(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
7. Oktober 2010 (07.10.2010)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2010/112368 A2

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2010/053733

(22) Internationales Anmeldedatum:
23. März 2010 (23.03.2010)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2009 001 959.6 30. März 2009 (30.03.2009) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **BUNDESDRUCKEREI GMBH** [DE/DE]; Oranienstraße 91, 10958 Berlin (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **KÜTER, Joachim** [DE/DE]; Am Krögel 3, 10179 Berlin (DE).

(74) Anwalt: **RICHARDT, Markus**; Wilhelmstraße 7, 65185 Wiesbaden (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

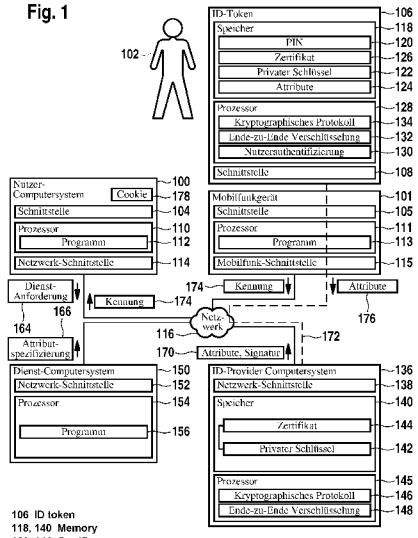
(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Fortsetzung auf der nächsten Seite]

(54) **Title**: METHOD FOR READING ATTRIBUTES FROM AN ID TOKEN VIA A MOBILE RADIO CONNECTION

(54) **Bezeichnung** : VERFAHREN ZUM LESEN VON ATTRIBUTEN AUS EINEM ID-TOKEN ÜBER EINE MOBILFUNK-VERBINDUNG

Fig. 1



106 ID token
118, 140 Memory
126, 144 Certificate
122, 142 Private key
134, 146 Cryptographic protocol
132 End-to-end encryption
130, 148 User authentication
108, 104 Interface
100 User computer system
114 Network interface
101 Mobile radio device
105 Interface
110, 111, 154, 145, 128 Processor
112, 113, 156 Program
115 Mobile radio interface
164 Service request
174 Identifier
116 Network
166 Attribute specification
170 Attribute, signature
150 Service computer system
152, 138 Network interface
136 ID provider computer system

(57) **Abstract**: The invention relates to a method for reading at least one attribute saved in an ID token (106, 106'), wherein the ID token is allocated to a user (102) and wherein the ID token has a first interface, having the following steps: authenticating the user compared to the ID token, establishing a mobile radio connection between a mobile radio device and a first computer system (136), wherein the mobile radio device has a second interface, establishing a secured connection via the mobile radio connection and via the first and second interfaces between the first computer system and the ID token, authenticating the first computer system (136) compared to the ID token via the secured connection, following successful authentication of the user and the first computer system compared to the ID token, read access of the first computer system to the at least one attribute saved in the ID token for transfer of the at least one attribute via a network (116) after signing thereof.

(57) **Zusammenfassung**: Die Erfindung betrifft ein Verfahren zum Lesen zumindest eines in einem ID-Token (106, 106') gespeicherten Attributs, wobei der ID-Token einem Nutzer (102) zugeordnet ist und wobei der ID-Token eine erste Schnittstelle aufweist, mit folgenden Schritten: Authentifizierung des Nutzers gegenüber dem ID-Token, Aufbau einer Mobilfunkverbindung zwischen einem Mobilfunkgerät und einem ersten Computersystem (136), wobei das Mobilfunkgerät eine zweite Schnittstelle aufweist, Aufbau einer geschützten Verbindung über die Mobilfunkverbindung und über die ersten und zweiten Schnittstellen zwischen dem ersten

[Fortsetzung auf der nächsten Seite]

WO 2010/112368 A2

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts (Regel 48 Absatz 2 Buchstabe g)*

Computersystems und dem ID-Token, Authentifizierung des ersten Computersystems (136) gegenüber dem ID-Token über die geschützte Verbindung, a. nach erfolgreicher Authentifizierung des Nutzers und des ersten Computersystems gegenüber dem ID-Token, Lesezugriff des ersten Computersystems auf das zumindest eine in dem ID-Token gespeicherte Attribut zur Übertragung des zumindest einen Attributs nach dessen Signierung über ein Netzwerk (116).

Verfahren zum Lesen von Attributen aus einem ID-Token über eine Mobilfunkverbindung

---

Beschreibung

Die Erfindung betrifft ein Verfahren zum Lesen von zumindest einem Attribut aus einem ID-Token, ein Computerprogrammprodukt, einen ID-Token sowie ein Computersystem.

Aus dem Stand der Technik sind verschiedene Verfahren zur Verwaltung der so genannten digitalen Identität eines Benutzers bekannt:

Microsoft Windows CardSpace ist ein Client-basiertes digitales Identitätssystem, welches es Internetbenutzern ermöglichen soll, deren digitale Identität gegenüber Online-Diensten mitzuteilen. Nachteilig ist hierbei unter anderem, dass der Nutzer seine digitale Identität manipulieren kann.

Bei OPENID handelt es sich dagegen um ein Server-basiertes System. Ein so genannter Identity-Server speichert eine Datenbank mit den digitalen Identitäten der registrierten Nutzer. Nachteilig ist hieran unter anderem ein mangelhafter Datenschutz, da die digitalen Identitäten der Nutzer zentral gespeichert werden und das Nutzerverhalten aufgezeichnet werden kann.

Aus US 2007/0294431 A1 ist ein weiteres Verfahren zur Verwaltung der digitalen Identitäten bekannt, welches ebenfalls eine Nutzerregistrierung erfordert.

Ferner sind Token-basierte Authentifizierungsverfahren beispielsweise aus US 2001/0045451 A1 und US 6 257 486 B1 bekannt

Weitere Token-basierte Authentifizierungsverfahren sind in den zum Anmeldezeitpunkt unveröffentlichten Patentanmeldungen DE 10 2008 000 067.1-31, DE 10 2008 040 416.0-31 und DE 10 2008 042 262.2-31 derselben Patentanmelderin offenbart.

Der Erfindung liegt demgegenüber die Aufgabe zugrunde, ein verbessertes Verfahren zum Lesen zumindest eines Attributs zu schaffen, sowie ein entsprechendes Computerprogrammprodukt, einen ID-Token und ein Computersystem.

Die der Erfindung zugrunde liegenden Aufgaben werden jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Ausführungsformen der Erfindung sind in den abhängigen Ansprüchen angegeben.

Nach Ausführungsformen der Erfindung wird ein Verfahren zum Lesen zumindest eines in einem ID-Token gespeicherten Attributs geschaffen, wobei der ID-Token einem Nutzer zugeordnet ist. Das Verfahren beinhaltet die folgenden Schritte: Authentifizierung des Nutzers gegenüber dem ID-Token, Aufbau einer Mobilfunkverbindung zwischen einem Mobilfunkgerät und einem ersten Computersystem, wobei das Mobilfunkgerät eine zweite Schnittstelle aufweist, Aufbau einer geschützten Verbindung über die Mobilfunkverbindung und über die ersten und zweiten Schnittstellen zwischen dem ersten Computersystems und dem ID-Token, Authentifizierung des ersten Computersystems gegenüber dem ID-Token über die geschützte Verbindung, nach erfolgreicher Authentifizierung des Nutzers und des ersten Computersystems gegenüber dem ID-Token, Lesezugriff des ersten Computersystems auf das zumindest eine in dem ID-Token gespeicherte Attribut zur Übertragung des zumindest einen Attributs nach dessen Signierung über ein Netzwerk. Hierdurch kann ein „Vertrauensanker“ geschaffen werden.

Die Erfindung ermöglicht das Lesen eines oder mehrerer der in einem ID-Token gespeicherten Attribute durch das erste Computersystem, wobei die Verbindung zwischen dem ID-Token und dem ersten Computersystem über eine Mobilfunkverbindung aufgebaut werden kann. Bei dem zumindest einem Attribut kann es sich um

eine Angabe bezüglich der Identität des dem ID-Token zugeordneten Nutzers handeln, insbesondere bezüglich dessen so genannter digitaler Identität. Beispielsweise werden durch das erste Computersystem die Attribute Name, Vorname, Adresse gelesen, um diese Attribute an ein zweites Computersystem, zum Beispiel eines Online-Dienstes, weiterzuleiten.

Es kann aber zum Beispiel auch nur ein einzelnes Attribut gelesen werden, welches nicht zur Feststellung der Identität des Nutzers, sondern beispielsweise zur Überprüfung der Berechtigung des Benutzers zur Inanspruchnahme eines bestimmten Online-Dienstes dient, wie zum Beispiel das Alter des Nutzers, wenn dieser einen Online-Dienst in Anspruch nehmen möchte, der einer bestimmten Altersgruppe vorbehalten ist, oder ein anderes Attribut, welches die Zugehörigkeit des Nutzers zu einer bestimmten Gruppe dokumentiert, welche zur Nutzung des Online-Dienstes berechtigt ist.

Bei dem ID-Token kann es sich um ein tragbares elektronisches Gerät, wie zum Beispiel einen so genannten USB-Stick, handeln oder um ein Dokument, insbesondere ein Wert- oder Sicherheitsdokument.

Unter einem „Dokument“ werden erfindungsgemäß papierbasierte und/oder kunststoffbasierte Dokumente verstanden, wie zum Beispiel Ausweisdokumente, insbesondere Reisepässe, Personalausweise, Visa sowie Führerscheine, Fahrzeugscheine, Fahrzeugbriefe, Firmenausweise, Gesundheitskarten oder andere ID-Dokumente sowie auch Chipkarten, Zahlungsmittel, insbesondere Bankkarten und Kreditkarten, Frachtbriefe oder sonstige Berechtigungsnachweise, in die ein Datenspeicher zur Speicherung des zumindest einen Attributs integriert ist.

Ausführungsformen der Erfindung sind also besonders vorteilhaft, da das zumindest eine Attribut aus einem besonders vertrauenswürdigen Dokument, beispielsweise einem amtlichen Dokument, ausgelesen wird. Von besonderem Vorteil ist weiterhin, dass eine zentrale Speicherung der Attribute nicht erforderlich ist. Die Erfindung ermöglicht also ein besonders hohes Maß an Vertrauenswürdigkeit hinsichtlich der

Mitteilung der zu einer digitalen Identität gehörenden Attribute, verbunden mit einem optimalen Datenschutz bei äußerst bequemer Handhabung.

Nach einer Ausführungsform der Erfindung hat das erste Computersystem zumindest ein Zertifikat, welches zur Authentifizierung des ersten Computersystems gegenüber dem ID-Token verwendet wird. Das Zertifikat beinhaltet eine Angabe derjenigen Attribute, für welche das erste Computersystem eine Leseberechtigung hat. Der ID-Token prüft anhand dieses Zertifikats, ob das erste Computersystem die erforderliche Leseberechtigung für den Lesezugriff auf das Attribut hat, bevor ein solcher Lesezugriff durch das erste Computersystem durchgeführt werden kann.

Unter einem „Zertifikat“ wird hier ein digitales Zertifikat verstanden, welches auch als Public-Key-Zertifikat bezeichnet wird. Bei einem Zertifikat handelt es sich um strukturierte Daten, die dazu dienen, einen öffentlichen Schlüssel eines asymmetrischen Kryptosystems einer Identität, wie z.B. einer Person, einer Organisation oder einem Computersystem, zuzuordnen. Beispielsweise kann das Zertifikat dem Standard X.509 oder einem anderen Standard entsprechen.

Nach einer Ausführungsform der Erfindung sendet das erste Computersystem das zumindest eine von dem ID-Token ausgelesene Attribut unmittelbar an ein zweites Computersystem. Bei dem zweiten Computersystem kann es sich zum Beispiel um einen Server zur Erbringung eines Online-Dienstes oder eines sonstigen Dienstes, wie zum Beispiel einer Bankdienstleistung oder zur Bestellung eines Produkts handeln. Beispielsweise kann der Nutzer ein Konto online eröffnen, wozu Attribute, die die Identität des Nutzers beinhalten, von dem ersten Computersystem an das zweite Computersystem einer Bank übertragen werden.

Nach einer Ausführungsform der Erfindung erfolgt die Übertragung der aus dem ID-Token gelesenen Attribute von dem ersten Computersystem zunächst an ein drittes Computersystem des Nutzers. Beispielsweise hat das dritte Computersystem einen üblichen Internetbrowser, mit dem der Nutzer eine Webseite des zweiten Compu-

tersystems öffnen kann. Der Nutzer kann in die Webseite eine Anforderung oder Bestellung für einen Dienst oder ein Produkt eingeben.

Das zweite Computersystem spezifiziert daraufhin diejenigen Attribute, zum Beispiel des Nutzers oder seines ID-Tokens, welche es für die Erbringung des Dienstes oder die Annahme der Bestellung benötigt. Die entsprechende Attributspezifikation, die die Spezifizierung dieser Attribute beinhaltet, wird sodann von dem zweiten Computersystem an das erste Computersystem gesendet. Dies kann mit oder ohne Zwischenschaltung des dritten Computersystems erfolgen. Im letzteren Fall kann der Nutzer das gewünschte erste Computersystem gegenüber dem zweiten Computersystem spezifizieren, beispielsweise durch Eingabe der URL des ersten Computersystems in eine Webseite des zweiten Computersystems von dem dritten Computersystem aus.

Nach einer Ausführungsform der Erfindung beinhaltet die Dienst-Anforderung des Nutzers an das zweite Computersystem die Angabe eines Identifikators, wobei der Identifikator das erste Computersystem identifiziert. Beispielsweise handelt es sich bei dem Identifikator um einen Link, beispielsweise eine URL des ersten Computersystems.

Nach einer Ausführungsform der Erfindung wird die Attributspezifizierung nicht unmittelbar von dem zweiten Computersystem an das erste Computersystem gesendet, sondern zunächst von dem zweiten Computersystem an das dritte Computersystem.

Nach einer Ausführungsform der Erfindung werden die aus dem ID-Token ausgelesenen Attribute von dem ersten Computersystem signiert und dann an das dritte Computersystem übertragen. Der Nutzer des dritten Computersystems kann die Attribute also lesen, ohne sie jedoch verändern zu können. Erst nach Freigabe durch den Nutzer werden die Attribute von dem dritten Computersystem an das zweite Computersystem weitergeleitet.

Nach einer Ausführungsform der Erfindung kann der Nutzer die Attribute vor deren Weiterleitung durch weitere Daten ergänzen.

Nach einer Ausführungsform der Erfindung hat das erste Computersystem mehrere Zertifikate mit verschiedenen Leserechten. Aufgrund des Empfangs der Attributspezifikation wählt das erste Computersystem eines oder mehrere dieser Zertifikate aus, um die entsprechenden Attribute aus dem ID-Token oder mehreren verschiedenen ID-Token auszulesen. Ausführungsformen der Erfindung sind ganz besonders vorteilhaft, da ein Mobilfunkgerät, wie zum Beispiel ein sogenanntes Handy oder ein Smartphone, für den Lesezugriff des ersten Computersystems auf den ID-Token verwendet werden kann. Hierzu hat der ID-Token eine erste Schnittstelle und das Mobilfunkgerät hat neben seiner Mobilfunk-Schnittstelle eine weitere, zweite Schnittstelle. Über die ersten und zweiten Schnittstellen können Daten zwischen dem ID-Token und dem Mobilfunkgerät ausgetauscht werden.

Die ersten und zweiten Schnittstellen haben beispielsweise eine relativ geringe Reichweite, von weniger als 1 m, insbesondere weniger als 20 cm. Insbesondere können die ersten und zweiten Schnittstellen für eine sogenannte Nahfeldkommunikation, insbesondere nach einem Near Field Communication (NFC) Standard und/oder nach dem Standard ISO/IEC 14443 ausgebildet sein.

Die Mobilfunk-Schnittstelle des Mobilfunkgeräts kann zur Kommunikation über ein digitales zellulares Mobilfunknetzwerk ausgebildet sein, wie zum Beispiel nach einem Mobilfunkstandard, insbesondere nach einem oder mehreren der GSM, UMTS, CDMA und/oder CDMA 2000 Standards. Von besonderem Vorteil ist hier insbesondere, dass ein Benutzer das üblicherweise ohnehin vorhandene Mobilfunkgerät zur Ermöglichung des Zugriffs des ersten Computersystems auf den ID-Token verwenden kann, ohne dass ein zusätzliches Lesegerät erforderlich ist.

Nach einer Ausführungsform der Erfindung wird von dem dritten Computersystem an das erste Computersystem eine Nachricht gesendet. Durch die Nachricht wird eine Anforderung von dem dritten Computersystem an das erste Computersystem

gerichtet, um zumindest eines der Attribute aus dem ID-Token auszulesen. Die Nachricht kann eine Attributspezifizierung der von dem ersten Computersystem aus dem ID-Token auszulesenden ein oder mehreren Attribute beinhalten. Alternativ werden aufgrund der Nachricht von dem ersten Computersystem ein oder mehrere vorbestimmte Attribute aus dem ID-Token ausgelesen oder beispielsweise sämtliche Attribute, auf die das erste Computersystem in dem ID-Token Zugriff hat.

Zum Senden der Nachricht wird zwischen dem dritten Computersystem und dem ersten Computersystem eine erste Verbindung aufgebaut, wie zum Beispiel über das Internet. Aufgrund des Empfangs der Nachricht von dem dritten Computersystem über die erste Verbindung erzeugt das erste Computersystem eine Kennung, durch welche die erste Verbindung und/oder die Nachricht und/oder das dritte Computersystem eindeutig identifiziert wird.

Diese Kennung sendet das erste Computersystem beispielsweise über die erste Verbindung zurück an das dritte Computersystem. Von dem dritten Computersystem wird dann die Kennung an das Mobilfunkgerät übertragen. Das Mobilfunkgerät überträgt dann diese Kennung über eine zweite Verbindung an das erste Computersystem, wobei es sich bei der zweiten Verbindung um eine Mobilfunkverbindung handelt.

Aufgrund des Empfangs derselben Kennung, die das erste Computersystem zuvor an das dritte Computersystem gesendet hatte, über die Mobilfunkverbindung durch das erste Computersystem ist somit die Mobilfunkverbindung bzw. das Mobilfunkgerät dem dritten Computersystem eindeutig zugeordnet.

Das erste Computersystem baut dann die geschützte Verbindung über diese Mobilfunkverbindung auf, um hierüber auf den ID-Token lesend zuzugreifen. Da über die Kennung die ersten und zweiten Verbindungen bzw. das dritte Computersystem und das Mobilfunkgerät eindeutig einander zugeordnet sind, so ist auch der ID-Token, auf den über das Mobilfunkgerät zugegriffen wird, dem dritten Computersystem eindeutig zugeordnet. Hieraus folgt, dass die von dem ersten Computersystem aus

dem ID-Token ausgelesenen ein oder mehreren Attribute dem dritten Computersystem und/oder dem Nutzer des dritten Computersystems, der gleichzeitig auch der Nutzer des ID-Tokens ist, zugeordnet sind.

Bei der Kennung kann es sich beispielsweise um eine Zufallszahl oder einen Globally Unique Identifier (GUID) handeln. Bei der Kennung kann es sich auch um einen kryptografischen Schlüssel, wie zum Beispiel einen symmetrischen oder einen asymmetrischen Schlüssel handeln, um die Zuordnung zwischen den ersten und zweiten Verbindungen bzw. dem dritten Computersystem und dem Mobilfunkgerät und damit dem ID-Token herzustellen.

Nach einer Ausführungsform der Erfindung sendet das erste Computersystem die Kennung alternativ oder zusätzlich über die zweite Verbindung, d.h. die Mobilfunkverbindung, an das Mobilfunkgerät. Die Kennung wird dann von dem Mobilfunkgerät an das dritte Computersystem übertragen. Das dritte Computersystem sendet dann die Kennung über die erste Verbindung zurück an das erste Computersystem, sodass die Zuordnung wiederum gegeben ist.

Nach einer Ausführungsform der Erfindung sendet das erste Computersystem das oder die signierten Attribute an das dritte Computersystem. Zusätzlich zu den Attributen und deren Signatur kann auch die Kennung und/oder eine Signatur der Kennung oder eine über die Attribute und die Kennung gebildete Signatur von dem ersten Computersystem an das dritte Computersystem gesendet werden.

Nach einer Ausführungsform der Erfindung wird die geschützte Verbindung mit einer Ende-zu-Ende-Verschlüsselung zwischen dem ID-Token und dem ersten Computersystem über die ersten und zweiten Schnittstellen sowie die Mobilfunkverbindung aufgebaut. Dadurch wird sichergestellt, dass die einseitige oder gegenseitige Authentifizierung des ersten Computersystems und des ID-Tokens sowie die Übertragung des oder der aus dem ID-Token ausgelesenen Attribute über die geschützte Verbindung unverfälscht stattfinden kann.

Nach einer Ausführungsform der Erfindung kann die Übertragung der Kennung von dem dritten Computersystem an das Mobilfunkgerät bzw. von dem Mobilfunkgerät an das dritte Computersystem manuell durch den Nutzer vorgenommen werden. Hierzu wird die Kennung auf einer Anzeige des dritten Computersystems bzw. des Mobilfunkgeräts angezeigt, sodass der Nutzer die Kennung von dort ablesen und manuell über eine Tastatur in das jeweils andere Gerät, d.h. das dritte Computersystem oder das Mobilfunkgerät, eingeben kann.

Nach einer Ausführungsform der Erfindung erfolgt die Übertragung der Kennung zwischen dem dritten Computersystem und dem Mobilfunkgerät zumindest teilweise automatisch. Dies kann zum Beispiel auf optischem Wege erfolgen. Beispielsweise wird die Kennung in Form eines maschinenlesbaren Musters auf der Anzeige ausgegeben, insbesondere in Form eines zweidimensionalen Barcodes. Dieses maschinenlesbare Muster, insbesondere also der zweidimensionale Barcode, wird dann optisch zum Beispiel mit Hilfe einer in das Mobilfunkgerät integrierten Kamera oder einer Kamera des dritten Computersystems, insbesondere einer sogenannten Webcam, optisch erfasst.

Nach einer weiteren Ausführungsform der Erfindung wird über das Mobilfunknetz eine Verbindung zwischen dem dritten Computersystem und dem Mobilfunkgerät aufgebaut, um hierüber die Kennung zu übertragen.

Nach einer weiteren Ausführungsform der Erfindung hat das dritte Computersystem eine weitere Schnittstelle, die in ihrer Funktionalität der ersten Schnittstelle des ID-Tokens entspricht, und über die das dritte Computersystem also beispielsweise über Funk nach einem NFC-Standard mit der zweiten Schnittstelle des Mobilfunkgeräts kommunizieren kann. Über diese weitere Schnittstelle des dritten Computersystems kann insbesondere die Kennung übertragen werden.

Nach einer Ausführungsform der Erfindung generiert das erste Computersystem auf die Nachricht des dritten Computersystems eine Antwort, die das oder die aus dem ID-Token ausgelesenen Attribute und/oder die Kennung sowie eine Signatur des

oder der Attribute und/oder der Kennung beinhaltet. Diese Antwort wird von dem ersten Computersystem an das dritte Computersystem gesendet.

Das dritte Computersystem leitet diese Antwort an das zweite Computersystem weiter und speichert vorzugsweise lokal eine Kopie der Kennung, beispielsweise in Form eines sogenannten Cookies. Dies hat den besonderen Vorteil, dass für eine nachfolgende weitere Dienst-Anforderung des dritten Computersystems an das zweite Computersystem auf die zuvor von dem im ersten Computersystem erzeugte Antwort zurückgegriffen werden kann, indem nämlich das zweite Computersystem die Antwort speichert und von dem dritten Computersystem die in dem Cookie gespeicherte Kennung nach dem Empfang der Dienstanforderung abfragt. Mit Hilfe der Kennung kann das zweite Computersystem nämlich auf die zu der Kennung passende Antwort des ersten Computersystems zugreifen und hat damit Kenntnis von den gewünschten Attributen des Nutzers.

Nach einer Ausführungsform der Erfindung hat die Kennung eine zeitlich und/oder hinsichtlich der Anzahl der Nutzungen beschränkte Gültigkeit. Diese beschränkte Gültigkeit der Kennung kann zum Beispiel in dem zu der Signatur der Kennung gehörenden Zertifikat angegeben sein. Wenn diese Gültigkeit abgelaufen ist, kann das zweite Computersystem nicht mehr die gespeicherte Antwort des ersten Computersystems verwenden, und es muss erneut ein Lesezugriff des ersten Computersystems zum Auslesen des oder der Attribute aus dem ID-Token erfolgen, um eine aktualisierte Antwort zu generieren.

Nach einer Ausführungsform der Erfindung handelt es sich bei dem ersten Computersystem um ein ID-Provider-Computersystem, wie zum Beispiel ein Trustcenter, welches von einem Zertifizierungsdienstanbieter (ZDA) betrieben wird, bei dem zweiten Computersystem um ein Dienst-Computersystem, wie zum Beispiel eine Internetplattform, die von einem kommerziellen Anbieter oder von einer Behörde zur Erbringung einer behördlichen Dienstleistung betrieben wird, und bei dem dritten Computersystem um ein Nutzer-Computersystem, wie zum Beispiel einen PC oder einen Laptopcomputer des Nutzers.

Ausführungsformen der Erfindung sind ferner besonders vorteilhaft, da eine Nutzung des ID-Provider-Computersystems von dem Nutzer-Computersystem aus auch dann möglich ist, wenn das Nutzer-Computersystem nicht über eine Schnittstelle zum Zugriff auf den ID-Token verfügt oder wenn an das Nutzer-Computersystem ein entsprechendes Lesegerät zum Zugriff auf den ID-Token nicht anschließbar ist, nicht verfügbar ist, oder aus Gründen der Netzwerkadministration nicht angeschlossen werden darf. In diesem Fall kann der Nutzer sein zumeist ohnehin vorhandenes Mobilfunkgerät ergänzend zu seinem Nutzer-Computersystem verwenden, um den von dem ID-Provider-Computersystem zur Verfügung gestellten Vertrauensanker zu nutzen.

In einem weiteren Aspekt betrifft die Erfindung ein Computerprogrammprodukt, insbesondere ein digitales Speichermedium, mit ausführbaren Programminstruktionen zur Durchführung eines erfindungsgemäßen Verfahrens.

Ausführungsformen des Computerprogrammprodukts sind zur Durchführung der folgenden Schritte ausgebildet: Aufbau einer ersten Verbindung zwischen dem ersten Computersystem und einem dritten Computersystem über ein Netzwerk, Aufbau einer zweiten Verbindung zwischen dem ersten Computersystem und einem Mobilfunkgerät, wobei es sich bei der zweiten Verbindung um eine Mobilfunkverbindung handelt, Erzeugung einer Kennung durch das erste Computersystem, Senden der Kennung über eine der ersten und zweiten Verbindungen von dem ersten Computersystem, Empfang der Kennung von dem ersten Computersystem über die andere der ersten und zweiten Verbindungen, Aufbau einer geschützten Verbindung zwischen dem ersten Computersystem und einem ID-Token, wobei der ID-Token eine erste Schnittstelle aufweist, wobei die geschützte Verbindung über die Mobilfunkverbindung und über die erste Schnittstelle und eine zweite Schnittstelle des Mobilfunkgeräts aufgebaut wird, Authentifizierung des ersten Computersystems gegenüber dem ID-Token über die geschützte Verbindung, nach erfolgreicher Authentifizierung des ersten Computersystems gegenüber dem ID-Token, Lesezugriff des ersten Computersystems auf zumindest ein in dem ID-Token gespeichertes Attribut

zur Übertragung des zumindest einen Attributs nach dessen Signierung über das Netzwerk.

In einem weiteren Aspekt betrifft die Erfindung einen ID-Token einer ersten Schnittstelle zur Kommunikation mit einem Mobilfunkgerät, einem geschützten Speicherbereich zur Speicherung von zumindest einem Attribut, Mitteln zur Authentifizierung eines dem ID-Token zugeordneten Nutzers (102) gegenüber dem ID-Token, Mitteln zur Authentifizierung eines ersten Computersystems gegenüber dem ID-Token, Mitteln zum Aufbau einer geschützten Verbindung über das Mobilfunkgerät zu dem ersten Computersystem, über die das erste Computersystem das zumindest eine Attribut auslesen kann, wobei eine notwendige Voraussetzung für das Auslesen des zumindest einen Attributs aus dem ID-Token durch das erste Computersystem die erfolgreiche Authentifizierung des Nutzers und des ersten Computersystems gegenüber dem ID-Token ist.

Zusätzlich zu der Authentifizierung des ersten Computersystems gegenüber dem ID-Token, wie sie an sich zum Beispiel als so genannte Extended Access Control für maschinenlesbare Reisedokumente (machine-readable travel documents – MRTD) bekannt und von der internationalen Luftfahrtbehörde ICAO spezifiziert ist, muss sich also der Nutzer gegenüber dem ID-Token authentifizieren. Beispielsweise wird durch eine erfolgreiche Authentifizierung des Nutzers gegenüber dem ID-Token dieser freigeschaltet, sodass die weiteren Schritte, nämlich die Authentifizierung des ersten Computersystems gegenüber dem ID-Token und/oder der Aufbau einer geschützten Verbindung zum Auslesen der Attribute, ablaufen können.

Nach einer Ausführungsform der Erfindung hat der ID-Token Mittel für eine Ende-zu-Ende-Verschlüsselung. Dies ermöglicht es, die Verbindung zwischen dem ID-Token und dem ersten Computersystem über ein drittes Computersystem des Nutzers aufzubauen, da der Nutzer aufgrund der Ende-zu-Ende-Verschlüsselung keine Änderungen der über die Verbindung übertragenen Daten vornehmen kann.

In einem weiteren Aspekt betrifft die Erfindung ein erstes Computersystem Mitteln zum Empfang einer Nachricht über ein Netzwerk, wobei durch die Nachricht zumindest ein Attribut angefordert wird, Mitteln zur Authentifizierung gegenüber einem ID-Token über eine Mobilfunkverbindung, Mitteln zum Lesen zumindest einen Attributs aus dem ID-Token über eine geschützte Verbindung, wobei das Lesen des zumindest einen Attributs voraussetzt, dass sich ein dem ID-Token zugeordneter Nutzer und das Computersystem gegenüber dem ID-Token authentifiziert haben.

Nach einer Ausführungsform der Erfindung kann das erste Computersystem Mittel zur Generierung einer Aufforderung an den Benutzer beinhalten. Nachdem das erste Computersystem die Attributspezifikation beispielsweise von dem zweiten Computersystem empfangen hat, sendet es daraufhin eine Aufforderung an das dritte Computersystem des Nutzers, sodass der Nutzer dazu aufgefordert wird, sich gegenüber dem ID-Token zu authentifizieren. Nachdem die Authentifizierung des Nutzers gegenüber dem ID-Token erfolgreich durchgeführt worden ist, erhält das erste Computersystem von dem dritten Computersystem eine Bestätigung. Daraufhin authentifiziert sich das erste Computersystem gegenüber dem ID-Token und es wird eine sichere Verbindung zwischen dem ID-Token und dem ersten Computersystem mit einer Ende-zu-Ende-Verschlüsselung aufgebaut.

Ausführungsformen des erfindungsgemäßen ersten Computersystems sind besonders vorteilhaft, da sie in Kombination mit der Notwendigkeit der Authentifizierung des Nutzers gegenüber dem ID-Token einen Vertrauensanker für die unverfälschte digitale Identität des Nutzers bilden. Hierbei ist von besonderem Vorteil, dass dies keine vorherige Registrierung des Nutzers gegenüber dem Computersystem erfordert sowie auch keine zentrale Speicherung der die digitalen Identitäten bildenden Attribute der Nutzer.

Nach einer Ausführungsform der Erfindung empfängt das erste Computersystem zusammen mit der Attributspezifikation einen Identifikator des zweiten Computersystems. Mit Hilfe des Identifikators identifiziert das Computersystem das zweite

Computersystem, welches die Identifikationsdienste in Anspruch nehmen möchte, um diese Dienstleistung gegenüber dem zweiten Computersystem zu vergebühren.

Nach einer Ausführungsform der Erfindung handelt es sich bei dem Computersystem um ein behördlich zertifiziertes Trust-Center, insbesondere ein Signaturgesetzkonformes Trust-Center.

Die verschiedenen funktionellen Mittel der Computersysteme, des Mobilfunkgeräts und/oder des ID-Token, wie zum Beispiels die Mittel zum Empfang, die Mittel zur Authentifizierung, die Mittel zum Lesen, die Mittel zur Generierung, die Mittel zur Erzeugung einer Kennung und/oder die Mittel zum Signieren können jeweils durch ein oder mehrere Prozessoren und durch Programminstruktionen realisiert werden, die in einem Speicher gespeichert und von dort zur Ausführung durch den oder die Prozessoren ausgelesen werden können. Ganz oder teilweise kann eine Realisierung der verschiedenen funktionellen Mittel auch schaltungstechnisch erfolgen. Ferner können die verschiedenen funktionellen Mittel auch durch voneinander räumlich getrennte Hardwareeinheiten realisiert werden, die über geeignete Kommunikationsverbindungen miteinander interoperieren.

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

Figur 1 ein Blockdiagramm einer ersten Ausführungsform erfindungsgemäßer Computersysteme,

Figur 2 ein Flussdiagramm einer Ausführungsform eines erfindungsgemäßen Verfahrens,

Figur 3 ein UML-Diagramm einer weiteren Ausführungsform eines erfindungsgemäßen Verfahrens,

Figur 4 ein UML-Diagramm einer weiteren Ausführungsform eines erfindungsgemäßen Verfahrens.

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

Die Figur 1 zeigt ein Nutzer-Computersystem 100 eines Nutzers 102. Bei dem Nutzer-Computersystem 100 kann es sich um einen Personalcomputer, einen tragbaren Computer, wie zum Beispiel einen Laptop oder Palmtop-Computer, einen Personal Digital Assistant, ein mobiles Telekommunikationsgerät, insbesondere ein Smart Phone, oder dergleichen handeln. Das Nutzer-Computersystem 100 hat eine Schnittstelle 104 zur Kommunikation mit einem ID-Token 106, der eine entsprechende Schnittstelle 108 aufweist.

Das Nutzer-Computersystem 100 hat zumindest einen Prozessor 110 zur Ausführung von Programminstruktionen 112 sowie eine Netzwerk-Schnittstelle 114 zur Kommunikation über ein Netzwerk 116. Bei dem Netzwerk 116 kann es sich um ein Computernetzwerk, wie zum Beispiel das Internet, handeln. Das Netzwerk 116 beinhaltet ein Mobilfunknetzwerk oder ist mit einem Mobilfunknetzwerk verbunden..

Der ID-Token 106 hat einen elektronischen Speicher 118 mit geschützten Speicherbereichen 120, 122 und 124. Der geschützte Speicherbereich 120 dient zur Speicherung eines Referenzwerts, der für die Authentifizierung des Nutzers 102 gegenüber dem ID-Token 106 benötigt wird. Bei diesem Referenzwert handelt es sich beispielsweise um eine so genannte Personal Identification Number (PIN), oder um Referenzdaten für ein biometrisches Merkmal des Nutzers 102, welches für die Authentifizierung des Nutzers gegenüber dem ID-Token 106 verwendet werden kann.

Der geschützte Bereich 122 dient zur Speicherung eines privaten Schlüssels und der geschützte Speicherbereich 124 dient zur Speicherung von Attributen, zum Beispiel des Nutzers 102, wie zum Beispiel dessen Name, Wohnort, Geburtsdatum, Geschlecht, und/oder von Attributen, die den ID-Token selbst betreffen, wie zum

Beispiel die Institution, die den ID-Token erstellt oder ausgegeben hat, die Gültigkeitsdauer des ID-Tokens, einen Identifikator des ID-Tokens, wie zum Beispiel eine Passnummer oder eine Kreditkartennummer.

Der elektronische Speicher 118 kann ferner einen Speicherbereich 126 zur Speicherung eines Zertifikats aufweisen. Das Zertifikat beinhaltet einen öffentlichen Schlüssel, der dem in dem geschützten Speicherbereich 122 gespeicherten privaten Schlüssel zugeordnet ist. Das Zertifikat kann nach einem Public Key Infrastruktur (PKI) Standard erstellt worden sein, beispielsweise nach dem X.509 Standard.

Das Zertifikat muss nicht zwangsläufig in dem elektronischen Speicher 118 des ID-Tokens 106 gespeichert sein. Alternativ oder zusätzlich kann das Zertifikat auch in einem öffentlichen Verzeichnisserver gespeichert sein.

Der ID-Token 106 hat einen Prozessor 128. Der Prozessor 128 dient zur Ausführung von Programminstruktionen 130, 132 und 134. Die Programminstruktionen 130 dienen zur Nutzerauthentifizierung, d.h. zur Authentifizierung des Nutzers 102 gegenüber dem ID-Token.

Die Figur 1 zeigt ferner ein Mobilfunkgerät 101 des Nutzers 102. Bei dem Mobilfunkgerät 101 kann es sich zum Beispiel um ein Handy oder ein Smartphone handeln. Das Mobilfunkgerät 101 hat eine Schnittstelle 105 zur Kommunikation mit der entsprechenden Schnittstelle 108 des ID-Tokens 106. Bei den Schnittstellen 104, 105 und 108 kann es sich um Schnittstellen für eine sogenannte Nahfeldkommunikation handeln.

Das Mobilfunkgerät 101 hat zumindest einen Prozessor 111 zur Ausführung von Programminstruktionen 113 sowie eine Mobilfunk-Schnittstelle 115 zur Kommunikation über das Netzwerk 116.

Bei einer Ausführungsform mit PIN gibt der Nutzer 102 seine PIN zu seiner Authentifizierung in den ID-Token 106 ein, beispielsweise über das Mobilfunkgerät 101.

Beispielsweise gibt der Nutzer 102 seine PIN über eine Tastatur des Mobilfunkgeräts 101 ein; die PIN wird dann von dem Mobilfunkgerät 101 über die Schnittstelle 105 zu dem ID-Token 106 übertragen.

Durch Ausführung der Programminstruktionen 130 wird dann von dem ID-Token 106 auf den geschützten Speicherbereich 120 zugegriffen, um die eingegebene PIN mit dem dort gespeicherten Referenzwert der PIN zu vergleichen. Für den Fall, dass die eingegebene PIN mit dem Referenzwert der PIN übereinstimmt, gilt der Nutzer 102 als authentifiziert.

Alternativ wird ein biometrisches Merkmal des Nutzers 102 erfasst. Beispielsweise hat der ID-Token 106 hierzu einen Fingerabdrucksensor oder ein Fingerabdrucksensor ist an das Mobilfunkgerät 101 angeschlossen oder darin integriert. Die von dem Nutzer 102 erfassten biometrischen Daten werden durch Ausführung der Programminstruktionen 130 bei dieser Ausführungsform mit den in dem geschützten Speicherbereich 120 gespeicherten biometrischen Referenzdaten verglichen. Bei hinreichender Übereinstimmung der von dem Nutzer 102 erfassten biometrischen Daten mit den biometrischen Referenzdaten gilt der Nutzer 102 als authentifiziert.

Die Programminstruktionen 134 dienen zur Ausführung der den ID-Token 106 betreffenden Schritte eines kryptographischen Protokolls zur Authentifizierung eines ID-Provider-Computersystems 136 gegenüber dem ID-Token 106. Bei dem kryptographischen Protokoll kann es sich um ein Challenge-Response-Protokoll basierend auf einem symmetrischen Schlüssel oder einem asymmetrischen Schlüsselpaar handeln.

Beispielsweise wird durch das kryptographische Protokoll ein Extended Access Control-Verfahren implementiert, wie es für maschinenlesbare Reisedokumente (machine-readable travel documents – MRTD) von der internationalen Luftfahrtbehörde (ICAO) spezifiziert ist. Durch erfolgreiche Ausführung des kryptographischen Protokolls authentifiziert sich das ID-Provider-Computersystem 136 gegenüber dem ID-Token und weist dadurch seine Leseberechtigung zum Lesen der in dem ge-

schützten Speicherbereich 124 gespeicherten Attribute nach. Die Authentifizierung kann auch gegenseitig sein, d.h. auch der ID-Token 106 muss sich dann gegenüber dem ID-Provider-Computersystem 136 nach demselben oder einem anderen kryptographischen Protokoll authentifizieren.

Die Programminstruktionen 132 dienen zur Ende-zu-Ende-Verschlüsselung von zwischen dem ID-Token 106 und dem ID-Provider-Computersystem 136 übertragenen Daten, zumindest aber der von dem ID-Provider-Computersystem 136 aus dem geschützten Speicherbereich 124 ausgelesenen Attribute. Für die Ende-zu-Ende-Verschlüsselung kann ein symmetrischer Schlüssel verwendet werden, der beispielsweise anlässlich der Ausführung des kryptographischen Protokolls zwischen dem ID-Token 106 und dem ID-Provider-Computersystem 136 vereinbart wird.

Das ID-Provider-Computersystem 136 hat eine Netzwerk-Schnittstelle 138 zur Kommunikation über das Netzwerk 116. Das ID-Provider-Computersystem 136 hat ferner einen Speicher 140, in dem ein privater Schlüssel 142 des ID-Provider-Computersystems 136 sowie das entsprechende Zertifikat 144 gespeichert sind. Auch bei diesem Zertifikat kann es sich beispielsweise um ein Zertifikat nach einem PKI-Standard, wie zum Beispiel X.509 handeln.

Das ID-Provider-Computersystem 136 hat ferner zumindest einen Prozessor 145 zur Ausführung von Programminstruktionen 146 und 148. Durch Ausführung der Programminstruktionen 146 werden die das ID-Provider-Computersystem 136 betreffende Schritte des kryptographischen Protokolls ausgeführt. Insgesamt wird also das kryptographische Protokoll durch Ausführung der Programminstruktionen 134 durch den Prozessor 128 des ID-Tokens 106 sowie durch Ausführung der Programminstruktionen 146 durch den Prozessor 145 des ID-Provider-Computersystems 136 implementiert.

Die Programminstruktionen 148 dienen zur Implementierung der Ende-zu-Ende-Verschlüsselung auf Seiten des ID-Provider-Computersystems 136, beispielsweise

basierend auf dem symmetrischen Schlüssel, der anlässlich der Ausführung des kryptographischen Protokolls zwischen dem ID-Token 106 und dem ID-Provider-Computersystem 136 vereinbart worden ist. Prinzipiell kann jedes an sich vor bekannte Verfahren zur Vereinbarung des symmetrischen Schlüssels für die Ende-zu-Ende-Verschlüsselung verwendet werden, wie zum Beispiel ein Diffie-Hellman-Schlüsselaustausch.

Das ID-Provider-Computersystem 136 befindet sich vorzugsweise in einer besonders geschützten Umgebung, insbesondere in einem so genannten Trust-Center, sodass das ID-Provider-Computersystem 136 in Kombination mit der Notwendigkeit der Authentifizierung des Nutzers 102 gegenüber dem ID-Token 106 den Vertrauensanker für die Authentizität der aus dem ID-Token 106 ausgelesenen Attribute bildet.

Ein Dienst-Computersystem 150 kann zur Entgegennahme einer Bestellung oder eines Auftrags für eine Dienstleistung oder ein Produkt, insbesondere eine Online-Dienstleistung, ausgebildet sein. Beispielsweise kann der Nutzer 102 online über das Netzwerk 116 ein Konto bei einer Bank eröffnen oder eine andere Finanz- oder Bankdienstleistung in Anspruch nehmen. Das Dienst-Computersystem 150 kann auch als Online-Warenhaus ausgebildet sein, sodass der Benutzer 102 beispielsweise online ein Mobiltelefon oder dergleichen erwerben kann. Ferner kann das Dienst-Computersystem 150 auch zur Lieferung von digitalen Inhalten ausgebildet sein, beispielsweise für den Download von Musik- und/oder Videodaten.

Das Dienst-Computersystem 150 hat hierzu eine Netzwerk-Schnittstelle 152 zur Verbindung mit dem Netzwerk 116. Ferner hat das Dienst-Computersystem 150 zumindest einen Prozessor 154 zur Ausführung von Programminstruktionen 156. Durch Ausführung der Programminstruktionen 156 werden beispielsweise dynamische HTML-Seiten generiert, über die der Nutzer 102 seinen Auftrag oder seine Bestellung eingeben kann.

Je nach der Art des beauftragten oder bestellten Produkts oder der Dienstleistung muss das Dienst-Computersystem 150 ein oder mehrere Attribute des Nutzers 102 und/oder dessen ID-Token 106 anhand eines oder mehrerer vorgegebener Kriterien überprüfen. Nur wenn diese Prüfung bestanden wird, wird die Bestellung oder der Auftrag des Nutzers 102 entgegengenommen und/oder ausgeführt.

Beispielsweise ist es für die Eröffnung eines Bankkontos oder den Kauf eines Mobiltelefons mit einem dazugehörigen Vertrag erforderlich, dass der Nutzer 102 seine Identität gegenüber dem Dienst-Computersystem 150 offenbart, und dass diese Identität überprüft wird. Im Stand der Technik muss der Nutzer 102 hierzu beispielsweise seinen Personalausweis vorlegen. Dieser Vorgang wird durch das Auslesen der digitalen Identität des Nutzers 102 aus seinem ID-Token 106 ersetzt.

Je nach Anwendungsfall muss der Nutzer 102 aber nicht seine Identität gegenüber dem Dienst-Computersystem 150 offenbaren, sondern es reicht die Mitteilung, zum Beispiel nur eines der Attribute aus. Beispielsweise kann der Nutzer 102 über eines der Attribute einen Nachweis erbringen, dass er zu einer bestimmten Personengruppe gehört, die zugangsberechtigt für auf dem Dienst-Computersystem 150 zum Download bereitgehaltener Daten ist. Beispielsweise kann ein solches Kriterium ein Mindestalter des Nutzers 102 sein oder die Zugehörigkeit des Nutzers 102 zu einem Personenkreis, der auf bestimmte vertrauliche Daten eine Zugriffsberechtigung hat.

Zur Inanspruchnahme des von dem Dienst-Computersystem 150 zur Verfügung gestellten Dienstes wird beispielsweise wie folgt vorgegangen:

1. Authentifizierung des Nutzers 102 gegenüber dem ID-Token 106.

Der Nutzer 102 authentifiziert sich gegenüber dem ID-Token 106. Bei einer Implementierung mit PIN gibt der Nutzer 102 hierzu seine PIN beispielsweise über das Nutzer-Computersystem 100 oder das Mobilfunkgerät 101 in den ID-Token 106 ein. Durch Ausführung der Programminstruktionen 130 prüft dann der ID-Token 106 die Korrektheit der eingegebenen PIN. Wenn die eingegebene PIN mit dem in dem ge-

schützten Speicherbereich 120 gespeicherten Referenzwert der PIN übereinstimmt, so gilt der Nutzer 102 als authentifiziert. Analog kann vorgegangen werden, wenn ein biometrisches Merkmal des Nutzers 102 zu dessen Authentifizierung verwendet wird, wie oben beschrieben.

2. Authentifizierung des ID-Provider-Computersystems 136 gegenüber dem ID-Token 106.

Hierzu wird eine geschützte Verbindung 172 zwischen dem ID-Token 106 und dem ID-Provider-Computersystem 136 über eine Mobilfunkverbindung sowie über die Schnittstellen 105 und 108 hergestellt. Zum Aufbau der Mobilfunkverbindung zwischen dem Mobilfunkgerät 101 und dem ID-Provider-Computersystem 136 über das Netzwerk 116 kann zum Beispiel ein Mobile IP Protokoll verwendet werden, und zwar nach dem Standard der Internet Engineering Task Force (IETF). Insbesondere kann das Mobilfunkgerät 101 einen Webbrowser oder eine andere TCP/IP fähige Anwendung haben, die für den Aufbau der Mobilfunkverbindung verwendet wird. Die geschützte Verbindung 172 ist in der Fig. 1 als eine gestrichelte Linie gezeigt.

Beispielsweise überträgt das ID-Provider-Computersystem 136 sein Zertifikat 144 über diese Verbindung 172 an den ID-Token 106. Durch die Programminstruktionen 134 wird dann eine so genannte Challenge generiert, d.h. beispielsweise eine Zufallszahl. Diese Zufallszahl wird mit dem in dem Zertifikat 144 beinhalteten öffentlichen Schlüssel des ID-Provider-Computersystems 136 verschlüsselt. Das resultierende Chiffrat wird von dem ID-Token 106 über die Verbindung 172 an das ID-Provider-Computersystem 136 gesendet. Das ID-Provider-Computersystem 136 entschlüsselt das Chiffrat mit Hilfe seines privaten Schlüssels 142 und erhält so die Zufallszahl. Die Zufallszahl sendet das ID-Provider-Computersystem 136 über die Verbindung 172 an den ID-Token 106 zurück. Durch Ausführung der Programminstruktionen 134 wird dort geprüft, ob die von dem ID-Provider-Computersystem 136 empfangene Zufallszahl mit der ursprünglich generierten Zufallszahl, d.h. der Challenge, übereinstimmt. Ist dies der Fall, so gilt das ID-Provider-Computersystem 136

als gegenüber dem ID-Token 106 authentifiziert. Die Zufallszahl kann als symmetrischer Schlüssel für die Ende-zu-Ende Verschlüsselung verwendet werden.

3. Nachdem sich der Nutzer 102 erfolgreich gegenüber dem ID-Token 106 authentifiziert hat, und nachdem sich das ID-Provider-Computersystem 136 erfolgreich gegenüber dem ID-Token 106 authentifiziert hat, erhält das ID-Provider-Computersystem 136 eine Leseberechtigung zum Auslesen, eines, mehrerer oder aller der in dem geschützten Speicherbereich 124 gespeicherten Attribute. Aufgrund eines entsprechenden Lesekommandos, welches das ID-Provider-Computersystem 136 über die Verbindung 172 an den ID-Token 106 sendet, werden die angeforderten Attribute aus dem geschützten Speicherbereich 124 ausgelesen und durch Ausführung der Programminstruktionen 132 verschlüsselt. Die verschlüsselten Attribute werden über die Verbindung 172 an das ID-Provider-Computersystem 136 übertragen und dort durch Ausführung der Programminstruktionen 148 entschlüsselt. Dadurch erhält das ID-Provider-Computersystem 136 Kenntnis der aus dem ID-Token 106 ausgelesenen Attribute.

   Diese Attribute werden von dem ID-Provider-Computersystem mit Hilfe seines Zertifikats 144 signiert und über das Nutzer-Computersystem 100 oder direkt an das Dienst-Computersystem 150 übertragen. Dadurch wird das Dienst-Computersystem 150 über die aus dem ID-Token 106 ausgelesenen Attribute in Kenntnis gesetzt, sodass das Dienst-Computersystem 150 diese Attribute anhand der vorgegebenen ein oder mehreren Kriterien prüfen kann, um danach ggf. den von dem Benutzer 102 angeforderten Dienst zu erbringen.

Durch die Notwendigkeit der Authentifizierung des Nutzers 102 gegenüber dem ID-Token 106 und der Authentifizierung des ID-Provider-Computersystems 136 gegenüber dem ID-Token 106 ist der notwendige Vertrauensanker geschaffen, sodass das Dienst-Computersystem 150 sicher sein kann, dass die ihm von dem ID-Provider-Computersystem 136 mitgeteilten Attribute des Nutzers 102 zutreffend und nicht verfälscht sind.

Je nach Ausführungsform kann die Reihenfolge der Authentifizierung unterschiedlich sein. Beispielsweise kann vorgesehen sein, dass sich zunächst der Nutzer 102 gegenüber dem ID-Token 106 authentifizieren muss und nachfolgend das ID-Provider-Computersystem 136. Es ist aber grundsätzlich auch möglich, dass sich zunächst das ID-Provider-Computersystem 136 gegenüber dem ID-Token 106 authentifizieren muss und erst nachfolgend der Nutzer 102.

In dem ersten Fall ist der ID-Token 106 beispielsweise so ausgebildet, dass er nur durch Eingabe einer korrekten PIN oder eines korrekten biometrischen Merkmals durch den Nutzer 102 freigeschaltet wird. Erst diese Freischaltung ermöglicht den Start der Programminstruktionen 132 und 134 und damit die Authentifizierung des ID-Provider-Computersystems 136.

Im zweiten Fall ist ein Start der Programminstruktionen 132 und 134 auch bereits möglich, wenn sich der Nutzer 102 noch nicht gegenüber dem ID-Token 106 authentifiziert hat. In diesem Fall sind beispielsweise die Programminstruktionen 134 so ausgebildet, dass das ID-Provider-Computersystem 136 erst dann einen Lesezugriff auf den geschützten Speicherbereich 124 zum Auslesen eines oder mehrerer der Attribute durchführen kann, nachdem von den Programminstruktionen 130 die erfolgreiche Authentifizierung auch des Nutzers 102 signalisiert worden ist.

Von besonderem Vorteil ist die Nutzbarmachung des ID-Tokens 106 für zum Beispiel E-Commerce und E-Government-Anwendungen, und zwar medienbruchfrei und rechtssicher aufgrund des durch die Notwendigkeit der Authentifizierung des Nutzers 102 und des ID-Provider-Computersystems 136 gegenüber dem ID-Token 106 gebildeten Vertrauensankers. Von besonderem Vorteil ist ferner, dass eine zentrale Speicherung der Attribute verschiedener Nutzer 102 nicht erforderlich ist, sodass die im Stand der Technik bestehenden Datenschutzprobleme hiermit gelöst sind. Was die Bequemlichkeit der Anwendung des Verfahrens betrifft, ist von besonderem Vorteil, dass eine vorherige Registrierung des Nutzers 102 zur Inanspruchnahme des ID-Provider-Computersystems 136 nicht erforderlich ist.

Vorzugsweise ist das ID-Provider-Computersystem 136 zur Nutzung durch eine Vielzahl von Nutzern ausgebildet. In diesem Fall erfolgt eine Zuordnung des Nutzer-Computersystems 100 des Nutzers 102 zu dem Mobilfunkgerät 101 desselben Nutzers 102, damit das ID-Provider-Computersystem 136 die aus dem ID-Token 106 des Nutzers 102 gelesenen Attribute an das Nutzer-Computersystem 100 dieses Nutzers 102 und nicht eines anderen Nutzers sendet.

Um eine solche Zuordnung herzustellen, wird beispielsweise wie folgt vorgegangen:

Zunächst wird von dem Nutzer-Computersystem 100 eine Dienst-Anforderung 164 über das Netzwerk 116 an das Dienst-Computersystem 150 gesendet. Das Dienst-Computersystem 150 antwortet auf die Dienst-Anforderung 164 mit der Anforderung zumindest eines Attributs des Nutzers 102 des Nutzer-Computersystems 100, beispielsweise also mit einer Attributspezifizierung 166. Diese Attributspezifizierung 166 sendet das Dienst-Computersystem 150 über das Netzwerk 116 an das Nutzer-Computersystem 100.

Zwischen dem Nutzer-Computersystem 100 und dem ID-Provider-Computersystem 136 wird über das Netzwerk 116 dann eine erste Verbindung aufgebaut, indem beispielsweise der Nutzer 102 in ein Browser-Programm des Nutzer-Computersystems 100 die URL des ID-Provider-Computersystems 136 eingibt. Über diese erste Verbindung wird dann die Attributspezifizierung 166 als Nachricht von dem Nutzer-Computersystem 100 an das ID-Provider-Computersystem 136 gesendet.

Das ID-Provider-Computersystem 136 generiert daraufhin eine Kennung, die dem Nutzer-Computersystem 100 zugeordnet ist. Bei der Kennung kann es sich um eine eindeutige Kennung, wie zum Beispiel eine GUID, einen Schlüssel, wie zum Beispiel einen symmetrischen oder asymmetrischen Schlüssel, handeln. Eine solche Kennung 174 sendet das ID-Provider-Computersystem 136 über die erste Verbindung an das Nutzer-Computersystem 100 zurück.

Die Kennung 174 wird dann von dem Nutzer-Computersystem 100 zu dem Mobilfunkgerät 101 übertragen. Beispielsweise sendet das Nutzer-Computersystem 100 hierzu die Kennung 174 von seiner Schnittstelle 104 an die entsprechende Schnittstelle 105 des Mobilfunkgeräts 101.

Von dem Mobilfunkgerät 101 wird dann eine Mobilfunkverbindung über das Netzwerk 116 mit dem ID-Provider-Computersystem 136 aufgebaut, beispielsweise indem der Nutzer 102 des Mobilfunkgeräts 101 die URL des ID-Provider-Computersystems 136 in ein Webbrowser-Programm des Mobilfunkgeräts 101, welches durch die Programminstruktionen 112 gebildet wird, eingibt. Durch die Mobilfunkverbindung wird also eine zweite Verbindung hergestellt.

Über die zweite Verbindung sendet das Mobilfunkgerät 101 die Kennung 174 an das ID-Provider-Computersystem 136. Da diese Kennung 174 identisch ist mit derdem Nutzer-Computersystem 100 zugeordneten Kennung 174, baut das ID-Provider-Computersystem 136 die geschützte Verbindung 172 mit Hilfe dieser zweiten Verbindung auf, um das oder die in der Attributspezifizierung 166 spezifizierten Attribute 176 aus dem ID-Token 106 auszulesen.

Nachdem das ID-Provider-Computersystem 136 die Attribute 176 von dem ID-Token 106 über die geschützte Verbindung 172 empfangen hat, so signiert es diese Attribute 176 mit Hilfe seines Zertifikats 144. Daraufhin sendet das ID-Provider-Computersystem 136 eine Antwort 170 über die erste Verbindung an das Nutzer-Computersystem 100, wobei die Antwort die Attribute 176 und deren Signatur beinhaltet. Die Antwort 170 kann auch eine Signatur der Kennung 174 und/oder die Kennung 174 selbst und/oder eine über eine Verkettung der Attribute 176 und der Kennung 174 gebildete Signatur aufweisen.

Von dem Nutzer-Computersystem 100 kann die Antwort 170 dann an das Dienst-Computersystem 150 weitergeleitet werden, welches somit in vertrauenswürdiger Art und Weise von dem in der Attributspezifizierung 166 genannten Attributen und

ggf. der Kennung Kenntnis erhält und dann den in der Dienst-Anforderung 164 spezifizierten Dienst erbringen kann.

Alternativ kann die Antwort 170 auch unmittelbar von dem ID-Provider-Computersystem 136 an das Dienst-Computersystem 150 über das Netzwerk 116 übermittelt werden.

Nach einer Ausführungsform wird die Kennung 174 in einem nichtflüchtigen Speicher des Nutzer-Computersystems 100, wie zum Beispiel in einem Festplattenspeicher des Nutzer-Computersystems 100, gespeichert, wie zum Beispiel in Form eines sogenannten Cookies 178. Ferner wird die Antwort 170 in einem nichtflüchtigen Speicher des Dienst-Computersystems 150 gespeichert.

Wenn der Nutzer 102 mittels seines Nutzer-Computersystems 100 zu einem späteren Zeitpunkt erneut eine weitere Dienst-Anforderung 164 an das Dienst-Computersystem 150 richtet, so kann das Dienst-Computersystem 150 über das Netzwerk 116 auf den Cookie 178 zugreifen und so die Kennung 174 aus dem Nutzer-Computersystem 100 auslesen. Wenn diese Kennung ebenfalls Teil der Antwort 170 ist, welche in dem Dienst-Computersystem 150 gespeichert ist, so ist das Dienst-Computersystem 150 dann bereits in Besitz der für die Erbringung des gewünschten Dienstes für den Nutzer 102 erforderlichen Attribute, da es diese gespeicherte Antwort über die Kennung dem Nutzer 102 zuordnen kann.

Nach einer Ausführungsform der Erfindung hat die Kennung 174 eine z.B. hinsichtlich der Zeitdauer oder der Anzahl von Nutzungen der gespeicherten Antwort 170 begrenzte Gültigkeit. Die maximale Gültigkeit der Kennung 174 kann zum Beispiel in Form eines Verfallsdatums in der Antwort 170 angegeben sein. Wenn dieses Verfallsdatum erreicht oder überschritten ist, kann das Dienst-Computersystem 150 die in dem Dienst-Computersystem 150 gespeicherte Antwort nicht mehr verwenden, sondern muss aufgrund einer nachfolgenden weiteren Dienst-Anforderung 164 mit der Attributspezifizierung 166 antworten, sodass der oben beschriebene Ablauf zum Auslesen des oder der Attribute aus dem ID-Token 106 erneut durchgeführt wird.

Die Figur 2 zeigt eine Ausführungsform eines erfindungsgemäßen Verfahrens. In dem Schritt 200 wird eine Dienst-Anforderung von dem Nutzer-Computersystem an das Dienst-Computersystem gesendet. Beispielsweise startet der Nutzer hierzu einen Internet-Browser des Nutzer-Computersystems und gibt eine URL zum Aufruf einer Webseite des Dienst-Computersystems ein. In die aufgerufene Webseite gibt der Nutzer dann seine Dienst-Anforderung ein, zum Beispiel zur Bestellung oder Auftragserteilung für einen Dienst oder ein Produkt.

In dem Schritt 201 spezifiziert das Dienst-Computersystem 150 daraufhin ein oder mehrere Attribute, welche es benötigt, um die Berechtigung des Nutzers für die Dienst-Anforderung zu prüfen. Insbesondere kann das Dienst-Computersystem solche Attribute spezifizieren, welche die digitale Identität des Nutzers 102 bestimmen. Diese Spezifizierung der Attribute durch das Dienst-Computersystem 150 kann fest vorgegeben sein oder je nach der Dienst-Anforderung im Einzelfall durch das Dienst-Computersystem 150 anhand vorgegebener Regeln bestimmt werden.

In dem Schritt 202 wird die Attributspezifikation, d.h. die in dem Schritt 201 erfolgte Spezifizierung der ein oder mehreren der Attribute, von dem Dienst-Computersystem an das ID-Provider-Computersystem übertragen, und zwar entweder direkt oder über das Nutzer-Computersystem.

Beispielsweise empfängt das Nutzer-Computersystem von dem Dienst-Computersystem die Attributspezifikation und baut daraufhin eine erste Verbindung über das Netzwerk zu dem ID-Provider-Computersystem auf. Das Nutzer-Computersystem sendet dann die Attributspezifikation über die erste Verbindung an das ID-Provider-Computersystem. In dem Schritt 203 erzeugt das ID-Provider-Computersystem daraufhin eine Kennung, die es dem Nutzer-Computersystem zuordnet, von dem es die Attributspezifikation erhalten hat. Diese Zuordnung wird durch das ID-Provider-Computersystem gespeichert. In dem Schritt 204 wird die Kennung von dem ID-Provider-Computersystem an das Nutzer-Computersystem

gesendet, wie zum Beispiel über die erste Verbindung, die zum Beispiel als eine sogenannte Session ausgebildet sein kann.

In dem Schritt 205 wird die Kennung von dem Nutzer-Computersystem an das Mobilfunkgerät übertragen. Dies kann automatisch erfolgen, wie zum Beispiel über eine NFC-Kommunikation zwischen dem Nutzer-Computersystem und dem Mobilfunkgerät oder auf einem anderen Kommunikationskanal, wie zum Beispiel optisch. Beispielsweise wird die Kennung auf einem Monitor des Nutzer-Computersystems angezeigt und von einer Kamera des Mobilfunkgeräts optisch erfasst.

In dem Schritt 206 wird zwischen dem Mobilfunkgerät und dem ID-Provider-Computersystem eine Mobilfunkverbindung aufgebaut und die Kennung über die Mobilfunkverbindung von dem Mobilfunkgerät an das ID-Provider-Computersystem übertragen. Da die Kennung, die das ID-Provider-Computersystem in dem Schritt 206 über die Mobilfunkverbindung empfängt, identisch ist mit der in dem Schritt 203 erzeugten und dem Nutzer-Computersystem zugeordneten Kennung, ist damit die Mobilfunkverbindung und der über die Mobilfunkverbindung von dem ID-Provider-Computersystem auslesbare ID-Token ebenfalls dem Nutzer-Computersystem bzw. dessen Nutzer zugeordnet.

Um dem ID-Provider-Computersystem die Möglichkeit zu geben, Attribute aus seinem ID-Token auszulesen, authentifiziert sich der Nutzer in dem Schritt 207 gegenüber dem ID-Token.

In dem Schritt 208 wird eine geschützte Verbindung zwischen dem ID-Token und dem ID-Provider-Computersystem aufgebaut (vgl. Verbindung 172 in Fig. 1). Hierbei handelt es sich vorzugsweise um eine Verbindung mit Ende-zu-Ende-Verschlüsselung, beispielsweise nach einem so genannten Secure Messaging-Verfahren.

In dem Schritt 210 erfolgt zumindest eine Authentifizierung des ID-Provider-Computersystems gegenüber dem ID-Token über die in dem Schritt 208 aufgebaute

geschützte Verbindung. Zusätzlich kann eine Authentifizierung auch des ID-Tokens gegenüber dem ID-Provider-Computersystem vorgesehen sein.

Nachdem sowohl der Nutzer als auch das ID-Provider-Computersystem erfolgreich gegenüber dem ID-Token authentifiziert worden sind, erhält das ID-Provider-Computersystem von dem ID-Token die Zugriffsberechtigung zum Auslesen der Attribute. In dem Schritt 212 sendet das ID-Provider-Computersystem ein oder mehrere Lesekommandos zum Auslesen der gemäß Attributspezifikation erforderlichen Attribute aus dem ID-Token. Die Attribute werden dann beispielsweise mittels Ende-zu-Ende-Verschlüsselung über die gesicherte Verbindung an das ID-Provider-Computersystem übertragen und dort entschlüsselt.

Die ausgelesenen Attributwerte werden in dem Schritt 214 von dem ID-Provider-Computersystem signiert. In dem Schritt 216 sendet das ID-Provider-Computersystem die signierten Attributwerte über das Netzwerk. Die signierten Attributwerte erreichen das Dienst-Computersystem entweder direkt oder über das Nutzer-Computersystem. Im letzteren Fall kann der Nutzer die Möglichkeit haben, die signierten Attributwerte zur Kenntnis zu nehmen und/oder durch weitere Daten zu ergänzen. Es kann vorgesehen sein, dass die signierten Attributwerte gegebenenfalls mit den ergänzten Daten erst nach Freigabe durch den Nutzer von dem Nutzer-Computersystem an das Dienst-Computersystem weitergeleitet werden. Hierdurch ist größtmögliche Transparenz für den Nutzer hinsichtlich der von dem ID-Provider-Computersystem an das Dienst-Computersystem gesendeten Attribute hergestellt.

Zusätzlich kann auch die Kennung in dem Schritt 214 von dem ID-Provider-Computersystem signiert und in dem Schritt 216 über das Netzwerk an das Dienst-Computersystem oder das Nutzer-Computersystem gesendet werden.

Die Figur 3 zeigt eine weitere Ausführungsform eines erfindungsgemäßen Verfahrens. Durch eine Nutzereingabe eines Nutzers 102 in ein Nutzer-Computersystem 100 spezifiziert der Nutzer 102 einen Dienst eines Dienst-

Computersystems, welchen er oder sie in Anspruch nehmen möchte. Dies erfolgt beispielsweise durch Aufruf einer Internetseite des Dienst-Computersystems und einer Auswahl eines der dort angebotenen Dienste. Die Dienst-Anforderung des Nutzers 102 wird von dem Nutzer-Computersystem 100 an das Dienst-Computersystem 150 übertragen.

Das Dienst-Computersystem 150 antwortet auf die Dienst-Anforderung mit einer Attributspezifizierung, d.h. beispielsweise einer Liste von Attributnamen. Nach Empfang der Attributspezifizierung fordert das Nutzer-Computersystem 100 den Nutzer 102, beispielsweise durch eine Eingabeaufforderung, zur Authentifizierung gegenüber dem ID-Token 106 auf.

Der Nutzer schaltet daraufhin sein Mobilfunkgerät 101 ein und authentifiziert sich zunächst gegenüber seinem Mobilfunkgerät 101. Danach authentifiziert sich der Nutzer 102 gegenüber dem ID-Token 106, beispielsweise durch Eingabe seiner PIN in eine Tastatur des Mobilfunkgeräts 101. Das Mobilfunkgerät 101 überträgt die von dem Nutzer 102 eingegebene PIN von seiner Schnittstelle 105 (vgl. Figur 1) an den ID-Token 106.

Die Attributspezifizierung wird von dem Nutzer-Computersystem 100 an ein ID-Provider-Computersystem 136 weitergeleitet. Das ID-Provider-Computersystem 136 generiert daraufhin eine Kennung, die das ID-Provider-Computersystem dem Nutzer-Computersystem 100 zuordnet und an das Nutzer-Computersystem 100 sendet. Die Zuordnung der Kennung zu dem Nutzer-Computersystem 100 wird von dem ID-Provider-Computersystem 136 gespeichert.

Die Kennung wird dann von dem Nutzer-Computersystem 100 zu dem Mobilfunkgerät 101 übertragen. Dies kann manuell erfolgen, indem der Nutzer 102 die auf einer Anzeige des Nutzer-Computersystems 100 angezeigte Kennung abliest und über eine Tastatur des Mobilfunkgeräts 101 in das Mobilfunkgerät 101 eingibt. Die Übertragung kann auch vollautomatisch ohne Involvierung des Nutzers 102 oder teilautomatisch erfolgen, und zwar beispielsweise durch eine Funkübertragung der Ken-

nung von dem Nutzer-Computersystem 100 zu dem Mobilfunkgerät 101 über das Netzwerk 116 (vgl. Figur 1) oder über eine NFC-Kommunikationsverbindung, die zwischen dem Nutzer-Computersystem 100 und dem Mobilfunkgerät 101 aufgebaut wird.

Ferner kann die Übertragung der Kennung zwischen dem Nutzer-Computersystem und dem Mobilfunkgerät 101 auch auf optischem Wege erfolgen, beispielsweise indem die im Klartext auf der Anzeige des Nutzer-Computersystems 100 angezeigte Kennung oder die als 2D-Barcode angezeigte Kennung mit Hilfe einer Kamera des Mobilfunkgeräts 101 optisch erfasst wird.

Zwischen dem Mobilfunkgerät 101 und dem ID-Provider-Computersystem 136 wird eine Mobilfunkverbindung aufgebaut, über die die Kennung von dem Mobilfunkgerät 101 zu dem ID-Provider-Computersystem 136 übertragen wird. Aufgrund der in dem ID-Provider-Computersystem 136 gespeicherten Zuordnung der Kennung zu dem Nutzer-Computersystem 100 ist damit auch diese Mobilfunkverbindung dem Nutzer-Computersystem 100 zugeordnet.

Das ID-Provider-Computersystem 136 kommuniziert dann über die Mobilfunkverbindung und das Mobilfunkgerät 101 mit dem ID-Token 106, um sich gegenüber dem ID-Token 106 zu authentifizieren und um eine Leseanforderung zum Lesen der Attribute gemäß der Attributspezifizierung an den ID-Token 106 zu richten.

Unter der Voraussetzung der vorherigen erfolgreichen Authentifizierung des Nutzers 102 und des ID-Provider-Computersystems 136 antwortet der ID-Token 106 auf die Leseanforderung mit den gewünschten Attributen. Das ID-Provider-Computersystem 136 signiert die Attribute und sendet die signierten Attribute an das Nutzer-Computersystem 100. Nach Freigabe durch den Nutzer 102 werden die signierten Attribute dann an das Dienst-Computersystem 150 übertragen, welches dann ggf. den gewünschten Dienst erbringen kann.

Neben den Attributen kann das ID-Provider-Computersystem 136 auch die Kennung signieren und zusammen mit den signierten Attributen an das Nutzer-Computersystem 100 senden.

Die Figur 4 zeigt eine weitere Ausführungsform eines erfindungsgemäßen Verfahrens. Von der Ausführungsform gemäß Figur 3 unterscheidet sich die Ausführungsform der Figur 4 insbesondere dadurch, dass das ID-Provider-Computersystem 136 die Kennung, welche es nach Empfang der Attributspezifikation von dem Nutzer-Computersystem 100 generiert, nicht an das Nutzer-Computersystem 100 sendet, sondern an das Mobilfunkgerät 101. Die Kennung wird dann von dem Mobilfunkgerät 101 an das Nutzer-Computersystem 100 übertragen, und zwar wiederum entweder manuell durch den Nutzer 102 oder automatisch oder teilautomatisch, z.B. über einen Funkkanal oder einen optischen Kanal.

Das Nutzer-Computersystem 100 sendet die Kennung dann an das ID-Provider-Computersystem 136, sodass die der Kennung zugeordnete Mobilfunkverbindung zwischen dem Mobilfunkgerät 101 und dem ID-Provider-Computersystem 136 auch dem Nutzer-Computersystem 100 zugeordnet ist.

In einem weiteren Ausführungsvariante ist es möglich, dass die Attributspezifizierung von dem Nutzer-Computersystem 100 an das Mobilfunkgerät 101 übertragen wird, und zwar manuell oder automatisch, und dass die Attributspezifizierung statt von dem Nutzer-Computersystem 100 von dem Mobilfunkgerät 101 an das ID-Provider-Computersystem 136 gesendet wird.

Ferner ist es auch möglich, dass das ID-Provider-Computersystem die Kennung sowohl an das Mobilfunkgerät 101 als auch an das Nutzer-Computersystem 100 überträgt. Die Übertragung der Kennung kann dann wahlweise von dem Mobilfunkgerät 101 an das Nutzer-Computersystem 100 oder in der anderen Richtung erfolgen.

Bezugszeichenliste

100	Nutzer-Computersystem
101	Mobilfunkgerät
102	Nutzer
104	Schnittstelle
105	Schnittstelle
106	ID-Token
108	Schnittstelle
110	Prozessor
111	Prozessor112 Programminstruktionen
113	Programminstruktionen
114	Netzwerk-Schnittstelle
115	Mobilfunk-Schnittstelle
116	Netzwerk
118	elektronischer Speicher
120	geschützter Speicherbereich
122	geschützter Speicherbereich
124	geschützter Speicherbereich
126	Speicherbereich
128	Prozessor
130	Programminstruktionen
132	Programminstruktionen
134	Programminstruktionen
136	ID-Provider-Computersystem
138	Netzwerk-Schnittstelle
140	Speicher
142	privater Schlüssel
144	Zertifikat
145	Prozessor
146	Programminstruktionen

148	Programminstruktionen
149	Programminstruktionen
150	Dienst-Computersystem
152	Netzwerk-Schnittstelle
154	Prozessor
156	Programminstruktionen
158	Konfigurationsdatensatz
160	Konfigurationsdatensatz
161	Konfigurationsdatensatz
162	Nutzereingabe
164	Dienst-Anforderung
166	Attributspezifizierung
168	Anforderung
170	Antwort
172	Verbindung
174	Kennung
176	Attribut
178	Cookie

Patentansprüche

1. Verfahren zum Lesen zumindest eines in einem ID-Token (106, 106') gespeicherten Attributs, wobei der ID-Token einem Nutzer (102) zugeordnet ist und wobei der ID-Token eine erste Schnittstelle (108) aufweist, mit folgenden Schritten:

   - Authentifizierung des Nutzers gegenüber dem ID-Token,

   - Aufbau einer Mobilfunkverbindung zwischen einem Mobilfunkgerät (101) und einem ersten Computersystem (136), wobei das Mobilfunkgerät eine zweite Schnittstelle (105) aufweist,

   - Aufbau einer geschützten Verbindung (172) über die Mobilfunkverbindung und über die ersten und zweiten Schnittstellen zwischen dem ersten Computersystems und dem ID-Token,

   - Authentifizierung des ersten Computersystems (136) gegenüber dem ID-Token über die geschützte Verbindung,

   - nach erfolgreicher Authentifizierung des Nutzers und des ersten Computersystems gegenüber dem ID-Token, Lesezugriff des ersten Computersystems auf das zumindest eine in dem ID-Token gespeicherte Attribut zur Übertragung des zumindest einen Attributs nach dessen Signierung über ein Netzwerk (116).

2. Verfahren nach Anspruch 1, wobei die Authentifizierung des ersten Computersystems gegenüber dem ID-Token mit Hilfe eines Zertifikats (144) des ersten Computersystems erfolgt, wobei das Zertifikat eine Angabe derjenigen in dem ID-Token gespeicherten Attribute beinhaltet, für welche das erste Computersystem für den Lesezugriff berechtigt ist.

3. Verfahren nach Anspruch 2, wobei der ID-Token die Leseberechtigung des ersten Computersystems für den Lesezugriff auf zumindest eines der Attribute mit Hilfe des Zertifikats überprüft.

4. Verfahren nach einem der Ansprüche 1, 2 oder 3, mit folgenden weiteren Schritten:

- Signierung des zumindest einen aus dem ID-Token gelesenen Attributs durch das erste Computersystem,

- Übertragung des signierten Attributs von dem ersten Computersystem an ein zweites Computersystem (150) oder ein drittes Computersystem (100).

5. Verfahren nach Anspruch 4, mit folgenden weiteren Schritten:

- Senden einer Anforderung (164) von einem dritten Computersystem (100) an das zweite Computersystem,

- Spezifizierung eines oder mehrerer Attribute durch das zweite Computersystem,

- Senden der Attributspezifizierung (166) von dem zweiten Computersystem an das erste Computersystem,

wobei der Lesezugriff des ersten Computersystems erfolgt, um die in der Attributspezifizierung spezifizierten ein oder mehrere Attribute aus dem ID-Token auszulesen.

6. Verfahren nach Anspruch 5, mit folgenden weiteren Schritten:

- Senden einer Nachricht von dem dritten Computersystem (100) an das erste Computersystem (136),

- Erzeugung einer Kennung aufgrund der Nachricht durch das erste Computersystem,

- Senden der Kennung von dem ersten Computersystem an das dritte Computersystem,

- Übertragung der Kennung von dem dritten Computersystem an das Mobilfunkgerät,

- Übertragung der Kennung von dem Mobilfunkgerät an das erste Computersystem über die Mobilfunkverbindung.

7. Verfahren nach Anspruch 5 oder 6, mit folgenden weiteren Schritten:

- Erzeugung einer Kennung durch das erste Computersystem,,

- Senden der Kennung von dem ersten Computersystem an das Mobilfunkgerät über die Mobilfunkverbindung,

- Übertragung der Kennung von dem Mobilfunkgerät an das dritte Computersystem,

- Senden der Kennung von dem dritten Computersystem an das erste Computersystem.

8. Verfahren nach Anspruch 6 oder 7, wobei das erste Computersystem das zumindest eine signierte Attribut an das durch die Kennung identifizierte dritte Computersystem sendet.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei die geschützte Verbindung eine Ende-zu-Ende-Verschlüsselung zwischen dem ID-Token und dem ersten Computersystem aufweist.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei die ersten und zweiten Schnittstellen für eine drahtlose Kommunikation ausgebildet sind, wobei die Reichweite weniger als 1 m, insbesondere weniger als 20 cm beträgt, und wobei die ersten und zweiten Schnittstellen insbesondere nach einem Near Field Communication (NFC) und/oder ISO/IEC 1443A Standard ausgebildet sein können.

11. Verfahren nach einem der vorhergehenden Ansprüche 6 bis 10, wobei die Übertragung der Kennung zwischen dem dritten Computersystem und dem Mobilfunkgerät optisch erfolgt.

12. Verfahren nach Anspruch 11, wobei die Kennung auf einer Anzeigevorrichtung angezeigt und mit einem optischen Sensor erfasst wird.

13. Verfahren nach Anspruch 12, wobei die Kennung als maschinenlesbares Muster, insbesondere als Barcode, vorzugsweise als 2D Barcode, angezeigt wird.

14. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Kennung von dem dritten Computersystem an das Mobilfunkgerät über eine Funkfrequenz übertragen wird.

15. Verfahren nach einem der vorhergehenden Ansprüche 6 bis 14, wobei die Kennung in einem nichtflüchtigen Speicher des dritten Computersystems ge-

speichert wird, insbesondere als Cookie (178), und wobei das zumindest eine Attribut und die Kennung von dem ersten Computersystem signiert und zusammen mit dieser Signatur über das Netzwerk übertragen werden.

16. Verfahren nach einem der vorhergehenden Ansprüche 6 bis 15, wobei die Kennung eine zeitlich und/oder hinsichtlich der Anzahl der Nutzungen beschränkte Gültigkeit hat.

17. Verfahren nach einem der vorhergehenden Ansprüche, wobei das zumindest eine von dem ersten Computersystem aus dem ID-Token gelesene Attribut an das dritte Computersystem gesendet wird, von wo es nach Freigabe durch den Nutzer an das zweite Computersystem weitergesendet wird.

18. Verfahren nach Anspruch 17, wobei der Nutzer die Attribute vor der Weiterleitung an das zweite Computersystem durch weitere Daten ergänzen kann.

19. Computerprogrammprodukt mit von einem ersten Computersystem (136) ausführbaren Instruktionen zur Durchführung der folgenden Schritte:

- Aufbau einer ersten Verbindung zwischen dem ersten Computersystem und einem dritten Computersystem (100) über ein Netzwerk (116),

- Aufbau einer zweiten Verbindung zwischen dem ersten Computersystem und einem Mobilfunkgerät (101), wobei es sich bei der zweiten Verbindung um eine Mobilfunkverbindung handelt,

- Erzeugung einer Kennung durch das erste Computersystem,

- Senden der Kennung über eine der ersten und zweiten Verbindungen von dem ersten Computersystem,

- Empfang der Kennung von dem ersten Computersystem über die andere der ersten und zweiten Verbindungen,

- Aufbau einer geschützten Verbindung (172) zwischen dem ersten Computersystem und einem ID-Token (106), wobei der ID-Token eine erste Schnittstelle (108) aufweist, wobei die geschützte Verbindung über die Mobilfunkverbindung und über die erste Schnittstelle und eine zweite Schnittstelle (105) des Mobilfunkgeräts aufgebaut wird,

- Authentifizierung des ersten Computersystems gegenüber dem ID-Token über die geschützte Verbindung,

- nach erfolgreicher Authentifizierung des ersten Computersystems gegenüber dem ID-Token, Lesezugriff des ersten Computersystems auf zumindest ein in dem ID-Token gespeichertes Attribut zur Übertragung des zumindest einen Attributs nach dessen Signierung über das Netzwerk.

20. Computerprogrammprodukt nach Anspruch 19, wobei das signierte Attribut von dem ersten Computersystem an das dritte Computersystem gesendet wird.

21. Computerprogrammprodukt nach Anspruch 20, wobei die von dem ersten Computersystem signierte Kennung an das dritte Computersystem gesendet wird.

22. ID-Token mit

- einer ersten Schnittstelle (108) zur Kommunikation mit einem Mobilfunkgerät (101),

- einem geschützten Speicherbereich (124) zur Speicherung von zumindest einem Attribut,

- Mitteln (120, 130) zur Authentifizierung eines dem ID-Token zugeordneten Nutzers (102) gegenüber dem ID-Token,

- Mitteln (134) zur Authentifizierung eines ersten Computersystems (136) gegenüber dem ID-Token,

- Mitteln (132) zum Aufbau einer geschützten Verbindung (172) über das Mobilfunkgerät zu dem ersten Computersystem, über die das erste Computersystem das zumindest eine Attribut auslesen kann,

wobei eine notwendige Voraussetzung für das Auslesen des zumindest einen Attributs aus dem ID-Token durch das erste Computersystem die erfolgreiche Authentifizierung des Nutzers und des ersten Computersystems gegenüber dem ID-Token ist.

23. ID-Token nach Anspruch 22, mit Mitteln (132) zur Ende-zu-Ende-Verschlüsselung der Verbindung für eine geschützte Übertragung des zumindest einen der Attribute zu dem ersten Computersystem.

24. ID-Token nach Anspruch 22 oder 23, wobei es sich um ein elektronisches Gerät, insbesondere einen USB-Stick, oder ein Dokument, insbesondere ein Wert- oder Sicherheitsdokument, handelt.

25. Computersystem mit

- Mitteln (138) zum Empfang einer Nachricht über ein Netzwerk (116), wobei durch die Nachricht zumindest ein Attribut angefordert wird,

- Mitteln (142, 144, 146) zur Authentifizierung gegenüber einem ID-Token (106) über eine Mobilfunkverbindung,

- Mitteln (138, 145) zum Lesen zumindest einen Attributs aus dem ID-Token über eine geschützte Verbindung (172),

wobei das Lesen des zumindest einen Attributs voraussetzt, dass sich ein dem ID-Token zugeordneter Nutzer (102) und das Computersystem gegenüber dem ID-Token authentifiziert haben.

26. Computersystem nach Anspruch 25, mit Mitteln (145) zur Generierung einer Anforderung an den Nutzer zur Authentifizierung gegenüber dem ID-Token aufgrund des Empfangs der Nachricht.

27. Computersystem nach Anspruch 25 oder 26, mit Mitteln (145) zur Erzeugung einer Kennung durch welche die Nachricht und die Mobilfunkverbindung eindeutig einander zugeordnet werden und mit Mitteln (138, 145) zum Senden des zumindest einen aus dem ID-Token gelesenen Attributs.

28. Computersystem nach Anspruch 25, 26 oder 27, mit Mitteln (144) zum Signieren des zumindest einen Attributs und/oder der Kennung, wobei das signierte Attribut und/oder die signierte Kennung gesendet werden.

Fig. 1

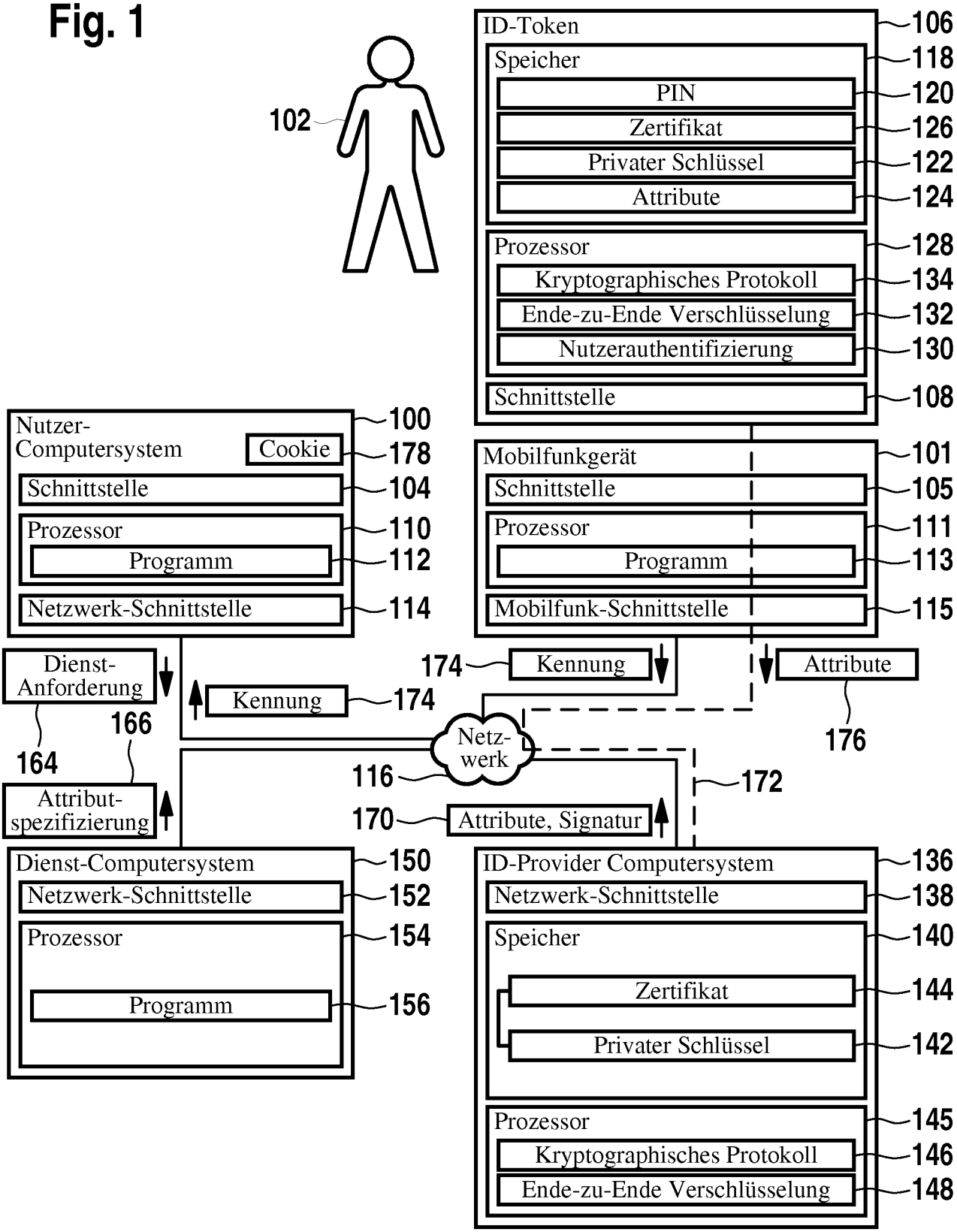
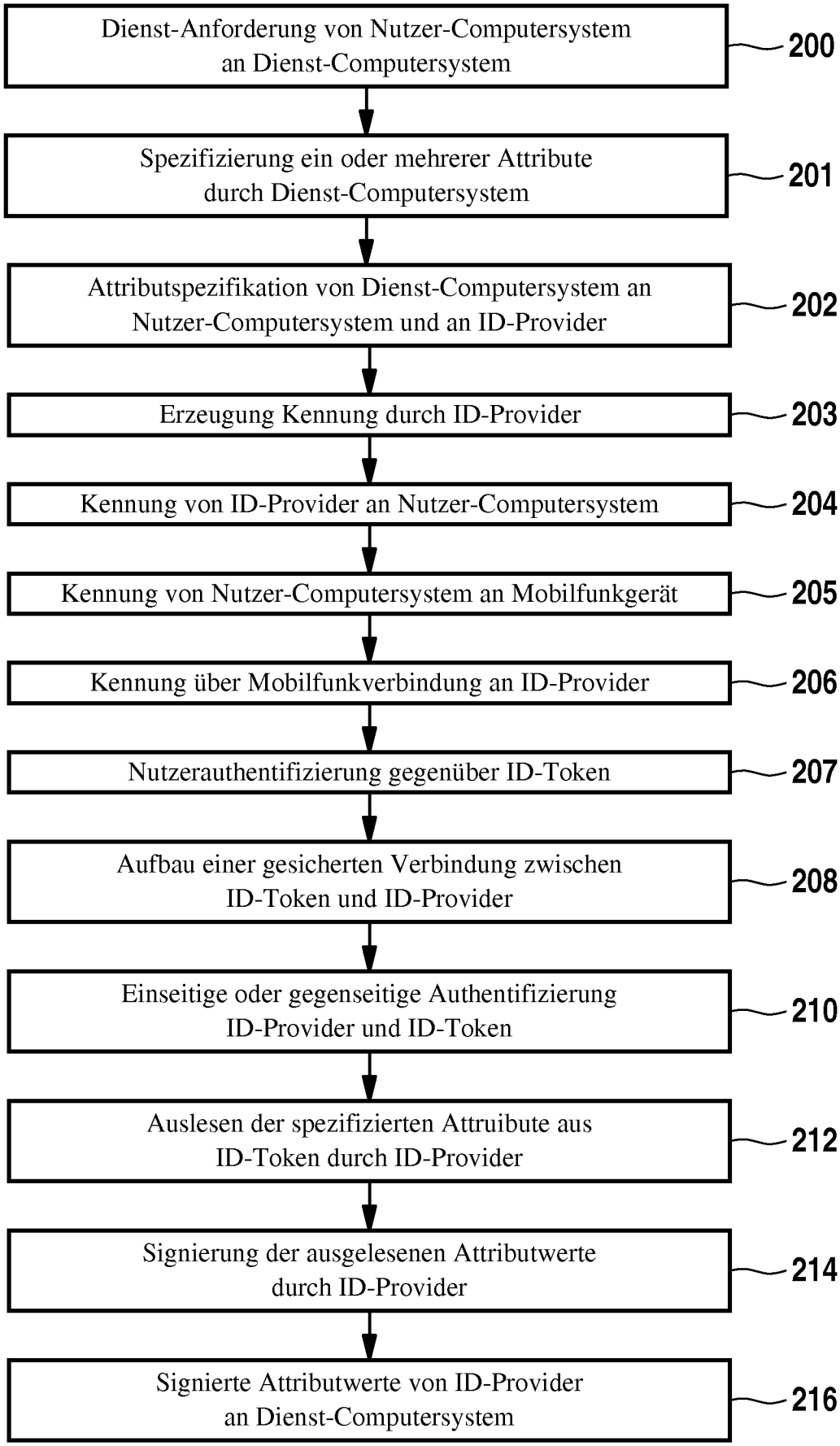

102
ID-Token
106
Speicher
118
PIN
120
Zertifikat
126
Privater Schlüssel
122
Attribute
124
Prozessor
128
Kryptographisches Protokoll
134
Ende-zu-Ende Verschlüsselung
132
Nutzerauthentifizierung
130
Schnittstelle
108
Nutzer-Computersystem
100
Cookie
178
Schnittstelle
104
Prozessor
110
Programm
112
Netzwerk-Schnittstelle
114
Mobilfunkgerät
101
Schnittstelle
105
Prozessor
111
Programm
113
Mobilfunk-Schnittstelle
115
Dienst-Anforderung
164
166
Kennung
174
174
Kennung
Attribute
176
Netz-werk
116
172
Attribut-spezifizierung
170
Attribute, Signatur
Dienst-Computersystem
150
Netzwerk-Schnittstelle
152
Prozessor
154
Programm
156
ID-Provider Computersystem
136
Netzwerk-Schnittstelle
138
Speicher
140
Zertifikat
144
Privater Schlüssel
142
Prozessor
145
Kryptographisches Protokoll
146
Ende-zu-Ende Verschlüsselung
148

Fig. 2


Dienst-Anforderung von Nutzer-Computersystem an Dienst-Computersystem
200
Spezifizierung ein oder mehrerer Attribute durch Dienst-Computersystem
201
Attributspezifikation von Dienst-Computersystem an Nutzer-Computersystem und an ID-Provider
202
Erzeugung Kennung durch ID-Provider
203
Kennung von ID-Provider an Nutzer-Computersystem
204
Kennung von Nutzer-Computersystem an Mobilfunkgerät
205
Kennung über Mobilfunkverbindung an ID-Provider
206
Nutzerauthentifizierung gegenüber ID-Token
207
Aufbau einer gesicherten Verbindung zwischen ID-Token und ID-Provider
208
Einseitige oder gegenseitige Authentifizierung ID-Provider und ID-Token
210
Auslesen der spezifizierten Attruibute aus ID-Token durch ID-Provider
212
Signierung der ausgelesenen Attributwerte durch ID-Provider
214
Signierte Attributwerte von ID-Provider an Dienst-Computersystem
216

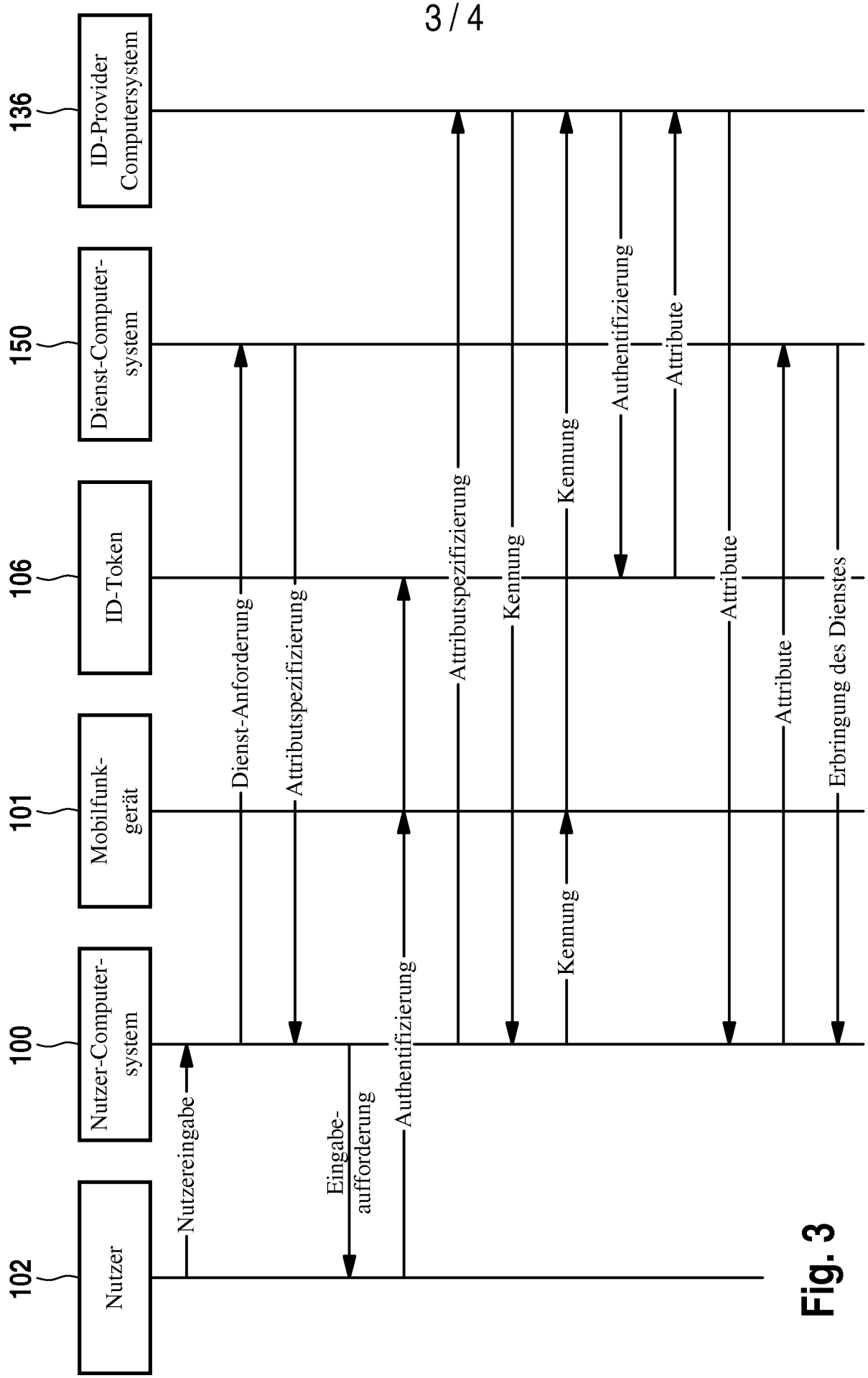

102
Nutzer
100
Nutzer-Computer-system
101
Mobilfunk-gerät
106
ID-Token
150
Dienst-Computer-system
136
ID-Provider Computersystem
Nutzereingabe
Eingabe-aufforderung
Authentifizierung
Dienst-Anforderung
Attributspezifizierung
Attributspezifizierung
Kennung
Kennung
Kennung
Authentifizierung
Attribute
Attribute
Attribute
Erbringung des Dienstes

Fig. 3

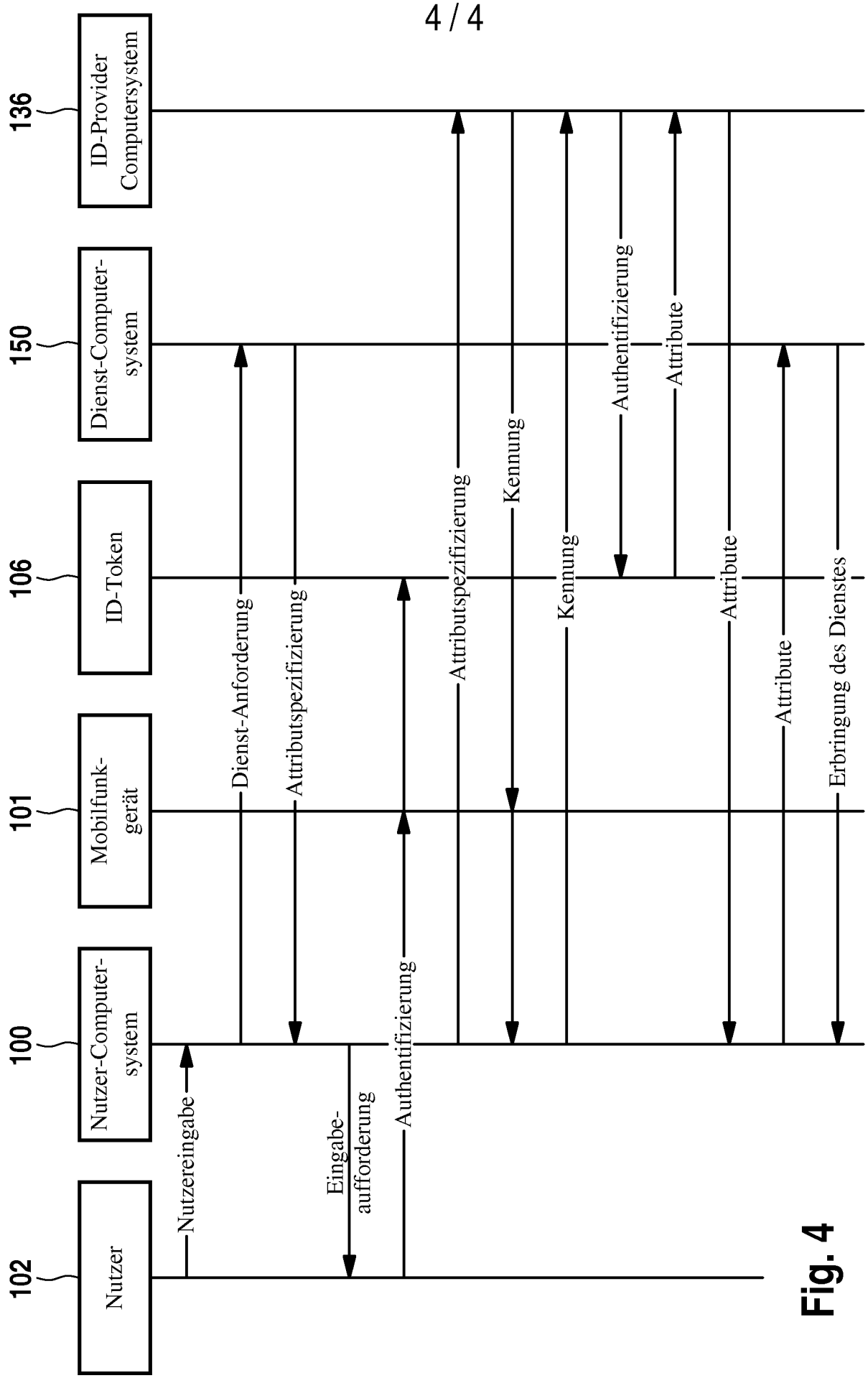

102
Nutzer
100
Nutzer-Computer-system
101
Mobilfunk-gerät
106
ID-Token
150
Dienst-Computer-system
136
ID-Provider Computersystem
Nutzereingabe
Eingabe-aufforderung
Authentifizierung
Dienst-Anforderung
Attributspezifizierung
Attributspezifizierung
Kennung
Kennung
Authentifizierung
Attribute
Attribute
Attribute
Erbringung des Dienstes

Fig. 4