



(10) **DE 10 2015 200 313 A1** 2016.07.14

(12)

Offenlegungsschrift

(21) Aktenzeichen: **10 2015 200 313.2**

(22) Anmeldetag: **13.01.2015**

(43) Offenlegungstag: **14.07.2016**

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

(62) Teilung in:
10 2015 017 060.0

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

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

(72) Erfinder:
**Schwan, Matthias, Dr., 10437 Berlin, DE; Müller,
Frank, 10435 Berlin, DE; Scholze, Steffen, 13469
Berlin, DE; Wirth, Klaus-Dieter, Dr., 12683 Berlin,
DE; Filzhuth, Elke, Dr., 12359 Berlin, DE**

(56) Ermittelter Stand der Technik:
siehe Folgeseiten

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

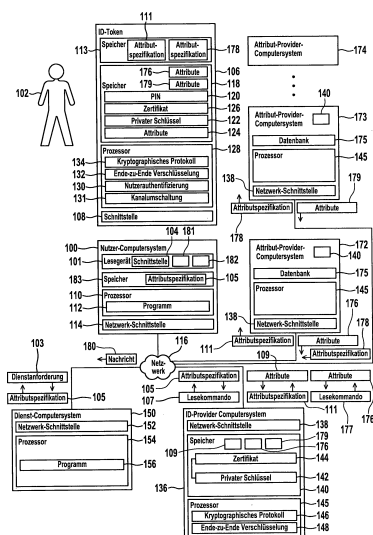
(54) Bezeichnung: **Verfahren zum Lesen von Attributen aus einem ID-Token**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Lesen von Attributen aus einem ID-Token mit folgenden Schritten:

- Authentifizierung des Nutzers gegenüber dem ID-Token und optional Aufbau eines gesicherten Übertragungskanals (SM-[PACE]) zwischen ID-Token und Nutzer-Computersystem,
- Gegenseitige Authentisierung und Aufbau eines ersten gesicherten Übertragungskanals (SM-[CA] #1) mit Ende-zu-Ende-Verschlüsselung zwischen dem ID-Token und dem ID-Provider-Computersystem über das Netzwerk,
- Durchführung eines ersten Lesezugriffs (107) des ID-Provider-Computersystems auf den ID-Token zum Lesen der Attribute gemäß der ersten Attributspezifikation aus dem ID-Token,
- Übertragung einer in dem Speicherbereich des ID-Tokens gespeicherten ersten Teilmenge der in der ersten Attributspezifikation spezifizierten Attribute (109) von dem ID-Token an das ID-Provider-Computersystem über den ersten gesicherten Übertragungskanal,
- Erzeugung einer zweiten Attributspezifikation (111) einer zweiten Teilmenge der Attribute der ersten Attributspezifikation, die diejenigen Attribute spezifiziert, welche in der ersten Teilmenge nicht beinhaltet sind und Übertragung der zweiten Attributspezifikation von dem ID-Provider-Computersystem an den ID-Token über den ersten gesicherten Übertragungskanal,
- Speicherung der zweiten Attributspezifikation in dem ID-Token,
- Authentifizierung eines Attribut-Provider-Computersystems (172) gegenüber dem ID-Token,
- Authentifizierung des ID-Tokens gegenüber dem Attribut-Provider-Computersystem,
- Aufbau eines zweiten gesicherten Übertragungskanals (SM-[CA] #2) mit Ende-zu-Ende-Verschlüsselung zwischen dem Attribut-Provider-Computersystem und dem ID-

Token, wobei der erste gesicherte Übertragungskanal bestehen bleibt,

- Übertragung der zweiten Attributspezifikation von dem ID-Token über den zweiten gesicherten Übertragungskanal an das Attribut-Provider-Computersystem,
- Durchführung eines Schreibzugriffs (176) des Attribut-Provider-Computersystems über den zweiten gesicherten Übertragungskanal zum Speichern von Attributen gemäß der zweiten Attributspezifikation in dem ID-Token,
- Optional Durchführung eines Schreibzugriffs (176) des Attribut-Provider-Computersystems über den zweiten gesicherten Übertragungskanal zum Speichern einer dritten Attributspezifikation in dem ID-Token für noch nicht geschriebene Attribute,
- Optional gegenseitige Authentisierung und Aufbau eines dritten gesicherten Übertragungskanals (SM-[CA] #3) mit Ende-zu-Ende-Verschlüsselung zwischen dem Attribut-Provider-Computersystem und dem ID-Token, wobei ...



(56) Ermittelter Stand der Technik:

DE 10 2008 042 262 A1

**Technical Guideline TR-03110-2, Advanced
Security Mechanisms for Machine Readable
Travel Documents and eIDAS Token – Part
2 – Protocols for electronic Identification,
Authentication and trust Services
(eIDAS), Bundesamt für Sicherheit in der
Informationstechnik BSI, Version 2.20 beta, 23.
September 2013, Seiten 1-25**

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Lesen von Attributen aus einem ID-Token, einen ID-Token und ein Computersystem.

[0002] 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.

[0003] 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.

[0004] Aus US 2007/0294431 A1 ist ein weiteres Verfahren zur Verwaltung der digitalen Identitäten bekannt, welches ebenfalls eine Nutzerregistrierung erfordert.

[0005] Aus DE 10 2008 000 067 A1 ist ein Verfahren zum Lesen von zumindest einem Attribut aus einem ID-Token bekannt, von dem die vorliegende Erfindung als dem nächstkommenden Stand der Technik ausgeht. Weiterbildungen dieses Verfahrens sind in den Patentanmeldungen DE 10 2008 040 416, DE 10 2008 042 262, DE 10 2009 026 953, DE 10 2009 027 723, DE 10 2009 027 681 und DE 10 2010 028 133 offenbart.

[0006] Der Erfindung liegt demgegenüber die Aufgabe zugrunde, ein verbessertes Verfahren zum Lesen von Attributen aus einem ID-Token zu schaffen sowie einen entsprechenden ID-Token und ein Computersystem.

[0007] Die der Erfindung zugrunde liegenden Aufgaben werden jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Ausführungsformen der Erfindung sind in den abhängigen Ansprüchen angegeben.

[0008] Unter einem „ID-Token“ wird hier insbesondere ein tragbares elektronisches Gerät verstanden, welches zumindest einen geschützten elektronischen Datenspeicher zur Speicherung der Attribute und eine Kommunikations-Schnittstelle zum Auslesen der Attribute aufweist. Der Speicherbereich ist geschützt, um zu verhindern, dass das in dem Speicherbereich gespeicherte Attribut in unerlaubter Weise verändert

oder ohne die dafür erforderliche Berechtigung ausgelesen wird. Mit anderen Worten kann auf den Speicherbereich nur dann zugegriffen werden, wenn eine hierzu erforderliche Zugriffsberechtigung gegeben ist.

[0009] Insbesondere kann es sich bei dem ID-Token um einen USB-Stick handeln oder ein Dokument, insbesondere ein Wert- oder Sicherheitsdokument. Unter einem „Dokument“ werden erfindungsgemäß papierbasierte und/oder kunststoffbasierte Dokumente verstanden, wie zum Beispiel elektronische Ausweisdokumente, insbesondere Reisepässe, Personalausweise, Visa sowie Führerscheine, Fahrzeugscheine, Fahrzeugbriefe, Firmenausweise, Gesundheitskarten oder andere ID-Dokumente sowie auch Chipkarten, Zahlungsmittel, insbesondere Banknoten, Bankkarten und Kreditkarten, Frachtbriefe oder sonstige Berechtigungsnachweise, in die ein Datenspeicher zur Speicherung des zumindest einen Attributs integriert ist.

[0010] Bei dem ID-Token kann es sich um einen Hardwaretoken handeln oder um einen Softtoken, wenn dieser kryptografisch an einen Hardwaretoken, das heißt beispielsweise an ein sogenanntes Secure Element, gebunden ist.

[0011] Insbesondere kann ein solcher kryptografisch an ein Secure Element gebundener Softtoken gemäß DE 10 2011 082 101, deren Offenbarungsgehalt voll umfänglich zum Offenbarungsgehalt der vorliegenden Patentanmeldung gemacht wird, erzeugt werden.

[0012] Unter einem „ID-Provider-Computersystem“ wird hier ein Computersystem verstanden, welches dazu ausgebildet ist, Attribute aus dem ID-Token eines Nutzers auszulesen und eine Attributspezifikation in den ID-Token zu schreiben. Vorzugsweise wird das ID-Provider-Computersystem in einem sogenannten Trustcenter betrieben, um ein möglichst hohes Maß an Sicherheit zu schaffen.

[0013] Unter einem „Attribut-Provider-Computersystem“ wird hier ein Computersystem verstanden, welches dazu ausgebildet ist, eine Attributspezifikation aus dem ID-Token eines Nutzers auszulesen und Attribute in den ID-Token zu schreiben.

[0014] Unter einem „Attribut“ werden hier insbesondere Daten verstanden, die den Nutzer des ID-Tokens oder den ID-Token selbst betreffen, insbesondere Personalisierungsdaten, wie zum Beispiel persönliche Daten des Nutzers, eine Gültigkeitsdauer oder den Herausgeber des ID-Tokens oder eine Zahlungsinformation, wie zum Beispiel Kreditkartendaten oder andere Daten für ein elektronisches Bezahlssystem.

[0015] Unter einer „Attributspezifikation“ wird hier eine Beschreibung von denjenigen Attributen verstanden, die zum Beispiel von einem Dienst-Computersystem zur Erbringung eines Dienstes benötigt werden. Die Attribute können über Feldnamen von Datenfeldern identifiziert werden, in denen die jeweiligen Attributwerte gespeichert sind, und/oder über ein semantisches Netz, d.h. eine Konvention, wie Attribute systemübergreifend bezeichnet werden.

[0016] Unter einem „Dienst-Computersystem“ wird hier ein Computersystem verstanden, welches über eine Netzwerk-Schnittstelle zur Verbindung mit dem Netzwerk verfügt, sodass mithilfe eines Internetbrowsers oder eines anderen Anwendungsprogramms auf von dem Dienst-Computersystem gespeicherte oder generierte Internetseiten zugegriffen werden kann. Insbesondere kann es sich bei dem Dienst-Computersystem um einen Internetserver zur Verfügungstellung einer eCommerce- oder eGovernment-Anwendung handeln, insbesondere einen Onlineshop oder einen Behördenserver.

[0017] Unter einem „Nutzer-Computersystem“ wird hier ein Computersystem verstanden, auf welches der Nutzer Zugriff hat. Hierbei kann es sich zum Beispiel um einen Personal Computer (PC), ein Tablet PC oder ein Mobilfunkgerät, insbesondere ein Smartphone, mit einem üblichen Internetbrowser, wie zum Beispiel Microsoft Internet Explorer, Safari, Google Chrome, Firefox oder einem anderen Anwendungsprogramm zum Zugriff auf das Dienst-Computersystem handeln. Das Nutzer-Computersystem hat eine Schnittstelle zur Verbindung mit dem Netzwerk, wobei es sich bei dem Netzwerk um ein privates oder öffentliches Netzwerk handeln kann, insbesondere das Internet. Je nach Ausführungsform kann diese Verbindung auch über ein Mobilfunknetz hergestellt werden.

[0018] Unter einem „Lesegerät“ wird hier ein elektronisches Gerät verstanden, welches einen Lesezugriff und auch einen Schreibzugriff auf den ID-Token ermöglicht, insbesondere ein sogenanntes Chipkartenterminal. Das Lesegerät kann einen integralen Bestandteil des Nutzer-Computersystems bilden oder als separate Komponente ausgeführt sein, beispielsweise als Peripheriegerät des Nutzer-Computersystems. Insbesondere kann es sich bei dem Lesegerät um ein sogenanntes Klasse 1, 2 oder 3 Chipkartenlesegerät handeln.

[0019] Unter einem „nichtflüchtigen elektronischen Speicher“ wird hier ein Speicher zur Speicherung von Daten, insbesondere von Attributen, verstanden, der auch als Non-Volatile Memory (NVM) bezeichnet wird. Insbesondere kann es sich hierbei um ein EEPROM, beispielsweise ein Flash-EEPROM, kurz als Flash bezeichnet, handeln.

[0020] Unter einem „geschützten Speicherbereich“ wird hier ein Speicherbereich verstanden, auf den ein Zugriff, das heißt ein Lesezugriff oder ein Schreibzugriff, von einem mit dem Speicher gekoppelten Prozessor nur dann ermöglicht wird, wenn eine hierzu erforderliche Bedingung erfüllt ist. Hierbei kann es sich zum Beispiel um eine kryptografische Bedingung, insbesondere eine erfolgreiche Authentisierung und/oder eine erfolgreiche Berechtigungsprüfung, handeln.

[0021] Unter einem „Prozessor“ wird hier eine Logikschaltung verstanden, die zur Ausführung von Programminstruktionen dient. Die Logikschaltung kann auf einem oder mehreren diskreten Bauelementen implementiert sein, insbesondere auf einem Chip.

[0022] 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 zum Beispiel einer Person oder einer Vorrichtung, zuzuordnen. Alternativ sind auch Zertifikate basierend auf zero-knowledge Kryptosystemen möglich. Beispielsweise kann das Zertifikat dem Standard X.509 oder einem anderen Standard entsprechen. Beispielsweise handelt es sich bei dem Zertifikat um ein Card Verifiable Certificate (CVC).

[0023] In dem Zertifikat kann spezifiziert sein, für welches Attribut oder welche Attribute des Nutzers, die in dem geschützten Speicherbereich des ID-Tokens gespeichert sind, das ID-Provider-Computersystem bzw. das Attribut-Provider-Computersystem zur Durchführung des Lesezugriffs berechtigt ist. Ferner können auch die jeweiligen Schreibrechte für Attributspezifikationen oder Attribute in einem Zertifikat definiert sein. Ein solches Zertifikat wird auch als Berechtigungszertifikat bezeichnet.

[0024] Nach Ausführungsformen der Erfindung wird zum Lesen von Attributen aus einem ID-Token eines Nutzers wie folgt vorgegangen:

1. Der Nutzer sendet eine Dienstanforderung von seinem Nutzer-Computersystem über ein Netzwerk, insbesondere ein öffentliches Netzwerk wie das Internet, an ein Dienst-Computersystem, welches mit einem ID-Provider-Computersystem gekoppelt ist. Hierzu gibt der Nutzer beispielsweise eine URL in einen Internetbrowser seines Nutzer-Computersystems ein, um eine sogenannte Internetsession mit dem Dienst-Computersystem aufzubauen.

Bei dem Dienst-Computersystem kann es sich zum Beispiel um einen Onlineshop oder ein anderes eCommerce-Portal oder einen Behördenserver, der eine eGovernment-Anwendung zur Verfügung stellt, handeln. Bei der Dienstanforde-

rung des Nutzers kann es sich um die Übertragung einer Kaufentscheidung des Nutzers handeln, die der Nutzer zum Beispiel durch Anklicken eines virtuellen Bedienelements auf der Webseite des Dienst-Computersystems, wie zum Beispiel „Kaufen“ oder „buy now“ eingibt, wobei diese Dienstanforderung zum Beispiel als http-Request oder https-Request über die Internetsession an das Dienst-Computersystem übertragen werden kann. Bei einer eGovernment-Anwendung kann es sich analog dazu bei der Dienstanforderung um die Übertragung einer Anforderung des Nutzers eines behördlichen Vorgangs, wie zum Beispiel die Ausstellung einer Meldebescheinigung, die Anmeldung eines Kraftfahrzeugs oder die Meldung einer Wohnortänderung oder dergleichen handeln.

2. Das Dienst-Computersystem benötigt für die Erbringung des mit der Dienstanforderung angeforderten Dienstes Attribute des Nutzers und – je nach Anwendungsfall – auch Attribute des ID-Tokens selbst. Beispielsweise kann die erste Attributspezifikation die Attribute Name, Geburtsdatum, Anschrift des Nutzers, Kontonummer des Nutzers, Kreditwürdigkeit des Nutzers sowie Gültigkeitsdauer des ID-Token beinhalten. Die Attribute gemäß dieser ersten Attributspezifikation benötigt das Dienst-Computersystem also zur Erbringung des Dienstes für den Nutzer. Diese erste Attributspezifikation sendet das Dienst-Computersystem an das ID-Provider-Computersystem, wobei dies über das Netzwerk erfolgen kann. Optional kann dies über das Nutzer-Computersystem erfolgen. Alternativ ist das ID-Provider-Computersystem ein integraler Bestandteil des Dienst-Computersystems, sodass das Senden der ersten Attributspezifikation zum Beispiel über einen internen Datenbus oder eine LAN-Verbindung erfolgt.

3. Authentifizierung des Nutzers gegenüber dem ID-Token. Hierzu gibt der Nutzer eine geheime Kennung, wie zum Beispiel die sogenannte Personal Identification Number (PIN) ein. Dies kann je nach Ausführungsform unmittelbar durch Eingabe in den ID-Token erfolgen, durch Eingabe in das Lesegerät oder durch Eingabe in das Nutzer-Computersystem. Vorzugsweise erfolgt die Authentifizierung des Nutzers gegenüber dem ID-Token mittels einer „Fernüberprüfung“, worunter hier jedes Verfahren verstanden wird, bei dem die zu überprüfende Kennung nicht in den ID-Token unmittelbar eingegeben wird, um sie mit der dort gespeicherten Kennung zu vergleichen, sondern bei dem die Überprüfung mittels eines das Lesegerät und den ID-Token involvierenden Protokolls erfolgt, bei dem die Kennung, die in das Lesegerät eingegeben wird, nicht an den ID-Token übertragen werden muss. Entsprechende Protokolle sind an sich aus dem Stand der Technik bekannt, wie zum Beispiel Strong Password Only Authentication Key Exch-

ange (SPEKE), Diffie-Hellman Encrypted Key Exchange (DH-EKE), Bellovin-Merritt Protokoll oder Password Authenticated Connection Establishment (PACE). Das SPEKE-Protokoll ist beispielsweise bekannt aus www.jablon.org/speke97.html, US 6,792,533 B2 und US 7,139,917 B2. Unter anderem ebenfalls aus www.jablon.org/speke97.html ist das DH-EKE-Protokoll bekannt. Unter anderem aus US 5,241,599 ist das Bellovin-Merritt-Protokoll bekannt. Aus Technical Guideline TR-03110 des Bundesamt für Sicherheit in der Informationstechnik ist das PACE-Protokoll bekannt, welches sich besonders für elliptische Kurven-Kryptographie eignet, vergleiche hierzu auch DE 10 2007 000 587 A1 und DE 10 2013 202 001 A1. Vorzugsweise authentifiziert sich neben dem Nutzer auch das Lesegerät gegenüber dem ID-Token, wobei auch ein gesicherter Übertragungskanal, das heißt ein sogenannter Secure Messaging-Kanal, zwischen dem ID-Token und dem Lesegerät aufgebaut werden kann, beispielsweise indem ein Session Key nach einem Diffie-Hellman-Protokoll zwischen dem ID-Token und dem Lesegerät vereinbart wird.

4. Das ID-Provider-Computersystem authentifiziert sich gegenüber dem ID-Token über das Netzwerk und weist vorzugsweise auch seine Berechtigung für einen Lesezugriff oder Schreibzugriff nach, indem es beispielsweise sein Berechtigungszertifikat über das Netzwerk an den ID-Token überträgt. Vorzugsweise authentifiziert sich auch der ID-Token gegenüber dem ID-Provider-Computersystem, das heißt es erfolgt sowohl die sogenannte Terminal Authentication (TA) des ID-Provider-Computersystems gegenüber dem ID-Token und die Chip Authentication (CA) des ID-Tokens, das heißt des in dem ID-Token beinhaltenen Chips mit dem Prozessor, gegenüber dem ID-Provider-Computersystem. Die TA und die CA können gemäß BSI TR-03110 durchgeführt werden.

5. Hierbei kann ein erster gesicherter Übertragungskanal nach einem Secure-Messaging-Verfahren aufgebaut werden, indem bei der TA und/oder der CA ein Session Key zwischen dem ID-Token und dem ID-Provider-Computersystem für eine Ende-zu-Ende-Verschlüsselung vereinbart wird.

6. Das ID-Provider-Computersystem führt dann einen ersten Lesezugriff aus, um Attribute gemäß der ersten Attributspezifikation aus dem ID-Token auszulesen.

7. Diejenigen Attribute gemäß der ersten Attributspezifikation, die in dem ID-Token gespeichert sind und für die das ID-Provider-Computersystem die erforderliche Leseberechtigung hat, werden aufgrund des ersten Lesezugriffs von dem ID-Token ausgegeben und über den ersten gesicherten Übertragungskanal von dem ID-Token an das ID-Provider-Computersystem über das Netzwerk

übertragen. Diese von dem ID-Token ausgegebenen Attribute werden als „erste Teilmenge“ der ersten Attributspezifikation bezeichnet. Beispielsweise sind in dem ID-Token lediglich der Name, das Geburtsdatum, die Anschrift des Nutzers sowie die Gültigkeitsdauer des ID-Tokens gespeichert, nicht aber die Kontonummer und die Kreditwürdigkeit des Nutzers. In diesem Fall beinhaltet also die erste Teilmenge den Namen, das Geburtsdatum, die Anschrift des Nutzers und die Gültigkeitsdauer, nicht aber die Kontonummer und die Kreditwürdigkeit des Nutzers, die nicht in dem ID-Token gespeichert sind.

8. Da aufgrund des ersten Lesezugriffs nicht alle erforderlichen Attribute gemäß der ersten Attributspezifikation gelesen werden konnten, wird eine zweite Attributspezifikation erzeugt, die eine zweite Teilmenge der Attribute der ersten Attributspezifikation spezifiziert, nämlich diejenigen Attribute, welche in der ersten Attributspezifikation spezifiziert sind, mit dem ersten Lesezugriff aber nicht ausgelesen werden konnten, das heißt hier die Kontonummer und die Kreditwürdigkeit des Nutzers. Die zweite Attributspezifikation wird zum Beispiel von dem ID-Provider-Computersystem erzeugt und über den ersten gesicherten Übertragungskanal an den ID-Token übertragen.

9. Die zweite Attributspezifikation wird in dem ID-Token gespeichert. Dabei kann bei Speicherung im nicht-flüchtigen Speicher des ID-Tokens eine aus vorherigen Protokollsitzungen gespeicherte Attributspezifikation ersetzt werden.

10. Ein Attribut-Provider-Computersystem authentifiziert sich gegenüber dem ID-Token über das Netzwerk. Dies kann analog zu der Authentifizierung des ID-Provider-Computersystems gegenüber dem ID-Token in dem oben genannten Schritt 4 erfolgen, nämlich mit einer sogenannten TA und einer CA.

11. Hierbei kann ein zweiter gesicherter Übertragungskanal mit Ende-zu-Ende-Verschlüsselung zwischen dem ID-Token und dem Attribut-Provider-Computersystem aufgebaut werden, wobei der erste gesicherte Übertragungskanal bestehen bleibt.

12. Die zweite Attributspezifikation wird dann von dem ID-Token ausgegeben und über den zweiten gesicherten Übertragungskanal an das Attribut-Provider-Computersystem übertragen. Auf diese Weise wird an das Attribut-Provider-Computersystem kommuniziert, welche Attribute zusätzlich von dem bereits durch das ID-Provider-Computersystem gelesenen Attribute erforderlich sind. Diese Attribute können in einem Speicher des Attribut-Provider-Computersystems vorhanden sein, wie zum Beispiel in einer Datenbank des Attribut-Provider-Computersystems, oder das Attribut-Provider-Computersystem greift auf eine externe Datenbank zu, um diese Attribute gemäß der zweiten Attributspezifikation zu lesen. Alternativ

ist es auch möglich, dass das Attribut-Provider-Computersystem selbst ein oder mehrere der Attribute gemäß der zweiten Attributspezifikation generiert.

13. Das Attribut-Provider-Computersystem führt dann einen Schreibzugriff über den zweiten gesicherten Übertragungskanal durch, um die von ihm gelesenen oder erzeugten Attribute gemäß der zweiten Attributspezifikation in dem ID-Token zu speichern.

14. Das ID-Provider-Computersystem führt dann einen zweiten Lesezugriff durch, und zwar über den noch bestehenden ersten gesicherten Übertragungskanal, um die noch fehlenden Attribute gemäß der zweiten Attributspezifikation aus dem ID-Token zu lesen, die zwischenzeitlich dort in dem Schritt 13 von dem Attribut-Provider-Computersystem gespeichert worden sind.

15. Die nun insgesamt in dem ID-Provider-Computersystem vorliegenden Attribute gemäß der ersten Attributspezifikation werden an das Dienst-Computersystem ausgegeben, damit dieses den angeforderten Dienst erbringen kann. Diese Ausgabe kann unmittelbar von dem ID-Provider-Computersystem an das Dienst-Computersystem erfolgen, wenn das ID-Provider-Computersystem einen integralen Bestandteil des Dienst-Computersystems bildet, oder über das Netzwerk, wobei vorzugsweise die von dem ID-Provider-Computersystem ausgegebenen Attribute von dem ID-Provider-Computersystem signiert werden, um Manipulationen zu unterbinden.

[0025] Ausführungsformen der Erfindung sind besonders vorteilhaft, da sie die Einbeziehung eines zusätzlichen Attribut-Provider-Computersystems ermöglichen, welches Attribute liefern kann, die in dem ID-Token zunächst nicht vorhanden sind. Dies kann mit der gleichen Sicherheit und Vertrauenswürdigkeit erfolgen, wie es für die ursprünglich in dem ID-Token gespeicherten Attribute der Fall ist und auch unter Wahrung der informationellen Selbstbestimmung des Nutzers und dem Gebot der Datensparsamkeit, da keine Mitteilung der in dem ID-Token ursprünglich gespeicherten Attribute an das Attribut-Provider-Computersystem erfolgen muss.

[0026] Nach einer Ausführungsform erfolgt die Speicherung der Attribute in dem oben genannten Schritt 13 in dem nichtflüchtigen elektronischen Speicher des ID-Tokens, sodass diese zusätzlich von dem Attribut-Provider-Computersystem in den ID-Token geschriebenen Attribute zur weiteren Verwendung zur Verfügung stehen. Bei einer nachfolgenden Dienst-anforderung des Nutzers an das Dienst-Computersystem müssen also diese zusätzlichen Attribute nicht erneut über das Attribut-Provider-Computersystem beschafft werden, sondern stehen in dem ID-Token bereits zur Verfügung, sodass sie bereits in dem

oben genannten Schritt 6 von dem ID-Provider-Computersystem ausgelesen werden können.

[0027] Nach einer Ausführungsform der Erfindung ist die Kommunikationsschnittstelle des ID-Tokens drahtlos ausgebildet, das heißt beispielsweise als sogenannte RFID- oder NFC-Schnittstelle. Neben der drahtlosen Kommunikation dient diese Schnittstelle auch zur Einkopplung von Energie in den ID-Token, um diesen mit der für seinen Betrieb erforderlichen elektrischen Energie zu versorgen. Zusätzlich zu dem nicht-flüchtigen elektronischen Speicher hat der ID-Token einen flüchtigen elektronischen Speicher, wie zum Beispiel ein RAM oder einen Arbeitsspeicher des Prozessors. Die zweite Attributspezifikation wird vorzugsweise in den flüchtigen elektronischen Speicher geschrieben (vergleiche oben Schritt 9). Wird nämlich nach dem Schritt 9 der ID-Token aus der Reichweite des Lesegeräts entfernt, so führt dies dazu, dass die zweite Attributspezifikation aus dem flüchtigen elektronischen Speicher gelöscht wird. Ein neuer Protokollablauf ist in diesem Fall zu starten. Hierdurch wird vermieden, dass sich der ID-Token in einem undefinierten Zustand befindet, wenn er zum Beispiel nach dem oben genannten Schritt 9 aus der Reichweite des Lesegeräts entfernt wird, um eventuelle Missbrauchsmöglichkeiten hierdurch zu unterbinden. Wird die zweite Attributspezifikation in den nicht-flüchtigen elektronischen Speicher geschrieben, bleibt auch nach Entfernung des ID-Tokens aus der Reichweite des Lesegeräts die zweite Attributspezifikation im Speicher erhalten.

[0028] Nach einer Ausführungsform wird zumindest ein zweites Attribut-Provider-Computersystem mit in den Ablauf eingebunden, wenn das erste Attribut-Provider-Computersystem die Attribute gemäß der zweiten Attributspezifikation nicht vollständig liefern kann. In diesem Fall werden die folgenden weiteren Schritte zwischen den o.g. Schritten 13 und 14 durchgeführt:

- Erzeugung einer dritten Attributspezifikation einer dritten Teilmenge der zweiten Teilmenge, wobei die dritte Attributspezifikation diejenigen Attribute der zweiten Teilmenge spezifiziert, die in dem aufgrund des Schreibzugriffs in den ID-Token geschriebenen Attribute nicht beinhaltet sind. Liefert beispielsweise das erste Attribut-Provider-Computersystem in dem oben genannten Schritt 13 zwar die Kontonummer des Nutzers, nicht aber die Kreditwürdigkeit des Nutzers, so beinhaltet die dritte Teilmenge dieses fehlende Attribut bezüglich der Kreditwürdigkeit des Nutzers. Diese dritte Attributspezifikation wird zum Beispiel von dem ersten Attribut-Provider-Computersystem erzeugt und in dem ID-Token über den zweiten gesicherten Übertragungskanal gespeichert.
- Anschließend authentifiziert sich das zweite Attribut-Provider-Computersystem gegenüber dem ID-Token, vorzugsweise analog zu den oben ge-

nannten Schritten 4. bzw. 10., wobei wiederum eine TA und eine CA durchgeführt wird und ein dritter gesicherter Übertragungskanal mit Ende-zu-Ende-Verschlüsselung zwischen dem ID-Token und dem zweiten Attribut-Provider-Computersystem über das Netzwerk aufgebaut wird.

- Die dritte Attributspezifikation wird dann über den dritten gesicherten Übertragungskanal von dem ID-Token an das zweite Attribut-Provider-Computersystem übertragen, und zwar analog zu dem oben genannten Schritt 12.

- Das zweite Attribut-Provider-Computersystem liefert dann das noch fehlende Attribut gemäß der dritten Attributspezifikation, das heißt in dem hier betrachteten Beispiel die Kreditwürdigkeit des Nutzers, und schreibt dieses Attribut über den dritten gesicherten Übertragungskanal in den ID-Token.

[0029] Mit dem zweiten Lesezugriff liest das ID-Provider-Computersystem dann sämtliche der von dem ersten und zweiten Attribut-Provider-Computersystem in dem ID-Token gespeicherten Attribute.

[0030] Falls auch das zweite Attribut-Provider-Computersystem nicht sämtliche der noch fehlenden Attribute liefern kann, kann dieser Vorgang iterativ solange durchgeführt werden, bis eine Abbruchbedingung erreicht ist. Beispielsweise wird dieser iterative Vorgang dann abgeschlossen, wenn sämtliche der Attribute gemäß der ersten Attributspezifikation in dem ID-Token gespeichert worden sind, da dann keine weiteren Attribut-Provider-Computersysteme mehr involviert werden müssen. Ferner kann ein Abbruch auch dann erfolgen, wenn eine maximale Anzahl von Schreibzugriffen erreicht ist und/oder eine maximale Zeitdauer, das heißt ein sogenanntes Time-out.

[0031] Nach einer Ausführungsform der Erfindung werden die aufgrund eines Schreibzugriffs eines der Attribut-Provider-Computersysteme in dem ID-Token zu speichernden Attribute auf einer Anzeigevorrichtung, das heißt einem sogenannten Display, angezeigt, damit der Nutzer diese Attribute zur Kenntnis nehmen kann. Vorzugsweise ist vor dem Schreiben der Attribute die Eingabe einer Bestätigung des Nutzers erforderlich.

[0032] In einem weiteren Aspekt betrifft die Erfindung einen ID-Token, der zur Verwendung in einem erfindungsgemäßen Verfahren konfiguriert ist.

[0033] In einem weiteren Aspekt betrifft die Erfindung ein Attribut-Provider-Computersystem, welches zur Verwendung in einem erfindungsgemäßen Verfahren konfiguriert ist.

[0034] In einem weiteren Aspekt betrifft die Erfindung ein Computersystem mit zumindest einem

erfindungsgemäßen ID-Token und einem ID-Provider-Computersystem, welches zur Ausführung eines erfindungsgemäßen Verfahrens konfiguriert ist. Zu diesem Computersystem kann auch zumindest ein erfindungsgemäßes Attribut-Provider-Computersystem gehören.

[0035] Im Weiteren werden Ausführungsformen der Erfindung mit Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen:

[0036] Fig. 1 ein Blockdiagramm einer Ausführungsform eines erfindungsgemäßen Computersystems,

[0037] Fig. 2 ein Flussdiagramm einer Ausführungsform eines erfindungsgemäßen Verfahrens,

[0038] Fig. 3 ein UML-Diagramm einer Ausführungsform eines erfindungsgemäßen Verfahrens,

[0039] Fig. 4 ein Flussdiagramm einer Ausführungsform eines erfindungsgemäßen Verfahrens mit zumindest einem weiteren Attribut-Provider-Computersystem,

[0040] Fig. 5 ein Flussdiagramm einer weiteren Ausführungsform eines erfindungsgemäßen Verfahrens.

[0041] Elemente der nachfolgenden Ausführungsformen, die einander gleichen oder einander entsprechen, sind jeweils mit identischen Bezugszeichen gekennzeichnet.

[0042] Die Fig. 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 ein Lesegerät **101** mit einer Schnittstelle **104** zur Kommunikation mit einem ID-Token **106**, der eine entsprechende Schnittstelle **108** aufweist.

[0043] 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 kann es sich um ein Computernetzwerk, wie zum Beispiel das Internet, handeln.

[0044] 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 Ken-

nung, insbesondere 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.

[0045] 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.

[0046] 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.

[0047] 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.

[0048] 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.

[0049] Bei einer Ausführungsform mit PIN gibt der Nutzer **102** seine PIN zu seiner Authentifizierung ein, beispielsweise in das Nutzer-Computersystem **100**. Durch Ausführung der Programminstruktionen **130** wird dann 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.

[0050] Alternativ wird ein biometrisches Merkmal des Nutzers **102** erfasst. Beispielsweise hat der ID-Token **106** hierzu einen Fingerabdrucksensor oder ein Fingerabdrucksensor ist an das Nutzer-Computersystem **100** angeschlossen. 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.

[0051] 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.

[0052] 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 geschützten 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.

[0053] 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.

[0054] Alternativ zu der in der **Fig. 1** dargestellten Ausführungsform kann das Nutzer-Computersystem **100** mit seiner Schnittstelle **104** nicht unmittelbar mit der Schnittstelle **108** kommunizieren, sondern über ein an die Schnittstelle **104** angeschlossenes Lesegerät für den ID-Token **106**. Über dieses Lesegerät, wie zum Beispiel einen so genannten Klasse 2-Chipkarten-Terminal, kann auch die Eingabe der PIN erfolgen.

[0055] 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-Compu-

tersystems **136** sowie das entsprechende Zertifikat **144** gespeichert ist. Auch bei diesem Zertifikat kann es sich beispielsweise um ein Zertifikat nach einem PKI-Standard, wie zum Beispiel X.509 handeln.

[0056] 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** betreffenden 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.

[0057] 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.

[0058] 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.

[0059] 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 oder als Behördenserver für eine eGovernment Anwendung.

[0060] 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.

[0061] Je nach der Art des beauftragten oder bestellten Produkts oder der Dienstleistung muss das Dienst-Computersystem **150** 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** entgegen genommen und/oder ausgeführt.

[0062] 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.

[0063] Je nach Anwendungsfall können für die Erbringung des Dienstes weitere Attribute erforderlich sein, die in dem ID-Token zunächst nicht vorhanden sind. Hierzu kann das in der **Fig. 1** gezeigte Computersystem ein oder mehrere Attribut-Provider-Computersysteme **172**, **173**, **174**, ... aufweisen. Diese können prinzipiell gleich aufgebaut sein wie das ID-Provider-Computersystem und verfügen über zusätzliche Funktionalitäten zum Lesen oder Generieren von Attributen sowie zum Schreiben von Attributen und erforderlichenfalls Attributspezifikationen in den ID-Token.

[0064] Zur Inanspruchnahme eines von dem Dienst-Computersystem **150** zur Verfügung gestellten Dienstes wird beispielsweise wie folgt vorgegangen:

a) Der Nutzer **102** baut mithilfe seines Nutzer-Computersystems **100** eine Internet-session über das Netzwerk **116** zu dem Dienst-Computersystem **150** auf. Über diese Internet-session wird eine Dienst-anforderung **103** von dem Nutzer-Computersystem **100** an das Dienst-Computersystem **150** übertragen, womit der Nutzer **102** die Erbringung eines Dienstes des Dienst-Computersystems **150** anfordert. Das Dienst-Computersystem **150** antwortet auf diese Dienst-anforderung **103** mit einer ersten Attributspezifikation **105**, die diejenigen Attribute spezifiziert, die für die Erbringung des mit der Dienst-anforderung **103** angeforderten Dienstes zu erfüllen sind. Diese erste Attributspezifikation spezifiziert beispielsweise eine Anzahl von M Attributen A1, A2, A3, ... AM.

b) Beispielsweise wird die Attributspezifikation **105** in einem Speicher **183** des Nutzer-Computersystems **100** zwischengespeichert. Aufgrund des Empfangs der Attributspezifikation **105** durch das Nutzer-Computersystem **100** wird der Nutzer **102** dazu aufgefordert, sich gegenüber dem ID-Token **106** zu authentifizieren. Hierzu gibt der Nutzer **102** seine PIN zum Beispiel über das Lesegerät **101** oder eine Tastatur des Nutzer-Computersystems **100** ein. Ferner baut das Nutzer-Computersystem **100** zu dem ID-Provider-Computersystem **136** eine weitere Internet-session über das Netzwerk **116** auf, über die sich das ID-Provider-Computersystem **136** gegenüber dem Nutzer-Computersystem **100** authentifiziert, und zwar unter Verwendung des Zertifikats **144**.

Vorzugsweise erfolgt eine gegenseitige Authentifizierung des ID-Tokens **106** und des ID-Provider-Computersystems **136** bzw. des jeweiligen Attribut-Provider-Computersystems unter Verwendung der Zertifikate **126** und **144**, das heißt eine sogenannte CA und eine TA. Hierbei wird auch ein Session Key vereinbart, mit dem der erste gesicherte Übertragungskanal mit Ende-zu-Ende-Verschlüsselung zwischen dem ID-Token **106** und dem ID-Provider-Computersystem über das Nutzer-Computersystem **100** und das Netzwerk **116** aufgebaut wird. Ferner leitet das Nutzer-Computersystem **100** die Attributspezifikation **105** über die mit dem ID-Provider-Computersystem **136** bestehende Session an das ID-Provider-Computersystem **136** weiter.

c) Das ID-Provider-Computersystem **136** antwortet auf die erste Attributspezifikation **105** mit einem Lesekommando **107** zum Lesen der in der ersten Attributspezifikation spezifizierten Attribute. Dieses Lesekommando **107** wird über den ersten gesicherten Übertragungskanal mit Ende-zu-Ende-Verschlüsselung von dem ID-Provider-Computersystem **136** an den ID-Token **106** übertragen. Der Prozessor **128** greift daraufhin auf den elektronischen Speicher **118** zu, um die Attribute gemäß der ersten Attributspezifikation **105** auszulesen. Im Weiteren wird ohne Beschränkung der Allgemeinheit davon ausgegangen, dass von den M Attributen gemäß der ersten Attributspezifikation **105** nur P Attribute A1, A2, A3, ..., AP vorhanden sind, wobei $P < M$. Auf das Lesekommando **107** antwortet der ID-Token **106** mit der Antwort **109**, die die erste Teilmenge der in der ersten Attributspezifikation **105** spezifizierten Attribute, nämlich die Attribute A1, A2, A3, ..., AP beinhaltet. Die Antwort **109** wird über den ersten gesicherten Übertragungskanal von dem ID-Token **106** an das ID-Provider-Computersystem **136** übertragen.

d) Das ID-Provider-Computersystem **136** speichert die Antwort **109** mit der ersten Teilmenge der Attribute in seinem Speicher **140** und erzeugt eine zweite Attributspezifikation **111**, welche die noch fehlenden Attribute spezifiziert, das heißt diejeni-

gen der ersten Attributspezifikation **105** spezifizierten Attribute, die in der Antwort **109** nicht beinhaltet sind, das heißt hier die Attribute AP + 1 bis AM. Die zweite Attributspezifikation **111** wird über den ersten gesicherten Übertragungskanal von dem ID-Provider-Computersystem **136** zu dem ID-Token **106** übertragen und dort gespeichert und kann bei Speicherung in dem nicht-flüchtigen oder flüchtigen Speicher eine bereits vorhandene Attributspezifikation ersetzen. Die Speicherung kann beispielsweise in einem flüchtigen Speicher **113** des ID-Tokens **106** erfolgen.

e) Das Nutzer-Computersystem **100** baut eine weitere Internet-Session über das Netzwerk **116** mit dem Attribut-Provider-Computersystem **172** auf. Das Attribut-Provider-Computersystem **172** authentifiziert sich dann gegenüber dem ID-Token **106**, wobei vorzugsweise eine gegenseitige Authentifizierung, das heißt eine CA und eine TA, durchgeführt werden. Hierbei wird ein zweiter gesicherter Übertragungskanal mit Ende-zu-Ende-Verschlüsselung mit einem Session Key zwischen dem ID-Token **106** und dem Attribut-Provider-Computersystem **172** über das Netzwerk **116** und das Nutzer-Computersystem **100** aufgebaut, wobei der erste gesicherte Übertragungskanal bestehen bleibt.

Der Prozessor **128** dient zur Ausführung von Programminstruktionen **131** für die Kanalschaltung, das heißt die Auswahl einer der gesicherten Übertragungskanäle, das heißt hier des ersten oder des zweiten gesicherten Übertragungskanals, für die externe Kommunikation. Aufgrund des Aufbaus des zweiten gesicherten Übertragungskanals wird durch Ausführung der Programminstruktionen **131** der zweite gesicherte Übertragungskanal von dem Prozessor **128** ausgewählt, über den der ID-Token **106** dann die zweite Attributspezifikation **111** an das Attribut-Provider-Computersystem **172** sendet.

f) Das Attribut-Provider-Computersystem **172** führt daraufhin einen Zugriff auf seine Datenbank **175** durch, um die Attribute gemäß der zweiten Attributspezifikation **111** zu lesen. Das Attribut-Provider-Computersystem **172** antwortet dann auf die Attributspezifikation **111** mit seiner Antwort **176**, die die aus der Datenbank **175** gelesenen Attribute beinhaltet und sendet diese Antwort **176** über den zweiten gesicherten Übertragungskanal an den ID-Token **106**, welcher die Antwort **176** mit diesen Attributen mit seinem elektronischen Speicher **118** speichert.

g) Durch Ausführung der Programminstruktionen **131** schaltet der ID-Token **106** dann auf den ersten gesicherten Übertragungskanal zurück. Das ID-Provider-Computersystem **136** greift dann durch ein zweites Lesekommando **177** über

den ersten gesicherten Übertragungskanal auf den ID-Token **106** zu und erhält als Antwort darauf von dem ID-Token **106** die Antwort **176** aus dem Speicher **118** mit den noch fehlenden Attributen.

[0065] Für den Fall, dass das Attribut-Provider-Computersystem **172** nicht auf sämtliche gemäß der zweiten Attributspezifikation **111** erforderlichen Attribute zugreifen kann, beispielsweise weil diese nicht sämtlich in der Datenbank **175** gespeichert sind, kann der oben genannte Vorgang iterativ unter Verwendung der weiteren Attribut-Provider-Computersysteme **173**, **174**, ... durchgeführt werden, und zwar so lange, bis sämtliche der Attribute gemäß der ersten Attributspezifikation **105** in dem Speicher **118** vorliegen oder eine andere Abbruchbedingung erreicht ist.

[0066] Falls das Attribut-Provider-Computersystem **172** nicht sämtliche der Attribute gemäß der zweiten Attributspezifikation **111** ermitteln kann, so generiert das Attribut-Provider-Computersystem **172** eine dritte Attributspezifikation **178**. Wenn beispielsweise die Antwort **176** die Attribute AP + 1 bis AQ beinhaltet mit $Q < M$, so werden in der dritten Attributspezifikation **178** die noch fehlenden Attribute AQ + 1 bis AM spezifiziert. Diese dritte Attributspezifikation **178** wird von dem Attribut-Provider-Computersystem **172** über den zweiten gesicherten Übertragungskanal zu dem ID-Token **106** übertragen und ersetzt oder aktualisiert die in dem Speicher **113** gespeicherte zweite Attributspezifikation **111**.

[0067] Anschließend wird dann nach vorheriger CA und TA ein dritter gesicherter Übertragungskanal zu dem Attribut-Provider-Computersystem **173** aufgebaut, welches die dritte Attributspezifikation **178** aus dem ID-Token **106** ausliest und darauf mit einer Antwort **179** antwortet, die die noch fehlenden Attribute gemäß der dritten Attributspezifikation **178** beinhaltet. Diese Antwort **179** wird über den dritten gesicherten Übertragungskanal von dem Attribut-Provider-Computersystem **173** an den ID-Token **106** übertragen und in dem Speicher **118** gespeichert.

[0068] Durch Ausführung der Programminstruktionen **131** wird dann wiederum auf den ersten gesicherten Übertragungskanal zurückgeschaltet, so dass aufgrund des zweiten Lesekommandos **177** in diesem Fall sowohl die Antwort **176** als auch die Antwort **179**, die insgesamt die Attribute AP + 1 bis AM beinhalten, an das ID-Provider-Computersystem **136** übertragen werden.

[0069] Falls seitens des Attribut-Provider-Computersystems **173** nicht sämtliche der Attribute gemäß der dritten Attributspezifikation **178** verfügbar sind, kann in analoger Art und Weise iterativ weiterverfahren werden, indem ein oder mehrere weitere Attribut-Provider-Computersysteme, wie zum Beispiel das Attri-

but-Provider-Computersystem **174**, in den Ablauf eingebunden werden.

[0070] Das ID-Provider-Computersystem **136** verfügt nach einer erfolgreichen Durchführung der oben genannten Verfahrensschritte in seinem Speicher **140** über sämtliche der Attribute, die mit der ersten Attributspezifikation **105** angefordert worden sind. Das ID-Provider-Computersystem **136** generiert daraufhin eine Nachricht **180**, die diese Attribute A1 bis AM beinhaltet, signiert diese Nachricht und sendet sie über das Netzwerk **116** an das Dienst-Computersystem **150**, wobei dies über das Nutzer-Computersystem **100** erfolgen kann. Das Dienst-Computersystem **150** kann dann gegebenenfalls mithilfe der in der Nachricht **180** beinhalteten Attribute den mit der Dienstanforderung **103** angeforderten Dienst erbringen.

[0071] Die Attribut-Provider-Computersysteme **172**, **173**, **174** ... können analog zu dem ID-Provider-Computersystem **136** aufgebaut sein, das heißt sie verfügen jeweils über eine Netzwerk-Schnittstelle **138**, einen Prozessor **145** zur Ausführung von Programmstrukturen **146**, **148** und einen Speicher **140**, in dem ein Zertifikat und ein privater Schlüssel gespeichert sind. Bei dem Zertifikat handelt es sich vorzugsweise um ein Berechtigungszertifikat, in dem jeweils eine Berechtigung für Lese- und Schreibzugriffe auf den ID-Token **106** spezifiziert ist.

[0072] Nach einer Ausführungsform der Erfindung werden die in der Antwort **176** bzw. **179** beinhalteten Attribute erst dann in dem Speicher **118** gespeichert, nachdem diese der Nutzer **102** zur Kenntnis nehmen konnte. Hierzu werden diese Attribute auf einem Display **181** angezeigt, welches zum Beispiel zu dem Lesegerät **101** gehört. Ferner kann beispielsweise auf dem Lesegerät **101** ein Bedienelement **182** vorhanden sein, über welches der Nutzer **102** eine Eingabe tätigen muss, um die Speicherung der in den Antworten **176** bzw. **179** beinhalteten Attribute in dem Speicher **118** zu genehmigen. Hierdurch erhält der Nutzer **102** eine Kontrollmöglichkeit bezüglich der möglicherweise seine Person betreffenden zusätzlichen Attribute in dem Speicher **118**.

[0073] Die Fig. 2 zeigt eine Ausführungsform eines entsprechenden erfindungsgemäßen Verfahrens. In dem Schritt **200** wird eine Dienstanforderung **103** von dem Nutzer-Computersystem **100** an das Dienst-Computersystem **150** gesendet. Das Dienst-Computersystem **150** erzeugt daraufhin eine Antwort mit der ersten Attributspezifikation **105** (Schritt **202**), die in dem Schritt **204** an das ID-Provider-Computersystem **136** gesendet wird.

[0074] In dem Schritt **206** authentifiziert sich der Nutzer **102** gegenüber dem ID-Token **106** und es erfolgt in dem Schritt **208** eine einseitige oder gegenseitige

Authentifizierung des ID-Tokens **106** und des ID-Provider-Computersystems **136**, insbesondere mit einer CA und einer TA.

[0075] In dem Schritt **210** wird die erste gesicherte Verbindung aufgebaut, über welche das ID-Provider-Computersystem in dem Schritt **212** das erste Lesekommando **107** sendet. Auf das erste Lesekommando antwortet der ID-Token **106** in dem Schritt **214** mit den in der Antwort **109** beinhalteten Attributen A1 bis AP.

[0076] Daraufhin erzeugt das ID-Provider-Computersystem **136** in dem Schritt **216** die zweite Attributspezifikation **111**, in der die noch fehlenden Attribute AP + 1 bis AM spezifiziert sind und schreibt diese zweite Attributspezifikation **111** in dem Schritt **218** über den ersten gesicherten Übertragungskanal in den ID-Token **106**, wo die Attributspezifikation **111** gespeichert wird.

[0077] Anschließend wird dann in dem Schritt **220** der zweite gesicherte Übertragungskanal zu dem Attribut-Provider-Computersystem **172** aufgebaut und die zweite Attributspezifikation **111** aus dem ID-Token **106** gelesen und zu dem Attribut-Provider-Computersystem **172** übertragen.

[0078] Das Attribut-Provider-Computersystem **172** greift dann auf die laut zweiter Attributspezifikation **111** angeforderten Attribute zu, beispielsweise über einen Datenbankzugriff, und schreibt diese zusätzlichen Attribute, in dem betrachteten Beispielsfall die Attribute AP + 1 bis AM in dem Schritt **224** über den zweiten gesicherten Übertragungskanal in den ID-Token **106**.

[0079] Der ID-Token **106** schaltet dann auf den ersten gesicherten Übertragungskanal in dem Schritt **226** zurück, sodass die zuvor in dem Schritt **224** zusätzlich in den ID-Token **106** geschriebenen Attribute von dem ID-Provider-Computersystem **136** über diesen ersten gesicherten Übertragungskanal aus dem ID-Token **106** ausgelesen werden (Schritt **228**). In dem Schritt **230** überträgt das ID-Provider-Computersystem **136** dann sämtliche der aus dem ID-Token **106** gelesenen Attribute an das Dienst-Computersystem **150**, sodass dieses dann gegebenenfalls nach Prüfung der Attribute den angeforderten Dienst erbringen kann.

[0080] Die Fig. 3 zeigt ein entsprechendes UML-Diagramm, wobei hier davon ausgegangen wird, dass das Dienst-Computersystem **150** das ID-Provider-Computersystem **136** beinhaltet.

[0081] In dem Schritt 1 wird durch den Nutzer **102** eine Serviceanfrage, das heißt eine Dienstanforderung **103**, an das Dienst-Computersystem **150** gesendet, und zwar mithilfe des Nutzer-Computersys-

tems **100**. Das Dienst-Computersystem **150** antwortet darauf mit einer Datenanfrage, das heißt mit der ersten Attributspezifikation **105**.

[0082] Daraufhin authentifiziert sich der Nutzer **102** gegenüber dem ID-Token **106**, indem er seine PIN in das Nutzer-Computersystem **100**, das heißt beispielsweise dessen Lesegerät **101**, eingibt. Aufgrund der Ausführung beispielsweise des PACE-Protokolls wird die PIN verifiziert und in dem Schritt 2 wird mithilfe von PACE ein Secure Messaging-Kanal zwischen ID-Token und Nutzer-Computersystem, das heißt SM-[PACE], aufgebaut.

[0083] In dem Schritt 3 erfolgt dann auf dieser Basis eine TA des in dem Dienst-Computersystem **150** beinhaltenen ID-Provider-Computersystems sowie in dem Schritt 4 eine CA des ID-Tokens **106** gegenüber dem ID-Provider-Computersystem.

[0084] In dem Schritt 5 wird dann der erste gesicherte Übertragungskanal zwischen dem ID-Token **106** und dem ID-Provider-Computersystem aufgebaut, nämlich SM-[CA] #1.

[0085] Die weitere Kommunikation in dem Schritt 6 verläuft dann über diesen ersten gesicherten Übertragungskanal, nämlich das Auslesen von Attributen aus dem ID-Token **106** gemäß der ersten Attributspezifikation **105** und das anschließende Schreiben der zweiten Attributspezifikation **111**, d.h. ein Attribute Request (AR). Ferner kann durch das ID-Provider-Computersystem **136** ein Umschaltsignal SC-[PACE] erzeugt werden, welches einerseits durch die Programminstruktionen **131** seitens des ID-Tokens **106** verarbeitet wird und andererseits durch das Nutzer-Computersystem **100** verarbeitet wird, um den Übertragungskanal SM-[PACE] zwischen ID-Token und Nutzer-Computersystem zurückzuschalten.

[0086] In dem Schritt 8 kann optional eine Auswahl des Attribut-Provider-Systems **172** durch den Nutzer **102** erfolgen. Auf eine solche explizite Auswahl kann auch verzichtet werden, wenn das Nutzer-Computersystem **100** das zu kontaktierende Attribut-Provider-Computersystem bereits kennt, beispielsweise wenn der Nutzer **102** vorab mit der Lieferung von Attributen durch das Attribut-Provider-Computersystem **172** sein Einverständnis erklärt hat. Entsprechendes gilt für die Attributsanfrage 2 gemäß **Fig. 5**.

[0087] Die Schritte 9 und 10 werden dann analog zu den Schritten 3 und 4 auf der Basis von SM-[PACE] durchgeführt, und zwar für eine TA des Attribut-Provider-Computersystems **172** bzw. eine CA des ID-Tokens **106** gegenüber dem Attribut-Provider-Computersystem **172**.

[0088] In dem Schritt 10 wird dann der zweite gesicherte Übertragungskanal SM-[CA] #2 aufgebaut,

über den dann die weitere Kommunikation in den Schritten 12, 13 und 14 erfolgt:

In dem Schritt 12 liest das Attribut-Provider-Computersystem **172** die zweite Attributspezifikation **111** und liest dann die entsprechenden Attribute, beispielsweise durch einen Zugriff auf seine Datenbank **175**. Das Attribut-Provider-Computersystem **172** schreibt dann diese zusätzlichen Attribute in den ID-Token **106** (Schritt 13) und löscht die dort gespeicherte zweite Attributspezifikation **111** (Schritt 14).

[0089] Ferner kann das Attribut-Provider-Computersystem **172** ein Umschaltsignal generieren, nämlich SC-[CA] #1, welches von den Programminstruktionen **131** verarbeitet wird, um den Übertragungskanal auf den ersten gesicherten Übertragungskanal SM-[CA] #1 in dem Schritt 15 zurückzuschalten. Alternativ kann das Attribut-Provider-Computersystem **172** ein Umschaltsignal generieren, nämlich SC-[PACE], welches von den Programminstruktionen **131** verarbeitet wird, um zunächst den Übertragungskanal SM [PACE] zwischen ID-Token und Nutzer-Computersystem zurückzuschalten. Das Nutzer-Computersystem kann dann ein Umschaltsignal generieren, nämlich SC-[CA] #1, welches von den Programminstruktionen **131** verarbeitet wird, um den Übertragungskanal auf den ersten gesicherten Übertragungskanal SM-[CA] #1 in dem Schritt 15 zurückzuschalten.

[0090] Über diesen ersten gesicherten Übertragungskanal liest dann das ID-Provider-Computersystem in dem Schritt 16 die noch fehlenden Attribute, die in dem Schritt 13 von dem Attribut-Provider-Computersystem geschrieben worden sind und sendet optional in dem Schritt 17 ein Reset-Kommando, um hiermit den Vorgang des Lesens von Attributen aus dem ID-Token abzuschließen. In dem Schritt 18 kann dann das Dienst-Computersystem **150** mittels der zuvor aus dem ID-Token **106** gelesenen Attribute den gewünschten Dienst erbringen.

[0091] Die **Fig. 4** zeigt eine weitere Ausführungsform eines erfindungsgemäßen Verfahrens. Die Schritte **200** bis **224** des Verfahrens gemäß **Fig. 4** können identisch sein zu den entsprechenden Schritten der Ausführungsform gemäß **Fig. 2**, wobei in dem Schritt **224** nicht in jedem Fall sämtliche Attribute bereits in dem ID-Token **106** vorhanden sind.

[0092] Hierzu wird in dem Schritt **226** geprüft, ob sämtliche Attribute gemäß der zweiten Attributspezifikation **111** in dem Schritt **224** geschrieben werden konnten. Ist dies nicht der Fall, so geht die Ablaufsteuerung zu dem Schritt **232**, in dem die dritte Attributspezifikation **178** erzeugt wird, um diese in dem Schritt **234** an den ID-Token **106** zu übertragen.

[0093] Dann wird in dem Schritt **236** der dritte gesicherte Übertragungskanal aufgebaut, um die dritte Attributspezifikation **178** in dem Schritt **238** an

ein zweites Attribut-Provider-Computersystem, beispielsweise das Attribut-Provider-Computersystem **173**, zu übertragen, welches daraufhin in dem Schritt **240** mit seiner Antwort **179** die angeforderten zusätzlichen Attribute in den ID-Token **106** schreibt.

[0094] Anschließend werden die Schritte **226** bis **230** so wie in der Ausführungsform gemäß **Fig. 2** ausgeführt.

[0095] Die **Fig. 5** zeigt ein entsprechendes UML-Diagramm. Im Unterschied zu dem UML-Diagramm gemäß **Fig. 3** können in dem Schritt **13** nicht sämtlich der erforderlichen Attribute von dem Attribut-Provider-Computersystem **172** gemäß der zweiten Attributspezifikation **111** geliefert werden.

[0096] Das Attribut-Provider-Computersystem passt daraufhin die zweite Attributspezifikationen **111**, das heißt den Attribute Request, dementsprechend an, indem es die dritte Attributspezifikation **138** erzeugt und in den ID-Token **106** schreibt. Im Unterschied zu der Ausführungsform gemäß **Fig. 3** wird ferner von dem Attribut-Provider-Computersystem ein Umschaltsignal SC-[PACE] erzeugt, um den Übertragungskanal SM-[PACE] zwischen ID-Token und Nutzer-Computersystem zurückzuschalten.

[0097] Auf dieser Basis werden dann die Schritte **8** bis **14** erneut in analoger Art und Weise mit Bezug auf das zweite Attribut-Provider-Computersystem **173** ausgeführt. Anschließend erzeugt das Nutzer-Computersystem **100** ein Umschaltsignal SC [CA] #1, sodass der ID-Token **106** auf den ersten gesicherten Übertragungskanal SM [CA] #1 zurückschaltet.

128	Prozessor
130	Programminstruktionen
131	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
172	Attribut-Provider-Computersystem
173	Attribut-Provider-Computersystem
174	Attribut-Provider-Computersystem
175	Datenbank
176	Antwort
177	Lesekommando
178	dritte Attributspezifikation
179	Antwort
180	Nachricht
181	Display
182	Bedienelement
183	Speicher

Bezugszeichenliste

100	Nutzer-Computersystem
101	Lesegerät
102	Nutzer
103	Dienstanforderung
104	Schnittstelle
105	erste Attributspezifikation
106	ID-Token
107	Lesekommando
108	Schnittstelle
109	Antwort
110	Prozessor
111	zweite Attributspezifikation
112	Programminstruktionen
113	flüchtiger Speicher
114	Netzwerk-Schnittstelle
116	Netzwerk
118	elektronischer Speicher
120	geschützter Speicherbereich
122	geschützter Speicherbereich
124	geschützter Speicherbereich
126	Speicherbereich

ZITATE ENTHALTEN IN DER BESCHREIBUNG

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

Zitierte Patentliteratur

- | | |
|-----------------------------|-----------------------------|
| - US 2007/0294431 A1 [0004] | - DE 102010028133 [0005] |
| - DE 102008000067 A1 [0005] | - DE 102011082101 [0011] |
| - DE 102008040416 [0005] | - US 6792533 B2 [0024] |
| - DE 102008042262 [0005] | - US 7139917 B2 [0024] |
| - DE 102009026953 [0005] | - US 5241599 [0024] |
| - DE 102009027723 [0005] | - DE 102007000587 A1 [0024] |
| - DE 102009027681 [0005] | - DE 102013202001 A1 [0024] |

Zitierte Nicht-Patentliteratur

- www.jablon.org/speke97.html [0024]

Patentansprüche

1. Verfahren zum Lesen von Attributen aus einem ID-Token (106), der einem Nutzer (102) zugeordnet ist, wobei der ID-Token einen nichtflüchtigen elektronischen Speicher (118) mit einem geschützten Speicherbereich (124) aufweist, in dem Attribute gespeichert sind, wobei ein Zugriff auf den geschützten Speicherbereich nur über einen Prozessor (128) des ID-Tokens möglich ist, und wobei der ID-Token eine Kommunikationsschnittstelle (108) zur Kommunikation mit einem Lesegerät (101) eines Nutzer-Computersystems (100) aufweist, mit folgenden Schritten:

- Senden einer Dienstanforderung (103) des Nutzers von dem Nutzer-Computersystem über ein Netzwerk an einen Dienst-Computersystem, welches mit einem ID-Provider-Computersystem gekoppelt ist,
- Senden einer ersten Attributspezifikation (105) von dem Dienst-Computersystem an das ID-Provider-Computersystem über das Netzwerk, wobei die erste Attributspezifikation diejenigen Attribute spezifiziert, die das Dienst-Computersystem zur Erbringung des mit der Dienstanforderung angeforderten Dienstes benötigt,
- Authentifizierung des Nutzers gegenüber dem ID-Token,
- Authentifizierung des ID-Provider-Computersystems gegenüber dem ID-Token,
- Authentifizierung des ID-Tokens gegenüber dem ID-Provider-Computersystem,
- Aufbau eines ersten gesicherten Übertragungskanal (SM[CA]#1) mit Ende-zu-Ende-Verschlüsselung zwischen dem ID-Token und dem ID-Provider-Computersystem über das Netzwerk,
- Durchführung eines ersten Lesezugriffs (107) des ID-Provider-Computersystems auf den ID-Token zum Lesen der Attribute gemäß der ersten Attributspezifikation aus dem ID-Token,
- Übertragung einer in dem Speicherbereich des ID-Tokens gespeicherten ersten Teilmenge der in der ersten Attributspezifikation spezifizierten Attribute (109) von dem ID-Token an das ID-Provider-Computersystem über den ersten gesicherten Übertragungskanal,
- Erzeugung einer zweiten Attributspezifikation (111) einer zweiten Teilmenge der Attribute der ersten Attributspezifikation, die diejenigen Attribute spezifiziert, welche in der ersten Teilmenge nicht beinhaltet sind und Übertragung der zweiten Attributspezifikation von dem ID-Provider-Computersystem an den ID-Token über den ersten gesicherten Übertragungskanal,
- Speicherung der zweiten Attributspezifikation in dem ID-Token,
- Authentifizierung eines Attribut-Provider-Computersystems (172) gegenüber dem ID-Token,
- Authentifizierung des ID-Tokens gegenüber dem Attribut-Provider-Computersystem,
- Aufbau eines zweiten gesicherten Übertragungskanal (SM[CA]#2) mit Ende-zu-Ende-Verschlüsse-

lung zwischen dem Attribut-Provider-Computersystem und dem ID-Token, wobei der erste gesicherte Übertragungskanal bestehen bleibt,

- Übertragung der zweiten Attributspezifikation von dem ID-Token über den zweiten gesicherten Übertragungskanal an das Attribut-Provider-Computersystem,
- Durchführung eines Schreibzugriffs (176) des Attribut-Provider-Computersystems über den zweiten gesicherten Übertragungskanal zum Speichern von Attributen gemäß der zweiten Attributspezifikation in dem ID-Token,
- Durchführung eines zweiten Lesezugriffs (177) des ID-Provider-Computersystems über den ersten gesicherten Übertragungskanal zum Lesen der von dem Attribut-Provider-Computersystem gemäß der zweiten Attributspezifikation in dem ID-Token gespeicherten Attribute,
- Ausgabe der aufgrund der Lesezugriffe von dem ID-Provider-Computersystem aus dem ID-Token ausgelesenen Attribute an das Dienst-Computersystem.

2. Verfahren nach Anspruch 1, wobei die Kommunikationsschnittstelle des ID-Token zur drahtlosen Kommunikation und zur drahtlosen Einkopplung von Energie in den ID-Token durch das Lesegerät ausgebildet ist, um den ID-Token mit der für seinen Betrieb erforderlichen elektrischen Energie zu versorgen, wobei der ID-Token einen flüchtigen elektronischen Speicher (113) aufweist, in dem die zweite Attributspezifikation gespeichert wird, sodass die zweite Attributspezifikation aus dem flüchtigen elektronischen Speicher gelöscht wird, wenn der ID-Token aus der Reichweite des Lesegeräts entfernt wird, und wobei die aufgrund des Schreibzugriffs des Attribut-Provider-Computersystems in dem ID-Token gespeicherten Attribute in dem nicht-flüchtigen elektronischen Speicher (118) gespeichert werden, sodass auf diese durch einen nachfolgenden weiteren ersten Lesezugriff aufgrund einer weiteren Dienstanforderung zugegriffen werden kann oder alternativ Speicherung der zweiten Attributspezifikation in dem nicht-flüchtigen Speicher.

3. Verfahren nach Anspruch 1 oder 2, wobei die folgenden weiteren Schritte durchgeführt werden, wenn die aufgrund des Schreibzugriffs (176) von dem Attribut-Provider-Computersystem geschriebenen Attribute eine dritte Teilmenge der zweiten Attributspezifikation sind:

- Erzeugung einer dritten Attributspezifikation (178) der dritten Teilmenge der zweiten Teilmenge, die diejenigen Attribute der zweiten Teilmenge spezifiziert, die in den aufgrund des Schreibzugriffs in den ID-Token geschriebenen Attributen nicht beinhaltet sind,
- Speicherung der dritten Attributspezifikation in dem ID-Token durch das Attribut-Provider-Computersystem zur Ersetzung der zweiten Attributspezifikation,
- Authentifizierung eines weiteren Attribut-Provider-Computersystems (173) gegenüber dem ID-Token,

- Authentifizierung des ID-Tokens gegenüber dem Attribut-Provider-Computersystem,
- Aufbau eines dritten gesicherten Übertragungskanal (SM[CA]#3) mit Ende-zu-Ende-Verschlüsselung zwischen dem ID-Token und dem weiteren Attribut-Provider-Computersystem über das Netzwerk, wobei der erste geschützte Übertragungskanal bestehen bleibt,
- Übertragung der dritten Attributspezifikation von dem ID-Token an das weitere Attribut-Provider-Computersystem über den dritten gesicherten Übertragungskanal,
- Durchführung eines weiteren Schreibzugriffs (**179**) durch das weitere Attribut-Provider-Computersystem über den dritten gesicherten Übertragungskanal zum Schreiben weiterer Attribute gemäß der dritten Attributspezifikation in den ID-Token, wobei mit dem zweiten Lesezugriff des ID-Provider-Computersystems über den ersten gesicherten Übertragungskanal auf den ID-Token auch die aufgrund des weiteren Schreibzugriffs in den ID-Token geschriebenen weiteren Attribute gelesen werden.

4. Verfahren nach Anspruch 3, wobei die dort genannten Schritte iterativ für weitere Attribut-Provider-Computersysteme (**174**, ...) durchgeführt werden, solange bis eine Abbruchbedingung erreicht ist.

5. Verfahren nach Anspruch 4, wobei es sich bei der Abbruchbedingung um Folgendes handelt:

- sämtliche der Attribute gemäß der ersten Attributspezifikation sind in dem ID-Token gespeichert,
- eine maximale Anzahl von Schreibzugriffen ist erreicht,
- eine maximale Zeitdauer seit dem Senden der Dienstanforderung wird überschritten.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Authentifizierung des ID-Provider-Computersystems gegenüber dem ID-Token mithilfe eines Berechtigungszertifikats (**144**) des ID-Provider-Computersystems erfolgt, in dem Leserechte des ID-Provider-Computersystems zum Lesen von Attributen aus dem ID-Token spezifiziert sind, wobei der ID-Token für die Lesezugriffe des ID-Provider-Computersystems eine Prüfung der Leseberechtigung des ID-Provider-Computersystems mithilfe des Berechtigungszertifikats durchführt.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Authentifizierung des Attribut-Provider-Computersystems mithilfe eines Berechtigungszertifikats des Attribut-Provider-Computersystems erfolgt, in dem Rechte des Attribut-Provider-Computersystems zum Lesen einer Attributspezifikation aus dem ID-Token und zum Schreiben von Attributen in den ID-Token spezifiziert sind, wobei der ID-Token das Recht zum Lesen des Attribut-Provider-Computersystems vor der Übertragung einer Attributspezifikation an das Attribut-Provider-Computersys-

tem prüft und wobei der ID-Token das Recht zum Schreiben von Attributen in den ID-Token vor dem Schreiben von Attributen durch das Attribut-Provider-Computersystem prüft.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei vor der Speicherung von Attributen in dem ID-Token aufgrund eines Schreibzugriffs die zu schreibenden Attribute auf einem Display (**181**) des ID-Tokens, des Leseegeräts oder des Nutzer-Computersystems angezeigt werden, und die zu schreibenden Attribute vorzugsweise erst nach Eingabe einer Bestätigung durch den Nutzer durch Betätigung eines Bedienelements (**182**) des ID-Tokens, des Leseegeräts bzw. des Nutzer-Computersystems in den nichtflüchtigen elektronischen Speicher geschrieben werden.

9. Verfahren nach einem der vorhergehenden Schritte, wobei es sich bei dem ID-Token um ein Wert- oder Sicherheitsdokument handelt, insbesondere ein Ausweisdokument, das heißt ein ID-Dokument, insbesondere einen elektronischen Personalausweis, Reisepass, Führerschein, Firmenausweis oder ein Zahlungsmittel, wie zum Beispiel eine Banknote, eine Kreditkarte oder einen sonstigen Berechtigungsnachweis, wie zum Beispiel eine Eintrittskarte, einen Frachtbrief oder ein Visum, insbesondere eine Chipkarte, insbesondere mit RFID- und/oder NFC-Schnittstelle.

10. ID-Token, der einem Nutzer (**102**) zugeordnet ist, wobei der ID-Token einen elektronischen Speicher (**118**) mit einem geschützten Speicherbereich (**124**) aufweist, in dem Attribute gespeichert sind, wobei ein Zugriff auf den geschützten Speicherbereich nur über einen Prozessor (**128**) des ID-Tokens möglich ist, wobei der ID-Token eine Kommunikationsschnittstelle (**108**) zur Kommunikation mit einem Leseegerät eines Nutzer-Computersystems (**100**) aufweist, und wobei der ID-Token zur Durchführung der folgenden Schritte konfiguriert ist:

- Authentifizierung des Nutzers gegenüber dem ID-Token und optional Aufbau eines gesicherten Übertragungskanal zwischen ID-Token und Nutzer-Computersystem,
- Authentifizierung eines ID-Provider-Computersystems gegenüber dem ID-Token,
- Authentifizierung des ID-Tokens gegenüber dem ID-Provider-Computersystem,
- Aufbau eines ersten gesicherten Übertragungskanal mit Ende-zu-Ende-Verschlüsselung zwischen dem ID-Token und dem ID-Provider-Computersystem über das Netzwerk,
- Ermöglichung eines ersten Lesezugriffs des ID-Provider-Computersystems auf den ID-Token zum Lesen der Attribute gemäß einer ersten Attributspezifikation aus dem ID-Token,
- Senden einer in dem Speicherbereich des ID-Tokens gespeicherten ersten Teilmenge der in der ers-

ten Attributspezifikation spezifizierten Attribute von dem ID-Token an das ID-Provider-Computersystem über den ersten gesicherten Übertragungskanal,

- Empfang einer zweiten Attributspezifikation von dem ID-Provider-Computersystem durch den ID-Token über den ersten gesicherten Übertragungskanal,
- Speicherung der zweiten Attributspezifikation in dem ID-Token,
- Authentifizierung eines Attribut-Provider-Computersystems gegenüber dem ID-Token,
- Authentifizierung des ID-Tokens gegenüber dem Attribut-Provider-Computersystem,
- Aufbau eines zweiten gesicherten Übertragungskanals mit Ende-zu-Ende-Verschlüsselung zwischen dem Attribut-Provider-Computersystem und dem ID-Token, wobei der erste gesicherte Übertragungskanal bestehen bleibt,
- Übertragung der zweiten Attributspezifikation von dem ID-Token über den zweiten gesicherten Übertragungskanal an das Attribut-Provider-Computersystem,
- Ermöglichung eines Schreibzugriffs des Attribut-Provider-Computersystems über den zweiten gesicherten Übertragungskanal zum Speichern von Attributen gemäß der zweiten Attributspezifikation in dem ID-Token,
- Ermöglichung eines zweiten Lesezugriffs des ID-Provider-Computersystems über den ersten gesicherten Übertragungskanal zum Lesen der von dem Attribut-Provider-Computersystem gemäß der zweiten Attributspezifikation in dem ID-Token gespeicherten Attribute.

11. ID-Token nach Anspruch 10, wobei die Kommunikationsschnittstelle des ID-Token zur drahtlosen Kommunikation und zur drahtlosen Einkopplung von Energie in den ID-Token durch das Lesegerät ausgebildet ist, um den ID-Token mit der für seinen Betrieb erforderlichen elektrischen Energie zu versorgen, wobei der ID-Token einen flüchtigen elektronischen Speicher aufweist, und der ID-Token so konfiguriert ist, dass die zweite Attributspezifikation in dem flüchtigen elektronischen Speicher gespeichert wird, sodass die zweite Attributspezifikation aus dem flüchtigen elektronischen Speicher gelöscht wird, wenn der ID-Token aus der Reichweite des Lesegeräts entfernt wird, und wobei die aufgrund des Schreibzugriffs des Attribut-Provider-Computersystems in dem ID-Token gespeicherten Attribute in dem nicht-flüchtigen elektronischen Speicher (**118**) gespeichert werden, sodass auf diese durch einen nachfolgenden weiteren ersten Lesezugriff aufgrund einer weiteren Dienstanforderung zugegriffen werden kann.

12. Attribut-Provider-Computersystem mit einer Netzwerk-Schnittstelle (**138**) zum Zugriff auf einen ID-Token (**106**) über ein Netzwerk (**116**), wobei das Attribut-Provider-Computersystem zur Durchführung der folgenden Schritte konfiguriert ist:

- Lesen einer Attributspezifikation (**111**, **178**) aus dem ID-Token durch einen Netzwerkzugriff über einen gesicherten Übertragungskanal,
- Durchführung eines Datenbankzugriffs um Attribute gemäß der Attributspezifikation aus einer Datenbank zu lesen,
- Durchführung eines Schreibzugriffs (**176**, **179**) über den gesicherten Übertragungskanal auf den ID-Token, um die aus der Datenbank gelesenen Attribute in den ID-Token zu schreiben,
- für den Fall, dass nicht sämtliche Attribute gemäß der Attributspezifikation aus der Datenbank auslesbar sind, Erzeugung einer weiteren Attributspezifikation (**178**), die diejenigen Attribute der Attributspezifikation spezifiziert, die in den aufgrund des Schreibzugriffs in den ID-Token geschriebenen Attributen nicht beinhaltet sind,
- Speicherung der weiteren Attributspezifikation in dem ID-Token um die vorherige Attributspezifikation zu ersetzen.

13. Attribut-Provider-Computersystem nach Anspruch 12, mit einem Berechtigungszertifikat zur Authentifizierung gegenüber dem ID-Token, wobei in dem Berechtigungszertifikat Rechte des Attribut-Provider-Computersystems zum Lesen der Attributspezifikation aus dem ID-Token und zum Schreiben von Attributen in den ID-Token spezifiziert sind.

14. Computersystem mit einem ID-Token nach einem der vorhergehenden Ansprüche 10 oder 11 und mit einem ID-Provider-Computersystem (**136**), wobei das ID-Provider-Computersystem (**136**) dazu konfiguriert ist, zum Lesen von Attributen aus dem ID-Token gemäß der ersten Attributspezifikation mehrfach hintereinander über denselben ersten gesicherten Übertragungskanal Attribute aus dem ID-Token auszulesen.

15. Computersystem nach Anspruch 14, mit zumindest einem Attribut-Provider-Computersystem gemäß Anspruch 12 oder 13.

Es folgen 5 Seiten Zeichnungen

Anhängende Zeichnungen

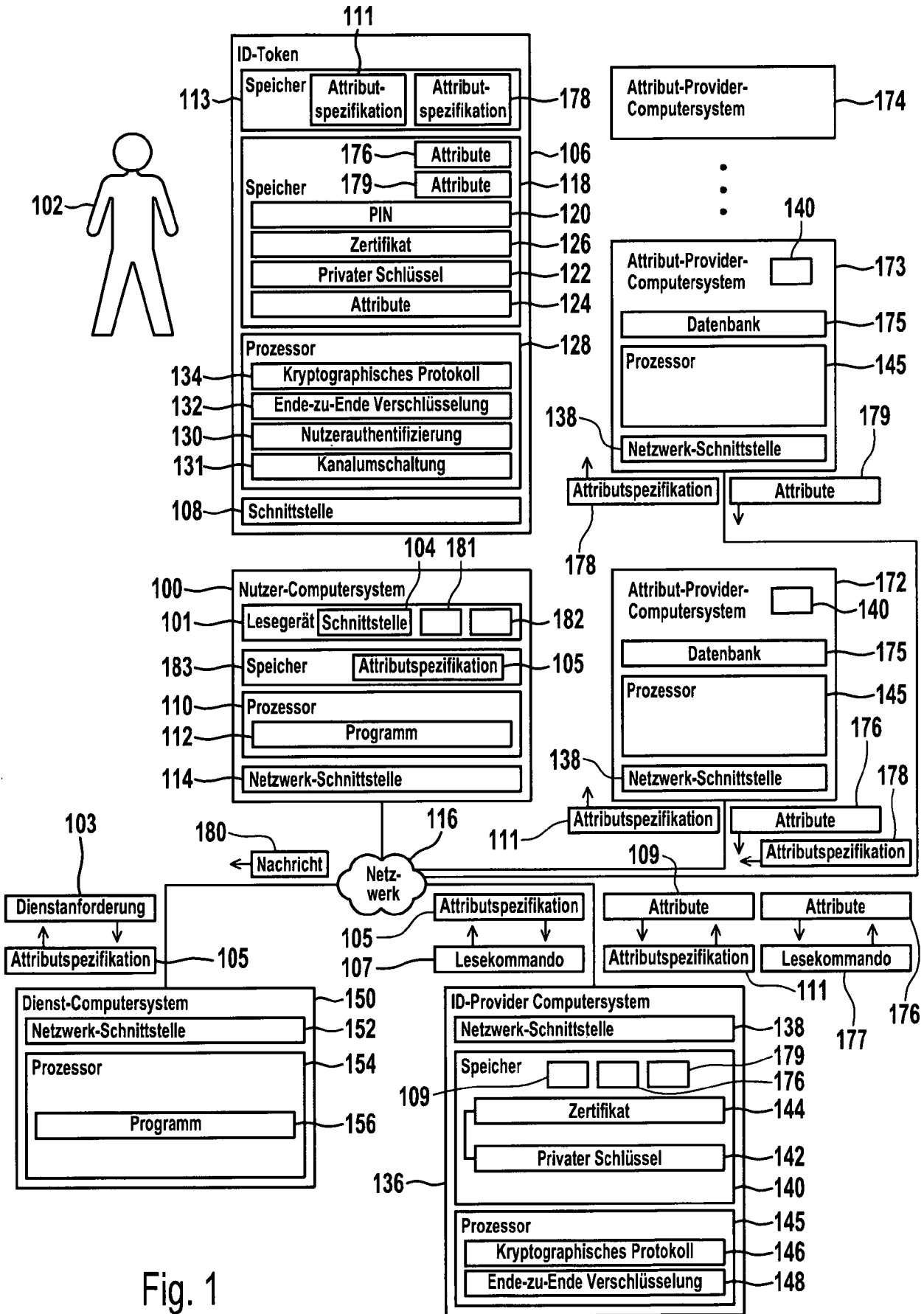


Fig. 1

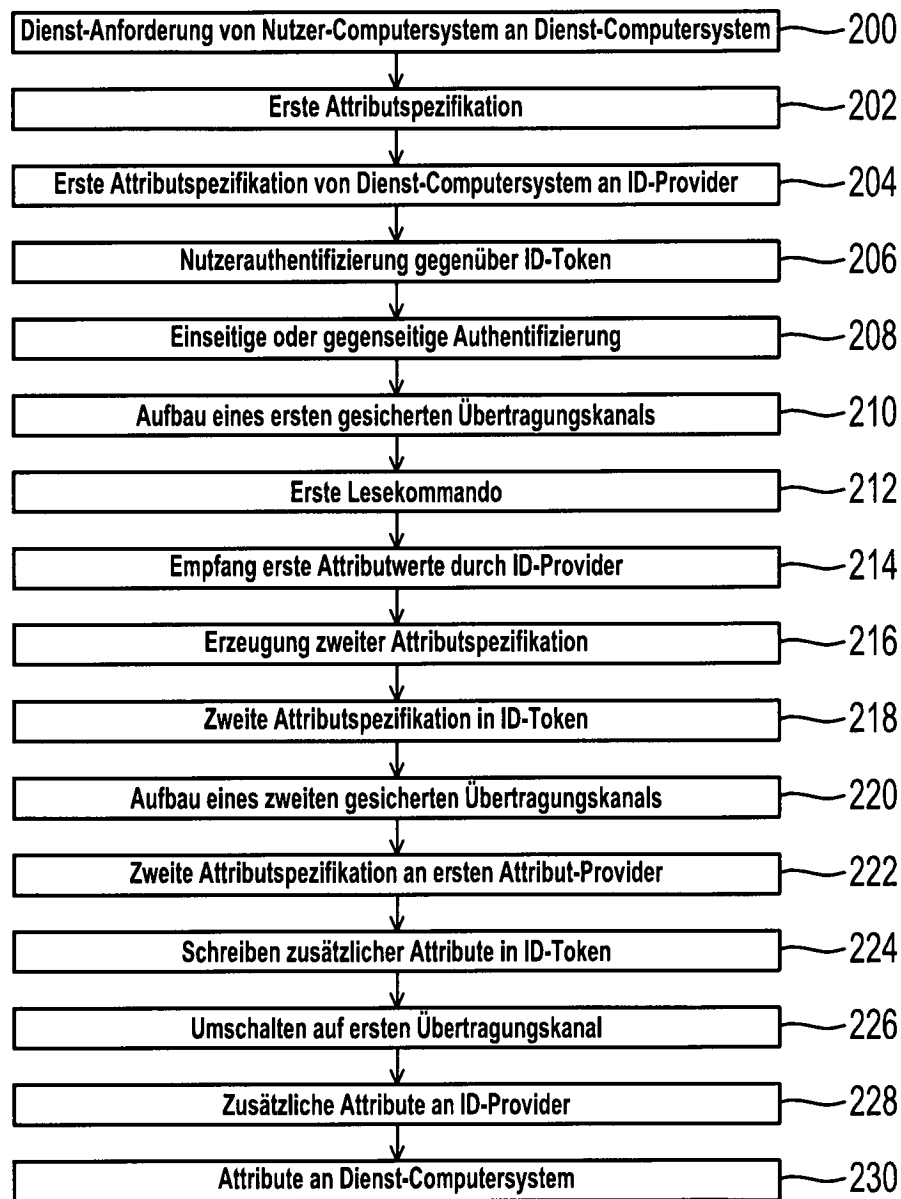


Fig. 2

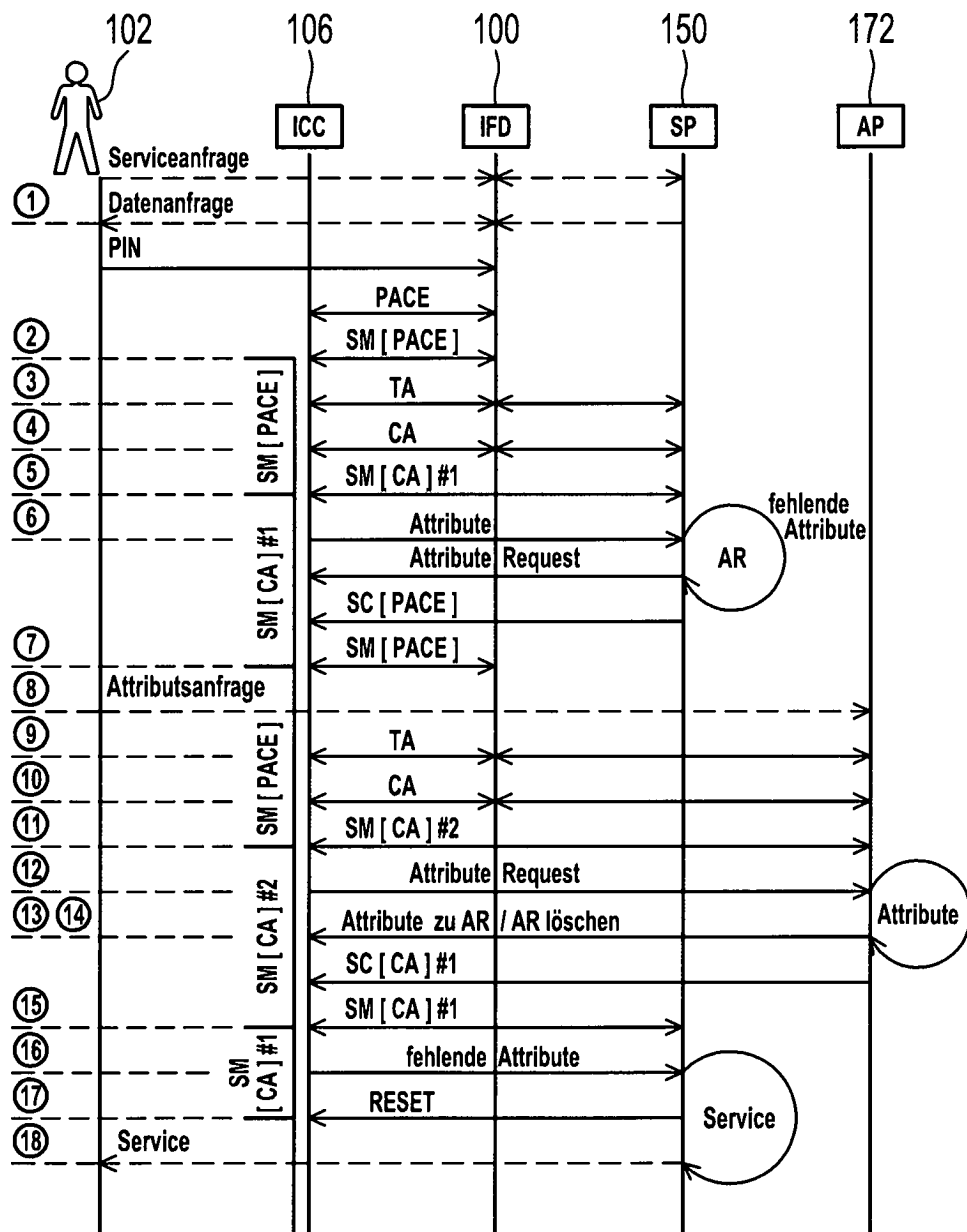


Fig. 3

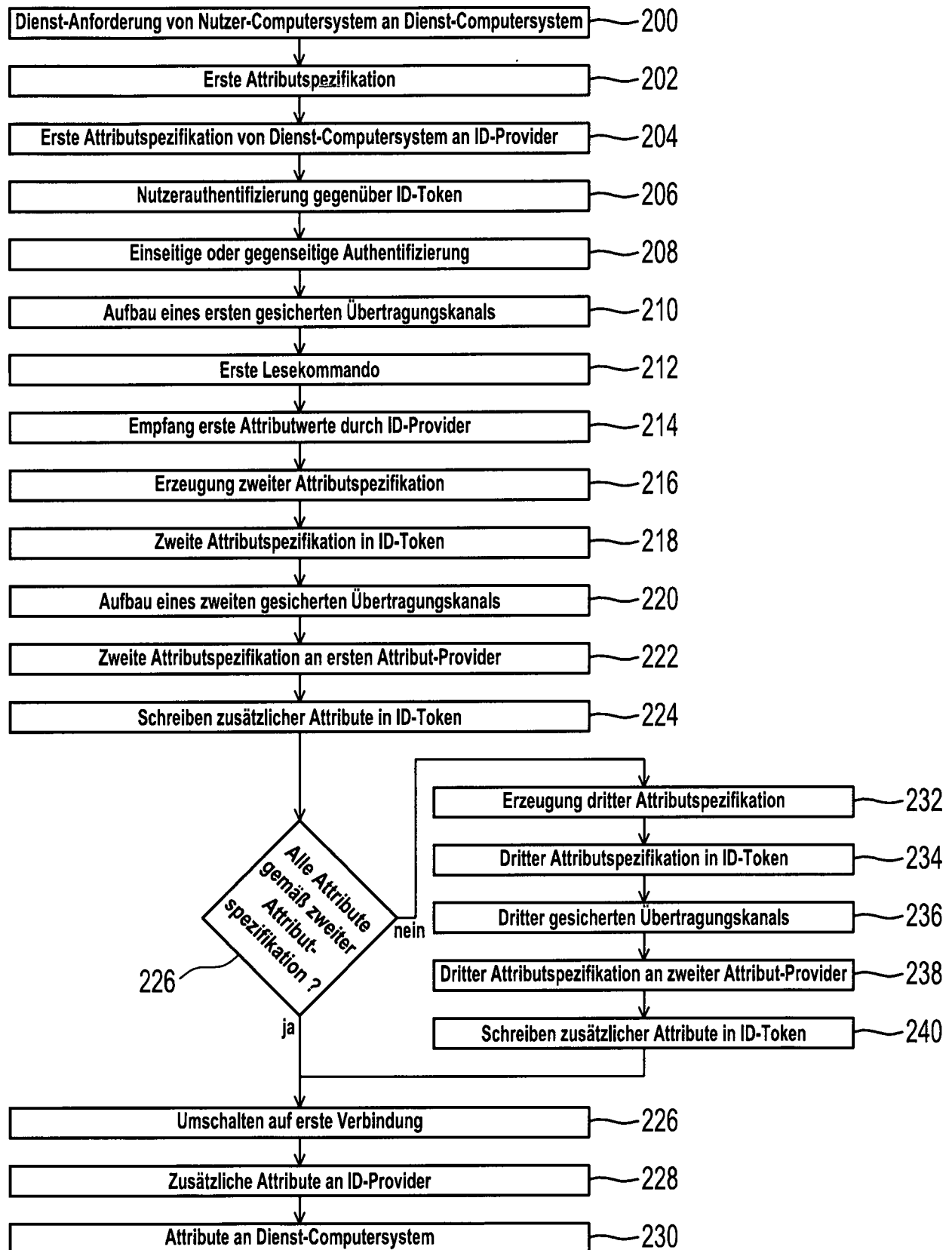


Fig. 4

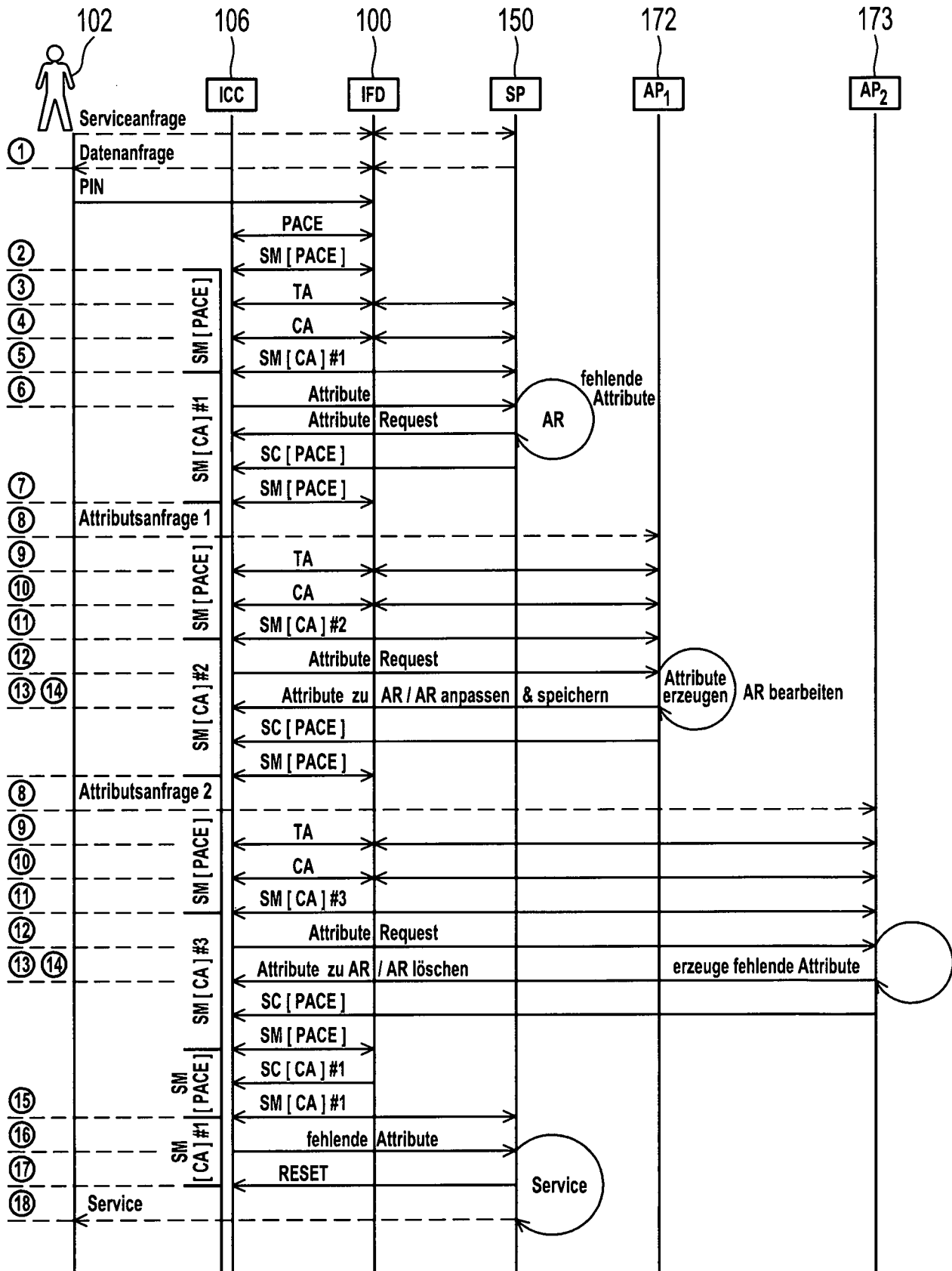


Fig. 5