anzumerken, dass bei einem Übermittlungsfehler die Signatur nicht übereinstimmen würde und der Auswertung in der SIM **202** vertraut werden kann.

• Nachweis **1210**:
Dieses Feld enthält den eigentlichen Nachweis, der gefordert wurde. Wird beispielsweise ange-

fragt, ob der Nachweisende mindestens 18 Jahre alt ist, enthält dieses Feld inhaltlich die Antwort „Nachweisender ist älter als 18 Jahre". Dies könnte ebenfalls im X.509-Standard erfolgen, oder eine andere zuvor festgelegte Datenstruktur beinhalten.

• Nachricht-Auth **1212**:
Dieses Feld enthält die digitale Signatur der Nachricht durch den Nachweisenden **304**. Dieses Feld sichert die Integrität der Nachricht **110** zu. Wird ein Feld der Nachricht verändert, passt das „Nachricht-Auth" Feld **1212** nicht mehr zu dem Rest der Nachricht **110** und die Bearbeitung führt zum Fehlerfall. Der angeführte Nachweis kann in diesem Fall nicht anerkannt werden.

[0099] Die Nachricht „certificate" **110** könnte zur Minimierung der Bandbreite binärcodiert und/oder komprimiert werden.

[0100] Die Nachricht „certificate" **110** kann gemäß weiteren Ausführungsbeispielen auch mehr oder weniger als die in Fig. 12 beispielhaft aufgeführten Felder aufweisen.

[0101] Die Nachrichten in den Fig. 9 bis Fig. 12 stellen Ausführungsbeispiele dar, die der Fachmann in geeigneter Weise verändern oder für einen bestimmten Anwendungsfall anpassen kann. So kann z. B. die Reihenfolge der Nachrichtenfelder variiert werden, wenn sie allen drei Beteiligten bekannt ist. Zusätzliche Felder zur weiteren Optimierung sind ebenfalls möglich.

[0102] Anstelle der in der SIM-Karte **202** generierten Antwortnachricht **110** könnte auch eine gespeicherte vorgefertigte Nachweis-Nachricht als Antwort zurückgesendet werden. Der Nutzen darin besteht in einer weniger komplexen Verarbeitung in der SIM-Karte **202** bzw. die sichere Speicherung ohne SIM-Karte **202**. Beeinträchtigend ist, dass nur vorgefertigte Nachweis-Nachrichten übertragen werden können und diese nicht dynamisch. erzeugt werden können. Insbesondere beim nicht selten vorkommenden Altersnachweis ist aber eine dynamische Generierung dienlich. Des Weiteren ist das System in diesem Fall sehr anfällig gegen die in 7. erwähnten Replay-Attacken. Dies gilt insbesondere, wenn die zum Nachweis erforderlichen Informationen über ein als unsicher geltendes Medium (wie z. B. das Internet) übertragen werden.

[0103] Fig. 13A zeigt ein Verfahren **1300** für ein Kommunikationsendgerät **102** gemäß einem Ausführungsbeispiel der Erfindung, um einen digitalen Nachweis zu führen.

[0104] In **1302** empfängt ein Kommunikationsendgerät **102** eine erste Nachricht **108**, die zumindest eine Anforderung nach einem Nachweis und eine erste digitale Signatur sowie eine Anfrage nach einer den Nutzer beschreibenden Information enthält.

[0105] Die Nachricht **108** kann gemäß einem Ausführungsbeispiel außer der Anfrage und der digitalen Signatur noch weitere Informationen, wie z. B. die in Fig. 9 dargestellten Informationen enthalten. Hierzu gehören beispielsweise eine Zufallszahl **904**, Datum und Zeit **906**, der Nachweis-Typ **908**, Nachweis-Parameter **910**, und Informationen **912**, **914** bezüglich einer digitalen Signatur, wie z. B. gemäß der Struktur des X.509-Standards (siehe Fig. 14) oder gemäß einer anderweitig vordefinierten Struktur. Die digitale Signatur kann, wie bereits weiter oben in der Beschreibung dargelegt, beispielsweise ein über die Nachricht gemäß einer Hashfunktion gebildeter Hashwert sein.

[0106] Bei den persönlichen Informationen über den Benutzer kann es sich z. B. um Daten handeln, die eine Person zu einer bestimmten Aktion berechtigen, wie z. B. ein Altersnachweis.

[0107] Bei dem Kommunikationsendgerät **102** kann es sich gemäß einem Ausführungsbeispiel um ein mobiles Kommunikationsendgerät, wie z. B. ein Mobilfunkendgerät, einen persönlichen digitalen Assistenten (Personal Digital Assistant, PDA), einen tragbaren Computer oder ein sonstiges tragbares Gerät mit digitalen Kommunikationsmöglichkeiten handeln.

[0108] Das Empfangen der Nachricht **108** kann gemäß einem Ausführungsbeispiel über eine Schnittstelle **210** eines Nahfeldkommunikationsstandards, wie z. B. Bluetooth, eines Standards eines Drahtlos-Kommunikationssystem, wie z. B. IEEE 802.11, WiMax, einer optischen Datenschnittstelle **112**, wie z. B. IrDA oder durch einen optischen Scanner, wie z. B. einen Barcode-Leser oder über eine Schnittstelle eines anderen Drahtlos-Standards übertragen werden. Im Falle eines optischen Scanners könnte z. B. ein Barcode von einem Display **204** (siehe **Fig.** 2) der Kommunikationseinrichtung **206** eingelesen werden.

[0109] In **1304** überprüft das Kommunikationsendgerät **102** die digitale Signatur und erstellt nach erfolgreicher Überprüfung eine Antwortnachricht **110**, die den Nachweis sowie die Antwort auf die Anfrage in der Anforderung enthält. Dies kann gemäß einem Ausführungsbeispiel von einer Applikation **124** durchgeführt werden, die in einem Datenspeicher des Kommunikationsendgerätes **102** gespeichert ist und von einem Prozessor in dem Kommunikationsendgerät **102** ausgeführt wird.

[0110] Das Kommunikationsendgerät **102** fügt gemäß einem Ausführungsbeispiel in die Antwortnachricht **110** eine zweite digitale Signatur ein, die z. B. über die Felder **1202** bis **1210** der Antwortnachricht **110** gebildet wird.

[0111] Das Kommunikationsendgerät **102** kann gemäß einem Ausführungsbeispiel zusätzlich die Authentizität des Benutzers **304** überprüfen, indem sie z. B. den Benutzer **304** dazu auffordert, eine PIN einzugeben. Es können jedoch auch andere Verfahren, wie z. B. biometrische Verfahren zur Authentifizierung eingesetzt werden. Der Prozess zur Erstellung des Nachweises wird gemäß einem Ausführungsbeispiel nur dann weitergeführt, wenn die Authentizität des Benutzers erfolgreich festgestellt wurde.

[0112] Weiterhin kann gemäß einem Ausführungsbeispiel des Verfahrens der Benutzer interaktiv über die Mensch-Maschine-Schnittstelle des Kommunikationsendgerätes **102** nach seinem Einverständnis der Erstellung und Übertragung der Antwortnachricht **110** mit dem Nachweis und der Antwort auf die Anforderung der den Nutzer beschreibenden Information gefragt werden.

[0113] Im Falle eines mobilen Kommunikationsendgerätes, das gemäß einem Mobilfunkstandard kommuniziert, kann die Applikation **124** auch auf einer SIM-Karte **202** gespeichert sein.

[0114] In **1306** sendet das Kommunikationsendgerät **102** die Antwortnachricht **110** z. B. an die Kommunikationseinrichtung **106**.

[0115] Fig. 13B zeigt ein Verfahren **1310** für eine Kommunikationseinrichtung **106** gemäß einem Ausführungsbeispiel der Erfindung, um einen digitalen Nachweis zu führen.

[0116] In **1312** erzeugt eine Kommunikationseinrichtung **106** gemäß einem Ausführungsbeispiel der Erfindung eine erste Nachricht **108**, die zumindest eine Anforderung eines Nachweises und eine erste digitale Signatur sowie eine Anfrage nach einer den Nutzer beschreibenden Information enthält. Die Nachricht **108** kann gemäß einem Ausführungsbeispiel außer der Anfrage und der digitalen Signatur noch weitere Informationen, wie z. B. die in Fig. 9 dargestellten Informationen enthalten. Hierzu gehören beispielsweise eine Zufallszahl **904**, Datum und Zeit **906**, der Nachweis-Typ **908** und Nachweis-Parameter **910** bezüglich des angeforderten Nachweises, und Informationen **912**, **914** bezüglich einer digitalen Signatur, wie z. B. gemäß der Struktur des X.509-Standards (siehe Fig. 14) oder gemäß einer anderweitig vordefinierten Struktur. Die digitale Signatur kann, wie bereits weiter oben in der Beschreibung dargelegt, beispielsweise ein über die Nachricht gemäß einer Hashfunktion gebildeter Hashwert sein.

[0117] Bei den persönlichen Informationen über den Benutzer kann es sich z. B. um Daten handeln, die eine Person zu einer bestimmten Aktion berechtigen, wie z. B. ein Altersnachweis.

[0118] In **1314** sendet die Kommunikationseinrichtung **106** die Nachricht **108** an ein Kommunikationsendgerät **102**. Das Kommunikationsendgerät kann gemäß einem Ausführungsbeispiel der Erfindung beispielsweise ein mobiles Kommunikationsendgerät, wie z. B. ein Mobilfunktelefon **218**, ein PDA, ein tragbarer Computer. oder auch ein digitales Musikabspielgerät oder ein sonstiges tragbares elektronisches Gerät mit digitalen Kommunikationsmöglichkeiten sein, in das die zur Ausführung des Verfahrens notwendigen Funktionen z. B. durch die Applikation **124** implementiert sind.

[0119] Das Senden der Nachricht **108** kann gemäß einem Ausführungsbeispiel über eine Schnittstelle **210** eines Nahfeldkommunikationsstandards, wie z. B. Bluetooth, eines Standards eines Drahtlos-Kommunikationssystem, wie z. B. IEEE 802.11, WiMax, einer optischen Datenschnittstelle **112**, wie z. B. IrDA oder durch einen optischen Scanner, wie z. B.

[0120] einen Barcode-Leser oder über eine Schnittstelle eines anderen Drahtlos-Standards übertragen werden. Im Falle eines optischen Scanners könnte z. B. ein Barcode von einem Display **204** (s. **Fig.** 2) der Kommunikationseinrichtung **206** eingelesen werden.

[0121] In **1316** empfängt die Kommunikationseinrichtung **106** eine Antwortnachricht **110**, die den Nachweis (beispielsweise enthaltend ein zweites digitales Zertifikat) mit einer Antwort auf die Anfrage in der Anforderung enthält und überprüft das zweite digitale Zertifikat und/oder die zweite digitale Signatur, so dass die Kommunikationseinrichtung sicherstellen kann, dass sie eine authentische Antwort auf die Anfrage der Anforderung erhält.

[0122] Durch die digitalen Nachweise gemäß Ausführungsbeispielen der Erfindung werden gegenüber dem physikalischen Ausweis folgende Wirkungen erzielt:

- Digitale Nachweise sind problemlos über weite Distanzen möglich. Erst so werden Nachweise für digitale Dienste wie Internet-Foren oder Video-on-Demand möglich.
- Die Nachweise sind leicht automatisierbar und können ohne menschliches Zutun auskommen, was in Anwendungen wie beispielsweise Zigarettenautomaten oder Videoausleihautomaten zum Tragen kommen kann.
- Die Sicherheit von digitalen Nachweisen ist durch die konsequente Verwendung von starker Kryptographie deutlich höher als bei herkömmlichen Verfahren.
- Eine Aktualisierung der Daten und der sicherheitsrelevanten Bestandteile wie beispielsweise Schlüssel sind über das Kommunikationsgerät **102** kostengünstig und über große Distanz möglich. Somit kann die Sicherheit (häufig Wechsel des Sicherheitskontextes) und die Aktualität der

Daten sichergestellt werden, ohne neue Nachweise zu erstellen und alte aus dem Verkehr zu ziehen.

• Durch die Authentifizierung des Nachweisenden **304** an der ausführenden Applikation **124** sind die Nachweise weniger leicht an andere Personen übertragbar und sind im Falle vor unberechtigter Verwendung Dritter geschützt.

• Es erfolgt immer eine für alle Nachweise gemeinsame Authentifizierung, so dass dem Nachweisenden **304** das Merken vieler unterschiedlicher Passwörter und PINs erspart bleibt.

• Die zum Nachweis erforderlichen Daten sind Dritten nicht einsichtig. Die Nachweise enthalten nur die nachzuweisenden Information und darüber hinaus keine weiteren Informationen. So sind beispielsweise anonyme Altersnachweise problemlos möglich.

• Digitale Nachweise unterliegen keinerlei Verschleißerscheinungen. Sie sind leicht auf andere Geräte übertragbar.

• Durch Verwendung eines Kommunikationsendgerätes **102** als Träger der Nachweise ist eine digitale Datenübertragung zwischen Kundendatensystem und Nachweisendem **304** automatisch implementiert und führt nicht zu zusätzlichen Kosten. Es besteht auch die Möglichkeit, nicht nur eine Kundennummer, sondern gleich einen kryptographischen Kundenschlüssel zu speichern, der für die Kommunikation der beiden Parteien für eine Verschlüsselung verwendet werden kann.

• Die digitalen Nachweise können ebenfalls wie herkömmliche Ausweise oder Kundenkarten biometrische Daten wie beispielsweise ein Bild des Teilnehmers **304** enthalten. Auch maschinenlesbare biometrische Daten (Gesichtsmuster, Fingerabdruck) sind somit möglich. Diese erhöhen die Sicherheit und können auch bei vollautomatisierter Anwendung Verwendung finden.

• Für die Erstellung digitaler Nachweise wird kein Material verwendet.

[0123] Es sei ferner noch auf die Wirkungen des Verfahrens zum Führen von digitalen Nachweisen hingewiesen:

• Es ist möglich, alle Nachweise mit Hilfe eines zentralen Gerätes zu führen, das sich im Alltag als ständiger Begleiter des Nachweisenden **304** erwiesen hat.

• Alle beteiligten Instanzen (nachfragende Instanz **306**, Mobilfunk-Teilnehmer **304**, Applikation **124** und Datenbereitsteller) können sich gegenseitig mit Hilfe digitaler Zertifikate ohne permanente oder häufig durchzuführende Kommunikation zwischen den Instanzen aufgrund der verwendeten asymmetrischen Kryptographie authentifizieren. Lediglich die öffentlichen Schlüssel sollten zu einem initialen Zeitpunkt verteilt werden. Durch regelmäßiges Ändern der Schlüssel kann die Sicherheit erhöht werden und einzelne Instanzen beispielsweise nach Ablauf des Abrechnungszeitraumes ausgeschlossen werden.

• Der Nachweisende **304** hat die letzte Kontrolle über die Informationen, die er über sich nachweisen und somit preisgeben möchte.

• Es ist möglich, dynamische Nachweise zu erzeugen. So kann ein Teilnehmer beispielsweise an seinem 18. Geburtstag sofort ohne Änderung irgendwelcher Zertifikate sein aktuelles Alter nachweisen, ohne dabei sein Geburtsdatum preiszugeben.

• Durch das Einbinden der zufälligen Zahlenfolge (Challenge-Response-Verfahren) ist eine gegen Replay-Attacken robuste Implementierung gewählt.

• Durch das Einbinden des Datums und gegebenenfalls der Uhrzeit werden Manipulationen durch Verstellen der internen Uhr verhindert und eine nur durch aufwendige Kommunikation zu realisierenden vertrauensvolle Systemzeit wird nicht benötigt.

• Durch optionale Fehlermeldungen können alle Beteiligten über Ursachen des Scheiterns eines Nachweises informiert werden.

[0124] Nachfolgend werden drei Ausführungsbeispiele veranschaulicht.

Anonymer Altersnachweis beim Erwerb von Zigaretten am Automaten

Voraussetzungen:

[0125] Ein Zigarettenautomatenhersteller nimmt an einem Nachweisprogramm mittels Mobilfunkgeräten teil, das von einem Zusammenschluss von nationalen Mobilfunkbetreibern angeboten wird.

[0126] Der öffentliche Schlüssel der Mobilfunkbetreiber wird in den Automaten des Herstellers gespeichert.

[0127] Des Weiteren stattet der Hersteller seine Automaten mit einer Bluetooth-Schnittstelle zur drahtlosen Kommunikation mit Mobilfunkendgeräten und einer internen Uhr aus.

[0128] Ein 17-jähriger Mobilfunkteilnehmer **304** verwendet einen Automaten der oben genannten Firma zum Erwerb von Zigaretten. Gemäß deutscher Rechtslage darf nur Jugendlichen ab 16 Jahren der Erwerb von Zigaretten ermöglicht werden. Aus diesem Grund sendet der Automat nach Erhalt des Geldes eine Altersnachweisanforderung über Bluetooth aus. Aufgrund der prinzipbedingten örtlichen Nähe zum Automaten wird auf eine Authentifizierung des Automaten gegenüber der nachweisführenden Applikation **124** verzichtet. Nach Bestätigung des Altersnachweises „größer oder gleich 16" durch den Teilnehmer und der Eingabe der PIN für die SIM-Karte

202 errechnet die Applikation **124** in der SIM-Karte **202** aus dem vom Mobilfunkanbieter gespeicherten Geburtsdatum des Teilnehmers und dem aktuellen Datum das aktuelle Alter des Teilnehmers und vergleicht es mit der im Nachweis geforderten Bedingung. Die mit der Anforderung vom Automaten mitgelieferte zufällige Zahlenfolge, das aktuelle Datum der im Mobilfunkendgerät enthaltenen internen Uhr und der eigentliche Nachweis „Teilnehmer ist 16 oder älter" wird zu einer Nachricht **110** zusammengefügt, mit dem geheimen in der SIM-Karte **202** befindlichen Schlüssel des Mobilfunkanbieters digital signiert und an den Automaten zurückgesendet. Dieser überprüft mit Hilfe des im Automaten gespeicherten öffentlichen Schlüssels des oder der Mobilfunkanbieter die digitale Signatur der Antwortnachricht **110** und liefert bei nachweislich unveränderter Nachricht **110** die gewünschten Zigaretten aus, wenn die Zufallszahl der zuvor gesendeten entspricht, und das Datum innerhalb der voreingestellten Toleranz dem der internen Uhr des Automaten entspricht.

Internetforum für Mädchen

Voraussetzungen:

[0129] Ein Anbieter einer Kommunikationsplattform im Internet für Mädchen im Alter zwischen 12 Jahren und 15 Jahren nimmt an einem Nachweisprogramm mittels Mobilfunkgeräten **218** teil, das von einem Zusammenschluss von Mobilfunkbetreibern angeboten wird.

[0130] Der öffentliche Schlüssel der Mobilfunkbetreiber wird in dem System des Anbieters gespeichert.

[0131] Eine vom Mobilfunkanbieter für den Anbieter der Plattform generierter Schlüssel wird an den Anbieter der Plattform digital ausgeliefert und ebenfalls im System gespeichert.

[0132] Eine 13-jährige Mobilfunkteilnehmerin **304** versucht, Zugang zu der Plattform des Anbieters zu erlangen. Bei der Anmeldung an der Portalseite werden die Teilnehmerinnen **304** aufgefordert, einen Nachweis über Alter und Geschlecht zu liefern. Es stehen mehrere Verfahren zur Auswahl.

[0133] Die Teilnehmerin **304** wählt die Möglichkeit, einen am Bildschirm **204** angezeigten Semacode (zweidimensionaler Barcode) mit Hilfe der in ihrem Mobilfunkendgerät **218** enthaltenen Kamera **212** einzulesen. Der Code wird in einer im Mobilfunkendgerät **218** enthaltenen Applikation **124** decodiert und die so decodierten Daten an die auf der SIM-Karte **202** befindlichen Applikation **124** weitergeleitet. Aufgrund der prinzipbedingten örtlichen Entfernung zum Plattformanbieter sind in der Anforderung **108** ebenfalls der Name des Anbieters und das aktuelle Datum mit Uhrzeit **906** enthalten. Die gesamte Nachricht **108** ist digital mit dem geheimen Schlüssel des Plattformanbieters signiert. Nach Bestätigung des Nachweises „weiblich UND Alter größer oder gleich 12 UND Alter kleiner 16" durch die Teilnehmerin **304** wird die digitale Signatur **914** des Plattformanbieters überprüft. Die Teilnehmerin **304** wird nach erfolgter Überprüfung der Signatur **914** aufgefordert, sich durch die Eingabe der PIN für die SIM-Karte **202** zu authentifizieren. Mit Hilfe der in der Applikation **124** auf der SIM-Karte **202** des Mobilfunkanbieters gespeichertem Geburtsdatum der Teilnehmerin **304** und dem aktuellen Datum der internen Uhr wird das aktuelle Alter der Teilnehmerin **304** errechnet und mit der im Nachweis geforderten Bedingungen verglichen. Ebenfalls wird mit Hilfe der in der Applikation **124** das Geschlecht der Teilnehmerin **304**, das auf der SIM-Karte **202** des Mobilfunkanbieters gespeichert ist, mit den im Nachweis geforderten Bedingungen verglichen. Die mit der Anforderung vom Anbieter mitgelieferte zufällige Zahlenfolge **904**, das aktuelle Datum der im Mobilfunkendgerät **218** enthaltenen internen Uhr und der eigentliche Nachweis „Teilnehmerin ist weiblich und zwischen 12 und 15 Jahre alt" wird zu einer Nachricht **110** zusammengefügt, mit dem geheimen, in der SIM-Karte **202** befindlichen Schlüssel des Mobilfunkanbieters digital signiert und am Bildschirm **204** des Mobilfunkendgerätes **218** angezeigt. Nach Eingabe der Nachricht an der Tastatur **206** (eine Übertragung der Daten via Bluetooth wäre auch möglich) überprüft der Plattformanbieter mit Hilfe des im System gespeicherten öffentlichen Schlüssels der Mobilfunkanbieter die digitale Signatur **1212** der Antwortnachricht **110** und gestattet bei nachweislich unveränderter Nachricht **110** den anonymen Zugang zum Portal, wenn die Zufallszahl **1204** der zuvor gesendeten Zufallszahl **904** entspricht, und das Datum **1206** innerhalb der voreingestellten Toleranz dem der internen Uhr des Systems (gegebenenfalls ist eine Umrechnung auf UTC (Coordinated Universal Time) vorgesehen) entspricht. In einem alternativen Ausführungsbeispiel der Erfindung ist es für den Fall, dass in der Anforderung ein Datum und/oder eine Uhrzeit mit gesendet wurde, könnte man diese(s) mit der internen Uhr vergleichen und nur bei Übereinstimmung in bestimmten Grenzen fortfahren. Die Übereinstimmung könnte zwar auch erst nach Übermittlung des Zertifikates (wenn dort Datum und/oder Uhrzeit mit gesendet werden) geschehen, aber somit wäre es möglich sich durch viele Anfragen, z. B. dem Geburtsdatum zu nähern.

Digitale Videothekenkarte

Vorraussetzungen:

[0134] Ein Videothekenbetreiber nimmt an einem Nachweisprogramm mittels Mobilfunkgeräten **218** teil, das von einem Zusammenschluss von nationalen Mobilfunkbetreibern angeboten wird.

[0135] Der öffentliche Schlüssel der Mobilfunkbetreiber wird in dem System des Herstellers gespeichert.

[0136] Des Weiteren stattet der Hersteller sein Videotheken-System mit einer Bluetooth-Schnittstelle **210** zur drahtlosen Kommunikation mit Mobilfunkendgeräten **218** und einer internen Uhr aus.

[0137] Ein 17-jähriger Mobilfunkteilnehmer **304** registriert sich für die Benutzung einer Videothek. Dabei legt er seinen Personalausweis vor, um die in der Kundendatenbank gespeicherten Daten wie Name, Adresse und Geburtsdatum nachzuweisen. Er nimmt an dem Programm „Elektronische Videothekenkarte" teil. Daher wird bei der Registrierung ein digitales Zertifikat mit der Kundennummer des Teilnehmers **304** generiert und in der Applikation **124** für digitale Nachweise auf der SIM-Karte **202** gespeichert. Dies kann entweder über den Mobilfunkanbieter oder nach Authentifizierung der Videothek in direkter Kommunikation mit der Applikation **124** für digitale Nachweise geschehen. Gemäß der deutschen Rechtslage darf nur Erwachsenen ab 18 Jahren der Zutritt zum Erwachsenenbereich der Videothek ermöglicht werden. Möchte der Teilnehmer **304** einen Film ausleihen, sendet das Kassensystem der Videothek über Bluetooth eine Kundenanforderung (Request) **108** aus. Die Anforderung **108** enthält wieder eine zufällige Zahlenfolge **904**. Aufgrund der prinzipbedingten örtlichen Nähe zum Kassensystem wird auf eine Authentifizierung der Videothek gegenüber der Nachweis führenden Applikation **124** verzichtet. Es folgt die Bestätigung des Kundennachweises durch den Teilnehmer **304** und die Eingabe der PIN für die SIM-Karte **202**. Die mit der Anforderung vom System mitgelieferte zufällige Zahlenfolge **904** und die gespeicherte Kundennummer werden zusammengefügt, mit dem geheimen, in der SIM-Karte **202** befindlichen Schlüssel des Mobilfunkanbieters digital signiert und an das System zurückgesendet. Dieses überprüft mit Hilfe des gespeicherten öffentlichen Schlüssels der Mobilfunkanbieter die digitale Signatur **1212** der Antwortnachricht **110** und ruft bei nachweislich unveränderter Nachricht **110** en Datensatz des Kunden auf, wenn die Zufallszahl **1204** der zuvor gesendeten Zufallszahl **904** entspricht. Auch ein Altersnachweis für den Zutritt zum Erwachsenenbereich kann so realisiert werden. Zusätzlich bietet die Videothek Ausleihautomaten an, die auch außerhalb der Geschäftszeiten zugänglich sind. Die Authentifizierung der Kunden erfolgt, wie in diesem Beispiel beschrieben, ohne das Mitwirken eines Mitarbeiters. Das Angebot an Filmen berücksichtigt das im Kundendatensatz enthaltene Alter des Kunden, und die am Automaten ausgeliehenen Filme werden im Kundendatensatz vermerkt.

[0138] Fig. 14 zeigt die beispielhafte Struktur eines ITU-T X.509-Zertifikats.

[0139] In Fig. 15 ist ein Schaubild zu digitalen Signaturen abgebildet. Aus der ursprüngliche Information (Original Information) **1502** wird zum einen auf Seiten des Empfängers **1526** über eine Hashfunktion **1520** unverschlüsselt ein Hashwert (Hashvalue) **1522** gebildet. Zum anderen wird auf Seiten des Senders **1524** aus der ursprünglichen Information **1502** über eine Hashfunktion **1504** ein Hashwert **1406** gebildet, der jedoch mit dem geheimen Schlüssel (Secret Key) **1516** in **1508** verschlüsselt wird. Dies bildet die digitale Signatur **1510**, die in **1512** empfängerseitig wieder mit dem öffentlichen Schlüssel (Public Key) **1518** entschlüsselt wird. Die daraus entstehende entschlüsselte digitale Signatur (Decrypted Signature) **1514** wird mit dem unverschlüsselten Hashwert **1522** verglichen.

[0140] Obwohl Ausführungsbeispiele der Erfindung vor allem im Zusammenhang mit spezifischen Ausführungsbeispielen gezeigt und beschrieben worden ist, sollte es von denjenigen mit dem Fachgebiet vertrauten Personen verstanden werden, dass vielfältige Änderungen der Ausgestaltung und der Details daran vorgenommen werden können, ohne vom Wesen und Bereich der Erfindung, wie er durch die nachfolgenden Ansprüche definiert wird, abzuweichen. Der Bereich der Erfindung wird daher durch die angefügten Ansprüche bestimmt, und es ist beabsichtigt, dass sämtliche Veränderungen, welche in Reichweite der Bedeutung und des Äquivalenzbereichs der Ansprüche liegen, von den Ansprüchen umfasst werden.

Patentansprüche

1. Kommunikationsendgerät zum Bereitstellen eines Zertifikats, aufweisend:
• eine Applikation, eingerichtet zum Empfangen einer ersten Nachricht von einer anfordernden Kommunikationseinrichtung, wobei die erste Nachricht eine Anforderung nach einem Nachweis, eine erste digitale Signatur sowie eine Anfrage nach einer den Nutzer beschreibenden Information enthält,
• wobei die Applikation ferner eingerichtet ist, die erste digitale Signatur zu überprüfen und bei erfolgreicher Überprüfung die Anforderung zu bearbeiten, und eine Antwortnachricht für die anfordernde Kommunikationseinrichtung zu erstellen, wobei die Antwortnachricht den Nachweis enthält mit einer Antwort auf die Anfrage in der Anforderung.

2. Kommunikationsendgerät nach Anspruch 1, wobei die erste Nachricht mindestens ein Zertifikat enthält.

3. Kommunikationsendgerät nach Anspruch 1 oder 2, wobei die Applikation ferner eingerichtet ist, in die Antwortnachricht eine zweite digitale Signatur einzufügen.

4. Kommunikationsendgerät gemäß einem der Ansprüche 1 bis 3, wobei das Kommunikationsendgerät ein mobiles Kommunikationsendgerät ist.

5. Kommunikationsendgerät gemäß Anspruch 4, wobei das mobile Kommunikationsgerät ein Mobilfunkendgerät ist.

6. Kommunikationsendgerät gemäß einem der Ansprüche 1 bis 5,
• mit einem Datenspeicher, in dem die Applikation gespeichert ist; und
• mit einem Prozessor zum Ausführen der Applikation.

7. Kommunikationsendgerät gemäß einem der Ansprüche 4 bis 6,
• mit einer SIM-Karte, welche einen SIM-Karten-Speicher enthält
• wobei die Applikation in dem SIM-Karten-Speicher gespeichert ist.

8. Kommunikationsendgerät gemäß einem der Ansprüche 1 bis 7, wobei die Applikation über einen sicheren Übertragungskanal aktualisiert werden kann.

9. Kommunikationsendgerät gemäß Anspruch 8, wobei der sichere Übertragungskanal zum Aktualisieren der Applikation ein drahtgebundener Übertragungskanal oder ein drahtloser Übertragungskanal ist.

10. Kommunikationsendgerät gemäß Anspruch 9, wobei der sichere Übertragungskanal zum Aktualisieren der Applikation ein Telekommunikations-Übertragungskanal ist.

11. Kommunikationsendgerät gemäß einem der Ansprüche 1 bis 10, mit einer Schnittstelle zum Übertragen von Nachrichten an die Kommunikationseinrichtung und zum Empfangen von Nachrichten von der Kommunikationseinrichtung.

12. Kommunikationsendgerät gemäß Anspruch 11, wobei die Schnittstelle als mindestens eine der folgenden Arten von Schnittstellen eingerichtet ist:
• eine Datenschnittstelle eines Funkkommunikationsstandards,
• eine optische Datenschnittstelle, oder
• eine Internetschnittstelle.

13. Kommunikationsendgerät einem der Ansprüche 1 bis 12, wobei die erste Nachricht und/oder die Antwortnachricht weiterhin eine Zufallszahl und/oder das Datum und/oder die Uhrzeit der Erstellung der ersten Nachricht bzw. der Antwortnachricht enthält.

14. Kommunikationsendgerät gemäß Anspruch 13,
• mit einer Verschlüsselungseinheit zum Verschlüsseln der Zufallszahl;
• wobei das Kommunikationsendgerät eingerichtet ist zum Einfügen der verschlüsselten Zufallszahl in die Antwortnachricht.

15. Kommunikationsendgerät gemäß einem der Ansprüche 1 bis 14, wobei die Applikation ferner eingerichtet ist, die Authentizität des Benutzers zu überprüfen.

16. Kommunikationsendgerät gemäß einem der Ansprüche 1 bis 15, wobei die Applikation eingerichtet ist, die Authentizität des Benutzers in der Applikation mittels einer über eine Benutzerschnittstelle eingegebene Kennzeichnung zu überprüfen.

17. Kommunikationsendgerät gemäß einem der Ansprüche 1 bis 16, mit einer Bestätigungs-Anforderungseinheit, die eingerichtet ist zum Anfordern einer Bestätigung von dem Nutzer des Kommunikationsendgerätes, dass das Kommunikationsendgerät die Antwortnachricht mit der Antwort auf die Anfrage in der Anforderungsnachricht erstellt.

18. Kommunikationseinrichtung zum Bereitstellen einer Nachricht, aufweisend:
• eine Applikation, eingerichtet, eine erste Nachricht zu erzeugen, die eine Anforderung nach einem Nachweis, und eine erste digitale Signatur sowie eine Anfrage nach einer den Nutzer beschreibenden Information enthält;
• wobei die Kommunikationseinrichtung dazu eingerichtet ist, die erste Nachricht an ein Kommunikationsendgerät zu senden; und
• wobei die Kommunikationseinrichtung ferner dazu eingerichtet ist, eine zweite Nachricht, welche von dem Kommunikationsendgerät auf Grundlage der Anforderung und der digitalen Signatur erstellt worden ist, von dem Kommunikationsendgerät zu empfangen.

19. Kommunikationseinrichtung nach Anspruch 18, wobei die erste Nachricht mindestens ein Zertifikat enthält.

20. Kommunikationseinrichtung nach Anspruch 18 oder 19, mit einer Auswerteeinheit zum Auswerten zumindest des in der zweiten Nachricht enthaltenen zweiten Zertifikats.

21. Kommunikationseinrichtung gemäß einem der Ansprüche 18 bis 20, eingerichtet zum Einfügen einer Zufallszahl in die erste Nachricht.

22. Kommunikationseinrichtung gemäß Anspruch 21, eingerichtet, nach dem Empfang der zweiten Nachricht zusätzlich die Zufallszahl bei der Auswertung der Antwort auf die Anfrage zu berücksichtigen.

23. Kommunikationseinrichtung gemäß einem der Ansprüche 18 bis 22, eingerichtet zum Einfügen des Datums und/oder der Uhrzeit in die zweite Nachricht.

24. Kommunikationseinrichtung gemäß einem der Ansprüche 18 bis 23, eingerichtet zum Einfügen des Typs des Nachweises in die erste Nachricht.

25. Kommunikationseinrichtung gemäß einem der Ansprüche 18 bis 24, mit einer Schnittstelle zum Übertragen von Nachrichten an das Kommunikationsendgerät und zum Empfangen von Nachrichten von dem Kommunikationsendgerät.

26. Kommunikationseinrichtung gemäß Anspruch 25, wobei die Schnittstelle als mindestens eine der folgenden Arten von Schnittstellen eingerichtet ist:
• eine Datenschnittstelle eines Funkkommunikationsstandards,
• eine optische Datenschnittstelle, oder
• eine Internetschnittstelle.

27. Elektronische Karte, aufweisend:
• Schaltkreise zur Verarbeitung elektronischer Signale und Informationen, wobei die Informationen zumindest eine Applikation bereitstellen, um eine erste Nachricht von einer Kommunikationseinrichtung zu empfangen, wobei die erste Nachricht mindestens. eine Anforderung nach einem Nachweis und eine erste digitale Signatur sowie eine Anfrage nach einer den Nutzer beschreibenden Information enthält; und
• wobei die Applikation ferner eingerichtet ist, die erste digitale Signatur zu überprüfen und bei erfolgreicher Überprüfung die Anforderung zu bearbeiten, und eine Antwortnachricht für die anfordernde Kommunikationseinrichtung zu erstellen, wobei die Antwortnachricht das angeforderte Zertifikat mit einer Antwort auf die Anfrage in der Anforderung enthält.

28. Elektronische Karte gemäß Anspruch 27, wobei die elektronische Karte eine SIM-Karte eines Mobilfunkendgerätes ist.

29. Elektronische Karte gemäß Anspruch 27 oder 28, wobei die Antwortnachricht ferner eine zweite digitale Signatur enthält.

30. Elektronische Karte gemäß einem der Ansprüche 27 bis 29, eingerichtet, die Authentizität des Benutzers zu überprüfen.

31. Elektronische Karte gemäß einem der Ansprüche 27 bis 29, mit einer Bestätigungs-Anforderungseinheit, die eingerichtet ist zum Anfordern einer Bestätigung von dem Nutzer der elektronischen Karte, dass die Applikation einen Nachweis mit der Antwort auf die Anfrage in der Anforderungsnachricht erstellt.

32. Verfahren zum Bereitstellen eines Zertifikats,
• wobei ein Kommunikationsendgerät eine erste Nachricht empfängt, die eine Anforderung nach einem Nachweis und eine erste digitale Signatur sowie eine Anfrage nach einer den Nutzer beschreibenden Information enthält,
• das Kommunikationsendgerät die erste digitale Signatur überprüft und nach erfolgreicher Überprüfung eine Antwortnachricht, die die Antwort auf die Anfrage in der Anforderung enthält, erstellt,
• das Kommunikationsendgerät die Antwortnachricht an eine Kommunikationseinrichtung sendet.

33. Verfahren gemäß Anspruch 32, wobei die erste Nachricht mindestens ein Zertifikat enthält.

34. Verfahren gemäß Anspruch 33, wobei das Kommunikationsendgerät in die Antwortnachricht eine zweite digitale Signatur einfügt.

35. Verfahren gemäß einem der Ansprüche 32 bis 34, wobei das Kommunikationsendgerät ein mobiles Kommunikationsendgerät ist.

36. Verfahren gemäß Anspruch 35, wobei das Kommunikationsendgerät ein Mobilfunkendgerät ist.

37. Verfahren gemäß Anspruch 36, wobei zumindest die Überprüfung der ersten digitalen Signatur und das Erstellen des zweiten Zertifikats von einer auf einer SIM-Karte gespeicherten Applikation durchgeführt werden.

38. Verfahren einem der Ansprüche 32 bis 37, wobei das Kommunikationsendgerät zusätzlich die Authentizität des Benutzers überprüft.

39. Verfahren gemäß Anspruch 38, wobei das Kommunikationsendgerät die Authentizität mittels einer über eine Benutzerschnittstelle eingegebene Kennzeichnung überprüft.

40. Verfahren gemäß einem der Ansprüche 32 bis 39, wobei das Kommunikationsendgerät von einem Nutzer des Kommunikationsendgerätes eine Bestätigung anfordert, um die Erstellung und anschließende Übertragung der Antwortnachricht mit der Antwort auf die Anforderung der den Nutzer beschreibenden Information zu bestätigen.

41. Verfahren gemäß einem der Ansprüche 32 bis 40, wobei das Kommunikationsendgerät die Nachrichten über mindestens eine der folgenden Arten von Schnittstellen sendet bzw. empfängt:
• eine Datenschnittstelle eines Funkkommunikationsstandards,
• eine optische Datenschnittstelle, oder
• eine Internetschnittstelle.

42. Verfahren gemäß einem der Ansprüche 32

bis 41, wobei das Kommunikationsendgerät in die Antwortnachricht weiterhin eine Zufallszahl und/oder das Datum und/oder die Uhrzeit der Erstellung der Antwortnachricht einfügt.

43. Verfahren zum Bereitstellen eines Zertifikats,
• wobei eine Kommunikationseinrichtung eine erste Nachricht erzeugt, die eine Anforderung nach einem Nachweis, eine erste digitale Signatur sowie eine Anfrage nach einer den Nutzer beschreibenden Information enthält,
• die Kommunikationseinrichtung die erste Nachricht an ein Kommunikationsendgerät sendet,
• die Kommunikationseinrichtung eine Antwortnachricht, die das zweite digitale Zertifikat mit einer Antwort auf die Anfrage in der Anforderung enthält, empfängt.

44. Verfahren gemäß Anspruch 43, wobei die erste Nachricht mindestens ein Zertifikat enthält.

45. Verfahren gemäß Anspruch 43 oder 44, wobei in der empfangenen Antwortnachricht eine zweite digitale Signatur enthalten ist.

46. Verfahren gemäß einem der Ansprüche 43 bis 45, wobei die Kommunikationseinrichtung die zweite digitale Signatur überprüft.

47. Verfahren gemäß einem der Ansprüche 43 bis 46, wobei die Kommunikationseinrichtung den Typ der angeforderten Antwortnachricht einfügt.

48. Verfahren gemäß einem der Ansprüche 43 bis 46, wobei die Kommunikationseinrichtung in die erste Nachricht ferner eine Zufallszahl und/oder das Datum und/oder die Uhrzeit der Erstellung der ersten Nachricht einfügt.

49. Verfahren gemäß einem der Ansprüche 42 bis 47, wobei die Kommunikationseinrichtung die Nachrichten über mindestens eine der folgenden Arten von Schnittstellen sendet bzw. empfängt:
• eine Datenschnittstelle eines Funkkommunikationsstandards,
• eine optische Datenschnittstelle, oder
• eine Internetschnittstelle.

Es folgen 9 Blatt Zeichnungen

Anhängende Zeichnungen

FIG 1

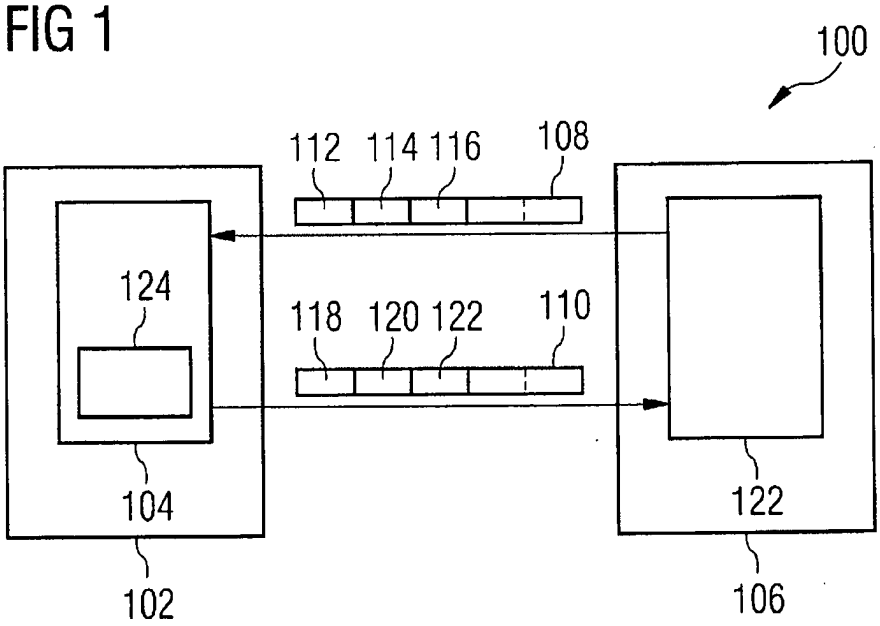


FIG 2A

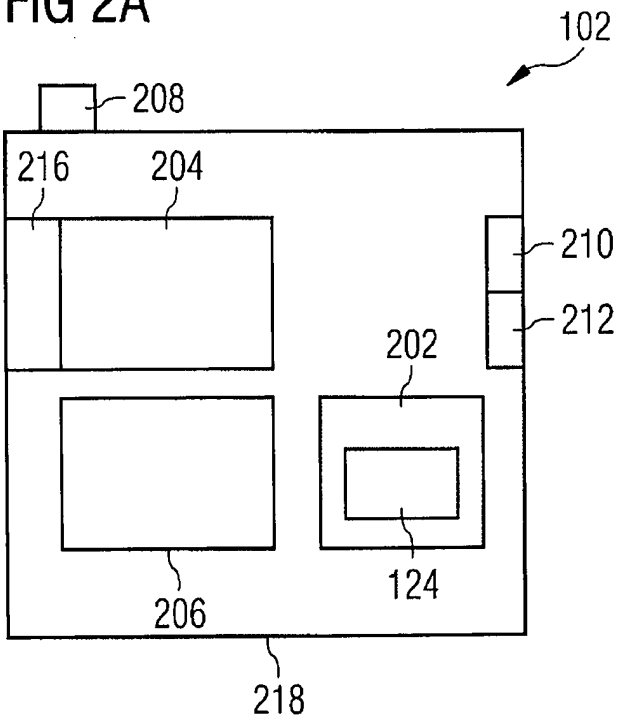

102
208
216
204
210
212
202
124
206
218

FIG 2B

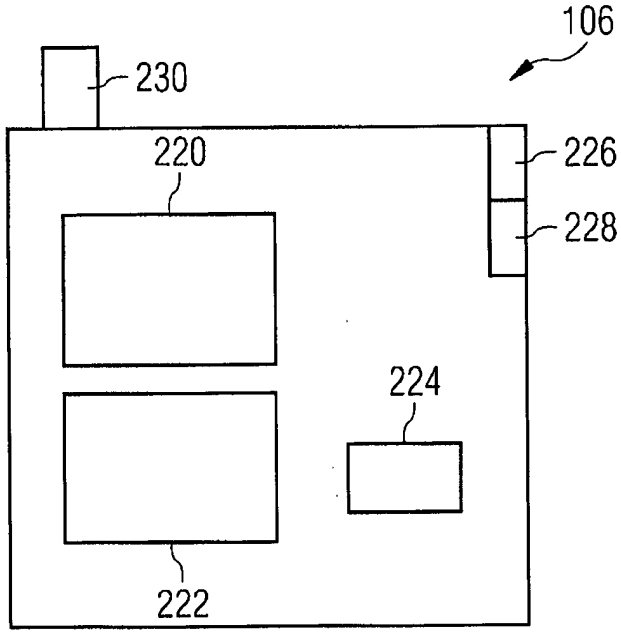

106
230
220
226
228
224
222

FIG 3

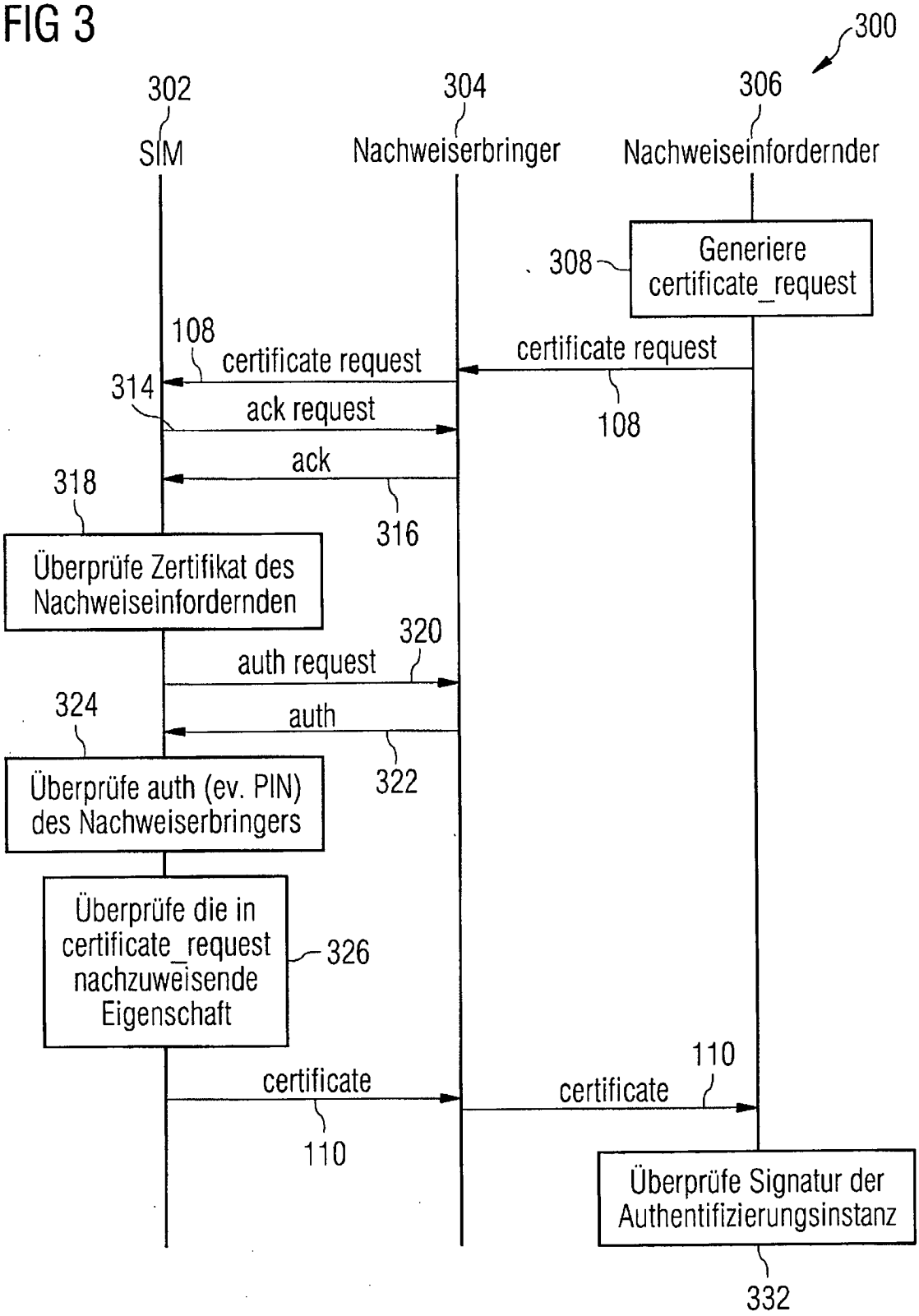

300
302
SIM
304
Nachweiserbringer
306
Nachweiseinfordernder
308
Generiere certificate_request
108
certificate request
certificate request
108
314
ack request
ack
316
318
Überprüfe Zertifikat des Nachweiseinfordernden
320
auth request
auth
322
324
Überprüfe auth (ev. PIN) des Nachweiserbringers
Überprüfe die in certificate_request nachzuweisende Eigenschaft
326
certificate
110
certificate
110
Überprüfe Signatur der Authentifizierungsinstanz
332

FIG 4

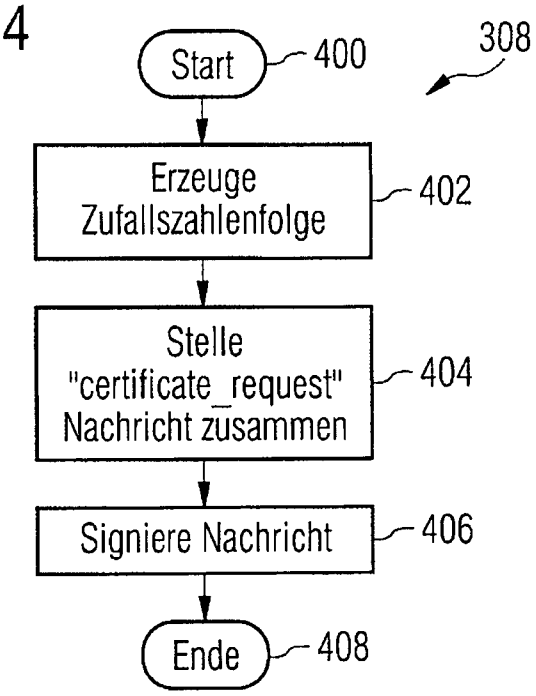

Start
400
308
Erzeuge Zufallszahlenfolge
402
Stelle "certificate_request" Nachricht zusammen
404
Signiere Nachricht
406
Ende
408

FIG 5

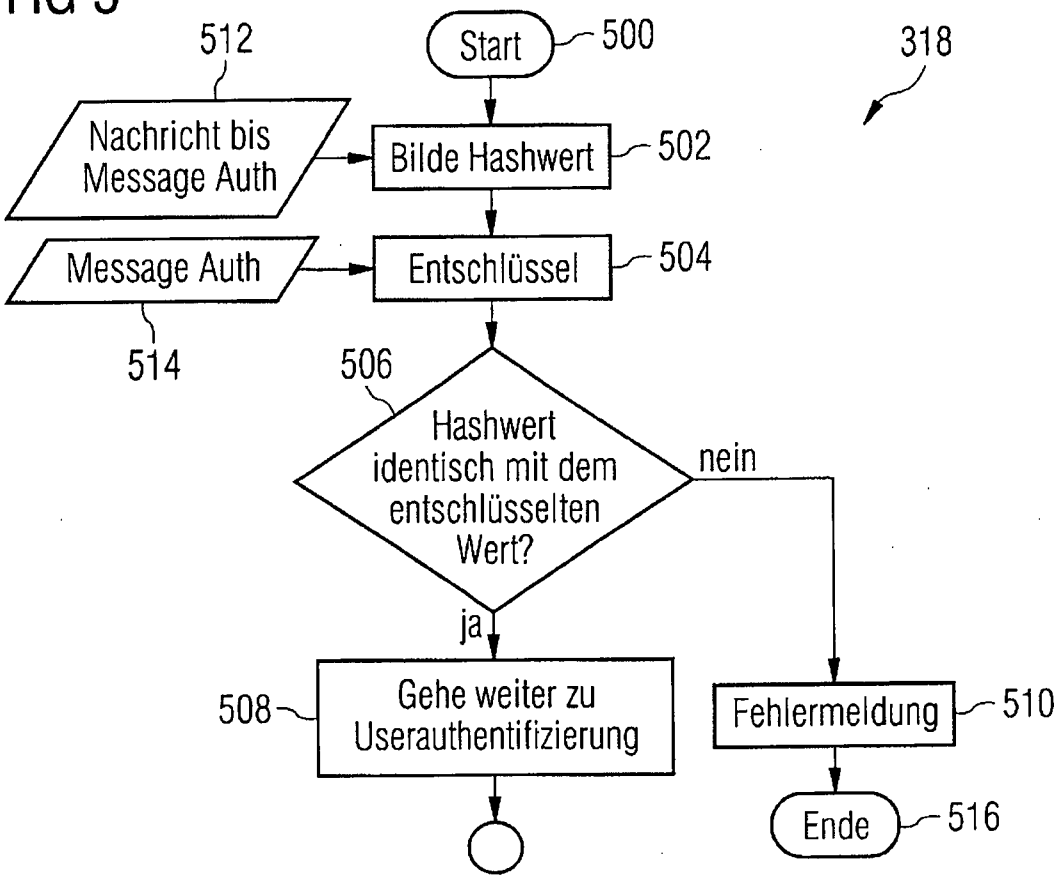

512
Start
500
318
Nachricht bis Message Auth
Bilde Hashwert
502
Message Auth
Entschlüssel
504
514
506
Hashwert identisch mit dem entschlüsselten Wert?
nein
ja
508
Gehe weiter zu Userauthentifizierung
Fehlermeldung
510
Ende
516

FIG 6

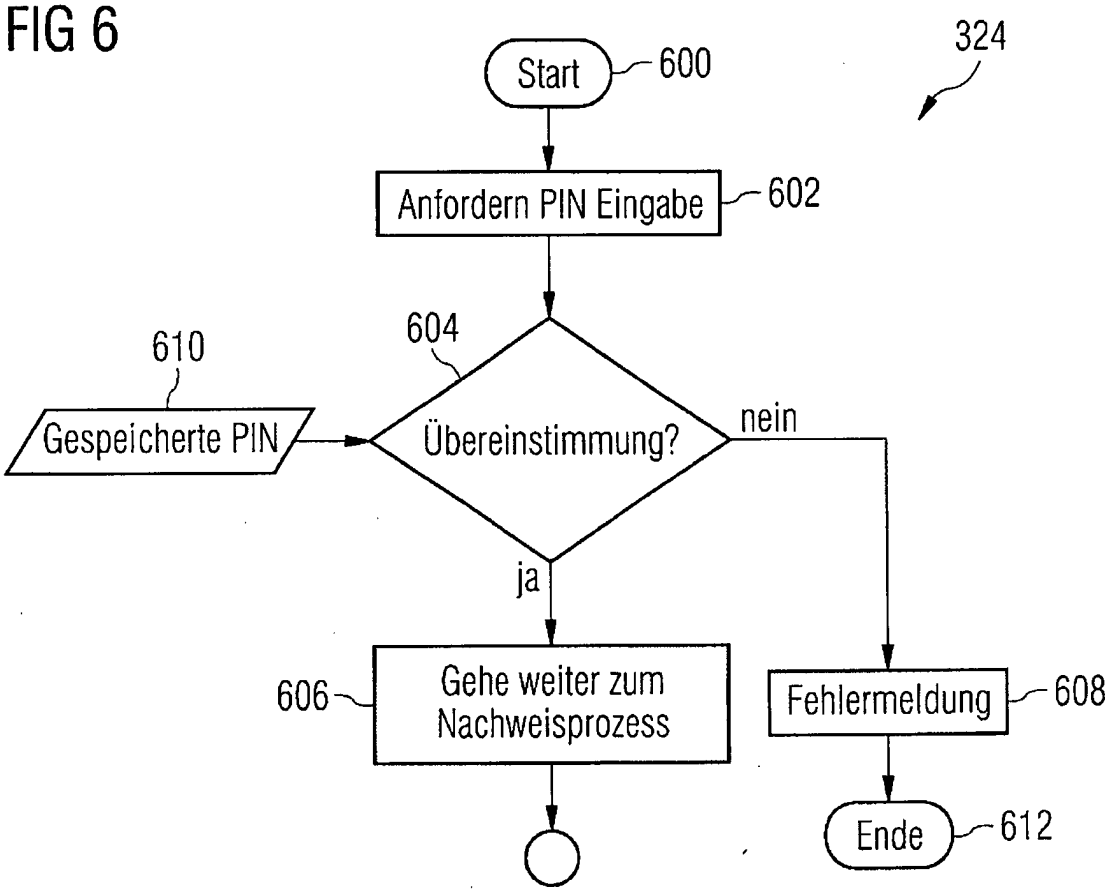

324
Start
600
Anfordern PIN Eingabe
602
604
610
Gespeicherte PIN
Übereinstimmung?
nein
ja
606
Gehe weiter zum Nachweisprozess
Fehlermeldung
608
Ende
612

FIG 7

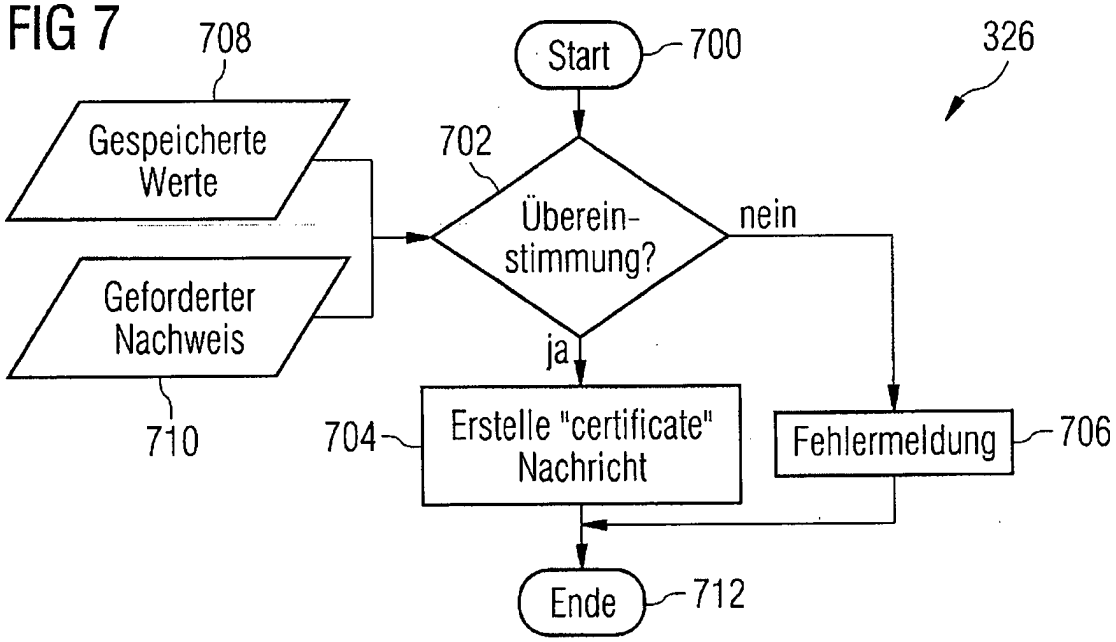

708
Start
700
326
Gespeicherte Werte
702
Überein-stimmung?
nein
Geforderter Nachweis
ja
710
704
Erstelle "certificate" Nachricht
Fehlermeldung
706
Ende
712

FIG 8

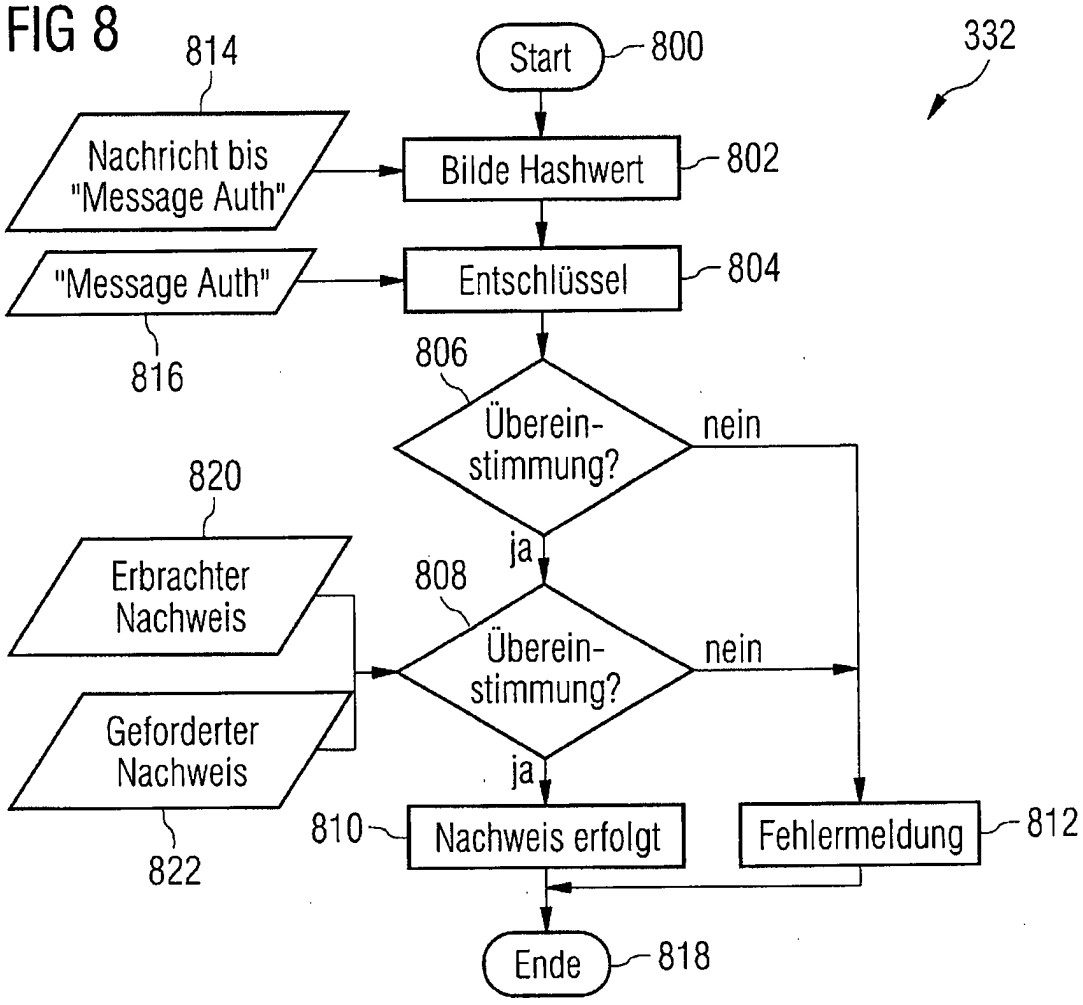

814
Start
800
332
Nachricht bis "Message Auth"
Bilde Hashwert
802
"Message Auth"
Entschlüssel
804
816
806
Überein-stimmung?
nein
820
ja
Erbrachter Nachweis
808
Überein-stimmung?
nein
Geforderter Nachweis
ja
822
810
Nachweis erfolgt
Fehlermeldung
812
Ende
818

FIG 9

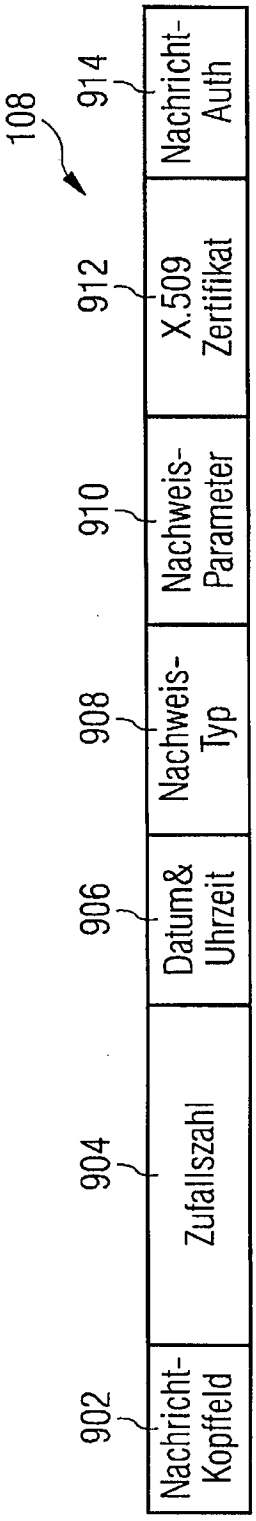


FIG 10

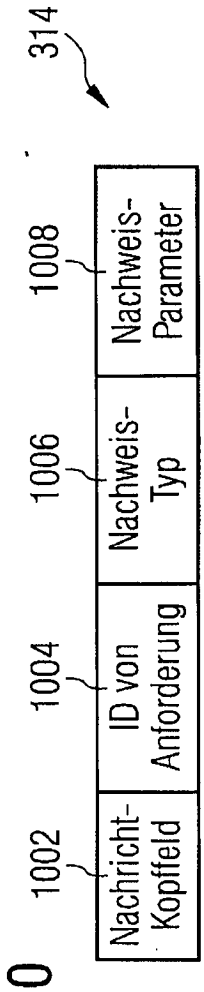


FIG 11

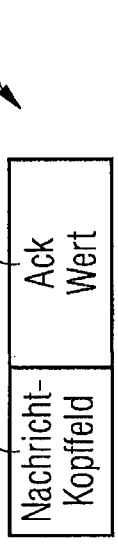


FIG 12

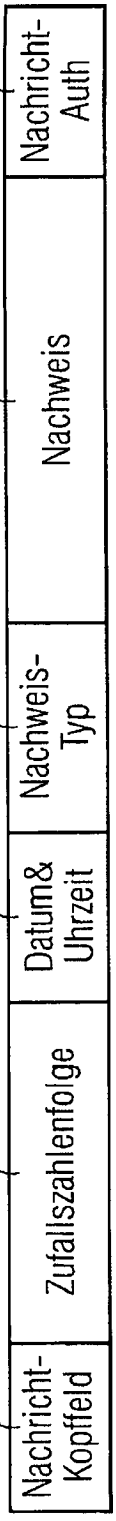


FIG 13A

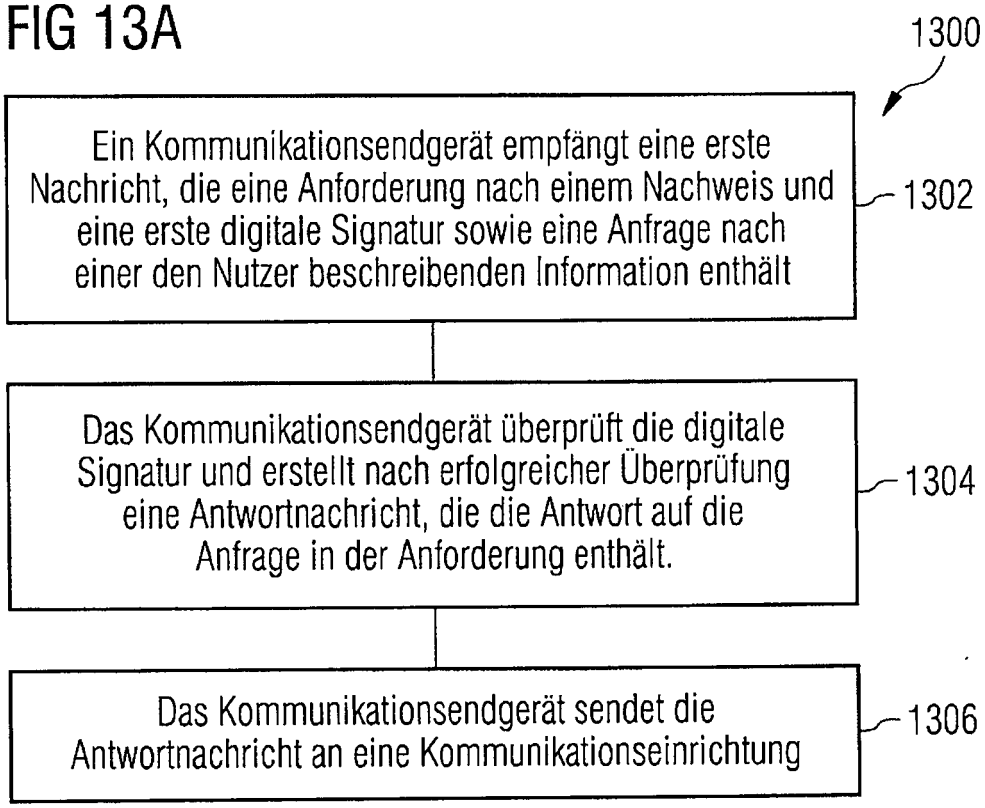


FIG 13B

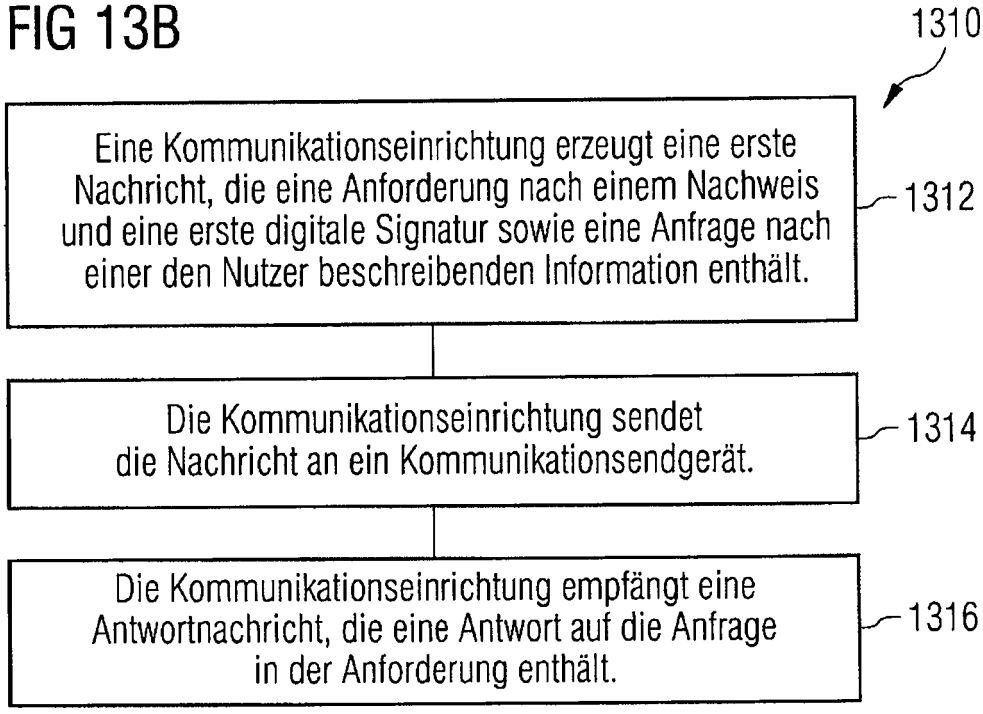


FIG 14

- Zertifikat
  - Version
  - Seriennummer
  - Algorithmen ID
  - Aussteller
  - Gültigkeit
    - von
    - bis
  - Subject
  - Subject Public Key info
    - Public Key Algorithmus
    - Subject Public Key
  - Eindeutige ID des Ausstellers (optional)
  - Eindeutige ID des Inhabers (optional)
  - Erweiterungen
    - ...
- Zertifikat Signaturalgorithmus
- Zertifikat Signatur

FIG 15

