(19) Deutsches Patent- und Markenamt

(10) **DE 11 2020 000 538 B4** 2025.04.17

(12) # Patentschrift

(21) Deutsches Aktenzeichen: **11 2020 000 538.0**
(86) PCT-Aktenzeichen: **PCT/IB2020/053254**
(87) PCT-Veröffentlichungs-Nr.: **WO 2020/225616**
(86) PCT-Anmeldetag: **06.04.2020**
(87) PCT-Veröffentlichungstag: **12.11.2020**
(43) Veröffentlichungstag der PCT Anmeldung in deutscher Übersetzung: **21.10.2021**
(45) Veröffentlichungstag der Patenterteilung: **17.04.2025**

(51) Int Cl.: ***H04L 9/32*** (2006.01)
G06F 21/33 (2013.01)
G06F 21/62 (2013.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(30) Unionspriorität:
19172926.8 **07.05.2019** **EP**

(73) Patentinhaber:
International Business Machines Corporation, Armonk, NY, US

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

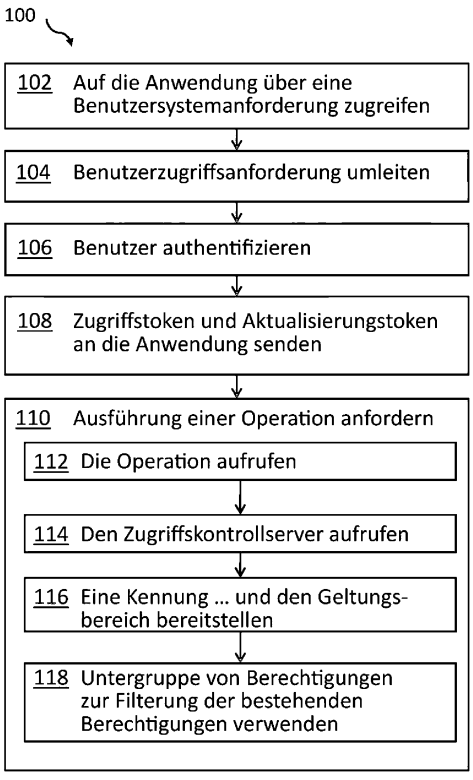
(72) Erfinder:
Smolny, Martin, 71032 Böblingen, DE; Duerr, Thomas, 71032 Böblingen, DE; Beck, Michael, 71032 Böblingen, DE; Schaeck, Juergen, 71032 Böblingen, DE

(56) Ermittelter Stand der Technik:

US	**2016 / 0 028 737**	**A1**
US	**2017 / 0 034 172**	**A1**

(54) Bezeichnung: **FEINKÖRNIGE ZUGRIFFSKONTROLLE AUF TOKEN-GRUNDLAGE**

(57) Zusammenfassung: Ein durch einen Computer umgesetztes Verfahren für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung kann bereitgestellt werden. Die Datenverarbeitungsumgebung weist mindestens ein Benutzersystem, eine Anwendung, einen Authentifizierungsserver und einen Zugriffskontrollserver auf. Das Verfahren weist ein Zugreifen auf die Anwendung über eine Benutzersystemanforderung, ein Umleiten der Benutzerzugriffsanforderung zu einem Authentifizierungsserver, ein Authentifizieren des Benutzers auf, wobei Authentifizierungs-Anmeldedaten eine Anforderung für eine eingeschränkte Berechtigung aufweisen, wobei die eingeschränkte Berechtigung eine Untergruppe von bestehenden Berechtigungen darstellt, die durch den Zugriffskontrollserver für eine Ressource verwaltet werden. Das Verfahren weist auch ein Senden eines Zugriffstokens von dem Authentifizierungsserver an die Anwendung auf, die eine Ausführung einer Operation anfordert, aufweisend ein Aufrufen der Operation durch die Anwendung, die das Zugriffstoken bereitstellt, das die eingeschränkten Berechtigungen aufweist, ein Aufrufen des Zugriffskontrollservers und ein Bereitstellen des Geltungsbereichs des Tokens, das die Untergruppe der bestehenden Berechtigungen aufweist.



Beschreibung

HINTERGRUND

Gebiet der Erfindung

[0001] Die Erfindung betrifft allgemein ein Verfahren für eine Autorisierung auf Token-Grundlage und insbesondere ein durch einen Computer umgesetztes Verfahren für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung. Die Erfindung bezieht sich ferner auf ein damit in Zusammenhang stehendes Zugriffssystem für eine Authentifizierung auf Token-Grundlage in einer Datenverarbeitungsumgebung und ein damit in Zusammenhang stehendes Computerprogrammprodukt.

Technisches Gebiet

[0002] Während des letzten Jahrzehnts entwickelten sich Systeme für Authentifizierung und Autorisierung auf Token-Grundlage. In diesen Systemen authentifiziert sich ein Endbenutzer gegenüber einem Autorisierungsserver und erhält ein temporäres Token zurück, das die Autorisierung dieses Endbenutzers und optional auch seine Identität nachweist. Dieses Token wird z.B. von Benutzerschnittstellen (UI) auf Web-Grundlage verwendet, um Backend-Dienste sicher aufzurufen. Da diesen Diensten keine Anmeldedaten zufließen, ermöglichen Systeme auf Token-Grundlage ein Ökosystem für Dienste von verschiedenen Anbietern, die dasselbe Autorisierungssystem nutzen können. Für komplexere Interaktionen zwischen Diensten ist es auch möglich, das Token von der UI durch einen Dienst zu einem weiteren nachgelagerten Dienst weiterzuleiten.

[0003] Als Bestandteil der Token-Daten übertragen die Nutzdaten für gewöhnlich Autorisierungsgruppen, die als „Geltungsbereiche“ bezeichnet werden. Die Geltungsbereiche werden in den verschiedenen Systemen auf Token-Grundlage sehr unterschiedlich behandelt. Von einer Standardisierungsperspektive aus werden nur ein paar Schlüsselwörter für Geltungsbereiche reserviert, während andere Autorisierung Aufgabe des Autorisierungs-Frameworks ist. Viele dieser Frameworks orientieren sich an einer Aktion und/oder an Modellen auf Rollengrundlage, die oft einen Dienst, eine Komponente und/oder eine Aktion beschreiben. Zum Beispiel wäre ein Funktionsaufruf wie „database.query.read“ ein derartiger potenzieller Geltungsbereich.

[0004] US 2017/0 034 172 A1 beschreibt Verfahren zur Erweiterung des OAuth2-Frameworks, um mit einer einmaligen Authentifizierung Zugriff auf Dienste mehrerer Ressourcenserver in verschiedenen Sicherheitsdomänen zu ermöglichen. Ein Zugriffstoken wird dabei in mehrere reduzierte Zugriffstoken mit eingeschränkten Berechtigungsbereichen aufgeteilt, die jeweils auf eine spezifische Sicherheitsdomäne beschränkt sind.

[0005] US 2016/0 028 737 A1 beschreibt ein OAuth-konformes Framework mit einem generischen Autorisierungsserver, der mehrere Ressourcenserver unterstützt, um den Zugriff gemäß der Zustimmung des Ressourcenbesitzers zu beschränken. Jeder Ressourcenserver registriert beim Autorisierungsserver Metadaten zu anerkannten Berechtigungsbereichen (Scopes), die der Autorisierungsserver bei der Einholung der Zustimmung und der Erstellung von Zugriffstokens berücksichtigt.

KURZDARSTELLUNG DER ERFINDUNG

[0006] Die Erfindung wird durch die Merkmale der unabhängigen Ansprüche beschrieben. Ausführungsformen sind in den abhängigen Ansprüchen angegeben.

[0007] Gemäß einem Aspekt der vorliegenden Erfindung kann ein durch einen Computer umgesetztes Verfahren für eine Autorisierung auf Token-Grundlage mindestens ein Benutzersystem, eine Anwendung, einen Authentifizierungsserver und einen Zugriffskontrollserver aufweisen. Damit kann das Benutzersystem über eine Netzwerkverbindung mit einem Server verbunden werden, der die Anwendung ausführt, und die Anwendung kann einen Zugriff auf eine Operation bereitstellen. Zumindest die Operation kann durch ihre Kennung identifizierbar sein.

[0008] Das Verfahren kann ein Zugreifen auf die Anwendung über eine Benutzersystemanforderung, ein Umleiten der Benutzerzugriffsanforderung zu einem Authentifizierungsserver und ein Authentifizieren des Benutzers durch Authentifizierungs-Anmeldedaten aufweisen, die zwischen dem Authentifizierungsserver und der Anwendung ausgetauscht werden. Damit können die Authentifizierungs-Anmeldedaten eine Anforderung für eine eingeschränkte Berechtigung unter Verwendung einer Standardsemantik eines Geltungsbe-

reichs aufweisen, und die eingeschränkte Berechtigung kann eine Untergruppe von bestehenden Berechtigungen darstellen, die durch den Zugriffskontrollserver für eine Ressource verwaltet oder kontrolliert werden.

[0009] Das Verfahren kann ferner ein Senden eines Zugriffstokens zusammen mit einem Aktualisierungstoken von dem Authentifizierungsserver an die Anwendung aufweisen, wenn die Authentifizierung erfolgreich war und die Anwendung an dem Authentifizierungsserver registriert worden ist, wobei das Zugriffstoken und das Aktualisierungstoken die eingeschränkte Berechtigung aufweisen.

[0010] Das Anfordern einer Ausführung einer Operation durch die Anwendung, initiiert durch das Benutzersystem, kann ein Aufrufen der Operation durch die Anwendung, die das Zugriffstoken bereitstellt, das die eingeschränkten Berechtigungen aufweist, ein Aufrufen des Zugriffskontrollservers durch die Operation, ein Bereitstellen einer Kennung des Benutzersystems und des Geltungsbereichs des Tokens, das die Untergruppe der bestehenden Berechtigungen für den Zugriffskontrollserver aufweist, ein Verwenden der Untergruppe von Berechtigungen zur Filterung der bestehenden Berechtigungen durch den Zugriffskontrollserver aufweisen, was zu einer Zugriffsentscheidung des Benutzersystems für die Operation führt.

[0011] Gemäß einem weiteren Aspekt der vorliegenden Erfindung kann ein damit in Zusammenhang stehendes Zugriffssystem für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung bereitgestellt werden.

[0012] Ferner können Ausführungsformen die Form eines damit in Zusammenhang stehenden Computerprogrammprodukts annehmen, auf das von einem durch einen Computer verwendbaren oder durch einen Computer lesbaren Medium zugegriffen werden kann, das Programmcode zur Verwendung durch einen oder in Verbindung mit einem Computer oder jedem Anweisungsausführungssystem bereitstellt. Für den Zweck dieser Beschreibung kann ein durch einen Computer verwendbares oder durch einen Computer lesbares Speichermedium jede Vorrichtung sein, die Mittel zum Speichern, Übertragen von Daten, Propagieren oder Transportieren des Programms zur Verwendung durch ein oder in Verbindung mit einem System, einer Vorrichtung oder einer Einheit zur Anweisungsausführung enthalten kann.

KURZBESCHREIBUNG DER VERSCHIEDENEN ANSICHTEN DER ZEICHNUNGEN

[0013] Es ist anzumerken, dass Ausführungsformen der Erfindung unter Bezugnahme auf verschiedene Anspruchsgegenstände beschrieben werden. Insbesondere werden einige Ausführungsformen unter Bezugnahme auf Verfahrenstyp-Ansprüche beschrieben, während andere Ausführungsformen unter Bezugnahme auf Vorrichtungstyp-Ansprüche beschrieben werden. Ein Fachmann wird jedoch aus der vorgenannten und der folgenden Beschreibung entnehmen, dass, sofern nichts anderes angegeben ist, zusätzlich zu jeder Kombination von Merkmalen, die zu einem Typ eines Anspruchsgegenstands gehören, auch jede Kombination zwischen Merkmalen, die sich auf verschiedene Anspruchsgegenstände beziehen, insbesondere Merkmale der Verfahrenstyp-Ansprüche und Merkmale der Vorrichtungstyp-Ansprüche, als in diesem Dokument offenbart zu betrachten sind.

[0014] Die oben definierten Aspekte und weitere Aspekte der vorliegenden Erfindung gehen aus den Beispielen von im Folgenden hierin zu beschreibenden Ausführungsformen hervor und werden unter Bezugnahme auf die Beispiele von Ausführungsformen erläutert, auf die die Erfindung jedoch nicht beschränkt ist.

[0015] Bevorzugte Ausführungsformen der Erfindung werden allein zu Beispielzwecken und unter Bezugnahme auf die folgenden Zeichnungen beschrieben:

Fig. 1 zeigt ein Blockschaubild einer Ausführungsform des erfindungsgemäßen, durch einen Computer umgesetzten Verfahrens für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung.

Fig. 2 zeigt ein Blockschaubild eines Interaktionsmodells, das dem hier vorgeschlagenen Konzept zugrunde liegt.

Fig. 3 zeigt ein Blockschaubild einer Ausführungsform einer alternativen Initiierungsinteraktion.

Fig. 4 zeigt eine selbsterklärende Datenübertragungsdarstellung, die auf **Fig.** 3 Bezug nimmt.

Fig. 5 zeigt ein Blockschaubild einer alternativen Interaktion, in der der Client Zugriffstokens und/oder Aktualisierungstokens für den Ressourcenbesitzer mit begrenzten Berechtigungen abruft.

Fig. 6 zeigt ein Blockschaubild eines zweiten Typs einer Interaktion 600, mit der ein Client 204 eine Operation auf einer ungeschützten Komponente 208 aufruft.

Fig. 7 zeigt eine selbsterklärende Datenübertragungsdarstellung, die auf **Fig.** 6 Bezug nimmt.

Fig. 8 zeigt ein Blockschaubild eines dritten Typs einer Interaktion, in der die nicht vertrauenswürdige Komponente mit einem Ressourcenserver 1 und einem Ressourcenserver 2 interagiert.

Fig. 9 zeigt eine selbsterklärende Datenübertragungsdarstellung, die auf **Fig.** 8 Bezug nimmt.

Fig. 10 zeigt ein Blockschaubild eines vierten Typs einer Interaktion, in der der Ressourcenserver 1 und der Ressourcenserver 2 mit einem Zugriffskontrollserver interagieren.

Fig. 11 zeigt eine selbsterklärende Datenübertragungsdarstellung, die auf **Fig.** 10 Bezug nimmt.

Fig. 12 zeigt ein beispielhaftes Pseudocode-Segment einer herkömmlichen Entscheidungsmaschine eines Zugriffskontrollservers.

Fig. 13 zeigt ein beispielhaftes Pseudocode-Segment der hier vorgeschlagenen Entscheidungsmaschine eines Zugriffskontrollservers.

Fig. 14 zeigt ein Blockschaubild des Zugriffssystems für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung.

Fig. 15 zeigt eine Ausführungsform eines Datenverarbeitungssystems, das zum Ausführen von Programmcode für die hier beschriebenen Komponenten geeignet ist.

AUSFÜHRLICHE BESCHREIBUNG

[0016] In dem Kontext dieser Beschreibung können die folgenden Konventionen, Begriffe und/oder Ausdrücke verwendet werden:

[0017] Der Begriff ‚Autorisierung auf Token-Grundlage' kann einen Mechanismus bezeichnen, durch den ein Benutzer eine temporäre Datenstruktur, die als Token bezeichnet wird, von einem Authentifizierungsserver erhalten kann, dem gegenüber er seine Authentifizierung nachgewiesen hat. Ein derartiges Token kann den Benutzer autorisieren, auf vordefinierte Systeme, Anwendungen und/oder Dienste auf beispielsweise anderen Serversystemen zuzugreifen.

[0018] Der Begriff ‚Benutzersystem' kann hier in der Regel eine von einem Benutzer bediente Einheit bezeichnen, wie zum Beispiel ein PC, eine Mobileinheit oder irgendein anderes computerisiertes System, das von einem Endbenutzer bedient wird.

[0019] Der Begriff ‚Anwendung' kann ausführbaren Software-Code bezeichnen, der einen oder mehrere Dienste und Funktionen bereitstellt, nachdem er von einem Benutzersystem aktiviert worden ist. In der Regel kann die Anwendung auf einem Serversystem verwaltet und ausgeführt werden, z.B. ein Serversystem, das in einem Rechenzentrum und/oder unter dem Cloud-Computing-Paradigma betrieben wird. Somit kann das Serversystem in der Regel von dem Benutzersystem entfernt angeordnet betrieben werden.

[0020] Der Begriff ‚Authentifizierungsserver' kann eine vertrauenswürdige Datenverarbeitungsumgebung bezeichnen - die in der Regel von einer Drittpartei für das Benutzersystem und das Serversystem betrieben wird - der gegenüber ein Endbenutzer, der das Benutzersystem betreibt - z.B. unter Verwendung eines Web-Browsers - sich als autorisiert für ein Zugreifen auf vordefiniere Anwendungen und Dienste authentifizieren kann.

[0021] Der Begriff ‚Zugriffskontrollserver' kann ein Hardware- oder Software-System bezeichnen, das befähigt ist, einen Zugriff auf einen spezifischen Dienst, auf eine Anwendung oder ein Benutzersystem, das die Anwendung verwendet, zu gewähren oder zu verweigern.

[0022] Der Begriff ‚Operation' kann eine einzelne Funktion einer Anwendung oder eine Mehrzahl von Funktionen und/oder Diensten von einer oder mehreren Anwendungen bezeichnen. Der Typ der Operation kann definiert und/oder durch einen Geltungsbereich des Zugriffs eingeschränkt werden. Beispiele für Operationen können ein Datenbanklesezugriff, der einen spezifizierten untergeordneten Satz von Daten liest, der diese Daten manipuliert, ein Kombinieren der Daten, ein Ausführen einer Suche in einem Inhaltsverwaltungssystem und ein Zugreifen auf eine spezifische Netzwerkadresse und viele weitere durch Software und/oder Hardware unterstützte Dienste und/oder Funktionen sein.

[0023] Der Begriff ‚Authentifizierungs-Anmeldedaten' kann einen Satz von Daten bezeichnen, die von einem Endbenutzer (oder einem damit in Zusammenhang stehenden System) verwendet werden, um ihn für ein Zugreifen auf vordefinierte Funktionen und Dienst zu autorisieren.

[0024] Der Begriff ‚eingeschränkte Berechtigung' kann auf die Tatsache verweisen, dass ein Benutzersystem und/oder der damit in Zusammenhang stehende Endbenutzer nur auf Funktionen zugreifen und/oder diese verwenden kann, die im Vergleich mit allen verfügbaren Funktionen einer Anwendung oder einer dienstbereitstellenden Entität begrenzt sind. Er kann daher nicht berechtigt sein, den vollständigen Satz von Funktionen oder Diensten zu verwenden, sondern nur einen eingeschränkten untergeordneten Satz, z.B. Daten lesen, aber die Daten nicht ändern, auch dann, wenn die Anwendung dazu imstande wäre.

[0025] Der Begriff ‚Geltungsbereich' kann den definierten Satz von Diensten und/oder Funktionen bezeichnen, auf die ein Benutzersystem oder ein damit in Zusammenhang stehender Endbenutzer oder - im Allgemeinen - ein Systembenutzer Zugriff haben kann. Der Geltungsbereich kann der komplette Satz von Diensten und Funktionen sein, die von einer Ressource zur Verfügung stehen, oder er kann nur auf eine Untergruppe begrenzt sein.

[0026] Der Begriff ‚Standardsemantik' kann hier einen definierten Satz von Befehlen und Funktionen beispielsweise eines standardisierten Autorisierungssystems wie OAuth in Version 2 bezeichnen. Es können jedoch auch andere Versionen unterstützt werden.

[0027] Der Begriff ‚OAuth2' kann den bekannten offenen Standard für Zugriffsdelegierung bezeichnen, der allgemein als eine Möglichkeit für Internet-Benutzer verwendet wird, um Websites und/oder Anwendungen Zugriff auf ihre Informationen auf anderen Websites zu bewilligen, ohne ihnen das Passwort zu geben. Dieser Mechanismus wird auf öffentlichen Internet-Sites weit verbreitet verwendet, um Benutzern zu erlauben, Informationen über ihre Accounts mit Anwendungen oder Websites von Drittparteien zu teilen. - Im Allgemeinen kann OAuth2, das die Version 2 des Standards bezeichnet, Clients einen „sicheren delegierten Zugriff“ auf Ressourcen stellvertretend für einen Ressourcenbesitzer bereitstellen. Es kann einen Prozess für einen Ressourcenbesitzer spezifizieren, um einen Zugriff von Drittparteien auf ihre Ressourcen zu autorisieren - d.h. Dienste und Funktionen - ohne ihre Anmeldedaten zu teilen (d.h. Authentifizierungs-Anmeldedaten). In der Regel werden Zugriffstokens, die durch den Autorisierungsserver an das Benutzersystem ausgegeben werden, zum Bestätigen einer Genehmigung des Ressourcenbesitzers verwendet. Die Drittpartei, d.h. der Endbenutzer mit seinem damit in Zusammenhang stehenden Benutzersystem kann das Zugriffstoken anschließend verwenden, um auf die geschützten Ressourcen zuzugreifen, die von einem Server gehostet werden.

[0028] Außerdem können einige Begriffe - insbesondere Rollen - der bevorzugten Umsetzungsumgebung auf Token-Grundlage von OAuth2 hier ebenfalls definiert werden.

[0029] Im Wesentlichen werden die verwendeten Rollen in der OAuth2-Spezifikation RFC 6749 beschrieben, siehe dazu https://tools.ietf.org/html/rfc6749.

[0030] Ein Ressourcenbesitzer (z.B. Endbenutzer, Systembenutzer) kann eine Entität sein, die fähig ist, Zugriff auf eine geschützte Ressource zu bewilligen. Wenn der Ressourcenbesitzer eine Person ist, wird auf ihn als Endbenutzer Bezug genommen.

[0031] Ein Ressourcenserver (d.h. Dienst) kann der Server sein, der die geschützten Ressourcen hostet, der fähig ist, Anforderungen von geschützten Ressourcen anzunehmen und darauf unter Verwendung von Zugriffstokens zu antworten. Für das hier vorgeschlagene Konzept kann der Ressourcenserver mit einem Zugriffskontrollserver verbunden sein, der helfen kann zu bestimmen, ob eine Operation auf Grundlage eines übergebenen Tokens zugelassen oder verweigert wird.

[0032] Ein Client kann eine Anwendung sein, die Anforderungen von geschützten Ressourcen stellvertretend für den Ressourcenbesitzer und mit dessen Autorisierung stellt. Der Begriff „Client“ impliziert keinerlei Umsetzungseigenschaften, d.h. es kann sich um eine Anwendung auf Web-Grundlage, eine Desktop-Anwendung oder eine auf einer anderen Einheit ausgeführte Anwendung handeln.

[0033] Ein Autorisierungsserver kann der Server sein, der nach einem erfolgreichen Authentifizieren des Ressourcenbesitzers (Endbenutzers) und Erhalten der Autorisierung Zugriffstokens an den Client ausgibt. Der Autorisierungsserver kann derselbe Server wie der Ressourcenserver oder eine separate Entität sein.

Ein einzelner Autorisierungsserver kann Zugriffstokens ausgeben, die von mehreren Ressourcenservern angenommen werden.

[0034] Eine nicht vertrauenswürdige Komponente kann - für das hier beschriebene Konzept und zusätzlich zu den durch OAuth2 definierten Rollen - ein Skript für den Ressourcenbesitzer ausführen. Dazu empfängt sie das Zugriffstoken des Ressourcenbesitzers und verwendet es, um einen oder mehrere Ressourcenserver aufzurufen.

[0035] Ein Zugriffskontrollserver kann - zusätzlich zu den durch OAuth2 definierten Rollen - dazu gedacht sein, Ressourcenserver beim Auswerten von Zugriffsanforderungen durch Vergleichen von Eigenschaften aus dem übergebenen Token mit vorher erstellten Richtlinien zu unterstützen.

[0036] Ferner kann angemerkt werden, dass die Funktion des einzelnen Autorisierungsservers gemäß OAuth2 in dem Kontext des hier vorgeschlagenen Konzepts in einen Authentifizierungsserver und einen Zugriffskontrollserver für die feinkörnigere Autorisierung und Zugriffskontrolle aufgeteilt wurde.

[0037] Das vorgeschlagene durch einen Computer umgesetzte Verfahren für eine Authentifizierung auf Token-Grundlage in einer Datenverarbeitungsumgebung kann viele Vorteile und technische Effekte bieten:

[0038] Das vorgeschlagene Konzept kann nahtlos in ein Identitäts- und Zugriffsmanagement- (Identity and Access Management) System integriert werden, das ein Autorisierungsmodell auf Token-Grundlage verwendet, das eine feinkörnige Zugriffskontrolle für Ressourcenmanagement-Richtlinien erlaubt. Gemäß einem derartigen Modell kann das Token nur den Handelnden - d.h. den Endbenutzer - der ausgeführten Operation identifizieren, kann aber jede Zugriffskontrolle an den aufgerufenen Dienst delegieren. Das Token selbst kann nur einen Mindestsatz an Autorisierungseigenschaften enthalten, es kann z.B. nur angeben, ob das Token zum Aufrufen des Dienstes und/oder der Funktion verwendet werden kann.

[0039] Außerdem kann das Token in bestimmten Szenarios an eine potenziell nicht vertrauenswürdige Komponente zum Ausführen einer Operation übergeben werden. Um die potenzielle Auswirkung von Fehlfunktionen dieser Komponente zu begrenzen, offenbart das vorgeschlagene Konzept eine elegante Möglichkeit zum Begrenzen der Autorisierung eines Tokens, sodass ein Dienst, der ein derartiges Token empfängt, nur Operationen auf einer Liste von spezifischen Diensttypen, Dienstinstanzen, Ressourcentypen und/oder Ressourceninstanzen zulassen wird. Eine derartige Liste kann diese verschiedenen Typen mischen. Der Ziel-Dienst und seine Autorisierungskomponente werden „in der zugrunde liegenden Struktur“ („under the hood“) modifiziert, um diese Begrenzungen effektiv einzuhalten. Der Geltungsbereich der damit in Zusammenhang stehenden Einschränkung der Autorisierung kann nur durch dieses Token vorgegeben werden, wogegen andere Tokens weiterhin ein Ausführen von Operationen auf Grundlage des vollständigen Satzes von Genehmigungen dieses Benutzers autorisieren.

[0040] Es kann ebenfalls angemerkt werden, dass die an dieser Stelle verwendeten Tokens eine Gültigkeit haben, die zeitabhängig jederzeit begrenzt ist. Somit können auch Aktualisierungstokens verwendet werden, die denselben Operationsprinzipien wie die Zugriffs- und/oder Authentifizierungstokens unterliegen.

[0041] Somit besteht das allgemeine Konzept des vorgeschlagenen Konzepts darin, den Zugriff eines Tokens auf eine Untergruppe von bestehenden Berechtigungen eines Ressourcenbesitzers auf eine Dienstinstanz und/oder Ressourceninstanz einzuschränken, indem die spezifische Semantik des Token-Geltungsbereichs definiert wird und die Zugriffskontrolle ohne Änderung der bestehenden Berechtigungen durch Anwenden des semantischen Geltungsbereichs des Tokens modifiziert wird. Somit können die definierten bestehenden Berechtigungen weiterhin unverändert bestehen bleiben; möglicherweise ist nur erforderlich, einen zusätzlichen untergeordneten Satz von begrenzteren Funktionen und/oder Diensten zu definieren.

[0042] Somit kann die aktuell verfügbare Zugriffskontrolle auf dem OAuth2, die aktuell einen Zugriff allein auf den Dienst begrenzen kann, der durch den Dienstnamen identifiziert wird, auf eine Mehrzahl von zusätzlichen Zugriffsbegrenzungen erweitert werden, die derzeit noch nicht zur Verfügung stehen und außerhalb des Standards von OAuth2 liegen, wie beispielsweise

- begrenzter Zugriff auf einen Ressourcentyp in einem Dienst <service-name>.<resource-type>, z.B. kubernetes.pods,
- begrenzter Zugriff auf einen Ressourcentyp in einer Dienstinstanz <service-name>:<service-instance>.<resource-type>, z.B. kubernetes:6271293102982712.pods

• begrenzter Zugriff auf eine Ressource in einem Dienst <service-name>.<resource-type>:<resource>, z.B. kubernetes.pods:mypod,

• begrenzter Zugriff auf eine Ressource in einer Dienstinstanz <service-name>:<service-instance>.<resource-type>:<resource>, z.B. kubernetes:6271293102982712.pods:mypod

[0043] In dem herkömmlichen OAuth2-Ansatz steht nur die folgende Zugriffseinschränkung zur Verfügung:

• begrenzter Zugriff auf nur einen Dienst <service-name>, z.B. kubernetes,

• begrenzter Zugriff auf eine Aktion von nur einem Dienst <service-name>.<action>, z.B. database.read.

[0044] Ferner können Tokens nur mit einer begrenzten Berechtigung erstellt werden; somit haben potenziell gestohlene Tokens einen geringeren Zerstörungsradius. Zum Beispiel können mobile Anwendungen, die Tokens bearbeiten, von einer bösartigen App auf derselben mobilen Einheit debuggt oder gehackt werden. Das Vorhandensein eines begrenzten Satzes von Berechtigungen kann helfen, den potenziellen Zerstörungsradius dieses gestohlenen Tokens zu reduzieren.

[0045] Auch wenn davon abgeraten wird, behalten einige Web-Anwendungen Tokens auf der Client-Seite bei, d.h. im Java-Script-Client des Browsers. Auch hier haben Tokens mit begrenzten Berechtigungen einen geringeren potenziellen Zerstörungsradius im Fall von Website-übergreifenden Scripting-Angriffen

[0046] Gemäß einer bevorzugten Ausführungsform des Verfahrens beruht die Standardsemantik auf OAuth2. Somit kann die verwendete Grundlage für das hier vorgeschlagene Konzept in einen bereits gut definierten Satz von Protokollen und Funktionen integriert werden, indem die bereits grobkörnigeren Zugriffskontrollmechanismen verfeinert oder verbessert werden, um Zugriffskontrollmechanismen umzusetzen, die eine feinkörnigere Kontrolle eines Zugriffs auf Dienste und Funktionen zu erlauben. Dadurch werden die weit verbreitet verwendeten OAuth-Sicherheitsfunktionen - derzeit verfügbar in Version 2 - erweitert und verbessert. Es steht zu erwarten, dass die hier vorgeschlagenen Erweiterungen auch in einer späteren Version von OAuth verwendet werden können.

[0047] Gemäß einer vorteilhaften Ausführungsform des Verfahrens kann die Anwendung eine ungeschützte Komponente, z.B. Jupyter Notebooks, oder ähnliches sein. Jupyter Notebooks - oder Jupyter-Dokumente - können Dokumente bezeichnen, die durch die bekannte Jupyter-Notebook-App erzeugt werden, die sowohl Computercode als auch Rich-Text-Elemente mit Abschnitten, Gleichungen, Figuren, Links usw. aufweisen kann. Dadurch kann die Jupyter-Notebook-App eine Server-Client-Anwendung sein, die ein Bearbeiten und Ausführen von Notebook-Dokumenten z.B. auf einem Serversystem über einen Web-Browser erlaubt.

[0048] Gemäß einer nützlichen Ausführungsform des Verfahrens kann die Anforderung für eine eingeschränkte Berechtigung in den Authentifizierungs-Anmeldedaten eine erste Anforderung aufweisen, wobei die erste Anforderung eine maximale Untergruppe von bestehenden Berechtigungen aufweisen kann. Somit kann die erste Autorisierung ein Zugreifen auf den vollständigen Satz von Diensten und Funktionen erlauben und darf nicht auf eine Untergruppe oder eine eingeschränkte Berechtigung eingeschränkt werden. Eine derartige Einschränkung kann zu einem späteren Zeitpunkt durch ein Anfordern eines Aktualisierungstokens mit der Begrenzung definiert oder angefordert werden.

[0049] Gemäß einer weiteren nützlichen Ausführungsform des Verfahrens kann eine anschließende Anforderung eines Aktualisierungstokens (und des damit in Zusammenhang stehenden Zugriffstokens) - d.h. Zugreifen auf die Anwendung und/oder Funktionen oder Dienst im Anschluss an die erste Anforderung - auch eine Anforderung für eine weitere eingeschränkte Berechtigung aufweisen. Auf diese Weise kann eine Differenzierung zwischen dem ersten Zugriff und anschließenden Zugriffen auf elegante Weise verwaltet werden.

[0050] Gemäß einer zulässigen Ausführungsform des Verfahrens kann die Operation mindestens eine aufweisen, die aus der Gruppe, die einen Zugriff auf vordefinierte Daten, einen Datenbankzugriff, einen Dateizugriff, eine vordefinierte Anwendungsprogrammierschnittstelle (z.B. eine spezifische Analyse oder Maschinenlernfunktionen) und/oder einen Zugriff auf ein spezifisches untergeordnetes Netz eines Netzwerks aufweist, ausgewählt wurde. Im Allgemeinen kann die Operation mit jeder verfügbaren Funktion unterster Ebene, jedem Dienst oder jeder Ressource in Zusammenhang stehen, die in der Datenverarbeitungsumgebung zur Verfügung stehen.

[0051] Gemäß einer vorteilhaften Ausführungsform des Verfahrens kann das Zugriffstoken eine vordefinierte Gültigkeitszeit haben. Wenn der Zugriff also weiterhin autorisiert ist, muss die Autorisierung möglicherweise aktualisiert werden, z.B. durch ein damit in Zusammenhang stehendes Aktualisierungstoken. Die Gültigkeitszeit kann gegenüber den standardmäßigen Token-Lebensdauern bedeutend verkürzt werden.

[0052] Gemäß einer weiteren vorteilhaften Ausführungsform des Verfahrens kann die vordefiniere Gültigkeitszeit durch ein privilegiertes Benutzersystem aktualisierbar sein. Daher kann die feinkörnige Zugriffskontrolle wie jede andere Zugriffskontrolle für eine Gruppe von Ressourcen, Funktionen und/oder Diensten in einer Datenverarbeitungsumgebung verwaltbar sein. Ein vorhandenes IAM-System kann für diese Aufgabe verwendet werden.

[0053] Im Folgenden werden die Figuren ausführlich beschrieben. Alle Anweisungen in den Figuren sind schematisch. Zunächst wird ein Blockschaubild einer Ausführungsform des erfindungsgemäßen, durch einen Computer umgesetzten Verfahrens für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung angegeben. Danach werden weitere Ausführungsformen sowie Ausführungsformen des Zugriffssystems für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung beschrieben.

[0054] **Fig.** 1 zeigt ein Blockschaubild einer Ausführungsform eines durch einen Computer umgesetzten Verfahrens 100 für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung. Die Datenverarbeitungsumgebung weist mindestens ein Benutzersystem, eine Anwendung, einen Authentifizierungsserver und einen Zugriffskontrollserver auf. Das Benutzersystem ist über eine Netzwerkverbindung mit einem Server verbunden, der die Anwendung ausführt, wobei die Anwendung einen Zugriff auf eine Operation bereitstellt - z.B. ein Datenbankzugriff - wobei mindestens die Operation durch ihre Kennung identifizierbar ist.

[0055] Das Verfahren weist ein Zugreifen, 102, auf die Anwendung über eine Benutzersystemanforderung - z.B. über einen Web-Browser, - ein Umleiten, 104, der Benutzerzugriffsanforderung zu einem Authentifizierungsserver und ein Authentifizieren, 106, des Benutzers durch Authentifizierungs-Anmeldedaten auf, die zwischen dem Authentifizierungsserver und der Anwendung ausgetauscht werden. Damit können die Authentifizierungs-Anmeldedaten eine Anforderung für eine eingeschränkte Berechtigung unter Verwendung einer Standardsemantik - insbesondere OAuth2 - eines Geltungsbereichs - gemäß OAuth2.0-Terminologie - aufweisen, wobei die eingeschränkte Berechtigung eine Untergruppe von bestehenden Berechtigungen darstellt, die durch den Zugriffskontrollserver für eine Ressource verwaltet oder kontrolliert werden. Die für die eingeschränkte Berechtigung erforderlichen Daten können in die Standardsemantik eingebettet oder Bestandteil von dieser sein, d.h. das bzw. die verwendeten Standardprotokolle (d.h. OAuth2).

[0056] Das Verfahren 100 weist ferner ein Senden, 108, eines Zugriffstokens zusammen mit einem Aktualisierungstoken von dem Authentifizierungsserver an die Anwendung auf, wenn die Authentifizierung erfolgreich war und die Anwendung an dem Authentifizierungsserver registriert worden ist, wobei das Zugriffstoken und das Aktualisierungstoken die eingeschränkte Berechtigung aufweisen.

[0057] Außerdem weist das Verfahren ein Anfordern, 110, einer Ausführung einer Operation durch die Anwendung auf, initiiert durch das Benutzersystem, wobei das Anfordern ein Aufrufen, 112, der Operation durch die Anwendung aufweist, die das Zugriffstoken bereitstellt, das die eingeschränkten Berechtigungen aufweist, ein Aufrufen, 114, des Zugriffskontrollservers durch die Operation, ein Bereitstellen, 116, einer Kennung des Benutzersystems und des Geltungsbereichs des Tokens, das die Untergruppe der bestehenden Berechtigungen für den Zugriffskontrollserver aufweist, und ein Verwenden, 118, der Untergruppe von Berechtigungen zur Filterung der bestehenden Berechtigungen durch den Zugriffskontrollserver, was zu einer Zugriffsentscheidung des Benutzersystems für die Operation führt.

[0058] Vor einer Fortsetzung der Beschreibung der Figuren sollte die hier verwendete Syntax und Semantik von begrenzten Berechtigungen erläutert werden. Um die Semantik und Syntax von begrenzten Berechtigungen in der bevorzugten Umsetzung zu verstehen, ist ein Verstehen von Cloud-Ressourcennamen (CRNs) nützlich, wie sie z.B. in IBM Cloud und dessen Identitäts- und Zugriffsmanagement-System verwendet werden.

[0059] Die Berechtigungen, CRNs und das gegenwärtige IAM können wie folgt charakterisiert werden: Jeder Dienst und jede Ressource, z.B. in der Cloud-Umgebung, ist eindeutige über einen CRN identifizierbar. Das grundlegende kanonische Format eines CRN lautet:

crn:<version>:<cname>:<ctype>:<service-name>:<location>:<scope>: <service-instance>:<resource-type>:<resource>

[0060] Die Parameter werden in Tabelle 1 beschrieben.

Tabelle 1:

Feld	Inhalt
<version>	Derzeit wird nur v1 unterstützt
<cname>	Für öffentliche Cloud: Bluemix
<ctype>	Für öffentliche Cloud: Öffentlich
<service-name>	Eindeutiger identifizierender Name für einen Diensttyp
<location>	Position der Ressource. Viele Werte sind möglich, global für globale Ressourcen
<scope>	In der Regel ein Account-Geltungsbereich in dem Format a/<account id>
<serviceinstance>	Kennung für eine Dienstinstanz, falls verfügbar. Kann leer sein.
<resource-type>	Optionaler Ressourcentyp in diesem Dienst. Kann leer sein.
<resource>	Optionale Ressourcenkennung. Kann leer sein.

[0061] Die Zugriffskontrollkomponente eines Cloud-IAM speichert Autorisierungen in Richtlinien. Richtlinien erlauben einzelnen Benutzern den Zugriff auf Dienste oder Ressourcen in der Cloud-Computing-Umgebung. Eine Beispiel-Richtlinie wäre:

Identität: IBMid-2700XYZ

Rolle: Administrator

Ziel: crn:v1:bluemix:public:kubernetes::a/1234::::

[0062] Diese Richtlinie erlaubt dem Benutzer mit der Identität „IBMid-2700XYZ“ jede Aktion, die von der Rolle „Administrator“ für jeden Dienst oder jede Ressource abgedeckt wird, die zum Diensttyp „kubernetes“ im Account „1234“ gehört.

[0063] Wenn ein Dienst entscheiden möchte, ob eine bestimmte Aktion zulässig ist, stellt der Dienst dem Zugriffskontrollserver die folgenden Informationen bereit: Identität / Account / erforderliche Aktion / Zielressource / Geltungsbereiche.

[0064] Derzeit wird eine erste Prüfung vorgenommen, ob die Geltungsbereiche das Schlüsselwort „ibm“ enthalten, oder ob die Geltungsbereiche den Dienstnamen enthalten, der in der Zielressource verwendet wird. Ist dies nicht der Fall, gibt die Richtlinienprüfung „Verweigern“ zurück. Nun werden alle potenziell anwendbaren Richtlinien auf Grundlage von Account und Identität ausgewertet. Wenn eine übereinstimmende Richtlinie gefunden wird, gibt die Richtlinienprüfung „GESTATTEN“ zurück.

[0065] Es sollte klar sein, dass die spezifischen Kennungen nur zu Beispielzwecken dienen. Alle anderen Kennungen und/oder Variablen können verwendet werden, ohne den Geltungsbereich des hier vorgeschlagenen Konzepts zu verlassen.

[0066] Fig. 2 zeigt ein Blockschaubild eines Interaktionsmodells 200, das dem hier vorgeschlagenen Konzept zugrunde liegt. Ein Ressourcenbesitzer 202 - in der Regel der Endbenutzer, der vor einem Web-Browser sitzt - agiert mit einem Client 204 - in der Regel eine Web-Anwendung, die dem Endbenutzer einen Dienst anbietet. Für ein interaktives Anmeldeerlebnis wird der Ressourcenbesitzer 202 zur Authentifizierung und Autorisierung der Zugriffsanforderung des Clients zu einem Authentifizierungsserver 206 umgeleitet. Der Client 204 - in der Regel eine Web-Anwendung - interagiert mit dem Authentifizierungsserver 206, um ein Zugriffstoken abzurufen oder zu aktualisieren. Außerdem, als Bestandteile des hier vorgeschlagenen Konzepts, interagiert der Client 204 auch mit einer nicht vertrauenswürdigen Komponente 208, um eine Operation auszuführen.

[0067] Die nicht vertrauenswürdige oder ungeschützte Komponente 208 interagiert mit einem Ressourcenserver 1, 210, und einem Ressourcenserver 2, 212, um ihre Operation auszuführen. Der Ressourcenserver 1, 210, und der Ressourcenserver 2, 212, interagieren mit dem Zugriffskontrollserver 214, um zu bestimmen, ob eine angeforderte Operation gestattet ist oder verweigert wurde.

[0068] In der folgenden bevorzugten Umsetzung verwenden die beispielhaften beiden Ressourcenserver 210, 212 (es können weitaus mehr verwendet werden) zu Beispielzwecken die folgenden Diensttypen, Dienstinstanzen, Ressourcentypen und Ressourceninstanzen gemäß Tabelle 2.

Tabelle 2:

Ressourcenserver 1, 210	Ressourcenserver 2, 212
Diensttyp: COS	Diensttyp: COS
Dienstinstanz: 1	Dienstinstanz: 2
Ressourcentyp: Zeitraum	Ressourcentyp: Zeitraum
Ressourceninstanz: 123	Ressourceninstanz: 456

[0069] Zum Ausführen der Interaktion in dem hier vorgeschlagenen Konzept können die folgenden Schritte erforderlich sein:

1. Der Client 204 ruft Zugriffstokens und Aktualisierungstokens für den Ressourcenbesitzer 202 (abgedeckt durch OAuth2) mit begrenzten Berechtigungen (Bestandteil des neuartigen Konzepts) ab.

2. Der Client 204 ruft eine Operation auf einer nicht vertrauenswürdigen Komponente ab (normales Verhalten in einer Web-Umgebung).

3. Die nicht vertrauenswürdige Komponente 210 interagiert mit dem Ressourcenserver 1, 210, und 2, 212 (normales Verhalten in einer Web-Umgebung).

4. Der Ressourcenserver 1, 210, und der Ressourcenserver 2, 212, interagieren mit einem Zugriffskontrollserver 214, um zu entscheiden, ob die angeforderte Operation gestattet werden soll (Bestandteil des neuartigen Konzepts).

[0070] Als Voraussetzungen können genannt werden: Dem Ressourcenbesitzer 202 wurden Richtlinien auf dem Zugriffskontrollserver 214 zugewiesen, die dem Ressourcenbesitzer 202 erlauben, auf Ressourcen sowohl auf dem Ressourcenserver 1, 210 als auch dem Ressourcenserver 2, 212 zuzugreifen. Diese Richtlinien werden während der folgenden Interaktion nicht geändert, d.h. sind Bestandteil des hier neu vorgeschlagenen Konzepts.

[0071] Fig. 3 zeigt ein Blockschaubild 300 einer Ausführungsform einer alternativen Initiierungsinteraktion: der Client 204 ruft die Zugriffs- und/oder Aktualisierungstokens für den Ressourcenbesitzer 202 mit begrenzten Berechtigungen ab. Der Client 204 ruft ein Zugriffs- und/oder Aktualisierungstoken für den Ressourcenbesitzer 202 durch einen der Bewilligungstypen ab, die im OAuth2-Standard beschrieben werden. Außerdem, und als Bestandteil des neuartigen Konzepts, übergibt der Client 204 bereits eine Liste mit Berechtigungen an den Autorisierungsserver 206, um den potenziellen Zugriff des Zugriffstokens zu begrenzen, das generiert werden soll. Die Angabe einer Liste von Geltungsbereichen während der Token-Erstellung ist Bestandteil des OAuth2-Standards, aber die Semantik der Geltungsbereiche und die Verwendung in späteren Interaktionen sind Bestandteile des hier neu vorgeschlagenen Konzepts. Für diese beispielhafte Interaktion kann angenommen werden, dass die Liste von eingeschränkten Berechtigungen nur ein Element „COS:1.bucket:123“ ist.

[0072] Fig. 4 zeigt eine damit in Zusammenhang stehende selbsterklärende Datenübertragungsdarstellung 400, die den Client 204, den Authentifizierungsserver 206 und den Ressourcenbesitzer 202 mit jeweiligen Meldungsflüssen zeigt.

[0073] Fig. 5 zeigt ein Blockschaubild einer alternativen Interaktion 500, in der der Client 204 Zugriffstokens und/oder Aktualisierungstokens für den Ressourcenbesitzer 202 mit begrenzten Berechtigungen abruft. Der Client 204 ruft ein Zugriffs- und/oder Aktualisierungstoken für den Ressourcenbesitzer 202 durch einen der Bewilligungstypen ab, die im OAuth2-Standard beschrieben werden. In einem nachfolgenden Schritt aktualisiert der Client 204 das Zugriffs- und/oder Aktualisierungstoken unter Verwendung des Bewilligungstyps

refresh_token und übergibt eine Liste von eingeschränkten Berechtigungen an den Autorisierungsserver 206, um den potenziellen Zugriff des Zugriffstokens und des Aktualisierungstokens zu begrenzen, die generiert werden sollen. Die Angabe einer Liste von Geltungsbereichen während einer Token-Aktualisierung ist Bestandteil des OAuth2-Standards, aber die Semantik der Geltungsbereiche und die Verwendung in späteren Interaktionen sind Bestandteile des hier neu vorgeschlagenen Konzepts. Für diese beispielhafte Interaktion kann angenommen werden, dass die Liste von eingeschränkten Berechtigungen nur ein Element „COS:1.bucket:123“ ist.

[0074] Fig. 6 zeigt ein Blockschaubild eines zweiten Typs einer Interaktion 600, mit der der Client 204 eine Operation auf einer ungeschützten Komponente 208 aufruft. Nach der Interaktion gemäß **Fig.** 3, 4, 5 ist ein Zugriffstoken vorhanden, das einen Satz von begrenzten Berechtigungen überträgt. In dieser Beschreibung kann angenommen werden, dass es eine Berechtigung für einen Zugriff auf den Ressourcenserver 2, 212, aber nicht auf den Ressourcenserver 1, 210 aufweist.

[0075] Der Client 204 ruft eine Operation auf einer nicht geschützten oder nicht vertrauenswürdigen Komponente 208 auf. Nicht vertrauenswürdige Komponenten 208 sind z.B. Skripte, die von anderen entwickelt worden sind und nicht als vertrauenswürdig bewertet oder überprüft worden sind. Der Aufruf der nicht vertrauenswürdigen Komponente 208 weist das Zugriffstoken mit begrenzter Berechtigung auf, was Bestandteil des hier vorgeschlagenen Konzepts ist.

[0076] Fig. 7 zeigt eine damit in Zusammenhang stehende selbsterklärende Datenübertragungsdarstellung 700, die den Client 204 und die ungeschützte Komponente 208 mit jeweiligen Meldungsflüssen und Verarbeitungen zeigt.

[0077] Fig. 8 zeigt ein Blockschaubild 800 eines dritten Typs einer Interaktion, in der die nicht vertrauenswürdige Komponente 208 mit einem Ressourcenserver 1, 210 und einem Ressourcenserver 2, 212 interagiert. Als Bestandteil der Ausführung dieser nicht vertrauenswürdigen Komponente 208 startet das Skript eine Operation auf dem Ressourcenserver 1, 210, der das Zugriffstoken mit begrenzten Berechtigungen bereitstellt. Als Bestandteil seiner normalen Verarbeitung interagiert der Ressourcenserver 1, 210 mit dem Zugriffskontrollserver 214, um zu bestimmen, ob der Ressourcenbesitzer, vertreten durch das Zugriffstoken, die Operation ausführen darf. Der Ressourcenserver 1, 210 stellt die Identität in dem Zugriffstoken, die Berechtigungen (Geltungsbereiche) des Zugriffstokens (COS:1.bucket:123) und die Zielressource (z.B. ern:v1:bluemix:public:COS::a/1234:1:bucket:123) bereit, um die Operation auszuführen, die eine explizite Komponente des hier vorgeschlagenen Konzepts ist.

[0078] Auf Grundlage der Berechtigung in dem Zugriffstoken und der bestehenden Richtlinien bestimmt der Zugriffskontrollserver 214, die Operation zu gestatten. Eine ähnliche Interaktion mit dem Ressourcenserver 2, 212 gibt „VERWEIGERN“ zurück, da die Berechtigungen (Geltungsbereiche) des Zugriffstokens (COS:1.bucket:123) nicht mit der Zielressource (crn:v1:blumix:public:COS::a/1234:2:bucket:456) übereinstimmen.

[0079] Fig. 9 zeigt eine damit in Zusammenhang stehende selbsterklärende Datenübertragungsdarstellung 900, die die nicht vertrauenswürdige Komponente 208 und den Ressourcenserver 1, 210 und den Ressourcenserver 2, 212 mit jeweiligen Meldungsflüssen und Verarbeitungen zeigt.

[0080] Fig. 10 zeigt ein Blockschaubild eines vierten Typs einer Interaktion 1000, in der der Ressourcenserver 1, 210 und der Ressourcenserver 2, 212 mit dem Zugriffskontrollserver 214 interagieren. Die nicht vertrauenswürdige Komponente 208 startet eine Operation auf dem Ressourcenserver 1, 210 und danach auf dem Ressourcenserver 2, 212, der das Zugriffstoken mit begrenzten Berechtigungen bereitstellt. Wiederum interagieren die Ressourcenserver 210, 212 als Bestandteil einer normalen OAuth2-Verarbeitung mit dem Zugriffskontrollserver 214, um zu bestimmen, ob es zulässig ist, die Operation auszuführen. Die Ressourcenserver 210, 212 stellen intern die Identität und die Berechtigungen (Geltungsbereiche) des Zugriffstokens und der Zielressource bereit, um die Operation auszuführen.

[0081] Da die eingeschränkten Berechtigungen in dem Token die Dienstinstanz des Ressourcenservers 2, 212 nicht enthalten, entscheidet der Zugriffskontrollserver 214, die Operation des Ressourcenservers 2, 212 zu verweigern, selbst wenn die Richtlinien der Identität in dem Zugriffstoken eine übereinstimmende Richtlinie in dem System aufweisen würden, was wiederum ein expliziter Teil des hier neu vorgeschlagenen Konzepts ist.

[0082] **Fig.** 11 zeigt die damit in Zusammenhang stehende selbsterklärende Datenübertragungsdarstellung 1100, die den Ressourcenserver 1, 210, den Ressourcenserver 2, 212 und den Zugriffskontrollserver 214 mit jeweiligen Meldungsflüssen und Verarbeitungen zeigt.

[0083] Die nächsten beiden **Fig.** 12, 13 zeigen einen Vergleich von Pseudocode-Segmenten einer herkömmlichen Entscheidungsmaschine eines Zugriffskontrollservers (**Fig.** 12) im Vergleich mit derjenigen, die für das hier vorgeschlagene Konzept (**Fig.** 13) erforderlich ist. Wie leicht zu ersehen ist, ist eine komplexere Bestimmung für eine korrekte feinkörnige Zugriffskontrolle für einschränkte Berechtigung erforderlich. Sie garantiert jedoch eine flexiblere und sicherere Ressourcenverwaltung im Vergleich mit der standardmäßigen OAuth2-Zugriffskontrolle.

[0084] Der Vollständigkeit halber zeigt **Fig.** 14 ein Blockschaubild eines Zugriffssystems 1400 für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung. Die Datenverarbeitungsumgebung weist mindestens ein Benutzersystem, eine Anwendung, einen Authentifizierungsserver und einen Zugriffskontrollserver auf (nichts davon ist gezeigt). Damit ist das Benutzersystem über eine Netzwerkverbindung mit einem Server verbunden, der die Anwendung ausführt, und die Anwendung stellt einen Zugriff auf die Operation bereit. Zumindest die Operation ist durch ihre Kennung identifizierbar. Es kann ebenfalls angemerkt werden, dass alle hier erörterten Komponenten mit einem Netzwerk verbunden sind, das die Komponenten verbindet.

[0085] Das Zugriffssystem 1400 weist ein Zugriffsmodul 1402 auf, das für ein Zugreifen auf die Anwendung über eine Benutzersystemanforderung angepasst ist, ein Umleitungsmodul 1404, das für ein Umleiten der Benutzerzugriffsanforderung auf einen Authentifizierungsserver 206 angepasst ist. Der Authentifizierungsserver 206 ist für ein Authentifizieren des Benutzers durch Authentifizierungs-Anmeldedaten angepasst, die zwischen dem Authentifizierungsserver und der Anwendung ausgetauscht werden, wobei die Authentifizierungs-Anmeldedaten eine Anforderung für eine eingeschränkte Berechtigung unter Verwendung einer Standardsemantik eines Geltungsbereichs aufweisen, wobei die eingeschränkte Berechtigung eine Untergruppe von bestehenden Berechtigungen darstellt, die durch den Zugriffskontrollserver für eine Ressource verwaltet werden.

[0086] Das Zugriffssystem 1400 weist ferner einen Sender auf, der zum Senden eines Zugriffstokens zusammen mit einem Aktualisierungstoken von dem Authentifizierungsserver 206 an die Anwendung angepasst ist, wenn die Authentifizierung erfolgreich war und die Anwendung an dem Authentifizierungsserver 206 registriert worden ist, wobei das Zugriffstoken und das Aktualisierungstoken die eingeschränkte Berechtigung aufweisen.

[0087] Somit ist das Benutzersystem für ein Anfordern einer Ausführung einer Operation durch die Anwendung angepasst, initiiert durch das Benutzersystem, wobei das Anfordern einer Ausführung einer Operation ein Aufrufen der Operation durch die Anwendung aufweist, die das Zugriffstoken bereitstellt, das die eingeschränkten Berechtigungen aufweist, ein Aufrufen des Zugriffskontrollservers durch die Operation, ein Bereitstellen einer Kennung des Benutzersystems und des Geltungsbereichs des Tokens, das die Untergruppe der bestehenden Berechtigungen für den Zugriffskontrollserver 214, ein Verwenden der Untergruppe von Berechtigungen zur Filterung der bestehenden Berechtigungen durch den Zugriffskontrollserver 214 aufweist, was zu einer Zugriffsentscheidung des Benutzersystems für die Operation führt.

[0088] Ausführungsformen der Erfindung können zusammen mit praktisch jedem Computertyp umgesetzt werden, unabhängig davon, ob die Plattform zum Speichern und/oder Ausführen von Programmcode geeignet ist. **Fig.** 15 zeigt als Beispiel ein Datenverarbeitungssystem 1500, das zum Ausführen von Programmcode geeignet ist, der mit dem vorgeschlagenen Verfahren in Zusammenhang steht. Praktisch jede Komponente der Verarbeitungsumgebung kann durch ein Datenverarbeitungssystem gemäß **Fig.** 15 dargestellt werden.

[0089] Das Datenverarbeitungssystem 1500 ist nur ein Beispiel für ein geeignetes Computersystem und soll keinerlei Einschränkung hinsichtlich des Schutzumfangs der Verwendung oder der Funktionalität von Ausführungsformen der hierin beschriebenen Erfindung andeuten, gleichgültig, ob das Computersystem 1500 umgesetzt werden kann und/oder irgendeine oben dargelegte Funktionalität ausführen kann. In dem Computersystem 1500 sind Komponenten vorhanden, die mit zahlreichen anderen Universal- oder Sonder-Datenverarbeitungssystemumgebungen oder -Konfigurationen betriebsbereit sind. Zu Beispielen für bekannte Datenverarbeitungssysteme, Umgebungen und/oder Konfigurationen, die für eine Verwendung mit dem Computersystem/Server 1500 geeignet sein können, zählen PC-Systeme, Servercomputersysteme, Thin

Clients, Thick Clients, Handheld- oder Laptop-Einheiten, Multiprozessorsysteme, Systeme auf der Grundlage von Mikroprozessoren, Set-Top-Boxen, programmierbare Unterhaltungselektronik, Netzwerk-PCs, Minicomputersysteme, Mainframe-Computersysteme und verteilte Cloud-Computing-Umgebungen, die beliebige der oben genannten Systeme oder Einheiten und dergleichen aufweisen, sie sind aber nicht darauf beschränkt. Das Computersystem/der Server 1500 kann in dem allgemeinen Kontext von Anweisungen beschrieben werden, die durch ein Computersystem ausführbar sind, wie beispielsweise Programmmodule, die von einem Computersystem 1500 ausgeführt werden. Im Allgemeinen können Programmmodule Routinen, Programme, Objekte, Komponenten, Logik, Datenstrukturen usw. enthalten, die bestimmte Aufgaben ausführen oder bestimmte abstrakte Datentypen umsetzen. Das Computersystem/der Server 1500 kann in verteilten Cloud-Computing-Umgebungen betrieben werden, wobei Aufgaben von entfernt angeordneten Verarbeitungseinheiten ausgeführt werden, die über ein Datenübertragungsnetzwerk verbunden sind. In einer verteilten Cloud-Computing-Umgebung können Programmmodule sich sowohl in lokalen als auch entfernt angeordneten Computersystem-Speichermedien befinden, die Arbeitsspeicher-Speichereinheiten enthalten.

[0090] Wie in der Figur gezeigt, wird das Computersystem/der Server 1500 in der Form einer Universal-Datenverarbeitungseinheit gezeigt. Die Komponenten des Computersystems/Servers 1500 können einen oder mehrere Prozessoren oder eine oder mehrere Verarbeitungseinheiten 1502, einen Systemarbeitsspeicher 1504 und einen Bus 1506 umfassen, die verschiedene Systemkomponenten einschließlich des Systemarbeitsspeichers 1504 mit dem Prozessor 1502 verbinden, sie sind aber nicht darauf beschränkt. Der Bus 1506 stellt einen oder mehrere von mehreren beliebigen Typen von Busstrukturen dar, einschließlich eines Arbeitsspeicherbusses oder Arbeitsspeichercontrollers, eines Peripheriebusses, eines Accelerated Graphics Ports (beschleunigter Grafikanschluss) und eines Prozessors oder lokalen Busses unter Verwendung von einer aus einer Vielfalt von Busarchitekturen. Zum Beispiel und nicht einschränkend umfassen derartige Architekturen einen Industry Standard Architecture- (ISA) Bus, Micro Channel Architecture- (MCA) Bus, Enhanced ISA- (EISA) Bus, einen lokalen Video Electronics Standards Association- (VESA) Bus und Peripheral Component Interconnect- (PCI) Bus. Das Computersystem/der Server 1500 umfasst in der Regel eine Vielfalt von durch ein Computersystem lesbaren Medien. Derartige Medien können alle verfügbaren Medien sein, auf die durch das Computersystem/den Server 1500 zugegriffen werden kann, und sie umfassen sowohl flüchtige als auch nicht flüchtige Medien, austauschbare und nicht austauschbare Medien.

[0091] Der Systemarbeitsspeicher 1504 kann durch ein Computersystem lesbare Medien in der Form von flüchtigem Arbeitsspeicher umfassen wie beispielsweise einen Direktzugriffspeicher (RAM) 1508 und/oder einen Cache-Arbeitsspeicher 1510. Das Computersystem/der Server 1500 kann ferner weitere austauschbare/nicht austauschbare, flüchtige/nicht flüchtige Computersystem-Speichermedien umfassen. Nur als Beispiel kann ein Speichersystem 1512 zum Lesen von einem und Schreiben auf einen nicht austauschbaren, nicht flüchtigen Magnetdatenträger bereitgestellt werden (nicht gezeigt und in der Regel als „Festplatte“ bezeichnet). Obwohl nicht gezeigt, kann ein Magnetplattenlaufwerk zum Auslesen und Beschreiben einer austauschbaren, nicht flüchtigen Magnetplatte (z.B. eine „Diskette“) und ein optisches Plattenlaufwerk zum Auslesen oder Beschreiben einer austauschbaren, nicht flüchtigen optischen Platte wie einem CD-ROM, DVD-ROM oder andere optische Datenträger bereitgestellt werden. In solchen Fällen können alle über eine oder mehrere Datenträgerschnittstellen mit dem Bus 1506 verbunden werden. Wie ferner im Folgenden dargestellt und beschrieben wird, kann der Arbeitsspeicher 1504 mindestens ein Programmprodukt mit einem Satz (z.B. mindestens einem) von Programmmodulen enthalten, die konfiguriert sind, um die Funktionen von Ausführungsformen der Erfindung auszuführen.

[0092] Das Programm/Dienstprogramm, das einen Satz (mindestens einen) von Programmmodulen 1516 aufweist, kann beispielsweise und nicht einschränkend im Arbeitsspeicher 1504 gespeichert werden, ebenso wie ein Betriebssystem, ein oder mehrere Anwendungsprogramme, andere Programmmodule und Programmdaten. Jedes der Betriebssysteme, ein oder mehrere Anwendungsprogramme, andere Programmmodule und Programmdaten oder eine Kombination davon können eine Umsetzung einer Netzwerkumgebung umfassen. Die Programmmodule 1516 führen im Allgemeinen die Funktionen und/oder Methodiken von Ausführungsformen der Erfindung aus, wie hierin beschrieben wird.

[0093] Das Computersystem/der Server 1500 kann auch mit einer oder mehreren externen Einheiten 1518 Daten austauschen, wie zum Beispiel einer Tastatur, einer Zeigeeinheit, einer Anzeige 1520 usw.; einer oder mehreren Einheiten, die es einem Benutzer ermöglichen, mit dem Computersystem/Server 1500 in Wechselbeziehung zu treten; und/oder allen Einheiten (z.B. Netzwerkkarte, Modem usw.), die es dem Computersystem/Server 1500 ermöglichen, mit einer oder mehreren anderen Datenverarbeitungseinheiten Daten auszutauschen. Ein derartiger Datenaustausch kann über Eingabe-/Ausgabe- (E/A) Schnittstellen 1514 erfolgen. Weiterhin kann das Computersystem/der Server 1500 mit einem oder mehreren Netzwerken, wie beispiels-

weise einem lokalen Netzwerk (LAN), einem allgemeinen Weitverkehrsnetzwerk (WAN) und/oder einem öffentlichen Netzwerk (z.B. dem Internet), über einen Netzwerkadapter 1522 Daten austauschen. Wie dargestellt, kann der Netzwerkadapter 1522 mit den anderen Komponenten des Computersystems/Servers 1500 über den Bus 1506 Daten austauschen. Es sollte klar sein, obwohl nicht gezeigt, dass andere Hardware- und/oder Software-Komponenten in Verbindung mit dem Computersystem/Server 1500 verwendet werden könnten. Zu Beispielen gehören Mikrocode, Einheitentreiber, redundante Verarbeitungseinheiten, externe Plattenlaufwerk-Arrays, RAID- (Redundant Array of Independent Disks) Systeme, Bandlaufwerke und Speichersysteme zur Datenarchivierung usw., sie sind aber nicht darauf beschränkt.

[0094] Die Beschreibungen der verschiedenen Ausführungsformen der vorliegenden Erfindung wurden zum Zweck der Veranschaulichung erstellt, sie sollen aber keineswegs erschöpfend oder auf die offenbarten Ausführungsformen eingeschränkt sein. Für Fachleute sind viele Modifizierungen und Variationen offenkundig, die nicht von dem Schutzumfang und Erfindungsgedanken der beschriebenen Ausführungsformen abweichen. Die hierin verwendete Terminologie wurde gewählt, um die Grundgedanken der Ausführungsformen, die praktische Anwendung oder technische Verbesserung gegenüber auf dem Markt gefundenen Technologien bestmöglich zu erklären oder anderen Fachleuten das Verständnis der hierin offenbarten Ausführungsformen zu ermöglichen.

[0095] Die vorliegende Erfindung kann als ein System, ein Verfahren und/oder ein Computerprogrammprodukt verkörpert werden. Das Computerprogrammprodukt kann ein durch einen Computer lesbares Speichermedium (oder -medien) enthalten, auf dem durch einen Computer lesbare Programmanweisungen gespeichert sind, um einen Prozessor dazu zu veranlassen, Aspekte der vorliegenden Erfindung auszuführen.

[0096] Das Medium kann ein elektronisches, magnetisches, optisches, elektromagnetisches, Infrarot- oder Halbleitersystem für ein Propagierungsmedium sein. Beispiele für ein durch einen Computer lesbares Medium können einen Halbleiter- oder Solid-State-Arbeitsspeicher, ein Magnetband, eine entfernbare Computerdiskette, einen Direktzugriffsspeicher (RAM), einen Nur-Lese-Speicher (ROM), eine magnetische Festplatte und eine optische Festplatte umfassen. Aktuelle Beispiele für optische Festplatten umfassen CD-ROM (Compact Disk - Read Only Memory), CD-R/W (Compact Disk - Read/Write), DVD und Blu-Ray-Disk.

[0097] Bei dem durch einen Computer lesbaren Speichermedium kann es sich um eine physische Einheit handeln, die Anweisungen zur Verwendung durch eine Einheit zum Ausführen von Anweisungen beibehalten und speichern kann. Das durch einen Computer lesbare Speichermedium kann zum Beispiel eine elektronische Speichereinheit, eine magnetische Speichereinheit, eine optische Speichereinheit, eine elektromagnetische Speichereinheit, eine Halbleiter-Speichereinheit oder jede geeignete Kombination aus dem Vorgenannten sein, es ist aber nicht darauf beschränkt. Zu einer nicht erschöpfenden Liste von spezifischeren Beispielen des durch einen Computer lesbaren Speichermediums gehören die Folgenden: eine tragbare Computerdiskette, eine Festplatte, ein Direktzugriffsspeicher (RAM), ein Nur-Lese-Speicher (ROM), ein löschbarer programmierbarer Nur-Lese-Speicher (EPROM bzw. Flash-Speicher), ein statischer Direktzugriffsspeicher (SRAM), ein tragbarer CD-ROM, eine DVD, ein Speicher-Stick, eine Diskette, eine mechanisch codierte Einheit wie zum Beispiel Lochkarten oder erhabene Strukturen in einer Rille, auf denen Anweisungen gespeichert sind, und jede geeignete Kombination des Vorgenannten. Ein durch einen Computer lesbares Speichermedium soll, wie hierin verwendet, nicht als flüchtige Signale an sich aufgefasst werden, wie zum Beispiel Funkwellen oder andere sich frei ausbreitende elektromagnetische Wellen, elektromagnetische Wellen, die sich durch einen Wellenleiter oder andere Übertragungsmedien ausbreiten (z.B. durch ein Lichtwellenleiterkabel geleitete Lichtimpulse) oder durch einen Draht übertragene elektrische Signale.

[0098] Hierin beschriebene durch einen Computer lesbare Programmanweisungen können von einem durch einen Computer lesbaren Speichermedium auf jeweilige Datenverarbeitungs-/Verarbeitungseinheiten oder über ein Netzwerk wie zum Beispiel das Internet, ein lokales Netzwerk, ein Weitverkehrsnetzwerk und/oder ein drahtloses Netzwerk auf einen externen Computer oder eine externe Speichereinheit heruntergeladen werden. Das Netzwerk kann Kupferübertragungskabel, Lichtwellenübertragungsleiter, drahtlose Übertragung, Leitwegrechner, Firewalls, Vermittlungseinheiten, Gateway-Computer und/oder Edge-Server aufweisen. Eine Netzwerkadapterkarte oder Netzwerkschnittstelle in jeder Datenverarbeitungs-/Verarbeitungseinheit empfängt durch einen Computer lesbare Programmanweisungen aus dem Netzwerk und leitet die durch einen Computer lesbaren Programmanweisungen zur Speicherung in einem durch einen Computer lesbaren Speichermedium innerhalb der entsprechenden Datenverarbeitungs-/Verarbeitungseinheit weiter.

[0099] Bei durch einen Computer lesbaren Programmanweisungen zum Ausführen von Arbeitsschritten der vorliegenden Erfindung kann es sich um Assembler-Anweisungen, ISA-Anweisungen (Instruction-Set-Archi-

tecture), Maschinenanweisungen, maschinenabhängige Anweisungen, Mikrocode, Firmware-Anweisungen, zustandssetzende Daten oder entweder Quellcode oder Objektcode handeln, die in einer beliebigen Kombination aus einer oder mehreren Programmiersprachen geschrieben sind, darunter objektorientierte Programmiersprachen wie Smalltalk, C++ o.ä. sowie herkömmliche prozedurale Programmiersprachen wie die Programmiersprache „C“ oder ähnliche Programmiersprachen. Die durch einen Computer lesbaren Programmanweisungen können vollständig auf dem Computer des Benutzers, teilweise auf dem Computer des Benutzers, als eigenständiges Software-Paket, teilweise auf dem Computer des Benutzers und teilweise auf einem entfernt angeordneten Computer oder vollständig auf dem entfernt angeordneten Computer oder Server ausgeführt werden. In dem letzteren Szenario kann der entfernt angeordnete Computer mit dem Computer des Benutzers durch jeden Typ von Netzwerk verbunden werden, darunter ein lokales Netzwerk (LAN) oder ein Weitverkehrsnetzwerk (WAN), oder die Verbindung kann zu einem externen Computer hergestellt werden (zum Beispiel über das Internet unter Verwendung eines Internet-Dienstanbieters). In einigen Ausführungsformen können elektronische Schaltungen, darunter zum Beispiel programmierbare Logikschaltungen, feldprogrammierbare Gatter-Anordnungen (FPGA, field programmable gate arrays) oder programmierbare Logikanordnungen (PLA, programmable logic arrays) die computerlesbaren Programmanweisungen ausführen, indem sie Zustandsinformationen der computerlesbaren Programmanweisungen nutzen, um die elektronischen Schaltungen zu personalisieren, um Aspekte der vorliegenden Erfindung durchzuführen.

[0100] Aspekte der vorliegenden Erfindung werden hierin unter Bezugnahme auf Veranschaulichungen von Ablaufplänen und/oder Blockschaubildern von Verfahren, Vorrichtungen (Systemen) und Computerprogrammprodukten gemäß Ausführungsformen der Erfindung beschrieben. Es sollte klar sein, dass jeder Block der Ablaufplanveranschaulichungen und/oder der Blockschaubilder und Kombinationen von Blöcken in den Ablaufplanveranschaulichungen und/oder den Blockschaubildern mittels durch einen Computer lesbare Programmanweisungen umgesetzt werden können.

[0101] Diese durch einen Computer lesbaren Programmanweisungen können einem Prozessor eines Universalcomputers, eines Spezialcomputers oder einer anderen programmierbaren Datenverarbeitungsvorrichtung bereitgestellt werden, um eine Maschine zu erzeugen, sodass die über den Prozessor des Computers bzw. eine andere programmierbare Datenverarbeitungsvorrichtung ausgeführten Anweisungen ein Mittel zur Umsetzung der in dem Block bzw. den Blöcken der Ablaufpläne und/oder der Blockschaubilder angegebenen Funktionen/Schritte erzeugen. Diese durch einen Computer lesbaren Programmanweisungen können auch auf einem durch einen Computer lesbaren Speichermedium gespeichert sein, das einen Computer, eine programmierbare Datenverarbeitungsvorrichtung und/oder andere Einheiten so steuern kann, dass sie auf eine bestimmte Art funktionieren, sodass das durch einen Computer lesbare Speichermedium, auf dem Anweisungen gespeichert sind, ein Herstellungsprodukt aufweist, darunter Anweisungen, die Aspekte der/des in dem Block bzw. den Blöcken des Ablaufplans und/oder der Blockschaubilder angegebenen Funktion/Schritts umsetzen.

[0102] Die durch einen Computer lesbaren Programmanweisungen können auch auf einen Computer, andere programmierbare Datenverarbeitungsvorrichtungen oder eine andere Einheit geladen werden, um das Ausführen einer Reihe von Arbeitsschritten auf dem Computer bzw. der anderen programmierbaren Vorrichtung oder anderen Einheit zu verursachen, um einen durch einen Computer umgesetzten Prozess zu erzeugen, sodass die auf dem Computer, anderen programmierbaren Vorrichtungen oder einer anderen Einheit ausgeführten Anweisungen die in dem Block bzw. den Blöcken der Ablaufpläne und/oder der Blockschaubilder angegebenen Funktionen/Schritte umsetzen.

[0103] Die Ablaufpläne und/oder Blockschaubilder in den Figuren veranschaulichen die Architektur, die Funktionalität und den Betrieb möglicher Ausführungen von Systemen, Verfahren und Computerprogrammprodukten gemäß verschiedenen Ausführungsformen der vorliegenden Erfindung. In diesem Zusammenhang kann jeder Block in den Ablaufplänen oder den Blockschaubildern ein Modul, ein Segment oder einen Teil von Anweisungen darstellen, die eine oder mehrere ausführbare Anweisungen zum Umsetzen der bestimmten logischen Funktion(en) aufweisen. In einigen alternativen Umsetzungen können die in dem Block angegebenen Funktionen in einer anderen Reihenfolge als in den Figuren gezeigt auftreten. Zum Beispiel können zwei nacheinander gezeigte Blöcke tatsächlich im Wesentlichen parallel ausgeführt werden, oder die Blöcke können manchmal in der umgekehrten Reihenfolge ausgeführt werden, was von der beteiligten Funktionalität abhängt. Es ist ferner anzumerken, dass jeder Block der Blockschaubilder und/oder der Ablaufplandarstellungen sowie Kombinationen von Blöcken in den Blockschaubildern und/oder der Ablaufplandarstellung durch spezielle auf Hardware beruhende Systeme umgesetzt werden können, welche die angegebenen Funktionen oder Handlungen durchführen oder Kombinationen aus Spezial-Hardware und Computeranweisung ausführen.

[0104] Die hierin verwendete Terminologie dient nur zum Zweck der Beschreibung von bestimmten Ausführungsformen und soll die Erfindung keinesfalls einschränken. Die hierin verwendeten Singularformen „ein“, „eine“ und „der/die/das“ sollen auch die Pluralformen mit einschließen, es sei denn, der Kontext gibt eindeutig anderes vor. Es versteht sich des Weiteren, dass die Begriffe „weist auf“ und/oder „aufweisend“ bei Verwendung in dieser Patentschrift das Vorhandensein ausgewiesener Merkmale, Ganzzahlen, Schritte, Vorgänge, Elemente und/oder Komponenten angeben, das Vorhandensein oder die Hinzufügung von einem oder mehreren anderen Merkmalen, Ganzzahlen, Schritten, Vorgängen, Elementen, Komponenten und/oder Gruppen davon aber nicht ausschließen.

[0105] Die entsprechenden Strukturen, Materialien, und Entsprechungen aller Mittel oder Schritte-plus-Funktion-Elemente in den nachstehenden Ansprüchen sollen alle Strukturen, Materialien oder Handlungen zum Ausführen der Funktion in Kombination mit anderen beanspruchten Elementen enthalten, wie speziell beansprucht. Die Beschreibung der vorliegenden Erfindung wurde zum Zweck der Veranschaulichung und Beschreibung erstellt, sie soll aber keineswegs erschöpfend oder auf die offenbarte Form der Erfindung eingeschränkt sein. Für Fachleute sind viele Modifizierungen und Variationen offenkundig, die nicht von dem Schutzumfang und Erfindungsgedanken der Erfindung abweichen. Die Ausführungsformen wurden ausgewählt und beschrieben, um die Grundgedanken der Erfindung und die praktische Anwendung am besten zu erklären und es anderen Fachleuten zu ermöglichen, die Erfindung für verschiedene Ausführungsformen mit verschiedenen Modifizierungen zu verstehen, die für die vorgesehene bestimmte Verwendung geeignet sind.

Patentansprüche

1. Durch einen Computer umgesetztes Verfahren für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung, wobei die Datenverarbeitungsumgebung mindestens ein Benutzersystem (202, 204), eine Anwendung (208), einen Authentifizierungsserver (206) und einen Zugriffskontrollserver (214) aufweist, wobei das Benutzersystem (202, 204) über eine Netzwerkverbindung mit einem Server verbunden ist, der die Anwendung (208) ausführt, wobei die Anwendung (208) einen Zugriff auf eine Operation bereitstellt, wobei mindestens die Operation durch ihre Kennung identifizierbar ist, wobei die Anwendung (208) eine ungeschützte Komponente (208) ist, wobei das Verfahren aufweist
- Interagieren mit der Anwendung (208) durch das Benutzersystem (202, 204) über eine Benutzersystemanforderung,
- Umleiten (104) der Benutzersystemanforderung zu dem Authentifizierungsserver (206),
- Authentifizieren (106) des Benutzersystems (202, 204) durch Authentifizierungs-Anmeldedaten, die zwischen dem Authentifizierungsserver (206) und der Anwendung (208) ausgetauscht werden, wobei die Authentifizierungs-Anmeldedaten eine Anforderung für eine eingeschränkte Berechtigung für eine Ressource unter Verwendung einer Standardsemantik eines Geltungsbereichs aufweisen, wobei die eingeschränkte Berechtigung eine Untergruppe von bestehenden Berechtigungen aufweist, die durch den Zugriffskontrollserver (214) für die Ressource verwaltet werden, durch Abrufen eines Zugriffstokens mit einem Aktualisierungstoken von dem Authentifizierungsserver (206), wobei das Zugriffstoken und das Aktualisierungstoken die eingeschränkte Berechtigung aufweisen,
- Anfordern (110) einer Ausführung der Operation durch die Anwendung (208), initiiert durch das Benutzersystem (202, 204), aufweisend:
- Aufrufen (112) der Operation durch die Anwendung (208), das das Bereitstellen des Zugriffstokens aufweist,
- Aufrufen (114) des Zugriffskontrollservers (214) durch die Operation,
- Bereitstellen (116) einer Kennung des Benutzersystems (202, 204) und des Geltungsbereichs des Zugriffstokens, das die eingeschränkte Berechtigung für den Zugriffskontrollserver (214) aufweist, und
- Verwenden (118) der eingeschränkten Berechtigung zur Filterung der bestehenden Berechtigungen durch den Zugriffskontrollserver (214), was zu einer Zugriffsentscheidung des Benutzersystems (202, 204) für die Operation führt.

2. Verfahren nach Anspruch 1, wobei die Standardsemantik auf OAuth2 beruht.

3. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Operation mindestens eine aufweist, die aus einer Gruppe, die einen Zugriff auf vordefinierte Daten, einen Datenbankzugriff, einen Dateizugriff, eine vordefinierte Anwendungsprogrammierschnittstelle, einen Zugriff auf ein spezifisches untergeordnetes Netz eines Netzwerks aufweist, ausgewählt wurde.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Zugriffstoken eine vordefinierte Gültigkeitszeit hat.

5. Verfahren nach Anspruch 4, wobei die vordefinierte Gültigkeitszeit durch ein privilegiertes Benutzersystem (202, 204) aktualisierbar ist.

6. Zugriffssystem für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung, wobei die Datenverarbeitungsumgebung mindestens ein Benutzersystem (202, 204), eine Anwendung (208), einen Authentifizierungsserver (206) und einen Zugriffskontrollserver (214) aufweist, wobei das Benutzersystem (202, 204) über eine Netzwerkverbindung mit einem Server verbunden ist, der die Anwendung (208) ausführt, wobei die Anwendung (208) einen Zugriff auf eine Operation bereitstellt, wobei mindestens die Operation durch ihre Kennung identifizierbar ist, wobei die Anwendung (208) eine ungeschützte Komponente (208) ist, wobei das Zugriffssystem aufweist
- ein Zugriffsmodul, das für ein Zugreifen auf die Anwendung (208) über eine Benutzersystemanforderung angepasst ist,
- ein Umleitungsmodul, das für ein Umleiten der Benutzersystemanforderung zu dem Authentifizierungsserver (206) angepasst ist,
- den Authentifizierungsserver (206), der für ein Authentifizieren des Benutzersystems (202, 204) durch Authentifizierungs-Anmeldedaten angepasst ist, die zwischen dem Authentifizierungsserver (206) und der Anwendung (208) ausgetauscht werden, wobei die Authentifizierungs-Anmeldedaten eine Anforderung für eine eingeschränkte Berechtigung für eine Ressource unter Verwendung einer Standardsemantik eines Geltungsbereichs aufweisen, wobei die eingeschränkte Berechtigung eine Untergruppe von bestehenden Berechtigungen aufweist, die durch den Zugriffskontrollserver (214) für die Ressource verwaltet werden, durch Abrufen eines Zugriffstokens mit einem Aktualisierungstoken von dem Authentifizierungsserver (206), wobei das Zugriffstoken und das Aktualisierungstoken die eingeschränkte Berechtigung aufweisen,
- wobei das Benutzersystem (202, 204) für ein Anfordern einer Ausführung der Operation durch die Anwendung (208) angepasst ist, initiiert durch das Benutzersystem (202, 204), wobei das Anfordern der Ausführung der Operation aufweist:
- Aufrufen der Operation durch die Anwendung (208), das das Bereitstellen des Zugriffstokens aufweist,
- Aufrufen des Zugriffskontrollservers (214) durch die Operation,
- Bereitstellen einer Kennung des Benutzersystems (202, 204) und des Geltungsbereichs des Tokens, das die eingeschränkte Berechtigung für den Zugriffskontrollserver (214) aufweist, und
- Verwenden der eingeschränkten Berechtigung zur Filterung der bestehenden Berechtigungen durch den Zugriffskontrollserver (214), was zu einer Zugriffsentscheidung des Benutzersystems (202, 204) für die Operation führt.

7. Zugriffssystem nach Anspruch 6, wobei die Standardsemantik auf OAuth2 beruht.

8. Zugriffssystem nach einem der Ansprüche 6 oder 7, wobei die Operation mindestens eine aufweist, die aus einer Gruppe, die einen Zugriff auf vordefinierte Daten, einen Datenbankzugriff, einen Dateizugriff, eine vordefinierte Anwendungsprogrammierschnittstelle, einen Zugriff auf ein spezifisches untergeordnetes Netz eines Netzwerks aufweist, ausgewählt wurde.

9. Zugriffssystem nach einem der Ansprüche 6 bis 8, wobei das Zugriffstoken eine vordefinierte Gültigkeitszeit hat.

10. Zugriffssystem nach Anspruch 9, wobei die vordefinierte Gültigkeitszeit durch ein privilegiertes Benutzersystem (202, 204) aktualisierbar ist.

11. Computerprogrammprodukt für eine Autorisierung auf Token-Grundlage in einer Datenverarbeitungsumgebung, wobei die Datenverarbeitungsumgebung mindestens ein Benutzersystem (202, 204), eine Anwendung (208), einen Authentifizierungsserver (206) und einen Zugriffskontrollserver (214) aufweist, wobei das Benutzersystem (202, 204) über eine Netzwerkverbindung mit einem Server verbunden ist, der die Anwendung (208) ausführt, wobei die Anwendung (208) einen Zugriff auf eine Operation bereitstellt, wobei mindestens die Operation durch ihre Kennung identifizierbar ist, wobei das Computerprogrammprodukt aufweist: ein durch einen Computer lesbares Speichermedium, das von einem Prozessor lesbar ist und Befehle zur Ausführung durch den Prozessor speichert, um ein Verfahren nach einem der Ansprüche 1 bis 5 durchzuführen.

12. Computerprogramm, das auf einem durch einen Computer lesbaren Medium gespeichert ist und in den internen Speicher eines Digitalcomputers geladen werden kann, mit Programmanweisungen, wenn das

Programm auf dem Computer ausgeführt wird, um das Verfahren nach einem der Ansprüche 1 bis 5 durchzuführen.

Es folgen 15 Seiten Zeichnungen

Anhängende Zeichnungen

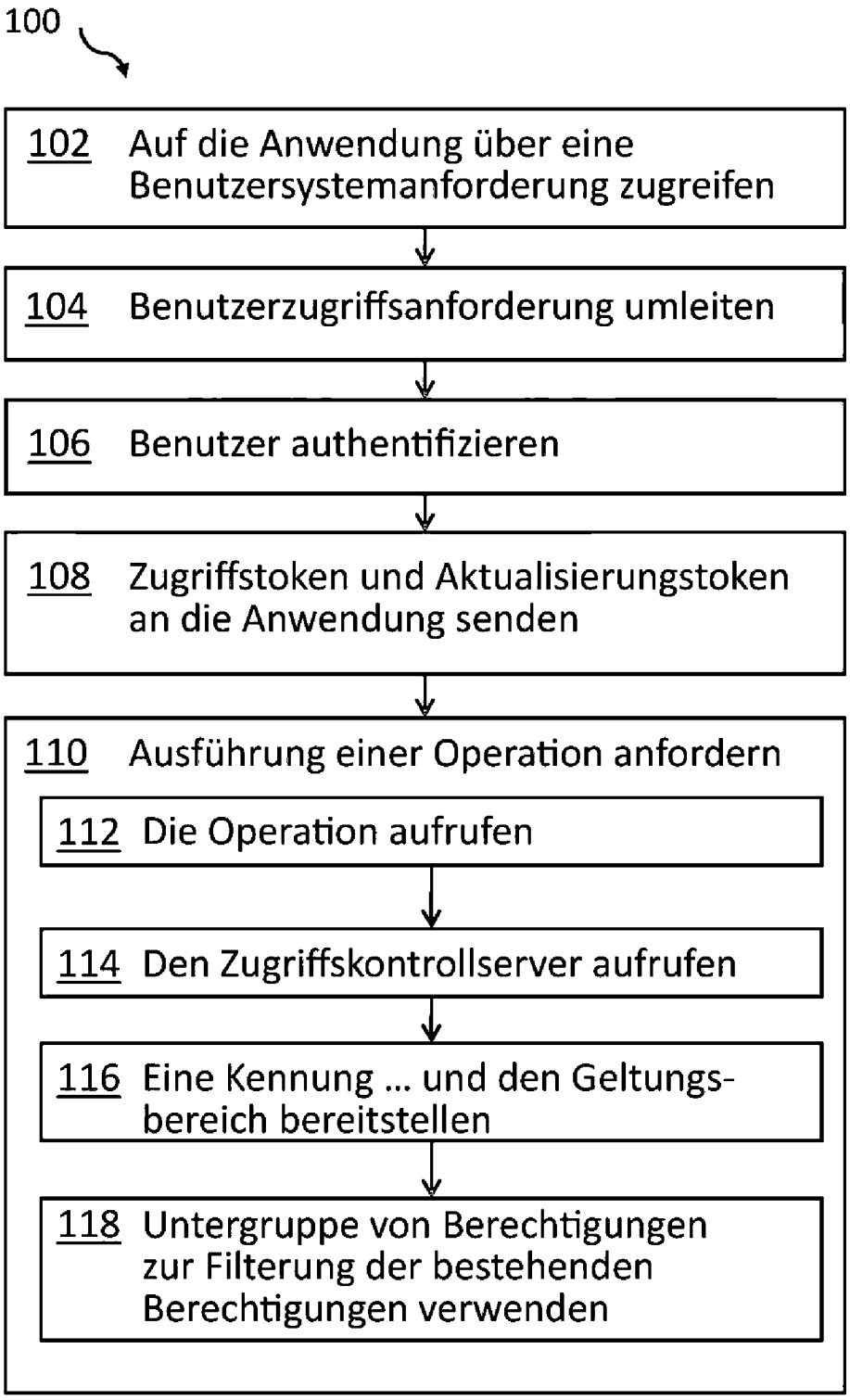


FIG. 1

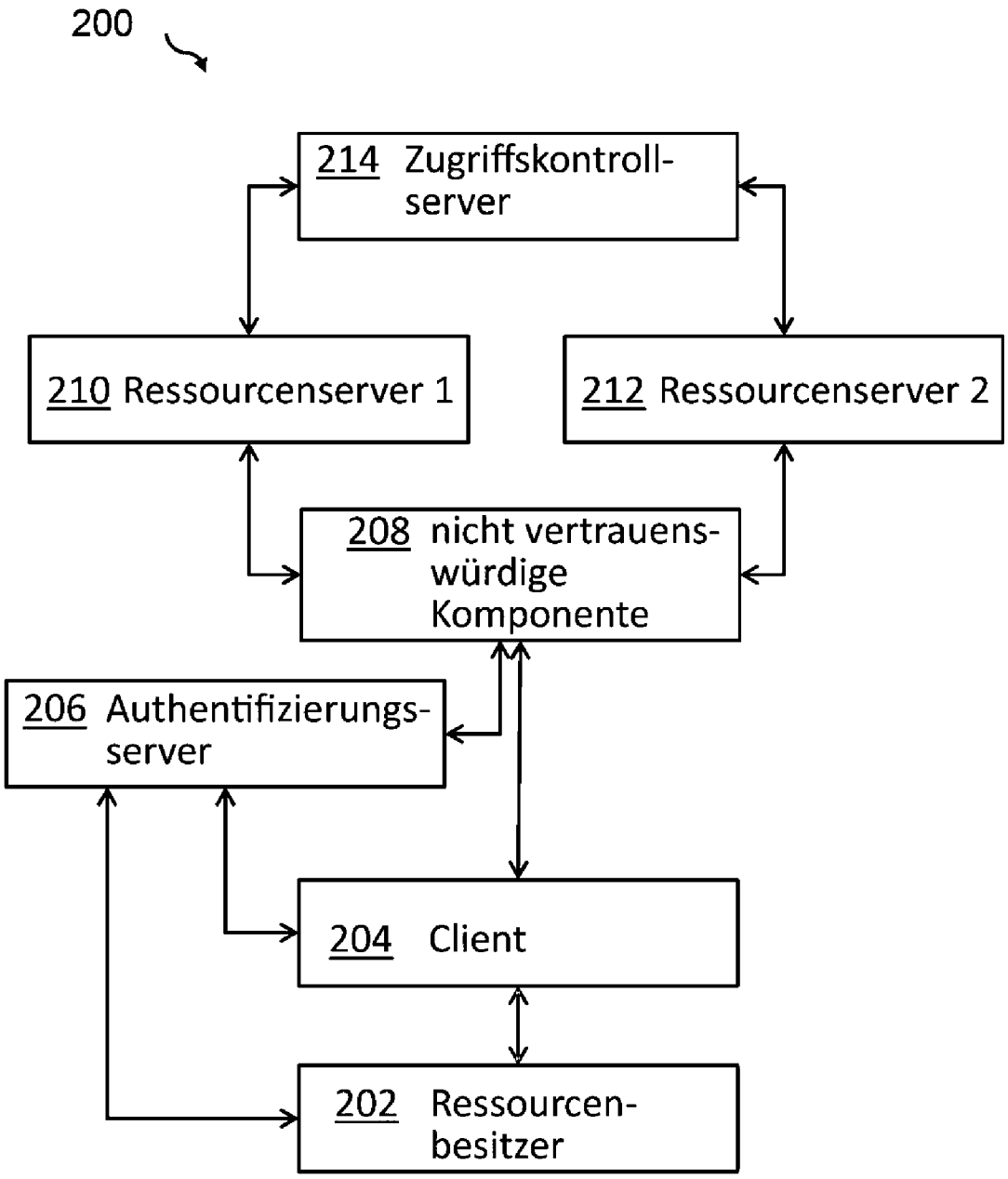

200
214 Zugriffskontroll-server
210 Ressourcenserver 1
212 Ressourcenserver 2
208 nicht vertrauens-würdige Komponente
206 Authentifizierungs-server
204 Client
202 Ressourcen-besitzer

FIG. 2

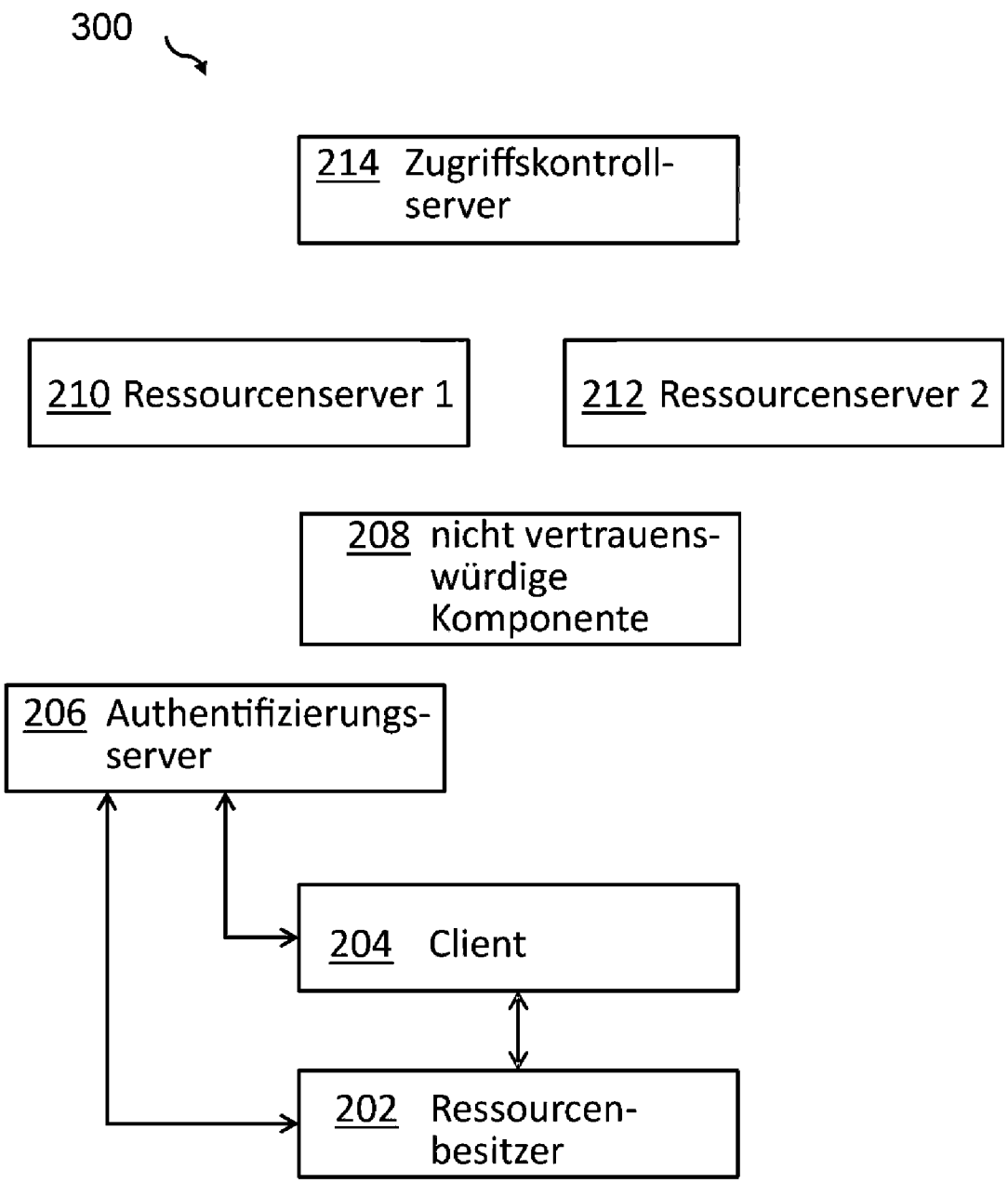

300
214 Zugriffskontroll-server
210 Ressourcenserver 1
212 Ressourcenserver 2
208 nicht vertrauens-würdige Komponente
206 Authentifizierungs-server
204 Client
202 Ressourcen-besitzer

FIG. 3

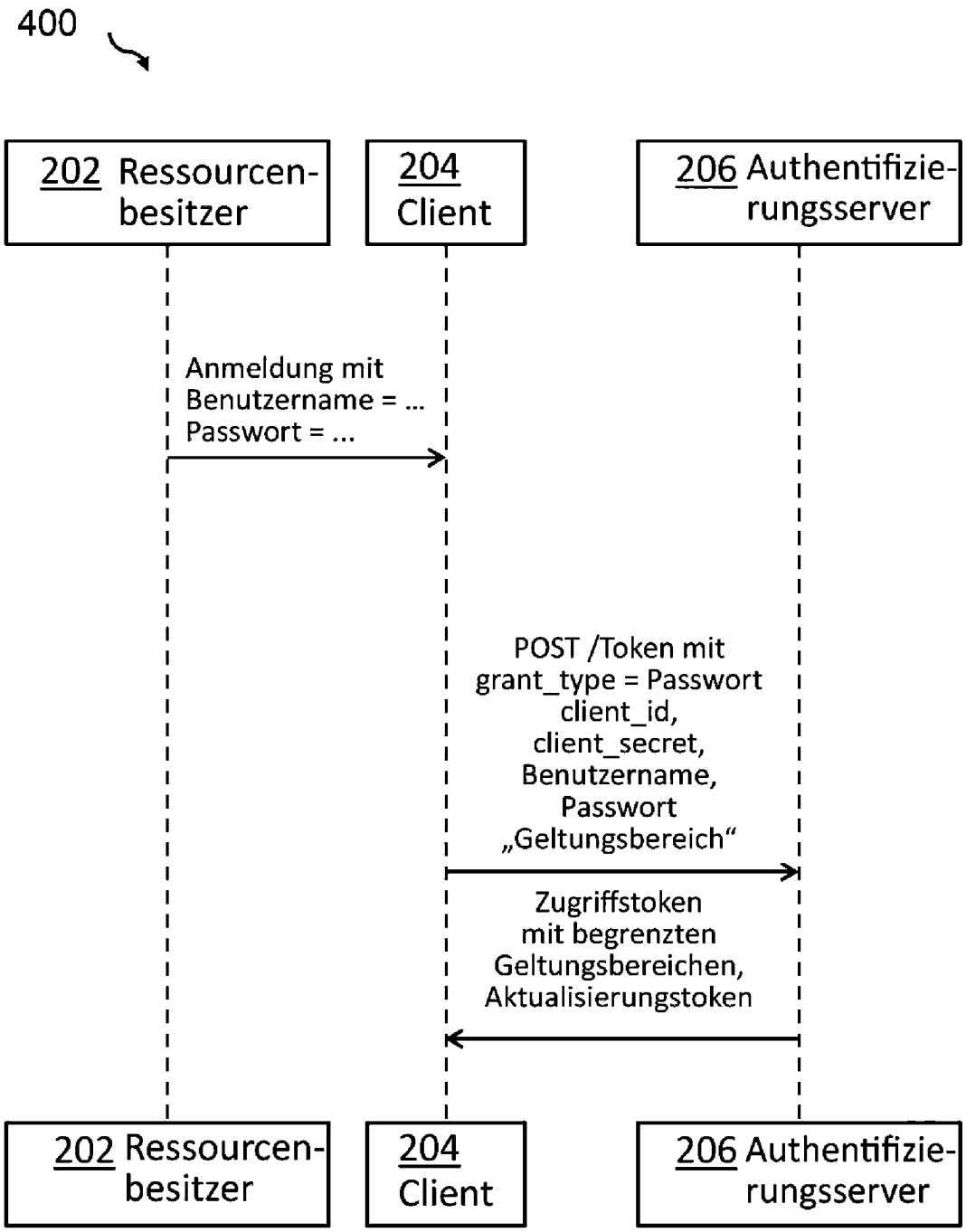

400
202 Ressourcen-besitzer
204 Client
206 Authentifizie-rungsserver
Anmeldung mit
Benutzername = ...
Passwort = ...
POST /Token mit
grant_type = Passwort
client_id,
client_secret,
Benutzername,
Passwort
„Geltungsbereich“
Zugriffstoken
mit begrenzten
Geltungsbereichen,
Aktualisierungstoken
202 Ressourcen-besitzer
204 Client
206 Authentifizie-rungsserver

FIG. 4

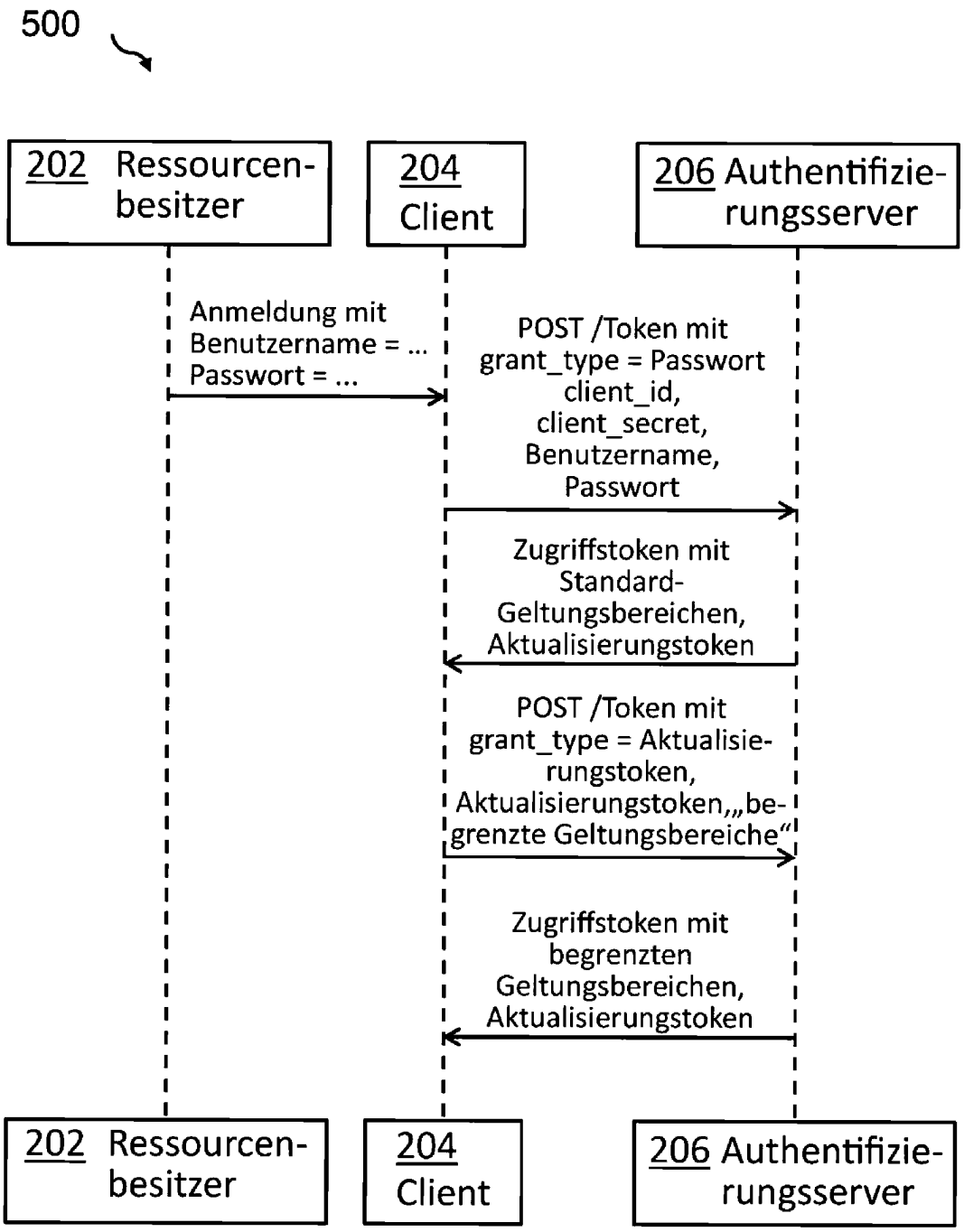

500
202 Ressourcen-besitzer
204 Client
206 Authentifizie-rungsserver
Anmeldung mit Benutzername = ... Passwort = ...
POST /Token mit grant_type = Passwort client_id, client_secret, Benutzername, Passwort
Zugriffstoken mit Standard-Geltungsbereichen, Aktualisierungstoken
POST /Token mit grant_type = Aktualisie-rungstoken, Aktualisierungstoken,„be-grenzte Geltungsbereiche“
Zugriffstoken mit begrenzten Geltungsbereichen, Aktualisierungstoken
202 Ressourcen-besitzer
204 Client
206 Authentifizie-rungsserver

FIG. 5

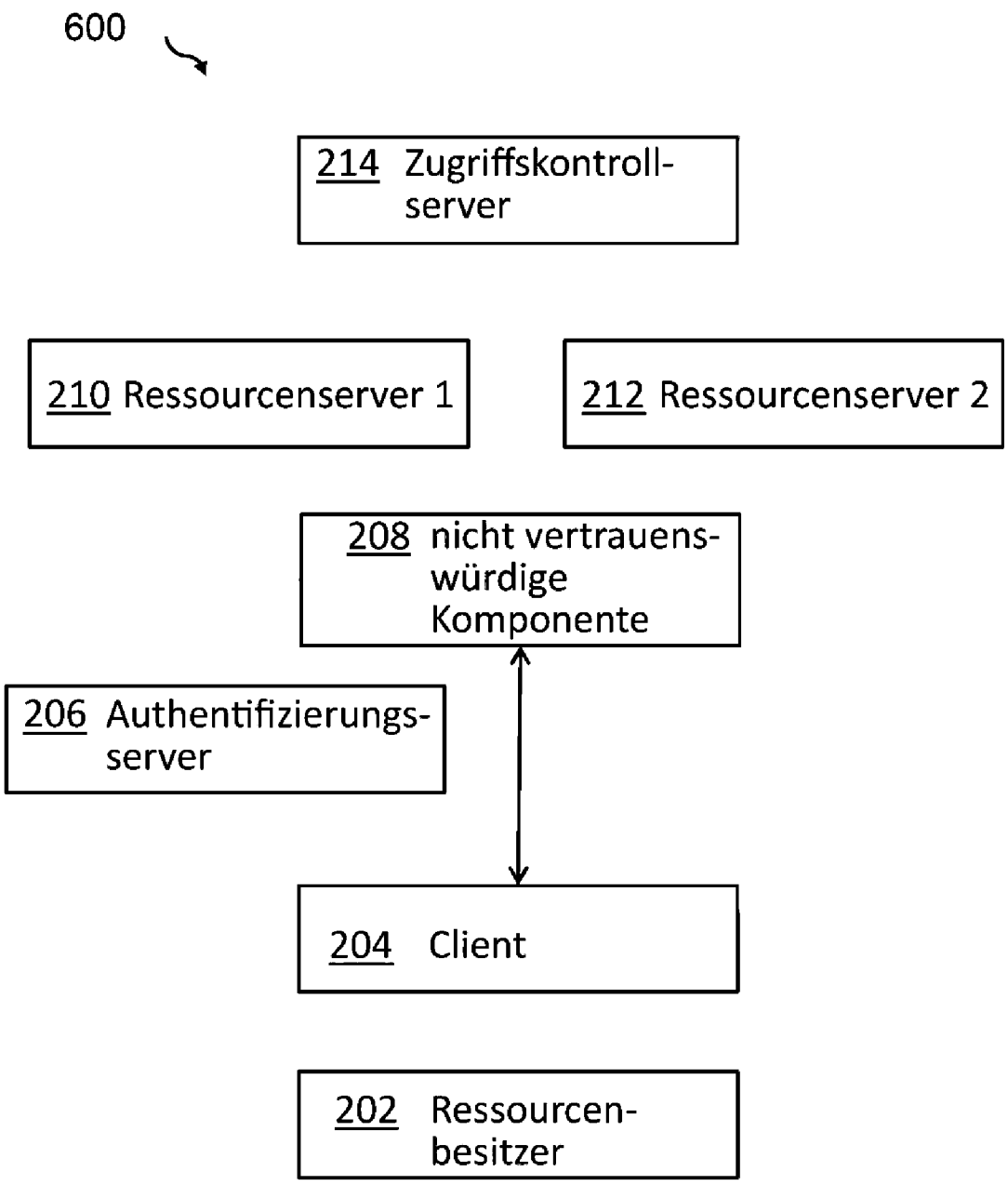

600
214 Zugriffskontroll-server
210 Ressourcenserver 1
212 Ressourcenserver 2
208 nicht vertrauens-würdige Komponente
206 Authentifizierungs-server
204 Client
202 Ressourcen-besitzer

FIG. 6

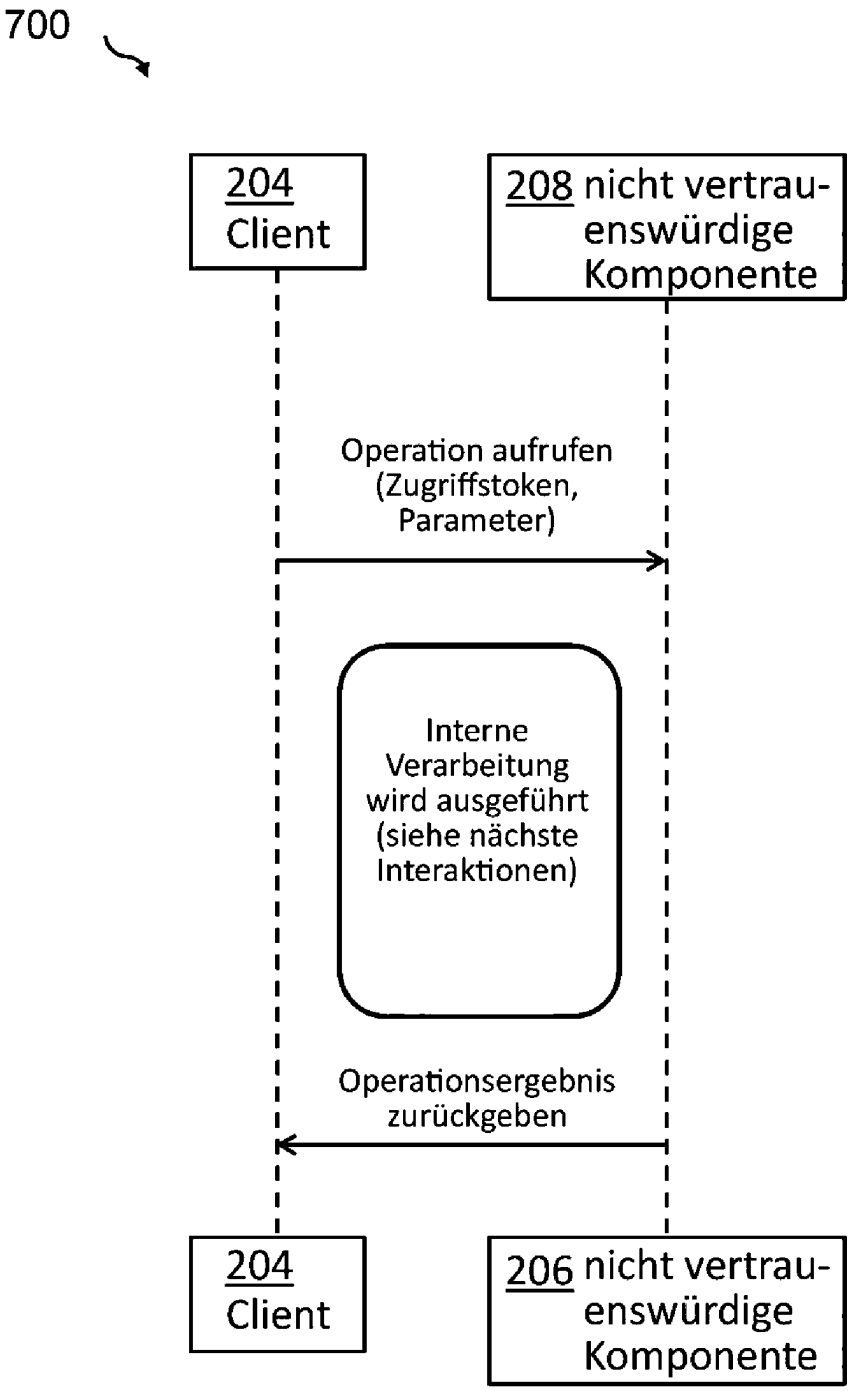

700
204 Client
208 nicht vertrau-enswürdige Komponente
Operation aufrufen (Zugriffstoken, Parameter)
Interne Verarbeitung wird ausgeführt (siehe nächste Interaktionen)
Operationsergebnis zurückgeben
204 Client
206 nicht vertrau-enswürdige Komponente

FIG. 7

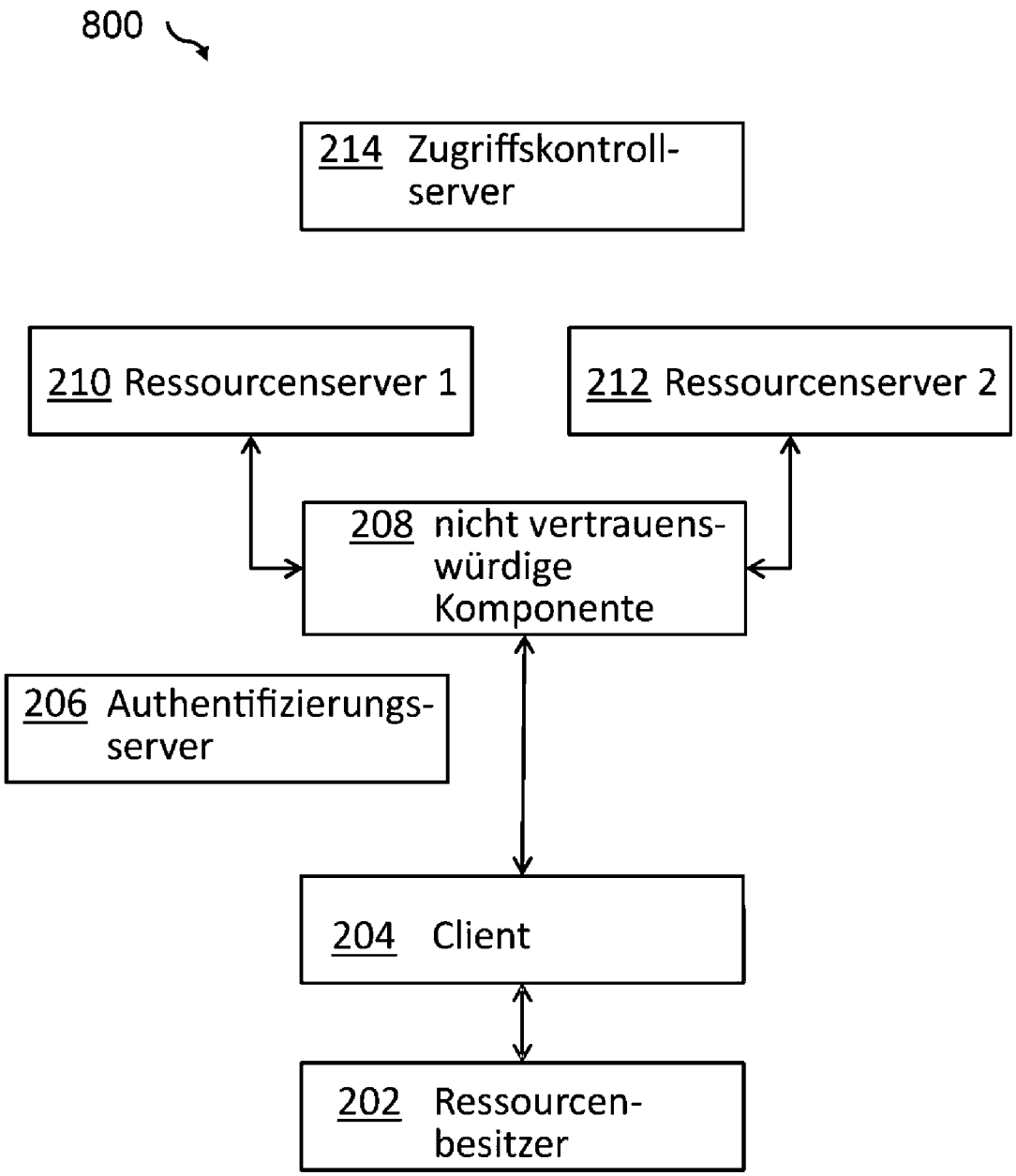

800
214 Zugriffskontroll-server
210 Ressourcenserver 1
212 Ressourcenserver 2
208 nicht vertrauens-würdige Komponente
206 Authentifizierungs-server
204 Client
202 Ressourcen-besitzer

FIG. 8

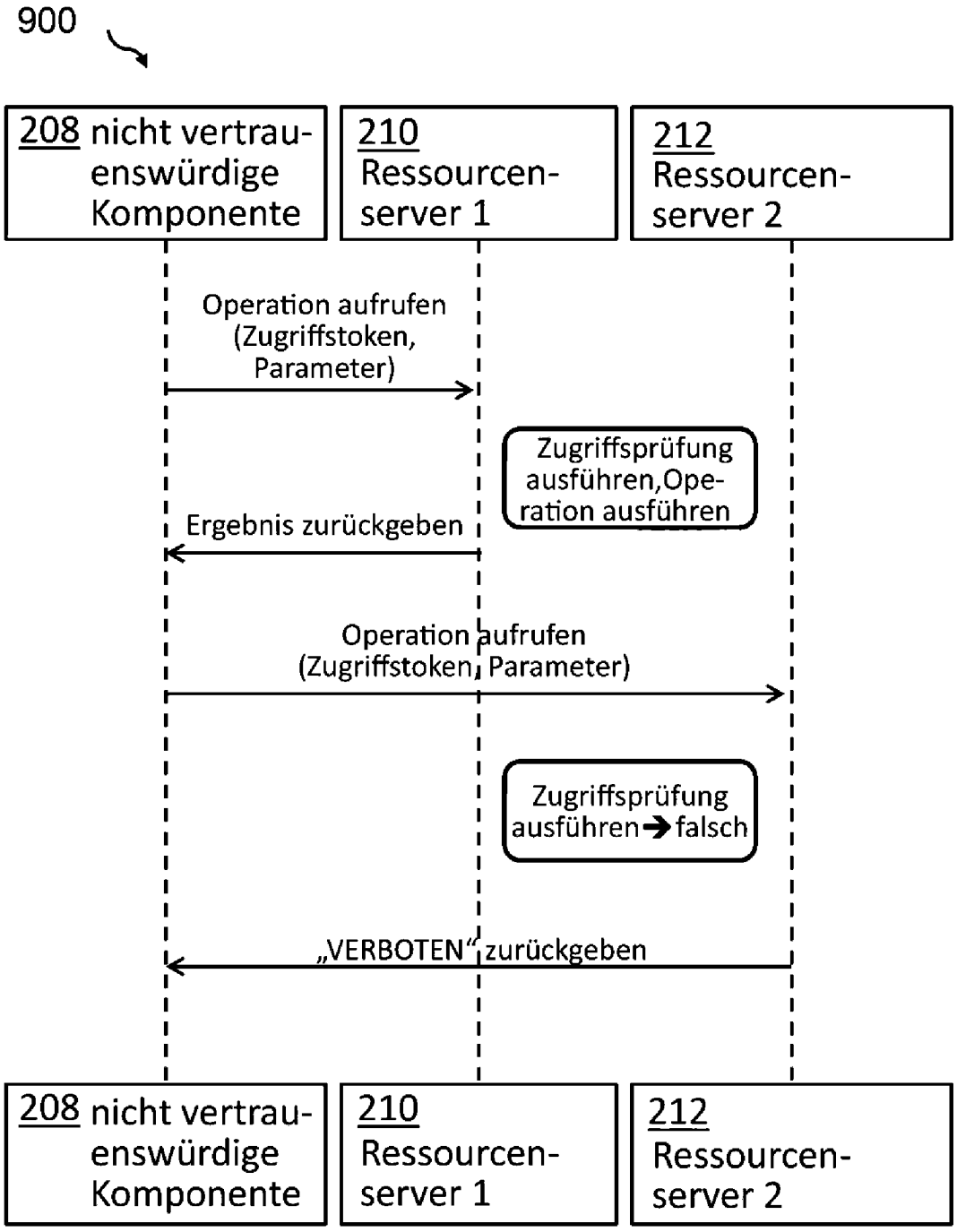

900
208 nicht vertrau-enswürdige Komponente
210 Ressourcen-server 1
212 Ressourcen-server 2
Operation aufrufen (Zugriffstoken, Parameter)
Zugriffsprüfung ausführen,Ope-ration ausführen
Ergebnis zurückgeben
Operation aufrufen (Zugriffstoken, Parameter)
Zugriffsprüfung ausführen → falsch
„VERBOTEN“ zurückgeben
208 nicht vertrau-enswürdige Komponente
210 Ressourcen-server 1
212 Ressourcen-server 2

FIG. 9

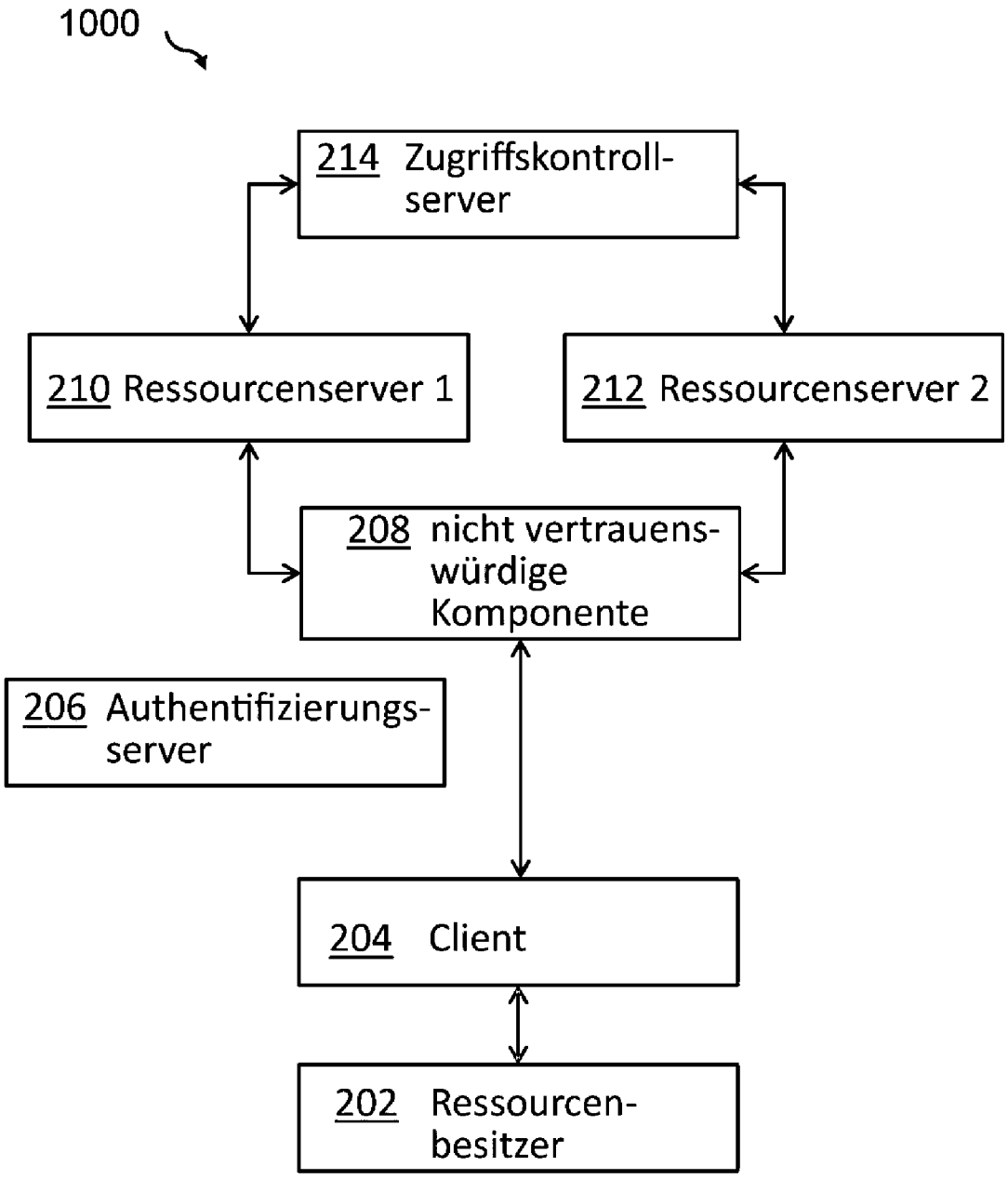

1000
214 Zugriffskontroll-server
210 Ressourcenserver 1
212 Ressourcenserver 2
208 nicht vertrauens-würdige Komponente
206 Authentifizierungs-server
204 Client
202 Ressourcen-besitzer

FIG. 10

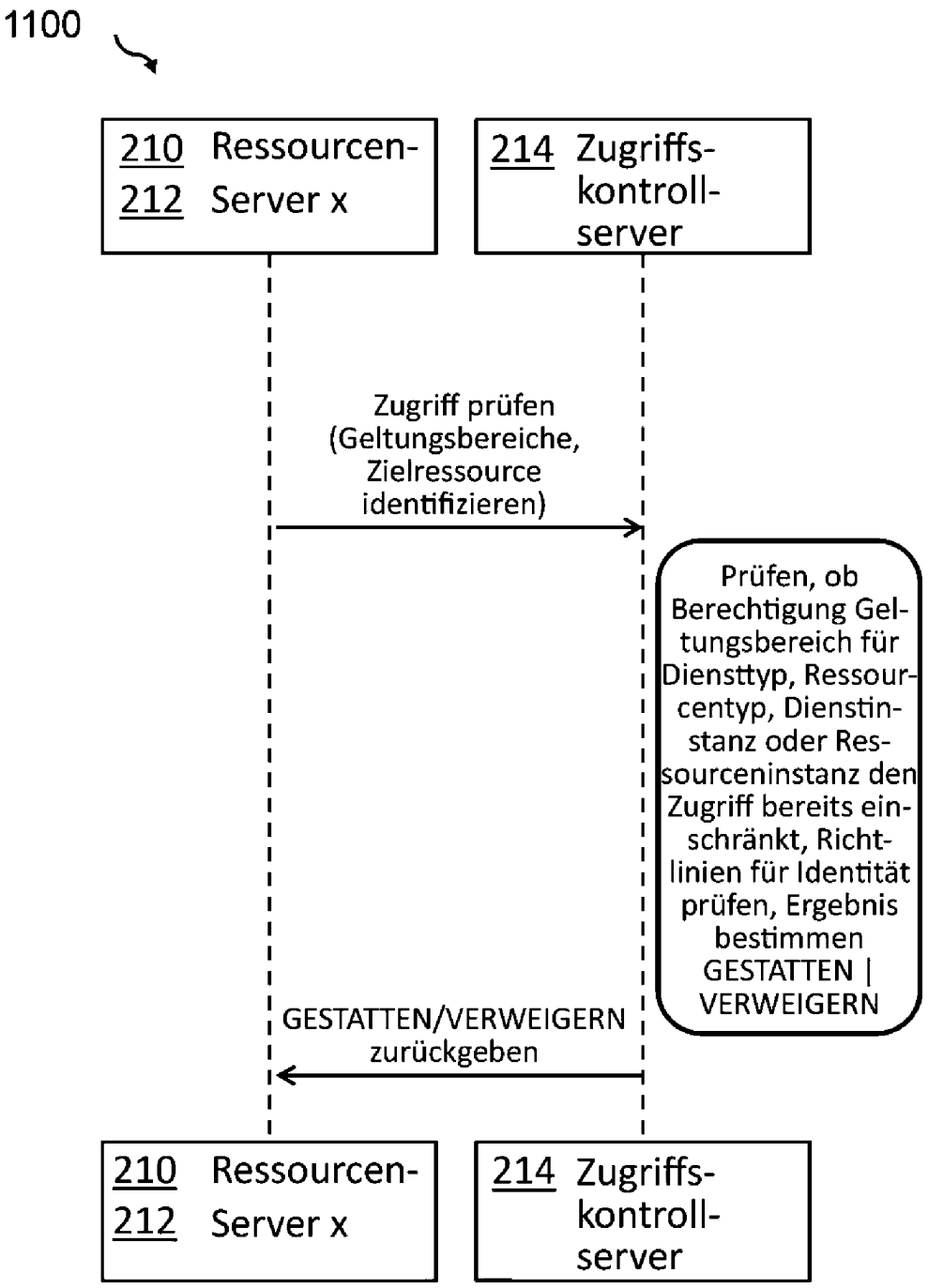

1100
210 Ressourcen-
212 Server x
214 Zugriffs-
kontroll-
server
Zugriff prüfen
(Geltungsbereiche,
Zielressource
identifizieren)
Prüfen, ob
Berechtigung Gel-
tungsbereich für
Diensttyp, Ressour-
centyp, Dienstin-
stanz oder Res-
sourceninstanz den
Zugriff bereits ein-
schränkt, Richt-
linien für Identität
prüfen, Ergebnis
bestimmen
GESTATTEN |
VERWEIGERN
GESTATTEN/VERWEIGERN
zurückgeben
210 Ressourcen-
212 Server x
214 Zugriffs-
kontroll-
server

FIG. 11

Prüfung 1: Enthält die Geltungsbereichliste „IBM“? Ja: Mit Richtlinienauswertung fortfahren Nein: Mit nächstem Schritt fortfahren
CRN der Ressource muss geprüft werden. **Dienstnamen** extrahieren.
Prüfung 2: Enthält die Geltungsbereichliste den Dienstnamen des CRN? Ja: Mit Richtlinienauswertung fortfahren Nein: VERWEIGERN zurückgeben
Richtlinienauswertung ...

FIG. 12

Prüfung 1: Enthält die Geltungsbereichliste „ibm“? Ja: Mit Richtlinienauswertung fortfahren Nein: Mit nächstem Schritt fortfahren
CRN der zu prüfenden Ressource analysieren. Details über die CRN-Syntax sind im Abschnitt *„Syntax and Semantic of limited entitlements“* (Syntax und Semantik von begrenzten Berechtigungen) zu finden. Extrahieren, falls verfügbar: **crn-service-name, crn-service-instance, crn-resource-type, crn-resource** (CRN-Servicename, CRN-Serviceinstanz, CRN-Ressourcentyp, CRN-Ressource)
Prüfung 2: Ausführen für jeden Geltungsbereich in der Geltungsbereichliste: Details über die Geltungsbereich-Syntax sind im Abschnitt *„Syntax and Semantic of limited entitlements“* zu finden. Geltungsbereich aufteilen in **scope-service-name, scope-service-instance, scope-resource-type, scope-resource** (Geltungsbereich-Dienstname, Geltungsbereich-Dienstinstanz, Geltungsbereich-Ressourcentyp, Geltungsbereich-Ressource); einzelne Teile können leer sein.
Prüfen (**crn-service-name** stimmt mit **scope-service-name** überein) UND ((**crn-service-instance** nicht verfügbar und **scope-service-name** nicht verfügbar) ODER (**crn-service-instance** verfügbar und **scope-service-name** nicht verfügbar) ODER (**crn-service-instance** verfügbar und stimmt mit **scope-service-name** überein)) UND ((**crn-resource-type** nicht verfügbar und **scope-resource-type** nicht verfügbar) ODER (**crn-resource-type** verfügbar und **scope-resource-type** nicht verfügbar) ODER (**crn-resource-type** verfügbar und stimmt mit **scope-resource-type** überein)) UND ((**crn-resource** nicht verfügbar und **scope-resource** nicht verfügbar) ODER (**crn-resource** verfügbar und **scope-resource** nicht verfügbar)´ODER (**crn-resource** verfügbar und stimmt mit **scope-resource** überein)) Stimmt der tatsächliche Geltungsbereich mit dieser Prüfung überein? Ja: Mit Richtlinienauswertung fortfahren Nein: Mit nächstem Schritt fortfahren Keinen übereinstimmenden Geltungsbereich gefunden? VERWEIGERN zurückgeben
Richtlinienauswertung ...

FIG. 13

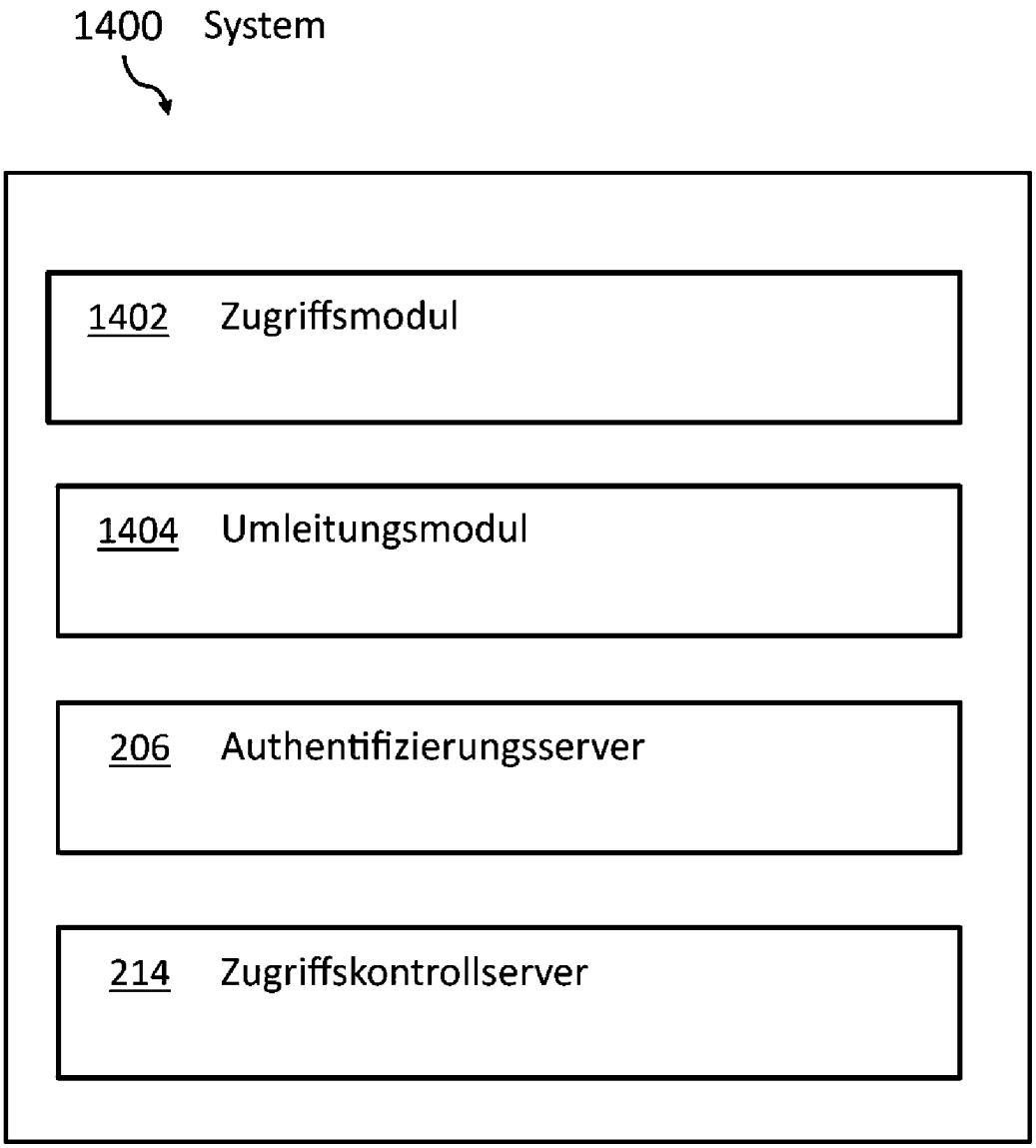

1400 System
1402 Zugriffsmodul
1404 Umleitungsmodul
206 Authentifizierungsserver
214 Zugriffskontrollserver

FIG. 14

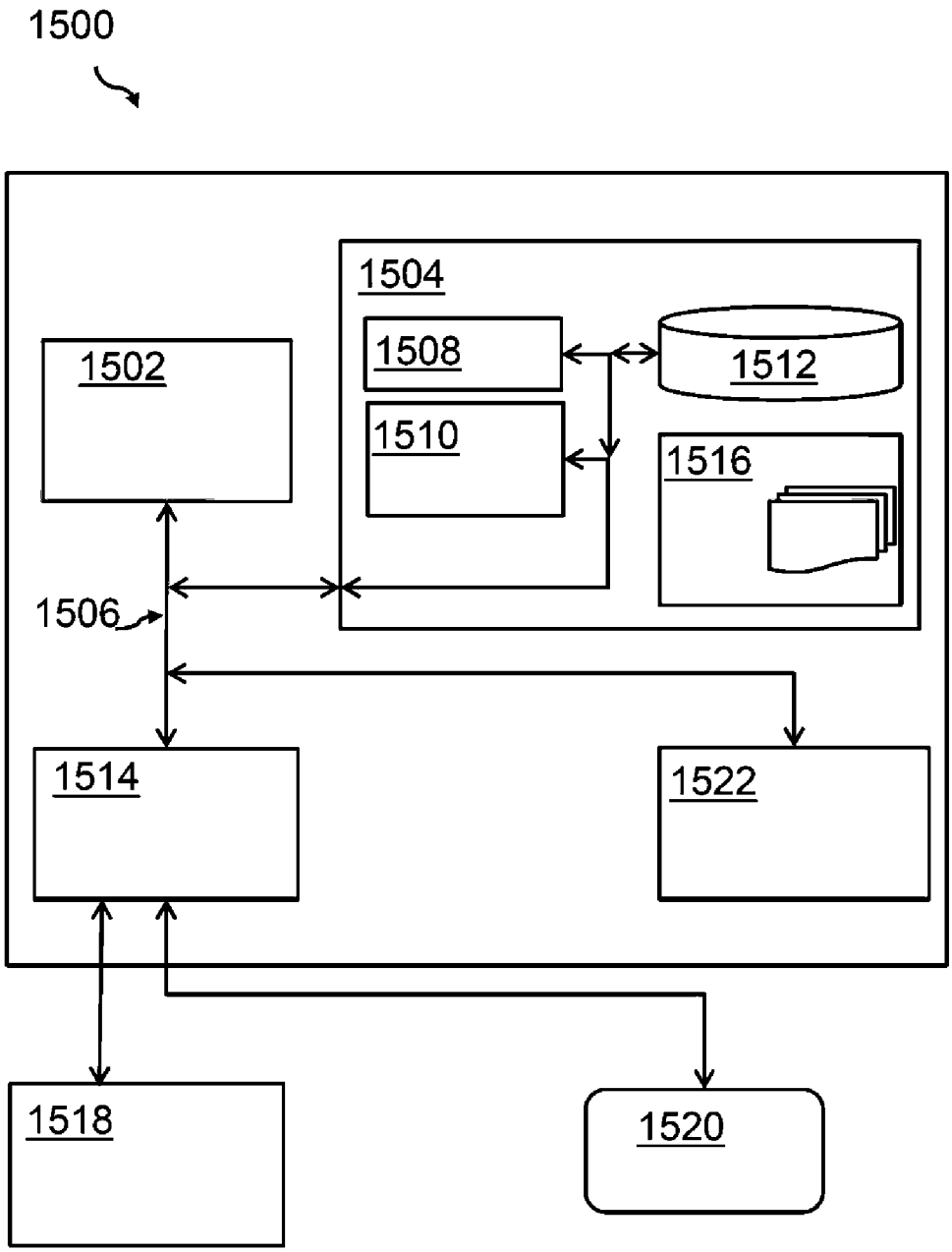


FIG. 15

 Das Dokument wurde durch die Firma Luminess hergestellt.