

(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
28. August 2014 (28.08.2014)



(10) Internationale Veröffentlichungsnummer
WO 2014/128199 A1

(51) Internationale Patentklassifikation:

H04L 29/06 (2006.01) *H04L 9/32* (2006.01)
H04L 29/08 (2006.01) *G06F 21/62* (2013.01)

(21) Internationales Aktenzeichen: PCT/EP2014/053295

(22) Internationales Anmeldedatum:
20. Februar 2014 (20.02.2014)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2013 101 834.3
25. Februar 2013 (25.02.2013) DE

(71) Anmelder: **BUNDESDRUCKEREI GMBH** [DE/DE];
Oranienstraße 91, 10969 Berlin (DE).

(72) Erfinder: **SELHORST, Marcel**; Florastraße 15, 12163
Berlin (DE). **MATEJEK, Ulrich**; Kellerstraße 2, 12167
Berlin (DE).

(74) Anwalt: **KLINSKI, Robert**; Elsenheimerstraße 65, 80687
München (DE).

(81) **Bestimmungsstaaten** (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,
RW, SA, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ,
TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ,
RU, TJ, TM), europäisches (AL, 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, RS, SE,

[Fortsetzung auf der nächsten Seite]

(54) **Title:** ATTRIBUTE NETWORK ENTITY FOR PROVIDING PERSON-SPECIFIC ATTRIBUTES IN ORDER TO
GENERATE DIGITAL ATTRIBUTE CERTIFICATES

(54) **Bezeichnung** : ATTRIBUTNETZWERKENTITÄT ZUR BEREITSTELLUNG VON PERSONENBEZOGENEN
ATTRIBUTEN FÜR DIE ERSTELLUNG VON DIGITALEN ATTRIBUTZERTIFIKATEN

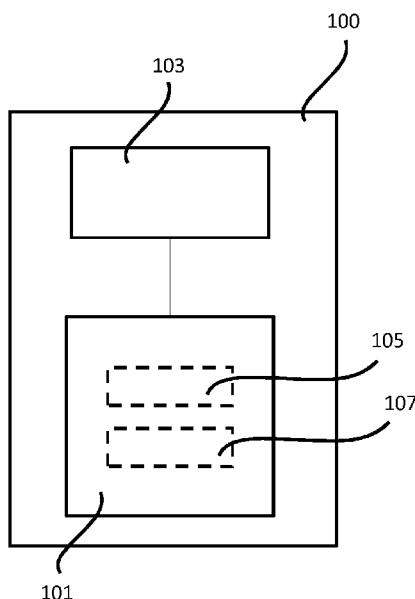


Fig. 1

(57) **Abstract:** The invention relates to an attribute network entity (100) for providing person-specific attributes in order to generate digital attribute certificates. The entity comprises: an attribute database (101) containing an attribute data record (105), said attribute data record (105) comprising at least one attribute for a person and an attribute identification being assigned to the attribute data record (105); and a communication interface (103) which is designed to transmit the attribute data record (105) via a communication network in response to the receipt of a reference identification via a communication network, if the reference identification corresponds to the attribute identification.

(57) **Zusammenfassung:** Die Erfindung betrifft eine Attributnetzwerkentität (100) zur Bereitstellung von personenbezogenen Attributen für die Erstellung von digitalen Attributzertifikaten, mit einer Attributdatenbank (101) mit einem Attributdatensatz (105), wobei der Attributdatensatz (105) zumindest ein Attribut einer Person umfasst, und wobei dem Attributdatensatz (105) eine Attributidentifikation zugeordnet ist, und einer Kommunikationsschnittstelle (103), welche ansprechend auf den Empfang einer Referenzidentifikation über ein Kommunikationsnetzwerk ausgebildet ist, den Attributdatensatz (105) über ein Kommunikationsnetzwerk auszusenden, falls die Referenzidentifikation der Attributidentifikation entspricht.



SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

— vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)

Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

5 Attributnetzwerkentität zur Bereitstellung von personenbezogenen Attributen für die Erstellung von digitalen Attributzertifikaten

Die vorliegende Erfindung betrifft das Gebiet der digitalen Attributzertifikate.

10 Zur elektronischen Signierung von Dokumenten können digitale Signaturzertifikate verwendet werden, welche einer signierenden Person zugeordnet sind. Digitale Signaturzertifikate werden üblicherweise von Zertifizierungsstellen, beispielsweise D-Trust, ausgestellt.

15 Ein digitales Signaturzertifikat kann beispielsweise die Angaben gemäß der EG-Signaturrechtlinie 1999/93/EG umfassen wie den Namen der Person und einen Signaturprüfchlüssel. Das Signaturzertifikat kann ferner eines oder mehrere Attribute der Person angeben. Hierbei kann es sich um eine Organisationszugehörigkeitsbestätigung (OZB) oder um eine Angabe einer Stellung der Person in einer Organisation,
20 beispielsweise in einem Unternehmen, handeln. Ein digitales Signaturzertifikat mit der Angabe des Attributs der Person wird auch als ein digitales Signaturzertifikat für die qualifizierte elektronische Signatur (QES) bezeichnet. Die digitalen Signaturzertifikate werden üblicherweise auf einer sicheren Signaturerstellungseinheit (SSEE), beispielsweise einer Signaturkarte, oder in einem elektronisch auslesbaren Chip eines
25 Identifikationsdokuments gespeichert.

Die Attribute von Personen werden derzeit durch die Zertifizierungsstellen verwaltet. Dadurch ist das Ausstellen von unterschiedlichen digitalen Attributzertifikaten für Personen unterschiedlicher Organisationen erschwert.

30

Es ist die Aufgabe der vorliegenden Erfindung, ein effizienteres Konzept zur Erzeugung von digitalen Attributzertifikaten zu schaffen.

Diese Aufgabe wird durch die Merkmale der unabhängigen Ansprüche gelöst. Vorteilhafte
35 Weiterbildungsformen sind Gegenstand der anhängigen Ansprüche, der Beschreibung und der Figuren.

5 Die Erfindung basiert auf der Erkenntnis, dass die obige Aufgabe durch die Schaffung
zumindest einer dezentralen Attributdatenbank, in welcher beispielsweise
organisationsspezifische bzw. unternehmensspezifische Attribute von Personen abgelegt
sind, gelöst werden kann. Die Attributdatenbank kann beispielsweise durch eine
Zertifizierungsstelle akkreditiert werden. Die Attributdatenbank kann mittels einer
10 Attributnetzwerkentität realisiert werden, welche mit einer Zertifizierungsstelle über ein
Kommunikationsnetzwerk kommunizieren kann. Dadurch wird die Verwaltung der
Attribute dezentralisiert, sodass die Zertifizierungsstellen beispielsweise auf
unterschiedliche Attributdatenbanken zugreifen können, um beispielsweise
unterschiedliche Attribute derselben Person für verschiedene Organisationen abzurufen.

15

Auf diese Weise wird eine vorteilhafte, dezentrale und von einer Zertifizierungsstelle
getrennte Verwaltung von Attributen von Personen erreicht. Dies ermöglicht das Betreiben
einer Mehrzahl von beispielsweise unternehmensspezifischen Attributnetzwerkentitäten,
sodass stets eindeutige Attribute bereitgestellt und zur Erzeugung von digitalen
20 Attributzertifikaten verwenden werden können.

Gemäß einem Aspekt betrifft die Erfindung eine Attributnetzwerkentität zur Bereitstellung
von personenbezogenen Attributen für die Erstellung von digitalen Attributzertifikaten, mit
einer Attributdatenbank mit einem Attributdatensatz, wobei der Attributdatensatz
25 zumindest ein Attribut einer Person umfasst, und wobei dem Attributdatensatz eine
Attributidentifikation zugeordnet ist, und einer Kommunikationsschnittstelle, welche
ansprechend auf den Empfang einer Referenzidentifikation über ein
Kommunikationsnetzwerk ausgebildet ist, den Attributdatensatz über ein
Kommunikationsnetzwerk auszusenden, falls die Referenzidentifikation der
30 Attributidentifikation entspricht. Hierzu kann die Kommunikationsschnittstelle ausgebildet
sein, die Referenzidentifikation von einer entfernten Zertifizierungsstelle über das
Kommunikationsnetzwerk zu empfangen.

Das digitale Attributzertifikat sowie das Attribut können Eigenschaften einer Person
35 gemäß dem Signaturgesetz in dem jeweiligen Land, beispielsweise in Deutschland, oder
einer vergleichbaren Regelung umfassen. So kann das Attribut beispielsweise Angaben
zur Stellung der Person in einer Organisation wie in einem Unternehmen, wie etwa
Geschäftsführer oder Prokurist und einen Namen der Person umfassen. Das Attribut liegt

- 5 in digitaler Form vor und formt den Attributdatensatz oder ist ein Element des Attributdatensatzes. Der Attributdatensatz kann mehrere Attribute derselben Person umfassen. Die Attributidentifikation ist vorgesehen, den Attributdatensatz in der Attributdatenbank eindeutig zu kennzeichnen.
- 10 Die Attributnetzwerkentität kann beispielsweise einem bestimmten Unternehmen zugeordnet sein. In diesem Falle betrifft das Attribut gemäß einer Ausführungsform ausschließlich die Stellung der Person in diesem bestimmten Unternehmen, beispielsweise als Geschäftsführer. Ist diese Person beispielsweise ebenfalls in einem anderen Unternehmen tätig, beispielsweise als Prokurist, so kann eine weitere
- 15 Attributnetzwerkentität, welche dem anderen Unternehmen zugeordnet ist, ein anderes Attribut dieser Person bereitstellen, welches ausschließlich die Stellung dieser Person in dem anderen Unternehmen betrifft.

Bei der Attributidentifikation kann es sich um eine Attributdatenbankangabe handeln,
20 welche ein Auffinden eines Datensatzes in der Attributdatenbank ermöglicht.

Gemäß einer Ausführungsform identifiziert die Attributidentifikation auch die Attributnetzwerkentität. Dies ist besonders dann vorteilhaft, wenn beispielsweise unterschiedlichen Unternehmen unterschiedliche Attributnetzwerkentitäten zugeordnet
25 sind, welche jeweils unterschiedliche Attribute derselben Person, welche in unterschiedlichen Unternehmen tätig sein kann, bereitstellen. Durch die eindeutige Identifizierung der Attributnetzwerkentität wird sichergestellt, dass genau das durch diese Attributnetzwerkentität bereitgestellte Attribut abgefragt wird.

30 Gemäß einer Ausführungsform ist die Attributdatenbank ausgebildet, einen weiteren Attributdatensatz bereitzustellen, welcher ein anderes Attribut der Person umfasst, und wobei dem weiteren Attributdatensatz eine weitere Attributidentifikation zugeordnet ist, und wobei die Kommunikationsschnittstelle ausgebildet ist, den weiteren Attributdatensatz über das Kommunikationsnetzwerk auszusenden, falls die Referenzidentifikation der
35 weiteren Attributidentifikation entspricht.

Das andere Attribut der Person kann beispielsweise Angaben zur Stellung der Person in einem anderen Unternehmen betreffen. Dadurch wird erreicht, dass dieselbe

- 5 Attributnetzwerkentität unterschiedliche Attribute derselben Person speichern kann. Die unterschiedlichen Attribute können beispielsweise Angaben zu unterschiedlichen Stellungen dieser Person in unterschiedlichen Unternehmen bereitstellen.

Gemäß einer Ausführungsform ist der jeweilige Attributdatensatz durch genau ein Attribut
10 oder durch mehrere Attribute der Person gebildet.

Gemäß einer Ausführungsform ist die Attributnetzwerkentität ausgebildet, die Referenzidentifikation mit der jeweiligen Attributidentifikation zu vergleichen. Der Vergleich kann beispielsweise durch die Kommunikationsschnittstelle oder durch die
15 Attributdatenbank oder durch einen Prozessor der Attributnetzwerkentität durchgeführt werden. Bei Übereinstimmung der Referenzidentifikation mit der jeweiligen Attributidentifikation ist festzustellen, dass die Referenzidentifikation der weiteren Attributidentifikation entspricht.

20 Gemäß einer Ausführungsform umfasst die jeweilige Attributidentifikation eine Attributnummer oder einen Attributindex, wobei die Referenzidentifikation eine Referenznummer oder einen Referenzindex umfasst. Bei dem jeweiligen Index oder bei der jeweiligen Nummer kann es sich um einen Attributdatenbankindex oder eine Attributdatenbanknummer handeln, welche ein Auffinden eines Datensatzes in der
25 Attributdatenbank ermöglicht.

Gemäß einer Ausführungsform stammt die Referenzidentifikation von einer Kommunikationsnetzwerkadresse, wobei die Kommunikationsschnittstelle ausgebildet ist, den Attributdatensatz über das Kommunikationsnetzwerk an die
30 Kommunikationsnetzwerkadresse auszusenden. Die Kommunikationsnetzwerkadresse kann beispielsweise eine URL einer Zertifizierungsstelle sein, wobei die Zertifizierungsstelle durch eine Zertifizierungsnetzwerkentität gebildet sein kann, welche über ein Kommunikationsnetzwerk mit der Attributnetzwerkentität kommunizieren kann, um das Attribut abzurufen und um ein digitales Attributzertifikat mit dem Attribut zu
35 erzeugen. Eine derartige Zertifizierungsstelle ist nachfolgend beschrieben.

Gemäß einer Ausführungsform ist die Attributdatenbank ausgebildet, eine Mehrzahl von Attributdatensätzen, welche jeweils zumindest ein Attribut einer Person umfassen,

5 bereitstellen, wobei jedem Attributdatensatz eine Attributidentifikation zugeordnet ist. Dadurch wird erreicht, dass die Attributnetzwerkentität Attribute unterschiedlicher Personen bereitstellen kann. Diese Personen können beispielsweise eine Personengruppe desselben Unternehmens bilden oder unterschiedlichen Unternehmen zugeordnet sein.

10

Gemäß einem weiteren Aspekt betrifft die Erfindung eine Zertifizierungsnetzwerkentität zum Erzeugen eines digitalen Attributzertifikates, mit einer Kommunikationsschnittstelle zum Aussenden einer mit einer Person assoziierbaren Referenznummer über ein Kommunikationsnetzwerk an eine Attributnetzwerkentität, um einen Attributdatensatz, 15 welcher zumindest ein Attribut der Person umfasst, von der Attributnetzwerkentität anzufordern, wobei die Kommunikationsschnittstelle ferner ausgebildet ist, den Attributdatensatz über das Kommunikationsnetzwerk ansprechend auf das Aussenden der Referenznummer zu empfangen, und einem Prozessor zum Erzeugen des digitalen Attributzertifikats auf der Basis des empfangenen Attributs.

20

Die Zertifizierungsnetzwerkentität bildet gemäß einer Ausführungsform eine Zertifizierungsstelle, welche ausgebildet sein kann, digitale Attributzertifikate und/oder digitale Signaturzertifikate gemäß dem Signaturgesetz in dem jeweiligen Land zu erzeugen.

25

Gemäß einer Ausführungsform ist die Kommunikationsschnittstelle ferner ausgebildet, ein digitales Signaturzertifikat der Person zu empfangen, insbesondere aus einem elektronisch auslesbaren Identifikationsdokument der Person auszulesen, wobei der Prozessor ausgebildet ist, das empfangene Attribut mit dem digitalen Signaturzertifikat zu 30 verknüpfen, um das digitale Attributzertifikat zu erzeugen. Die Verknüpfung kann durch einen Verweis auf das digitale Signaturzertifikat in dem digitalen Attributzertifikat erfolgen. Ein Beispiel hierfür ist der Verweis auf das digitale Signaturzertifikat in dem digitalen Attributzertifikat gemäß dem deutschen Signaturgesetz.

35

Gemäß einer Ausführungsform ist die Kommunikationsschnittstelle ausgebildet, die Referenznummer vor dem Aussenden zu empfangen. Die Referenznummer kann beispielsweise durch die Person selbst der Zertifizierungsnetzwerkentität übermittelt werden. Hierzu kann die Person die Referenznummer beispielsweise mithilfe einer

5 graphischen Benutzerschnittstelle oder einer Web-Maske eingeben und ggf. über ein Kommunikationsnetzwerk an die Zertifizierungsnetzwerkentität übermitteln. Die Referenznummer kann jedoch auch durch einen Bediener der Zertifizierungsnetzwerkentität eingegeben werden, falls die Referenznummer beispielsweise als Ausdruck oder postalisch übermittelt wird. Die Referenznummer kann
10 beispielsweise durch die vorgenannte Attributnetzwerkentität vorgegeben und der Person zugeteilt sein.

Gemäß einer Ausführungsform ist die Kommunikationsschnittstelle ferner ausgebildet, das digitale Attributzertifikat über das Kommunikationsnetzwerk auszusenden.

15

Gemäß einer Ausführungsform ist die Kommunikationsschnittstelle ferner ausgebildet, ein digitales Signaturzertifikat der Person aus einem elektronisch auslesbaren Identifikationsdokument der Person auszulesen, wobei der Prozessor ausgebildet ist, das digitale Attributzertifikat nur bei Gültigkeit des digitalen Signaturzertifikats zu erzeugen.

20 Dadurch wird sichergestellt, dass die Person ein gültiges digitales Signaturzertifikat hat, mit dem das digitale Attributzertifikat, beispielsweise durch einen Verweis, verknüpft wird. Hierbei kann auch die Signatur der Person überprüft werden.

Gemäß einer Ausführungsform ist die Zertifizierungsnetzwerkentität ferner ausgebildet,
25 ein digitales Signaturzertifikat einer Person zu erzeugen.

Gemäß einer Ausführungsform ist die Zertifizierungsnetzwerkentität durch einen Zertifizierungsserver gebildet. Auf diese Weise wird eine elektronisch-basierte Zertifizierungsstelle geschaffen.

30

Gemäß einem weiteren Aspekt betrifft die Erfindung ein Verfahren zum Erstellen eines digitalen Attributzertifikats, mit Aussenden einer mit einer Person assoziierbaren Referenznummer über ein Kommunikationsnetzwerk an eine Attributnetzwerkentität, um einen Attributdatensatz, welcher zumindest ein Attribut der Person umfasst, von der
35 Attributnetzwerkentität anzufordern, ansprechend auf das Aussenden der Referenznummer, Empfangen des Attributdatensatzes mit dem Attribut der Person über das Kommunikationsnetzwerk, und Erzeugen des digitalen Attributzertifikats auf der Basis des empfangenen Attributs.

5

Das Verfahren wird gemäß einer Ausführungsform durch ein Betreiben der erfindungsgemäßen Attributnetzwerkentität und der erfindungsgemäßen Zertifizierungsnetzwerkentität ausgeführt. Dabei wird das digitale Attributzertifikat durch die Zertifizierungsnetzwerkentität erzeugt.

10

Das Kommunikationsnetzwerk kann beispielsweise das Internet sein.

Das Identifikationsdokument ist beispielsweise ein Ausweisdokument, ein Reisepass, ein Zahlungsmittel, beispielsweise eine Bankkarte oder eine Kreditkarte, ein Führerschein, ein

15 Unternehmensausweis, ein Frachtbrief oder ein Berechtigungsausweis mit einem integrierten Schaltkreis zur Bereitstellung eines digitalen Signaturzertifikats der Person.

Weitere Ausführungsbeispiele werden Bezug nehmend auf die beiliegenden Zeichnungen erläutert. Es zeigen:

20

Fig. 1 ein Blockdiagramm einer Attributnetzwerkentität gemäß einer Ausführungsform;

25

Fig. 2 ein Blockdiagramm einer Zertifizierungsnetzwerkentität gemäß einer Ausführungsform; und

Fig. 3 ein Blockdiagramm eines Systems zur Erstellung eines digitalen Attributzertifikats gemäß einer Ausführungsform.

30

Fig. 1 zeigt ein Blockdiagramm einer Attributnetzwerkentität 100 zur Bereitstellung von personenbezogenen Attributen für die Erstellung von digitalen Attributzertifikaten gemäß dem jeweiligen Signaturgesetz in dem jeweiligen Land oder einer analogen Regelung.

35

Ein digitales Attributzertifikat ist die ggf. elektronisch signierte Bindung zwischen Eigenschaften, welche durch ein oder mehrere Attribute angegeben sind und einem digitalen Signaturzertifikat einer Person. Das Attribut kann als Eigenschaft beispielsweise

- 5 die Stellung einer Person in einem Unternehmen, wie etwa Geschäftsführung oder Prokura, umfassen.

Die Attributnetzwerkentität 100 ist gemäß einer Ausführungsform jedoch keine Zertifizierungsstelle und daher nicht vorgesehen, digitale Attributzertifikate zu erzeugen.

- 10 Vielmehr ist die Attributnetzwerkentität 100 vorgesehen, Attribute bereitzustellen, welche von einer Zertifizierungsstelle zur Erstellung von digitalen Attributzertifikaten über ein Kommunikationsnetzwerk von der Attributnetzwerkentität 100 abgerufen werden können. Auf diese Weise wird eine dezentrale Verwaltung von Attributen ermöglicht.

- 15 Die Attributnetzwerkentität 100 umfasst eine Attributdatenbank 101 und eine Kommunikationsschnittstelle 103. Die Attributnetzwerkentität 100 kann optional einen in Fig. 1 nicht dargestellten Prozessor umfassen. Der Prozessor kann der Attributdatenbank 101 oder der Kommunikationsschnittstelle 103 zugeordnet oder ein separates Element der Attributnetzwerkentität 100 sein.

20

Die Attributdatenbank 101 ist vorgesehen, einen Attributdatensatz 105 bereitzustellen, wobei der Attributdatensatz 105 zumindest ein Attribut einer Person umfasst, wobei dem Attributdatensatz 105 eine Attributidentifikation zugeordnet ist. Die Attributidentifikation ermöglicht das Auffinden des Attributdatensatzes 105 in der Attributdatenbank 101. Der Attributdatensatz 105 stellt das Attribut beispielsweise in digitaler Form bereit. Der Attributdatensatz 105 kann auch mehrere Attribute derselben Person umfassen.

25

Die Attributdatenbank 101 kann eine Mehrzahl von unterschiedlichen Attributdatensätzen bereitstellen, welche unterschiedlichen Personen zugeordnet sind. Diese Personen können beispielsweise demselben Unternehmen oder unterschiedlichen Unternehmen angehören. Die Attributdatenbank 101 kann jedoch auch unterschiedliche Attributdatensätze bereitstellen, welche dieselbe Person betreffen und beispielsweise jeweils die Stellung dieser Person in unterschiedlichen Unternehmen angeben.

30

- 35 Die Attributdatenbank 101 kann daher einen weiteren Attributdatensatz 107 bereitstellen, welcher einer anderen Person oder derselben Person zugeordnet ist. Der Attributdatensatz 107 ist durch eine weitere Attributidentifikation in der Attributdatenbank 101 eindeutig identifizierbar.

5

Die Attributidentifikationen, welche jeweils unterschiedliche Attributdatensätze identifizieren, können gemäß einer Ausführungsform auch die Attributnetzwerkentität 100 eindeutig identifizieren. Hierzu kann die Kommunikationsnetzwerkadresse der Attributnetzwerkentität 100, beispielsweise die URL, oder eine Netzwerkkennung der Attributnetzwerkentität 100, welche die Attributnetzwerkentität 100 in einem Kommunikationsnetzwerk eindeutig identifiziert, herangezogen werden. Dadurch wird erreicht, dass beispielsweise nur das Attribut oder die Attribute der Person abgerufen werden, welche deren Stellung beispielsweise nur in einem bestimmten Unternehmen betreffen.

15

Die Kommunikationsschnittstelle 103 ist ausgebildet, die Attributnetzwerkentität 100 an ein Kommunikationsnetzwerk, beispielsweise das Internet, anzubinden. Dadurch wird erreicht, dass eine Zertifizierungsstelle das Attribut bei der Attributnetzwerkentität 100 über das Kommunikationsnetzwerk abrufen kann. Hierzu kann die Zertifizierungsstelle beispielsweise eine Referenznummer an die Attributnetzwerkentität 100 aussenden, um das Attribut abzurufen.

20

Die Kommunikationsschnittstelle 103 ist hierzu ausgebildet, eine Referenzidentifikation über das Kommunikationsnetzwerk zu empfangen und denjenigen Attributdatensatz über das Kommunikationsnetzwerk auszusenden, dessen Attributidentifikation der Referenzidentifikation entspricht. Dies kann auf der Basis einer Attributdatenbankabfrage mit der empfangenen Referenzidentifikation durchgeführt werden.

25

Fig. 2 zeigt ein Blockdiagramm einer Zertifizierungsnetzwerkentität 200 zum Erzeugen eines digitalen Attributzertifikates. Die Zertifizierungsnetzwerkentität 200 kann beispielsweise durch einen Zertifizierungsserver gebildet sein, welcher eine elektronische Zertifizierungsstelle formt oder ein Element einer Zertifizierungsstelle ist.

30

Die Zertifizierungsnetzwerkentität 200 umfasst eine Kommunikationsschnittstelle 201 zum Aussenden einer mit einer Person assoziierbaren Referenznummer über ein Kommunikationsnetzwerk an eine Attributnetzwerkentität, beispielsweise an die Attributnetzwerkentität 100, um einen Attributdatensatz, welcher zumindest ein Attribut der Person umfasst, von der Attributnetzwerkentität anzufordern.

35

5

Die Kommunikationsschnittstelle 201 ist ferner ausgebildet, den Attributdatensatz über das Kommunikationsnetzwerk von der Attributnetzwerkentität, beispielsweise von der Attributnetzwerkentität 100, zu empfangen. Dadurch werden eines oder mehrere Attribute der Person für die Ausstellung eines digitalen Attributzertifikats bereitgestellt.

10

Zur Erzeugung des digitalen Attributzertifikats umfasst die Zertifizierungsnetzwerkentität 200 einen Prozessor 203. Der Prozessor 203 ist gemäß einer Ausführungsform ausgebildet, das digitale Attributzertifikat in an sich bekannter Weise zu erzeugen. Hierbei kann der Prozessor 203 das digitale Attributzertifikat mit einem digitalen Signaturzertifikat der Person verknüpfen.

15

Der Prozessor 203 kann gemäß einer Ausführungsform ausgebildet sein, das digitale Signaturzertifikat der Person zu erzeugen.

20

Gemäß einer Ausführungsform kann die Zertifizierungsnetzwerkentität 200, beispielsweise über die Kommunikationsschnittstelle 201 oder über eine andere Kommunikationsschnittstelle eine weitere, interne oder externe, Netzwerkentität anweisen, das digitale Signaturzertifikats zu erzeugen. Gemäß einer Ausführungsform kann die Attributzertifikat generierende Funktionalität des Prozessors 203 auf die weitere

25

Fig. 3 zeigt ein Blockdiagramm eines Systems zur Erstellung eines digitalen Attributzertifikats mit der Attributnetzwerkentität 100 und der Zertifizierungsnetzwerkentität 200, welche miteinander über die jeweilige Kommunikationsschnittstelle 201 und 103 sowie ein Kommunikationsnetzwerk 301, beispielsweise das Internet, kommunizieren können.

30

35

Zur Erzeugung eines digitalen Attributzertifikates übermittelt beispielsweise eine Person der Zertifizierungsnetzwerkentität 200 eine Referenzidentifikation, unter welcher in der Attributnetzwerkentität 100 ein Attributdatensatz mit einem oder mehreren Attributen der Person in der Attributdatenbank 101 abgelegt ist. Die Referenzidentifikation, beispielsweise eine Referenznummer, kann über eine Web-Maske der Zertifizierungsnetzwerkentität 200 eingegeben und übermittelt werden.

5

Daraufhin übermittelt die Zertifizierungsnetzwerkentität 200 die Referenzidentifikation über das Kommunikationsnetzwerk 301 an die Attributnetzwerkentität 100, um den Attributdatensatz der Person abzurufen.

10

Die Attributnetzwerkentität 100 vergleicht daraufhin die empfangene Referenzidentifikation mit Attributidentifikationen, welche jeweils einem Attributdatensatz zugeordnet sind, und übermittelt einen Attributdatensatz, dessen Attributidentifikation der Referenzidentifikation entspricht, über das Kommunikationsnetzwerk an die Zertifizierungsnetzwerkentität 200. Der übermittelte Attributdatensatz umfasst eines oder

15 mehrere Attribute der Person, welche die Stellung und/oder Befugnisse dieser Person in einem bestimmten Unternehmen angeben.

20

Die Zertifizierungsnetzwerkentität 200 kann auf der Basis des von der Attributnetzwerkentität 100 übermittelten Attributdatensatzes bzw. Attributs überprüfen, ob die Person als Antragsteller und die in dem Attributdatensatz bzw. ob die in dem Attribut hinterlegten Daten identisch sind. Hierzu kann die Zertifizierungsnetzwerkentität 200 über das Kommunikationsnetzwerk 301 eine Kommunikationsverbindung zu einem Identifikationsdokument 303 der Person aufbauen. Das Identifikationsdokument 303 kann elektronisch mittels eines Dokumentenlesers auslesbar sein und hierzu einen digitalen

25 Schaltkreis 305 umfassen, welcher beispielsweise einen RFID-Chip realisiert. Der digitale Schaltkreis 305 kann beispielsweise einen öffentlichen Signaturprüfchlüssel der Person sowie ein digitales Signaturzertifikat der Person umfassen. Der digitale Schaltkreis 305 kann ferner Angaben zu der Person wie etwa einen Namen, Geburtsdatum und eine Adresse bereitstellen. Diese Angaben können ebenfalls in dem Attributdatensatz

30 enthalten sein.

Die Zertifizierungsnetzwerkentität 200 erzeugt auf der Basis des empfangenen Attributes ein digitales Attributzertifikat in an sich bekannter Weise.

35

Hierzu kann die Zertifizierungsnetzwerkentität 200 über das Kommunikationsnetzwerk 301 eine Kommunikationsverbindung zu dem Identifikationsdokument 303 aufbauen, um festzustellen, ob die Person bereits ein digitales Signaturzertifikat hat.

- 5 Falls der digitale Schaltkreis 305 kein digitales Signaturzertifikat der Person umfasst, so kann die Zertifizierungsnetzwerkentität 200 ein digitales Signaturzertifikat der Person erzeugen und dieses in einem Speicherbereich des digitalen Schaltkreises 305 ablegen. Dieses digitale Signaturzertifikat wird für die Erzeugung des digitalen Attributzertifikats der Person, beispielsweise durch einen Verweis, verwendet.
- 10 Gemäß einer Ausführungsform kann die Zertifizierungsnetzwerkentität 200 mit dem digitalen Signaturzertifikat eine Sichere Signaturerstellungseinheit (*SSEE*), beispielsweise gemäß der Richtlinie 1999/93/EG, personalisieren.
- 15 Falls der digitale Schaltkreis 305 bereits ein digitales Signaturzertifikat der Person umfasst, so kann die Zertifizierungsnetzwerkentität 200 dieses digitale Signaturzertifikat auslesen und zur Erzeugung des digitalen Attributzertifikats verwenden. Um die Echtheit des digitalen Signaturzertifikats zu verifizieren kann dieses vor der Übermittlung mit einer digitalen Signatur der Person versehen sein.
- 20 Das digitale Signaturzertifikat kann gemäß einer Ausführungsform ein qualifiziertes digitales Signaturzertifikat (*QES*) sein.
- 25 Durch die dezentrale Verwaltung von Attributen wird gemäß einer Ausführungsform eine kostengünstige Einbindung einer Mehrzahl von Bestätigungsstellen erreicht, wobei ein elektronisch auslesbares Identifikationsdokument sowohl privat als auch beruflich genutzt werden kann.

5 Bezugszeichenliste

	100	Attributnetzwerkentität
	101	Attributdatenbank
	103	Kommunikationsschnittstelle
10	105	Attributdatensatz
	107	Attributdatensatz
	200	Zertifizierungsnetzwerkentität
	201	Kommunikationsschnittstelle
15	203	Prozessor
	301	Kommunikationsnetzwerk
	303	Identifikationsdokument
	305	Digitaler Schaltkreis
20		

5

PATENTANSPRÜCHE

1. Attributnetzwerkentität (100) zur Bereitstellung von personenbezogenen Attributen für die Erstellung von digitalen Attributzertifikaten, mit:
- 10 einer Attributdatenbank (101) mit einem Attributdatensatz (105), wobei der Attributdatensatz (105) zumindest ein Attribut einer Person umfasst, und wobei dem Attributdatensatz (105) eine Attributidentifikation zugeordnet ist; und
- 15 einer Kommunikationsschnittstelle (103), welche ansprechend auf den Empfang einer Referenzidentifikation über ein Kommunikationsnetzwerk ausgebildet ist, den Attributdatensatz (105) über ein Kommunikationsnetzwerk auszusenden, falls die Referenzidentifikation der Attributidentifikation entspricht.
- 20 2. Attributnetzwerkentität (100) nach Anspruch 1, wobei die Attributidentifikation auch die Attributnetzwerkentität (100) identifiziert.
3. Attributnetzwerkentität (100) nach Anspruch 1 oder 2, wobei die Attributdatenbank (101) ausgebildet ist, einen weiteren Attributdatensatz (107) bereitzustellen, welcher ein
- 25 anderes Attribut der Person umfasst, und wobei dem weiteren Attributdatensatz (107) eine weitere Attributidentifikation zugeordnet ist, und wobei die Kommunikationsschnittstelle (103) ausgebildet ist, den weiteren Attributdatensatz (107) über das Kommunikationsnetzwerk auszusenden, falls die Referenzidentifikation der weiteren Attributidentifikation entspricht.
- 30 4. Attributnetzwerkentität (100) nach einem der vorstehenden Ansprüche, wobei der jeweilige Attributdatensatz (105, 107) durch genau ein Attribut oder durch mehrere Attribute der Person gebildet ist.
- 35 5. Attributnetzwerkentität nach einem der vorstehenden Ansprüche, welche ausgebildet ist, die Referenzidentifikation mit der jeweiligen Attributidentifikation zu vergleichen.

5

6. Attributnetzwerkentität (100) nach einem der vorstehenden Ansprüche, wobei die jeweilige Attributidentifikation eine Attributnummer oder einen Attributindex umfasst, und wobei die Referenzidentifikation eine Referenznummer oder einen Referenzindex umfasst.

10

7. Attributnetzwerkentität (100) nach einem der vorstehenden Ansprüche, wobei die Referenzidentifikation von einer Kommunikationsnetzwerkadresse stammt, und wobei die Kommunikationsschnittstelle (103) ausgebildet ist, den Attributdatensatz (105, 107) über das Kommunikationsnetzwerk an die Kommunikationsnetzwerkadresse auszusenden.

15

8. Attributnetzwerkentität nach einem der vorstehenden Ansprüche, wobei die Attributdatenbank (101) ausgebildet ist, eine Mehrzahl von Attributdatensätzen (105, 107), welche jeweils zumindest ein Attribut einer Person umfassen, bereitzustellen, wobei jedem Attributdatensatz (105, 107) eine Attributidentifikation zugeordnet ist.

20

9. Zertifizierungsnetzwerkentität (200) zum Erzeugen eines digitalen Attributzertifikates, mit:

einer Kommunikationsschnittstelle (201) zum Aussenden einer mit einer Person

25

assoziierbaren Referenznummer über ein Kommunikationsnetzwerk an eine Attributnetzwerkentität, um einen Attributdatensatz, welcher zumindest ein Attribut der Person umfasst, von der Attributnetzwerkentität anzufordern, wobei die Kommunikationsschnittstelle (201) ferner ausgebildet ist, den Attributdatensatz über das Kommunikationsnetzwerk ansprechend auf das Aussenden der Referenznummer zu empfangen; und

30

einem Prozessor (203) zum Erzeugen des digitalen Attributzertifikats auf der Basis des empfangenen Attributs.

35

10. Zertifizierungsnetzwerkentität (200) nach Anspruch 9, wobei die Kommunikationsschnittstelle (201) ferner ausgebildet ist, ein Signaturzertifikat der Person zu empfangen, insbesondere aus einem elektronisch auslesbaren Identifikationsdokument der Person auszulesen, und wobei der Prozessor (203) ausgebildet ist, das empfangene

- 5 Attribut mit dem digitalen Signaturzertifikat zu verknüpfen, um das digitale Attributzertifikat zu erzeugen.
11. Zertifizierungsnetzwerkentität (200) nach Anspruch 9 oder 10, wobei die Kommunikationsschnittstelle (201) ausgebildet ist, die Referenznummer vor dem
- 10 Aussenden zu empfangen.
12. Zertifizierungsnetzwerkentität (200) nach Anspruch 9, 10 oder 11, wobei die Kommunikationsschnittstelle (201) ferner ausgebildet ist, das digitale Attributzertifikat über das Kommunikationsnetzwerk auszusenden.
- 15
13. Zertifizierungsnetzwerkentität (200) nach einem der Ansprüche 9 bis 12, wobei die Kommunikationsschnittstelle (201) ferner ausgebildet ist, ein digitales Signaturzertifikat der Person aus einem elektronisch auslesbaren Identifikationsdokument der Person auszulesen, und wobei der Prozessor (203) ausgebildet ist, das digitale Attributzertifikat
- 20 nur bei Gültigkeit des digitalen Signaturzertifikats zu erzeugen.
14. Zertifizierungsnetzwerkentität (200) nach einem der Ansprüche 9 bis 13, welche ferner ausgebildet ist, ein digitales Signaturzertifikat einer Person zu erzeugen.
- 25 15. Verfahren zum Erstellen eines digitalen Attributzertifikats, mit:
- Aussenden einer mit einer Person assoziierbaren Referenznummer über ein Kommunikationsnetzwerk an eine Attributnetzwerkentität, um einen Attributdatensatz, welcher zumindest ein Attribut der Person umfasst, von der Attributnetzwerkentität
- 30 anzufordern;
- Empfangen des angeforderten Attributdatensatzes mit dem Attribut der Person über das Kommunikationsnetzwerk; und
- 35 Erzeugen des digitalen Attributzertifikats auf der Basis des empfangenen Attributs.

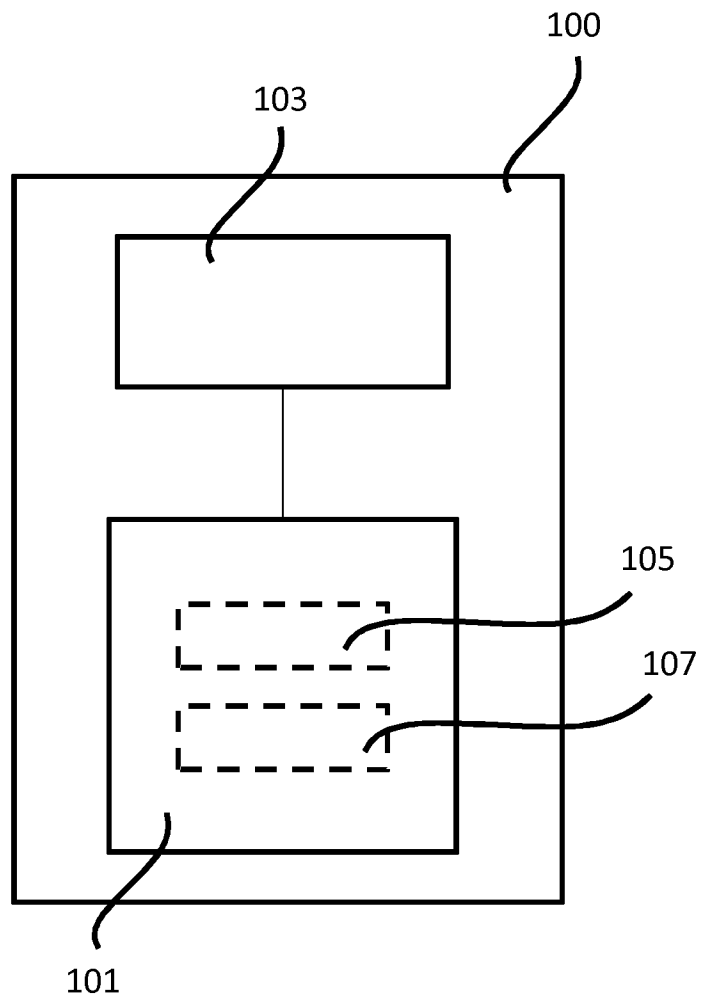


Fig. 1

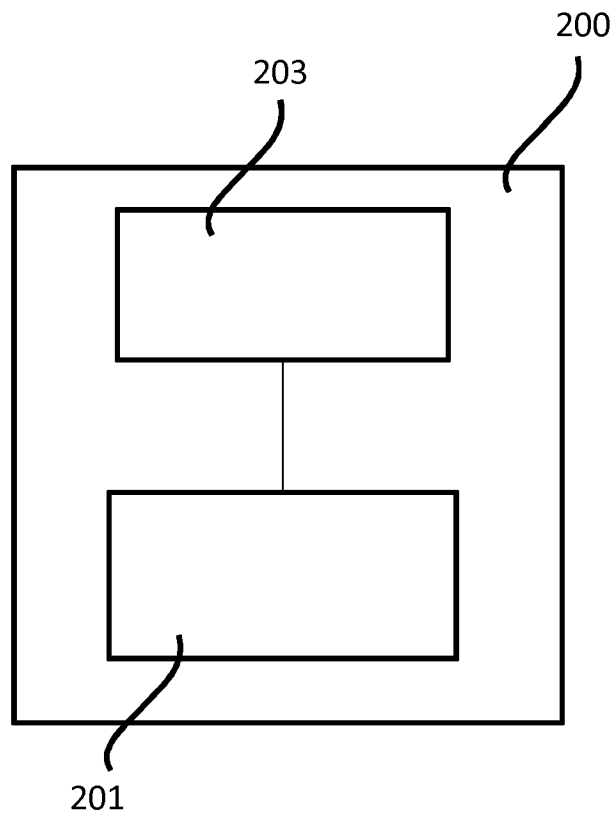


Fig. 2

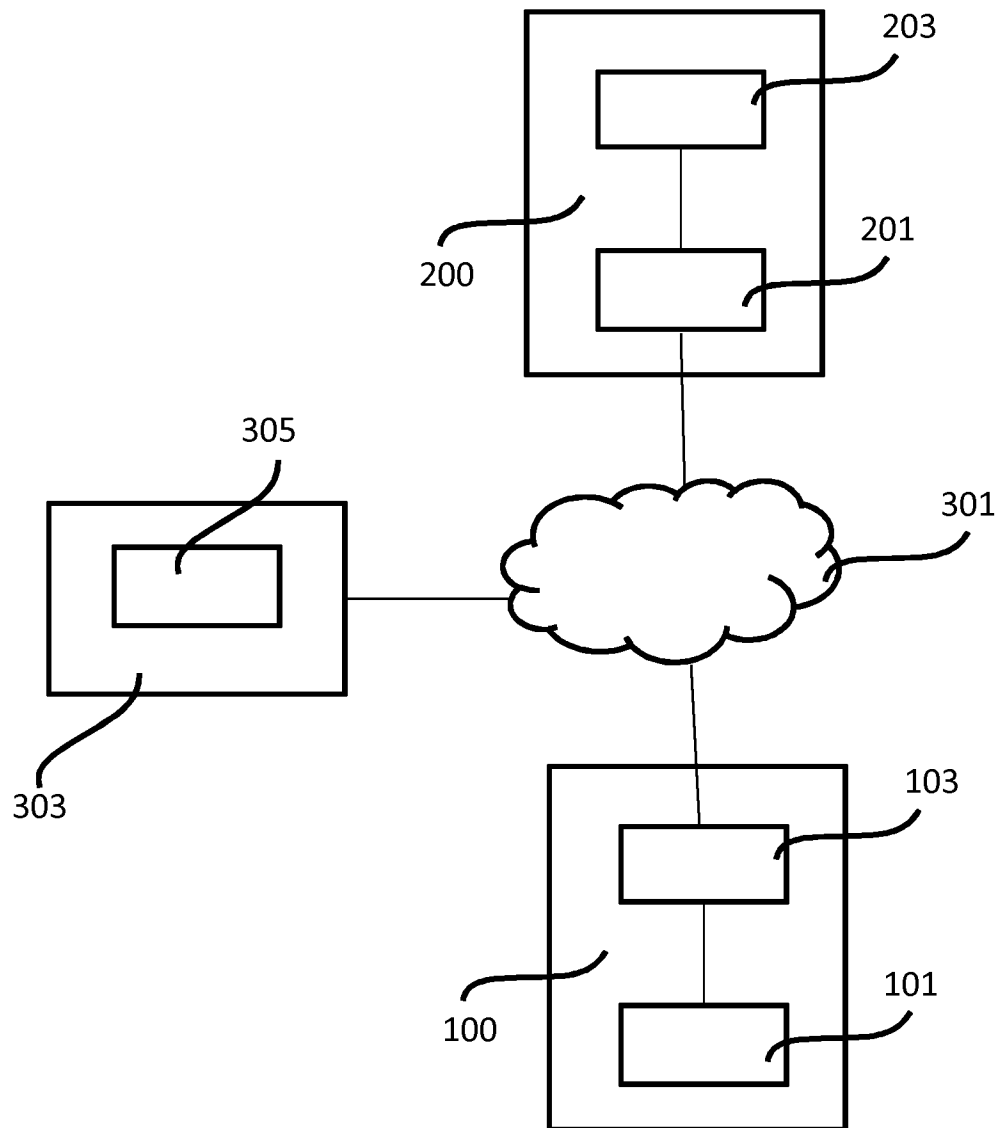


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/053295

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L29/08 H04L9/32 G06F21/62
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/301768 A1 (PARKINSON STEVEN W [US]) 4 December 2008 (2008-12-04) abstract; figures 1-4, 8, 9 paragraphs [0003], [0004], [0016] paragraphs [0023], [0024], [0027] paragraphs [0028], [0031], [0035] paragraphs [0036], [0063], [0069] -----	1-15
X	US 2009/268912 A1 (NAKAE MASAYUKI [JP]) 29 October 2009 (2009-10-29) abstract; figures 1, 16-20 paragraphs [0049], [0101], [0102] paragraphs [0201] - [0206] paragraphs [0214] - [0220] ----- -/-	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

7 July 2014

Date of mailing of the international search report

15/07/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Schossmaier, Klaus

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2014/053295

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/200671 A1 (ISHIGAKI YOSHINOBU [JP] ET AL) 7 September 2006 (2006-09-07) abstract; figures 1,2,4,5 paragraphs [0002], [0003] paragraphs [0049] - [0057] paragraphs [0064], [0070], [0076] -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2014/053295

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008301768	A1	04-12-2008	NONE

US 2009268912	A1	29-10-2009	US 2009268912 A1 29-10-2009
		WO 2008029723 A1	13-03-2008

US 2006200671	A1	07-09-2006	CN 1842817 A 04-10-2006
			JP 5078257 B2 21-11-2012
			US 2006200671 A1 07-09-2006
			US 2012117657 A1 10-05-2012
			WO 2005022428 A1 10-03-2005

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 INV. H04L29/06 H04L29/08 H04L9/32 G06F21/62
 ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 H04L G06F

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2008/301768 A1 (PARKINSON STEVEN W [US]) 4. Dezember 2008 (2008-12-04) Zusammenfassung; Abbildungen 1-4, 8, 9 Absätze [0003], [0004], [0016] Absätze [0023], [0024], [0027] Absätze [0028], [0031], [0035] Absätze [0036], [0063], [0069] -----	1-15
X	US 2009/268912 A1 (NAKAE MASAYUKI [JP]) 29. Oktober 2009 (2009-10-29) Zusammenfassung; Abbildungen 1, 16-20 Absätze [0049], [0101], [0102] Absätze [0201] - [0206] Absätze [0214] - [0220] ----- -/-	1-15



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

7. Juli 2014

Absendedatum des internationalen Recherchenberichts

15/07/2014

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Schossmaier, Klaus

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2006/200671 A1 (ISHIGAKI YOSHINOBU [JP] ET AL) 7. September 2006 (2006-09-07) Zusammenfassung; Abbildungen 1,2,4,5 Absätze [0002], [0003] Absätze [0049] - [0057] Absätze [0064], [0070], [0076] -----	1-15

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2014/053295

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2008301768 A1	04-12-2008	KEINE	

US 2009268912 A1	29-10-2009	US 2009268912 A1	29-10-2009
		WO 2008029723 A1	13-03-2008

US 2006200671 A1	07-09-2006	CN 1842817 A	04-10-2006
		JP 5078257 B2	21-11-2012
		US 2006200671 A1	07-09-2006
		US 2012117657 A1	10-05-2012
		WO 2005022428 A1	10-03-2005
