



(10) **DE 11 2020 002 343 B4** 2024.12.19

(12)

Patentschrift

(21) Deutsches Aktenzeichen: **11 2020 002 343.5**
(86) PCT-Aktenzeichen: **PCT/IB2020/055961**
(87) PCT-Veröffentlichungs-Nr.: **WO 2020/261134**
(86) PCT-Anmeldetag: **24.06.2020**
(87) PCT-Veröffentlichungstag: **30.12.2020**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **27.01.2022**
(45) Veröffentlichungstag
der Patenterteilung: **19.12.2024**

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

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:
16/455,168 **27.06.2019** **US**

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

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

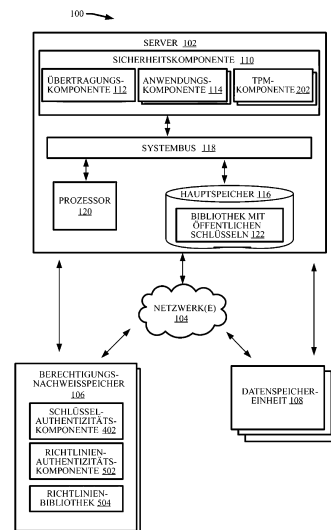
(72) Erfinder:
Sabath, Mariusz, Yorktown Heights, NY, US; Lum,
Jia Jun Brandon, Yorktown Heights, NY, US;
Steinder, Malgorzata, Yorktown Heights, NY, US;
Pittner, Daniel, 71032 Böblingen, DE

(56) Ermittelter Stand der Technik:
siehe Folgeseiten

(54) Bezeichnung: **Verteilung von Sicherheitsberechtigungs-nachweisen**

(57) Hauptanspruch: System (100) zur Verteilung eines Sicherheitsberechtigungs-nachweises, wobei das System (100) aufweist:
einen Hauptspeicher (116, 1216), der durch einen Computer ausführbare Komponenten speichert;
einen Prozessor (120, 1214), der mit dem Hauptspeicher (116, 1216) betriebsfähig verbundenen ist und der die in dem Hauptspeicher (116, 1216) gespeicherten, durch einen Computer ausführbaren Komponenten ausführt, wobei die durch einen Computer ausführbaren Komponenten aufweisen:
eine vertrauenswürdige Plattformmodulkomponente (202), die ausführbar ist, um ein Digitale-Identität-Token (300) zu erzeugen (802, 904), das an einen Computeranwendungsprozess (600) gebunden ist, wobei das Erzeugen (802, 904) auf ein oder mehreren Messwerten basiert, die ein oder mehrere Arbeitslasten des Computeranwendungsprozesses (600) beschreiben; und
eine Authentizitätskomponente, die ausführbar ist, um das Digitale-Identität-Token (300) zu analysieren, um einen Sicherheitsberechtigungs-nachweis abzurufen, wobei die Authentizitätskomponente eine Schlüsselauthentizitätskomponente (402) aufweist, um das Digitale-Identität-Token (300) mit einem Sicherheitsschlüssel zu vergleichen (804, 906), um auf der Grundlage des Vergleichs (804, 906) einen Sicherheitsberechtigungs-nachweis abzurufen; und wobei die Authentizitätskomponente eine Richtlinien-

authentizitätskomponente (502) aufweist, die ausführbar ist, um einen Vergleich (806, 908) des Digitale-Identität-Tokens (300) mit einer definierten Richtlinie durchzuführen, die den Computeranwendungsprozess (600) steuert, wobei ein Abrufen des Sicherheitsberechtigungs-nachweises des Weiteren auf dem Vergleich (806, 908) beruht.



(56) Ermittelter Stand der Technik:

US 2014 / 0 208 409 A1

Hardware security module. In: Wikipedia, the free encyclopedia. Bearbeitungsstand: 04.06.2019. URL: [https://en.wikipedia.org/w/index.php?](https://en.wikipedia.org/w/index.php?title=Hardware_security_module&oldid=900229769)

title=Hardware_security_module&oldid=900229769 [abgerufen am 28.09.2023]

Public-key cryptography. In: Wikipedia, the free encyclopedia. Bearbeitungsstand: 11.06.2019. URL: https://en.wikipedia.org/w/index.php?title=Public-key_cryptography&oldid=901437054 [abgerufen am 28.09.2023]

Beschreibung

Technisches Gebiet

[0001] Die vorliegende Offenbarung betrifft die Verteilung von Datensicherheitsberechtigungs-nachweisen und, genauer gesagt, einen oder mehrere Datensicherheitsprozesse, die den Zugriff auf Sicherheitsberechtigungs-nachweise für Serviceanbieter-Administratoren über ein Berechtigungs-nachweis-Freigabesystem auf der Grundlage einer Berechtigung von einer oder mehreren Computeranwendungsarbeitslasten einschränken können.

HINTERGRUND

[0002] Einige Cloud-Computing-Kunden benötigen eine Cloud, in der der Serviceanbieter nicht auf die Kundendaten zugreifen kann. Herkömmliche Technologien, die ausgeführt werden, um dieses Ziel zu erreichen, können sichere Schlüsselübertragungsprotokolle, vertrauenswürdige Plattformmodule und/oder Hostherkunft und -integrität umfassen. Jedoch können herkömmliche Technologien durch nachlässige und/oder böswillige Administratoren und/oder sich als Administratoren ausgebende Entitäten beeinträchtigt werden.

[0003] Folglich besteht in der Technik ein Bedarf, das vorstehend genannte Problem anzugehen.

[0004] Die US 2014 / 0 208 409 A1 beschreibt ein System, umfassend: einen Server, der in einer lokalen Umgebung angeordnet ist, wobei der Server eine Zugriffs-Policy speichert, die einen ersten Satz von Zugriffsrechten umfasst, die den Zugriff auf in einer Cloud-Umgebung verschlüsselt gespeicherte Daten durch eine anfragende Anwendung und einen ersten Benutzer definieren, wobei die lokale Umgebung unter der Kontrolle eines zweiten Benutzers steht, wobei die Cloud-Umgebung nicht unter der Kontrolle des zweiten Benutzers steht und wobei der Server eingerichtet ist zum: Empfangen einer Anfrage, die mit der anfragenden Anwendung und dem ersten Benutzer verbunden ist, um auf die Daten zuzugreifen, die in der Cloud-Umgebung gespeichert sind, von einer Rechte-Applikation; und Übertragen des ersten Satzes von Zugriffsrechten und eines Entschlüsselungsschlüssels für die Daten an die Rechte-Applikation in Reaktion darauf, dass der erste Benutzer laut der Zugriffs-Policy die erforderlichen Rechte für den Zugriff auf die Daten durch die anfragende Anwendung hat, wobei die Rechte-Applikation so konfiguriert ist, dass sie die Daten entschlüsselt, die entschlüsselten Daten an die anfragende Anwendung weiterleitet und ihr den Zugriff auf die entschlüsselten Daten in Übereinstimmung mit dem ersten Satz von Zugriffsrechten erlaubt.

[0005] Der Enzyklopädieartikel „Hardware security module“, in: Wikipedia, the free encyclopedia, Bearbeitungsstand: 04.06.2019, URL:

[https://en.wikipedia.org/w/index.php?title=Hardware security module&oldid=9002 29769](https://en.wikipedia.org/w/index.php?title=Hardware%20security%20module&oldid=900229769), beschreibt ein Hardware-Sicherheitsmodul (HSM) als ein physisches Computergerät, das Geheimnisse (vor allem digitale Schlüssel) schützt und verwaltet, Verschlüsselungs- und Entschlüsselungsfunktionen für digitale Signaturen, starke Authentifizierung und andere kryptografische Funktionen ausführt. Diese Module sind traditionell als Steckkarte oder externes Gerät erhältlich, das direkt an einen Computer oder Netzwerkserverserver angeschlossen wird. Ein Hardware-Sicherheitsmodul kann einen oder mehrere sichere Kryptoprozessor-Chips enthalten. HSMs können Funktionen aufweisen, die einen Manipulationsnachweis ermöglichen, wie sichtbare Anzeichen von Manipulation oder Protokollierung und Warnung, oder Manipulationsresistenz, die eine Manipulation erschwert, ohne das HSM funktionsunfähig zu machen, oder Manipulationsreaktion, wie das Löschen von Schlüsseln bei Erkennung einer Manipulation. Die überwiegende Mehrheit der vorhandenen HSMs ist hauptsächlich für die Verwaltung geheimer Schlüssel ausgelegt. Viele HSM-Systeme verfügen über Mittel zur sicheren Sicherung der von ihnen verwalteten Schlüssel außerhalb des HSM. Die Schlüssel können in verpackter Form gesichert und auf einer Computerfestplatte oder einem anderen Medium oder extern auf einem sicheren tragbaren Gerät wie einer Smartcard oder einem anderen Sicherheitstoken gespeichert werden. HSMs werden für die Echtzeit-Autorisierung und -Authentifizierung in kritischen Infrastrukturen eingesetzt und sind daher in der Regel so konzipiert, dass sie Standard-Hochverfügbarkeitsmodelle wie Clustering, automatisches Failover und redundante, vor Ort austauschbare Komponenten unterstützen. Zu den möglichen Funktionen eines HSM gehören: integrierte Generierung sicherer kryptografischer Schlüssel; integrierte Speicherung sicherer kryptografischer Schlüssel, zumindest für die oberste Ebene und die sensiblen Schlüssel, die oft als Hauptschlüssel bezeichnet werden; Schlüsselverwaltung; Verwendung kryptografischer und sensibler Daten, z. B. zur Durchführung von Entschlüsselungs- oder digitalen Signaturfunktionen; integrierte sichere Löschung von kryptografischen und anderen sensiblen Daten, die von ihm verwaltet wurden. HSMs werden auch zur Verwaltung transparenter Datenverschlüsselungsschlüssel für Datenbanken und Schlüssel für Speichergeräte wie Festplatten oder Bänder eingesetzt.

[0006] Der Enzyklopädieartikel „Public-key cryptography“, in: Wikipedia, the free encyclopedia, Bearbeitungsstand: 11.06.2019, URL:

[https://en.wikipedia.org/w/index.php?title=Public-key cryptography&oldid=901437054](https://en.wikipedia.org/w/index.php?title=Public-key%20cryptography&oldid=901437054), beschreibt Kryptografie mit öffentlichen Schlüsseln oder asym-

metrische Kryptografie als einen Bereich kryptografischer Systeme, die Paare verwandter Schlüssel verwenden. Jedes Schlüsselpaar besteht aus einem öffentlichen Schlüssel und einem entsprechenden privaten Schlüssel. Schlüsselpaare werden mit kryptografischen Algorithmen generiert, die auf mathematischen Problemen basieren, die als Einwegfunktionen bezeichnet werden. Die Sicherheit der Kryptografie mit öffentlichen Schlüsseln hängt davon ab, dass der private Schlüssel geheim gehalten wird; der öffentliche Schlüssel kann offen verteilt werden, ohne die Sicherheit zu beeinträchtigen. In einem System mit öffentlichem Schlüssel können die öffentlichen Schlüssel weit verbreitet und offen zugänglich gemacht werden, und nur die entsprechenden privaten Schlüssel müssen von ihrem Besitzer geheim gehalten werden. Zwei der bekanntesten Anwendungen der Kryptografie mit öffentlichem Schlüssel sind: die Verschlüsselung mit öffentlichem Schlüssel, bei der eine Nachricht mit dem öffentlichen Schlüssel des vorgesehenen Empfängers verschlüsselt wird, und digitale Signaturen, bei denen eine Nachricht mit dem privaten Schlüssel des Absenders signiert wird und von jedem überprüft werden kann, der Zugriff auf den öffentlichen Schlüssel des Absenders hat. Eine mögliche Anwendung eines Verschlüsselungssystems mit öffentlichem Schlüssel ist die Verschlüsselung von Kommunikation, um Vertraulichkeit zu gewährleisten - eine Nachricht, die ein Absender mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, der nur mit dem dazugehörigen privaten Schlüssel des Empfängers entschlüsselt werden kann. Eine weitere Anwendung der Kryptografie mit öffentlichem Schlüssel ist die digitale Signatur. Digitale Signaturschemata können zur Absenderauthentifizierung verwendet werden. Nichtabstreitbarkeitssysteme verwenden digitale Signaturen, um sicherzustellen, dass eine Partei die Urheberschaft eines Dokuments oder einer Mitteilung nicht erfolgreich abstreiten kann. Weitere Anwendungen, die auf dieser Grundlage aufbauen, sind: digitales Bargeld, passwortauthentifizierte Schlüsselvereinbarung, Zeitstempeldienste und Nichtabstreitbarkeitsprotokolle.

KURZDARSTELLUNG

[0007] Von einem ersten Aspekt aus betrachtet, stellt die vorliegende Erfindung ein System zur Verteilung eines Sicherheitsberechtigungsnaachweises dar, wobei das System aufweist: einen Hauptspeicher, der durch einen Computer ausführbare Komponenten speichert; einen Prozessor, der mit dem Hauptspeicher betriebsfähig verbunden ist und die in dem Hauptspeicher gespeicherten, durch einen Computer ausführbaren Komponenten ausführt; wobei die durch einen Computer ausführbaren Komponenten aufweisen: eine vertrauenswürdige Plattformmodulkomponente, die ausführbar ist, um ein Digitale-Identität-Token zu erzeugen, das an einen

Computeranwendungsprozess gebunden ist; und eine Authentizitätskomponente, die ausführbar ist, um das Digitale-Identität-Token in einen Sicherheitsschlüssel zu analysieren, um einen Sicherheitsberechtigungsnaachweis abzurufen.

[0008] Von einem weiteren Aspekt aus betrachtet, stellt die vorliegende Erfindung ein durch einen Computer ausgeführtes Verfahren zur Verteilung eines Sicherheitsberechtigungsnaachweises bereit, wobei das Verfahren umfasst: Erzeugen, durch ein mit einem Prozessor betriebsfähig verbundenes System, eines Digitale-Identität-Tokens, das an einen Computeranwendungsprozess gebunden ist; und Analysieren, durch das System, des Digitale-Identität-Tokens in einen Sicherheitsschlüssel, um einen Sicherheitsberechtigungsnaachweis abzurufen.

[0009] Von einem weiteren Aspekt aus betrachtet, stellt die vorliegende Erfindung ein System bereit, das aufweist: einen Hauptspeicher, der durch einen Computer ausführbare Komponenten speichert; einen Prozessor, der mit dem Hauptspeicher betriebsfähig verbunden ist und die in dem Hauptspeicher gespeicherten, durch einen Computer ausführbaren Komponenten ausführt, wobei die durch einen Computer ausführbaren Komponenten aufweisen: eine vertrauenswürdige Plattformmodulkomponente, die ein Digitale-Identität-Token erzeugt, das an einen Computeranwendungsprozess gebunden ist; und eine Schlüsselauthentizitätskomponente, die das Digitale-Identität-Token mit einem Sicherheitsschlüssel vergleicht, um einen Sicherheitsberechtigungsnaachweis abzurufen.

[0010] Von einem weiteren Aspekt aus betrachtet, stellt die vorliegende Erfindung ein System bereit, das aufweist: einen Hauptspeicher, der durch einen Computer ausführbare Komponenten speichert; einen Prozessor, der mit dem Hauptspeicher betriebsfähig verbunden ist und die in dem Hauptspeicher gespeicherten, durch einen Computer ausführbaren Komponenten ausführt; wobei die durch einen Computer ausführbaren Komponenten aufweisen: eine vertrauenswürdige Plattformmodulkomponente, die ein Digitale-Identität-Token erzeugt, das an einen Computeranwendungsprozess gebunden ist; und eine Richtlinienauthentizitätskomponente, die das Digitale-Identität-Token mit einer definierten Richtlinie vergleicht, die den Computeranwendungsprozess steuert, um einen Sicherheitsberechtigungsnaachweis abzurufen.

[0011] Von einem weiteren Aspekt aus betrachtet, stellt die vorliegende Erfindung ein durch einen Computer ausgeführtes Verfahren bereit, das umfasst: Erzeugen, durch ein mit einem Prozessor betriebsfähig verbundenes System, eines Digitale-Identität-Tokens, das an einen Computeranwendungsprozess gebunden ist; und Vergleichen, durch das System,

des Digitale-Identität-Tokens mit einem Sicherheitsschlüssel, um einen Sicherheitsberechtigungs-nachweis abzurufen.

[0012] Durch einen Computer ausgeführtes Verfahren, das umfasst: Erzeugen, durch ein mit einem Prozessor betriebsfähig verbundenes System, eines Digitale-Identität-Tokens, das an einen Computeranwendungsprozess gebunden ist; und Vergleichen, durch das System, des Digitale-Identität-Tokens mit einer definierten Richtlinie, die den Computeranwendungsprozess steuert, um einen Sicherheitsberechtigungs-nachweis abzurufen.

[0013] Von einem weiteren Aspekt aus betrachtet, stellt die vorliegende Erfindung ein Computerprogrammprodukt zur Verteilung eines Sicherheitsberechtigungs-nachweises bereit, wobei das Computerprogrammprodukt ein durch einen Computer lesbares Speichermedium mit damit verkörpertem Programmanweisungen aufweist, wobei die Programmanweisungen durch einen Prozessor ausführbar sind, um den Prozessor dazu zu veranlassen: durch ein mit dem Prozessor betriebsfähig verbundenes System ein Digitale-Identität-Token zu erzeugen, das an einen Computeranwendungsprozess gebunden ist; und das Digitale-Identität-Token durch das System mit einem Sicherheitsschlüssel zu vergleichen, um einen Sicherheitsberechtigungs-nachweis abzurufen.

[0014] Von einem weiteren Aspekt aus betrachtet, stellt die vorliegende Erfindung ein Computerprogrammprodukt zur Verteilung eines Sicherheitsberechtigungs-nachweises bereit, wobei das Computerprogrammprodukt ein durch einen Computer lesbares Speichermedium aufweist, das durch eine Verarbeitungsschaltung gelesen werden kann und Anweisungen zur Ausführung durch die Verarbeitungsschaltung speichert, um ein Verfahren zur Durchführung der Schritte der Erfindung durchzuführen.

[0015] Von einem weiteren Aspekt aus betrachtet, stellt die vorliegende Erfindung ein Computerprogramm bereit, das auf einem durch einen Computer lesbaren Datenträger gespeichert ist und in den internen Hauptspeicher eines digitalen Computers geladen werden kann, wobei das Computerprogramm Teile von Software-Code aufweist, wenn das Programm auf einem Computer ausgeführt wird, um die Schritte der Erfindung durchzuführen.

[0016] Im Folgenden wird eine Kurzdarstellung präsentiert, um ein grundlegendes Verständnis von einer oder mehreren Ausführungsformen der Erfindung zu vermitteln. Diese Kurzdarstellung soll keine wichtigen oder kritischen Elemente identifizieren oder einen beliebigen Umfang der jeweiligen Ausführungsformen oder einen beliebigen Umfang der

Ansprüche skizzieren. Ihr alleiniger Zweck besteht darin, Konzepte in vereinfachter Form als Einleitung zu der ausführlicheren Beschreibung zu präsentieren, welche später präsentiert wird. In einer oder mehreren hierin beschriebenen Ausführungsformen werden Systeme, durch einen Computer ausgeführte Verfahren, Vorrichtungen und/oder Computerprogrammprodukte beschrieben, die eine Verwaltung von digitalen Sicherheitsberechtigungs-nachweisen erleichtern können.

[0017] Gemäß einer Ausführungsform wird ein System bereitgestellt. Das System kann einen Hauptspeicher aufweisen, der durch einen Computer ausführbare Komponenten speichern kann. Das System kann auch einen mit dem Hauptspeicher betriebsfähig verbundenen Prozessor aufweisen, der die in dem Hauptspeicher gespeicherten, durch einen Computer ausführbaren Komponenten ausführen kann. Die durch einen Computer ausführbaren Komponenten können eine vertrauenswürdige Plattformmodulkomponente aufweisen, die ein Digitale-Identität-Token erzeugen kann, das an einen Computeranwendungsprozess gebunden ist. Die durch einen Computer ausführbaren Komponenten können auch eine Schlüsselauthentizitätskomponente aufweisen, die das Digitale-Identität-Token mit einem Sicherheitsschlüssel vergleichen kann, um einen Sicherheitsberechtigungs-nachweis abzurufen.

[0018] Gemäß einer Ausführungsform wird ein System bereitgestellt. Das System kann einen Hauptspeicher aufweisen, der durch einen Computer ausführbare Komponenten speichern kann. Das System kann auch einen mit dem Hauptspeicher betriebsfähig verbundenen Prozessor aufweisen, der die in dem Hauptspeicher gespeicherten, durch einen Computer ausführbaren Komponenten ausführen kann. Die durch einen Computer ausführbaren Komponenten können eine vertrauenswürdige Plattformmodulkomponente aufweisen, die ein Digitale-Identität-Token erzeugen kann, das an einen Computeranwendungsprozess gebunden ist. Die durch einen Computer ausführbaren Komponenten können auch eine Richtlinienauthentizitätskomponente aufweisen, die das Digitale-Identität-Token mit einer definierten Richtlinie vergleichen kann, welche den Computeranwendungsprozess steuert, um einen Sicherheitsberechtigungs-nachweis abzurufen.

[0019] Gemäß einer Ausführungsform wird ein durch einen Computer ausgeführtes Verfahren bereitgestellt. Das durch einen Computer ausgeführte Verfahren kann ein Erzeugen, durch ein mit einem Prozessor betriebsfähig verbundenes System, eines Digitale-Identität-Tokens umfassen, das an einen Computeranwendungsprozess gebunden ist. Das durch einen Computer ausgeführte Verfahren kann auch ein Vergleichen, durch das System,

des Digitale-Identität-Tokens mit einem Sicherheits-schlüssel umfassen, um einen Sicherheitsberechtigungs-nachweis abzurufen.

[0020] Gemäß einer Ausführungsform wird ein durch einen Computer ausgeführtes Verfahren bereitgestellt. Das durch einen Computer ausgeführte Verfahren kann ein Erzeugen, durch ein mit einem Prozessor betriebsfähig verbundenes System, eines Digitale-Identität-Tokens umfassen, das an einen Computeranwendungsprozess gebunden ist. Das durch einen Computer ausgeführte Verfahren kann auch ein Vergleichen, durch das System, des Digitale-Identität-Tokens mit einer definierten Richtlinie umfassen, die den Computeranwendungsprozess steuert, um einen Sicherheitsberechtigungs-nachweis abzurufen.

[0021] Gemäß einer Ausführungsform wird ein Computerprogrammprodukt zur Verteilung eines Sicherheitsberechtigungs-nachweises bereitgestellt. Das Computerprogrammprodukt kann ein durch einen Computer lesbares Speichermedium aufweisen, das über damit verkörperte Programmanweisungen verfügt. Die Programmanweisungen können durch einen Prozessor ausführbar sein, um den Prozessor dazu zu veranlassen, durch ein mit einem Prozessor betriebsfähig verbundenes System ein Digitale-Identität-Token zu erzeugen, das an einen Computeranwendungsprozess gebunden ist. Die Programmanweisungen können auch durch einen Prozessor ausführbar sein, um das Digitale-Identität-Token durch das System mit einem Sicherheits-schlüssel zu vergleichen, um den Sicherheitsberechtigungs-nachweis abzurufen.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0022] Die vorliegende Erfindung wird nun lediglich beispielhalber unter Bezugnahme auf bevorzugte Ausführungsformen beschrieben, die in den folgenden Figuren veranschaulicht sind:

Fig. 1 veranschaulicht ein Blockschaubild eines beispielhaften, nicht einschränkenden Systems, das Sicherheitsberechtigungs-nachweise verwalten kann, um eine oder mehrere Computeranwendungen gemäß einer oder mehreren hierin beschriebenen Ausführungsformen auszuführen.

Fig. 2 veranschaulicht ein Blockschaubild eines beispielhaften, nicht einschränkenden Systems, das den Zugriff auf einen oder mehrere Sicherheitsberechtigungs-nachweise für Serviceanbieter-Administratoren über ein Berechtigungs-nachweis-Freigabesystem auf der Grundlage einer Berechtigung von einer oder mehreren Computeranwendungsarbeitslasten gemäß einer oder mehreren hierin beschriebenen Ausführungsformen einschränken kann.

Fig. 3 veranschaulicht ein Schaubild eines beispielhaften, nicht einschränkenden Digitale-Identität-Tokens, das eine Verwaltung von Sicherheitsberechtigungs-nachweisen in einem oder mehreren Datensicherheitssystemen gemäß einer oder mehreren hierin beschriebenen Ausführungsformen vereinfachen kann.

Fig. 4 veranschaulicht ein Schaubild eines beispielhaften, nicht einschränkenden Systems, das einen oder mehrere Identitätsauthentizitäts-mechanismen auf der Grundlage eines Vergleichs von einem oder mehreren Digitale-Identität-Tokens und öffentlich verfügbaren digitalen Schlüsseln gemäß einer oder mehreren hierin beschriebenen Ausführungsformen ausführen kann.

Fig. 5 veranschaulicht ein Schaubild eines beispielhaften, nicht einschränkenden Systems, das einen oder mehrere Identitätsauthentizitäts-mechanismen auf der Grundlage eines Vergleichs von einem oder mehreren Digitale-Identität-Tokens und steuernden Richtlinien gemäß einer oder mehreren hierin beschriebenen Ausführungsformen ausführen kann.

Fig. 6 veranschaulicht ein Schaubild eines beispielhaften, nicht einschränkenden Computeranwendungsprozesses, der durch ein oder mehrere Systeme ausgeführt werden kann, welche den Zugriff auf einen oder mehrere Sicherheitsberechtigungs-nachweise für Serviceanbieter-Administratoren über ein Berechtigungs-nachweis-Freigabesystem auf der Grundlage einer Berechtigung von einer oder mehreren Computeranwendungsarbeitslasten gemäß einer oder mehreren hierin beschriebenen Ausführungsformen einschränken können.

Fig. 7 veranschaulicht ein Blockschaubild eines beispielhaften, nicht einschränkenden Systems, das den Zugriff auf einen oder mehrere Sicherheitsberechtigungs-nachweise für Serviceanbieter-Administratoren über ein Berechtigungs-nachweis-Freigabesystem auf der Grundlage einer Berechtigung von einer oder mehreren Computeranwendungsarbeitslasten gemäß einer oder mehreren hierin beschriebenen Ausführungsformen einschränken kann.

Fig. 8 veranschaulicht einen Ablaufplan eines beispielhaften, nicht einschränkenden Verfahrens, das ein Einschränken des Zugriffs auf Berechtigungs-nachweise für Serviceanbieter-Administratoren über ein Berechtigungs-nachweis-Freigabesystem auf der Grundlage einer Berechtigung von einer oder mehreren Computeranwendungsarbeitslasten gemäß einer oder mehreren hierin beschriebenen Ausführungsformen vereinfachen kann.

Fig. 9 veranschaulicht einen Ablaufplan eines beispielhaften, nicht einschränkenden Verfahrens, das ein Einschränken des Zugriffs auf Berechtigungsnachweise für Serviceanbieter-Administratoren über ein Berechtigungsnachweis-Freigabesystem auf der Grundlage einer Berechtigung von einer oder mehreren Computeranwendungsarbeitslasten gemäß einer oder mehreren hierin beschriebenen Ausführungsformen vereinfachen kann.

Fig. 10 stellt eine Cloud-Computing-Umgebung gemäß einer oder mehreren hierin beschriebenen Ausführungsformen dar.

Fig. 11 stellt Abstraktionsmodellschichten gemäß einer oder mehreren hierin beschriebenen Ausführungsformen dar.

Fig. 12 veranschaulicht ein Blockschaubild einer beispielhaften, nicht einschränkenden Betriebsumgebung, in der eine oder mehrere hierin beschriebene Ausführungsformen vereinfacht werden können.

AUSFÜHRLICHE BESCHREIBUNG

[0023] Die folgende ausführliche Beschreibung ist lediglich veranschaulichend und soll keine Ausführungsformen und/oder eine Anwendung oder Verwendungen von Ausführungsformen einschränken. Darüber hinaus besteht keine Absicht, durch beliebige, in den vorhergehenden Abschnitten „Hintergrund“ oder „Kurzdarstellung“ oder in dem Abschnitt „Ausführliche Beschreibung“ präsentierte ausdrückliche oder stillschweigende Informationen gebunden zu sein.

[0024] Eine oder mehrere Ausführungsformen werden nun unter Bezugnahme auf die Zeichnungen beschrieben, in denen gleiche Bezugszahlen verwendet werden, um überall auf gleiche Elemente Bezug zu nehmen. In der folgenden ausführlichen Beschreibung werden zum Zweck der Erklärung zahlreiche spezifische Einzelheiten angegeben, um ein eingehendes Verständnis der einen oder der mehreren Ausführungsformen zu ermöglichen. Es ist jedoch in verschiedenen Fällen offensichtlich, dass die eine oder die mehreren Ausführungsformen ohne diese spezifischen Einzelheiten in die Praxis umgesetzt werden können.

[0025] Verschiedene Ausführungsformen der vorliegenden Erfindung können auf Computer-Verarbeitungssysteme, durch Computer ausgeführte Verfahren, Vorrichtungen und/oder Computerprogrammprodukte gerichtet sein, die die effizienten, effektiven und autonomen (z.B. ohne direkte Anleitung durch einen Benutzer) Datensicherheitsprozesse vereinfachen, welche den Zugriff auf Berechtigungsnachweise für Serviceanbieter-Administratoren über ein Berechtigungsnachweis-

Freigabesystem auf der Grundlage einer Berechtigung von einer oder mehreren Computeranwendungsarbeitslasten einschränken können. Zum Beispiel können eine oder mehrere Ausführungsformen die autonome Erzeugung von einem oder mehreren Digitale-Identität-Tokens aufweisen, die an einen Computeranwendungsprozess gebunden und/oder durch eine Vertrauenskette signiert sein können, die aus einer oder mehreren Hardwareeinheiten stammen kann. Das eine oder die mehreren Digitale-Identität-Tokens können des Weiteren mit einem oder mehreren öffentlichen Schlüsseln und/oder Richtlinien verglichen werden, um ein Authentifizieren des Computeranwendungsprozesses und einen Abruf eines Sicherheitsberechtigungsnachweises zur Entnahme des Computeranwendungsprozesses zu vereinfachen. Zum Beispiel können das eine oder die mehreren Digitale-Identität-Tokens eine vorliegende Computeranwendung beschreiben und/oder verwendet werden, um Berechtigungen für vertrauliche Daten auf der Grundlage von einer oder mehreren benutzerdefinierten Richtlinien zu erhalten.

[0026] Die Computer-Verarbeitungssysteme, durch einen Computer ausgeführten Verfahren, Vorrichtungen und/oder Computerprogrammprodukte nutzen Hardware und/oder Software, um Probleme zu lösen, die in hohem Maße technischer Natur sind (z.B. Einschränken des Zugriffs auf Sicherheitsberechtigungsnachweise), nicht abstrakt sind und nicht als eine Reihe von geistigen Tätigkeiten durch einen Benutzer durchgeführt werden können. Verschiedene, hierin beschriebene Ausführungsformen erreichen erweiterte Datensicherheitsmaßnahmen, indem der Zugriff auf Sicherheitsberechtigungsnachweise auf einen oder mehrere Benutzer beschränkt und dadurch die Möglichkeit für eine durch eine nachlässige oder böswillige Benutzeraktion verursachte Verletzung der Datensicherheit verringert wird.

[0027] **Fig. 1** veranschaulicht ein Blockschaubild eines beispielhaften, nicht einschränkenden Systems 100, das den Zugriff auf einen oder mehrere Sicherheitsberechtigungsnachweise für Serviceanbieter-Administratoren auf der Grundlage einer Berechtigung von einer oder mehreren Computeranwendungsarbeitslasten einschränken kann. Auf eine wiederholte Beschreibung von gleichen Elementen, die in weiteren hierin beschriebenen Ausführungsformen genutzt werden, wird der Einfachheit halber verzichtet. Aspekte von Systemen (z.B. dem System 100 und dergleichen), Vorrichtungen oder Prozessen in verschiedenen Ausführungsformen der vorliegenden Erfindung können eine oder mehrere maschinenausführbare Komponenten darstellen, die innerhalb von einer oder mehreren Maschinen verkörpert sind, z.B. verkörpert in einem oder mehreren durch einen Computer lesbaren Datenträgern, der bzw. die zu der einen oder den mehreren Maschinen gehören.

Diese Komponenten können, wenn sie durch die eine oder die mehreren Maschinen, z.B. Computer, Datenverarbeitungseinheiten, virtuellen Maschinen usw., ausgeführt werden, die Maschinen dazu veranlassen, die beschriebenen Operationen durchzuführen.

[0028] Wie in **Fig. 1** gezeigt ist, kann das System 100 einen oder mehrere Server 102, ein oder mehrere Netzwerke 104, Berechtigungsnachweisspeicher 106 und/oder Datenspeichereinheiten 108 aufweisen. Der Server 102 kann eine Sicherheitskomponente 110 aufweisen. Die Sicherheitskomponente 110 kann des Weiteren eine oder mehrere Übertragungskomponenten 112 und/oder Anwendungskomponenten 114 aufweisen. Auch kann der Server 102 mindestens einen Hauptspeicher 116 aufweisen oder andernfalls mindestens einem Hauptspeicher 116 zugeordnet sein. Der Server 102 kann des Weiteren einen Systembus 118 aufweisen, der sich mit verschiedenen Komponenten wie beispielsweise, ohne darauf beschränkt zu sein, der Sicherheitskomponente 110 und zugehörigen Komponenten, dem Hauptspeicher 116 und/oder einem Prozessor 120 verbinden kann. Während in **Fig. 1** ein Server 102 in **Fig. 1** veranschaulicht ist, können in weiteren Ausführungsformen mehrere Einheiten unterschiedlicher Art den in **Fig. 1** gezeigten Merkmalen zugeordnet sein oder diese aufweisen. Des Weiteren kann der Server 102 mit einer oder mehreren Cloud-Computing-Umgebungen Daten austauschen.

[0029] Das eine oder die mehreren Netzwerke 104 können Fest- und Funknetze, darunter, ohne darauf beschränkt zu sein, ein Mobilfunknetz, ein Weitverkehrsnetz (WAN, wide area network) (z.B. das Internet) oder ein lokales Netz (LAN, local area network) aufweisen. Zum Beispiel kann der Server 302 mit der/dem einen oder den mehreren Berechtigungsnachweisspeichern 106 und/oder Datenspeichereinheiten 108 (und umgekehrt) unter Verwendung von praktisch jeder beliebigen gewünschten drahtgebundenen oder drahtlosen Technologie Daten austauschen, darunter zum Beispiel, ohne darauf beschränkt zu sein: Mobilfunk-, WAN-, Wireless-Fidelity-(Wi-Fi-), Wi-Max-, WLAN-, Bluetooth-Technologie, einer Kombination daraus und/oder dergleichen. Obgleich die Sicherheitskomponente 110 in der gezeigten Ausführungsform auf dem einen oder den mehreren Servern 102 bereitgestellt werden kann, ist des Weiteren darauf hinzuweisen, dass die Architektur des Systems 100 nicht in dieser Weise beschränkt ist. Zum Beispiel können sich die Sicherheitskomponente 110 oder eine oder mehrere Komponenten der Sicherheitskomponente 110 in einer weiteren Computereinheit, wie beispielsweise einer weiteren Server-Einheit, einer Client-Einheit usw., befinden.

[0030] Der eine oder die mehreren Berechtigungsnachweisspeicher 106 können einen oder mehrere dynamische Sicherheitsberechtigungs-nachweise speichern, darauf zugreifen und/oder sie verteilen. In verschiedenen Ausführungsformen kann es sich bei den dynamischen Sicherheitsberechtigungs-nachweisen, die durch den einen oder die mehreren Berechtigungsnachweisspeicher 106 gespeichert, auf die durch den einen oder die mehreren Berechtigungsnachweisspeicher 106 zugegriffen und/oder die durch den einen oder die mehreren Berechtigungsnachweisspeicher 106 verteilt werden, um geheime Schlüssel für eine oder mehrere Anwendungen und/oder Datenverarbeitungssysteme handeln. Zu beispielhaften Sicherheitsberechtigungs-nachweisen können gehören, ohne darauf beschränkt zu sein: Tokens, Kennwörter, Zertifikate, Verschlüsselungsschlüssel, Anwendungsprogramm-schnittstellen-("API-)Schlüssel, Secure-Shell-("SSH-)Berechtigungsnachweise, geheime Schlüssel, eine Kombination daraus und/oder dergleichen. In verschiedenen Ausführungsformen können der eine oder die mehreren Berechtigungsnachweisspeicher 106 den einen oder die mehreren Sicherheitsberechtigungs-nachweise verschlüsseln und/oder speichern. Des Weiteren können der eine oder die mehreren Sicherheitsberechtigungs-nachweise ephemere sein (z.B. programmatisch erzeugt, wenn darauf zugegriffen wird, und nicht vorhanden, bis sie gelesen werden).

[0031] Die eine oder die mehreren Datenspeichereinheiten 108 können eine oder mehrere Datenbanken mit vertraulichen Informationen aufweisen. In verschiedenen Ausführungsformen kann es sich bei der einen oder den mehreren Datenspeichereinheiten 108 um ein oder mehrere Datenbankverwaltungssysteme handeln, das bzw. die die Erzeugung von und/oder den Zugriff auf eine(r) oder mehrere(n) Datenbanken vereinfachen kann/können. Des Weiteren können die eine oder die mehreren Datenbanken innerhalb von der einen oder den mehreren Cloud-Computing-Umgebungen gespeichert sein, wobei die eine oder die mehreren Datenspeichereinheiten 108 den Zugriff auf die eine oder die mehreren Datenbanken verwalten können. Ferner können die eine oder die mehreren Datenbanken Daten aufweisen, die in einer oder mehreren Programmiersprachen wie beispielsweise JavaScript Object Notation („JSON“) und/oder Structured Query Language („SQL“) gespeichert sind. Zu beispielhaften Datenspeichereinheiten 108 können gehören, ohne darauf beschränkt zu sein: eine oder mehrere Datenbanken, Cloudobjektspeicher („COS“), eine Kombination daraus und/oder dergleichen.

[0032] Die eine oder die mehreren Übertragungskomponenten 112 können von dem Server 102 empfangene Daten mit einer oder mehreren weiteren Komponenten des Servers (z.B. der einen oder den

mehreren weiteren zu der Sicherheitskomponente 110 gehörenden Komponenten) gemeinsam nutzen. Ferner können die eine oder die mehreren Übertragungskomponenten 112 eine oder mehrere Ausgaben der Sicherheitskomponente 110 mit dem einen oder den mehreren Berechtigungsnachweisspeichern 106 und/oder Datenspeichereinheiten 108 senden. In einer oder mehreren Ausführungsformen können die eine oder die mehreren Übertragungskomponenten 112 Daten über eine direkte elektrische Verbindung und/oder das eine oder die mehreren Netzwerke 104 senden und/oder empfangen.

[0033] Die eine oder die mehreren Anwendungskomponenten 114 können eine oder mehrere Computeranwendungen ausführen. Zum Beispiel kann es sich bei der einen oder den mehreren Anwendungskomponenten 114 um eine oder mehrere physische und/oder virtuelle Maschinen handeln, die ein(e) oder mehrere Anwendungen und/oder Programme ausführen. Des Weiteren können eine oder mehrere Anwendungen, die auf der einen oder den mehreren Anwendungskomponenten 114 ausgeführt werden, aus einem oder mehreren Containern bestehen, wobei die eine oder die mehreren Anwendungskomponenten 114 eine oder mehrere Containerorchestrierungsplattformen verwenden können. Eine vorliegende Anwendung kann aus einem einzelnen Container oder mehreren benachbarten Containern bestehen, die eng verbunden sind und/oder Ressourcen gemeinsam nutzen. Zum Beispiel können Container Ressourcen und/oder Abhängigkeiten gemeinsam nutzen, miteinander Daten austauschen und/oder koordinieren, wann und/oder wie die Container beendet werden. Ferner können der eine oder die mehreren Container durch einen oder mehrere Pods gekapselt sein, die steuern können, wie der eine oder die mehreren Container durch die eine oder die mehreren Anwendungskomponenten 114 ausgeführt werden können.

[0034] In verschiedenen Ausführungsformen können die eine oder die mehreren Anwendungskomponenten 114 einen oder mehrere Sidecar-Container mit Bezug auf die eine oder die mehreren Anwendungen erzeugen. In der Verwendung hierin kann sich der Begriff „Sidecar-Container“ auf den einen oder die mehreren Container beziehen, die sich zusammen mit einer oder mehreren Anwendungen innerhalb eines Pods befinden, wobei der eine oder die mehreren Sidecar-Container mit der einen oder den mehreren Anwendungen verbunden sein und Ressourcen mit ihr/ihnen gemeinsam nutzen können. Der eine oder die mehreren Sidecar-Container können die eine oder die mehreren Anwendungen analysieren. In einer oder mehreren Ausführungsformen können die eine oder die mehreren Anwendungen und Sidecar-Container innerhalb eines Pods zusammen gekapselt sein, um eine einzelne verwaltbare Entität zu bilden. Ferner können der eine oder die

mehreren Sidecar-Container die eine oder die mehreren Anwendungen innerhalb des Pods analysieren, um einen oder mehrere Ansprüche zu erfassen, bei denen es sich um einen oder mehrere Messwerte handeln kann, der bzw. die eine oder mehrere Arbeitslasten der einen oder der mehreren Anwendungen beschreibt/beschreiben.

[0035] Fig. 2 veranschaulicht ein Blockschaubild des beispielhaften, nicht einschränkenden Systems 100, das des Weiteren eine oder mehrere vertrauenswürdige Plattformmodul- („TPM“- , Trusted-Platform-Module-)Komponenten 202 gemäß einer oder mehreren hierin beschriebenen Ausführungsformen aufweist. Auf eine wiederholte Beschreibung von gleichen Elementen, die in weiteren hierin beschriebenen Ausführungsformen genutzt werden, wird der Einfachheit halber verzichtet. Die eine oder die mehreren TPM-Komponenten 202 können Hardware aufweisen, die ein oder mehrere Digitale-Identität-Tokens erzeugen kann. Zum Beispiel können das eine oder die mehreren Digitale-Identität-Tokens den einen oder die mehreren Ansprüche in einem in Uniform Resource Locator („URL“) codierten Format darstellen, wobei der eine oder die mehreren Ansprüche digital signiert und/oder verschlüsselt sein können. Zum Beispiel kann es sich bei dem einen oder den mehreren Digitale-Identität-Tokens um JSON-Webtokens („JWT“) handeln, wobei der eine oder die mehreren Ansprüche als ein oder mehrere JSON-Objekte codiert sein können; dadurch wird ermöglicht, dass der eine oder die mehreren Ansprüche digital signiert und/oder verschlüsselt sein können.

[0036] In verschiedenen Ausführungsformen können die eine oder die mehreren TPM-Komponenten 202 ein oder mehrere Digitale-Identität-Tokens auf der Grundlage des einen oder der mehreren Ansprüche erzeugen, die durch den einen oder die mehreren Sidecar-Container erfasst werden, welche durch die eine oder die mehreren Anwendungskomponenten 114 erzeugt werden. Zum Beispiel können die eine oder die mehreren TPM-Komponenten 202 einen oder mehrere private Schlüssel verwenden, um das eine oder die mehreren Digitale-Identität-Tokens auf der Grundlage des einen oder der mehreren Ansprüche zu erzeugen. Des Weiteren können der eine oder die mehreren privaten Schlüssel durch die eine oder die mehreren TPM-Komponenten 202 vertraulich behandelt werden. Zum Beispiel können die privaten Schlüssel im Besitz von der einen oder den mehreren TPM-Komponenten 202 bleiben, unzugänglich für die eine oder die mehreren Anwendungen, Sidecar-Container, Administratoren des Systems 100, weitere Komponenten des Systems 100 und/oder sonstige Dritte. In einer oder mehreren Ausführungsformen kann jede Anwendungskomponente 114 einer jeweiligen TPM-Komponente 202 zugeordnet sein. Alternativ können ein

oder mehrere Cluster der Anwendungskomponenten 114 derselben TPM-Komponente 202 zugeordnet sein.

[0037] In einer oder mehreren Ausführungsformen können der eine oder die mehreren privaten Schlüssel und dadurch das eine oder die mehreren Digitale-Identität-Tokens mit einem oder mehreren öffentlichen Schlüsseln korrelieren, die in einer oder mehreren Bibliotheken 122 mit öffentlichen Schlüsseln enthalten sind. Wie in **Fig. 2** gezeigt ist, können die eine oder die mehreren Bibliotheken 122 mit öffentlichen Schlüsseln in dem einen oder den mehreren Hauptspeichern 116 gespeichert sein und/oder die eine oder die mehreren Bibliotheken 122 mit öffentlichen Schlüsseln können außerhalb des Servers 102 gespeichert sein (z.B. in einem zweiten Server 102, einer externen Hauptspeichereinheit und/oder einer Cloud-Computing-Umgebung). Der eine oder die mehreren öffentlichen Schlüssel können durch eine oder mehrere Komponenten und/oder Administratoren des Systems 100 gelesen werden. Eine Verwaltung der einen oder der mehreren Bibliotheken 122 mit öffentlichen Schlüsseln kann jedoch Administratoren des vertrauenswürdigen Systems 100 vorbehalten sein. Dadurch können verschiedene Komponenten des Systems 100 und/oder externe Parteien des Systems 100 den einen oder die mehreren öffentlichen Schlüssel lesen, die eine oder die mehreren Bibliotheken 122 mit öffentlichen Schlüsseln jedoch nicht ändern (z.B. können sie einen öffentlichen Schlüssel nicht ändern, einen öffentlichen Schlüssel nicht aus der Bibliothek 122 mit öffentlichen Schlüsseln entfernen und/oder einen öffentlichen Schlüssel nicht zu der Bibliothek 122 mit öffentlichen Schlüsseln hinzufügen).

[0038] Die eine oder die mehreren TPM-Komponenten 202 können die in den Ansprüchen enthaltenen Daten verwenden, um ein oder mehrere Digitale-Identität-Tokens zu erzeugen, die an eine Ausführung der vorliegenden Anwendung gebunden sind. Ferner können die eine oder die mehreren TPM-Komponenten 202 den einen oder die mehreren privaten Schlüssel verwenden, um eine Vertrauenskette zu bilden, die durch eine Signatur bezeichnet wird, welche in dem einen oder den mehreren Digitale-Identität-Tokens enthalten sind. Darüber hinaus können die eine oder die mehreren TPM-Komponenten 202 ein Ablaufdatum für das eine oder die mehreren Digitale-Identität-Tokens definieren. Zum Beispiel können das eine oder die mehreren Digitale-Identität-Tokens nach einer definierten Zeitdauer (z.B. Bruchteilen von einer Sekunde, Sekunden, Minuten, Stunden, Tagen und/oder dergleichen) ablaufen.

[0039] **Fig. 3** veranschaulicht ein Schaubild einer beispielhaften, nicht einschränkenden Struktur 300 von einem oder mehreren Digitale-Identität-Tokens,

die durch die eine oder die mehreren TPM-Komponenten 202 gemäß einer oder mehreren hierin beschriebenen Ausführungsformen erzeugt werden kann. Auf eine wiederholte Beschreibung von gleichen Elementen, die in weiteren hierin beschriebenen Ausführungsformen genutzt werden, wird der Einfachheit halber verzichtet. Wie in **Fig. 3** gezeigt ist, können das eine oder die mehreren Digitale-Identität-Tokens eine Kopfzeile, Nutzdaten und eine Signatur aufweisen.

[0040] Die Kopfzeile kann einen Referenztitel für das vorliegende Digitale-Identität-Token aufweisen und/oder eine oder mehrere Verschlüsselungsoperationen beschreiben. In einem Beispiel, in dem die eine oder die mehreren Digitale-Identität-Tokens JWTs sind, kann die Kopfzeile eine JSON-Web-Signature- („JWS“-)Kopfzeile oder eine JSON-Web-Encryption- („JWE“-)Kopfzeile sein. Die Nutzdaten können die in dem einen oder den mehreren Ansprüchen enthaltenen Daten aufweisen. Beispieldaten, die in dem einen oder den mehreren Ansprüchen enthalten sind, und/oder dadurch die Nutzdaten des einen oder der mehreren Digitale-Identität-Tokens können, ohne darauf beschränkt zu sein, umfassen: eine geografische Region, die einer oder mehreren Anwendungskomponenten 114 zugeordnet ist, welche die vorliegende Anwendung ausführen (z.B. in **Fig. 3** durch „cluster-region“ dargestellt), einen Referenznamen, der einer oder mehreren Anwendungskomponenten 114 zugeordnet ist, welche die vorliegende Anwendung ausführen (z.B. in **Fig. 3** durch „cluster-name“ mit Bezug auf ein Cluster von Anwendungskomponenten 114 und/oder „machineid“ mit Bezug auf eine bestimmte Anwendungskomponente 114 innerhalb des Clusters dargestellt), einen Referenznamen, der einem Pod zugeordnet ist, welcher die vorliegenden Container der Anwendung kapselt (z.B. in **Fig. 3** durch „pod“ dargestellt), eine Arbeitslast des einen oder der mehreren Container (z.B. in **Fig. 3** durch „images“ dargestellt), ein Ablaufdatum für das Digitale-Identität-Token (z.B. in **Fig. 3** durch „exp“ dargestellt, ein Startdatum für das Digitale-Identität-Token (z.B. in **Fig. 3** durch „iat“ dargestellt), einen Aussteller der vorliegenden Anwendung (z.B. in **Fig. 3** durch „iss“ dargestellt), einen Namensbereich (z.B. in **Fig. 3** durch „namespace“ dargestellt), Ergebnisse einer Konformitätsprüfung, eine Sicherheitslücke, bestimmte Versionsinformationen, aktuelle Netzwerkkonfigurationen und/oder -Informationen, offene Ports, eine Kombination daraus und/oder dergleichen. Des Weiteren kann die Signatur eine Signatur aus der einen oder den mehreren TPM-Komponenten 202 aufweisen, die das Digitale-Identität-Token unter Verwendung des einen oder der mehreren privaten Schlüssel erzeugt hat.

[0041] **Fig. 4** veranschaulicht ein Schaubild des beispielhaften, nicht einschränkenden Systems 100,

das des Weiteren eine Schlüsselauthentizitätskomponente 402 gemäß einer oder mehreren hierin beschriebenen Ausführungsformen aufweist. Auf eine wiederholte Beschreibung von gleichen Elementen, die in weiteren hierin beschriebenen Ausführungsformen genutzt werden, wird der Einfachheit halber verzichtet. Wie in **Fig. 4** gezeigt ist, können die eine oder die mehreren Schlüsselauthentizitätskomponenten 402 in dem einen oder den mehreren Berechtigungsnachweisspeichern 106 enthalten sein.

[0042] In verschiedenen Ausführungsformen kann der Berechtigungsnachweisspeicher 106 feststellen, ob die eine oder die mehreren Anwendungen, die auf der einen oder den mehreren Anwendungskomponenten 114 ausgeführt werden, auf der Grundlage des einen oder der mehreren Digitale-Identität-Tokens zum Empfang von einem oder mehreren Sicherheitsberechtigungs-nachweisen berechtigt sind. Zum Beispiel kann die Schlüsselauthentizitätskomponente 402 das eine oder die mehreren Digitale-Identität-Tokens verwenden, um die eine oder die mehreren Anwendungen zu authentifizieren. In einer oder mehreren Ausführungsformen kann die Schlüsselauthentizitätskomponente 402 das Digitale-Identität-Token mit dem einen oder den mehreren öffentlichen Schlüsseln vergleichen, der bzw. die in der einen oder den mehreren Bibliotheken 122 mit öffentlichen Schlüsseln enthalten sind. In einer oder mehreren Ausführungsformen kann die Schlüsselauthentizitätskomponente 402 das Digitale-Identität-Token mit einer Zertifizierungskette und/oder einer Zwischenzertifizierungsstelle vergleichen. Als Reaktion darauf, dass das eine oder die mehreren Digitale-Identität-Tokens mit einem oder mehreren öffentlichen Schlüsseln verglichen wird/werden, kann die Schlüsselauthentizitätskomponente 402 feststellen, dass die vorliegende Anwendung zum Empfang von einem oder mehreren Sicherheitsberechtigungs-nachweisen berechtigt ist.

[0043] **Fig. 5** veranschaulicht ein Schaubild des beispielhaften, nicht einschränkenden Systems 100, das des Weiteren eine Richtlinienauthentizitätskomponente 502 und/oder eine Richtlinienbibliothek 504 gemäß einer oder mehreren hierin beschriebenen Ausführungsformen aufweist. Auf eine wiederholte Beschreibung von gleichen Elementen, die in weiteren hierin beschriebenen Ausführungsformen genutzt werden, wird der Einfachheit halber verzichtet. Wie in **Fig. 5** gezeigt ist, können die eine oder die mehreren Richtlinienauthentizitätskomponenten 502 und/oder Richtlinienbibliotheken 504 in dem einen oder den mehreren Berechtigungsnachweisspeichern 106 enthalten sein.

[0044] In verschiedenen Ausführungsformen kann der Berechtigungsnachweisspeicher 106 des Weiteren feststellen, welche Sicherheitsberechtigungs-

nachweise der einen oder den mehreren Anwendungen auf der Grundlage von einer oder mehreren steuernden Richtlinien und/oder des Digitale-Identität-Tokens zugeordnet werden sollen. Zum Beispiel kann die Richtlinienauthentizitätskomponente 502 die in den Nutzdaten des einen oder der mehreren Digitale-Identität-Tokens enthaltenen Daten mit einer oder mehreren in einer oder mehreren Richtlinienbibliotheken 504 enthaltenen steuernden Richtlinien vergleichen. Die eine oder die mehreren steuernden Richtlinien können skizzieren, auf welche durch die eine oder die mehreren Datenspeichereinheiten 108 verwaltete Daten zugegriffen werden kann, die Menge an Daten, auf die zugegriffen werden kann und/oder die Umstände, unter denen auf die Daten zugegriffen werden kann. Zum Beispiel können die eine oder die mehreren steuernden Richtlinien verschiedenen Anwendungen verschiedene Ebenen des Zugriffs auf die durch die eine oder die mehreren Datenspeichereinheiten 108 verwalteten Daten bieten. In einem weiteren Beispiel können die eine oder die mehreren steuernden Richtlinien derselben Anwendung in Abhängigkeit vom Kontext der Ausführung der Anwendung (z.B. welche Anwendungskomponenten 114 die Anwendung ausführen und/oder wie die Anwendungskomponenten 114 die Anwendung ausführen) verschiedene Ebenen des Zugriffs auf die durch die eine oder die mehreren Datenspeichereinheiten 108 verwalteten Daten bieten. In einer oder mehreren Ausführungsformen können die eine oder die mehreren steuernden Richtlinien durch einen oder mehrere Eigner der durch die eine oder die mehreren Datenspeichereinheiten 108 verwalteten Daten definiert werden.

[0045] Auf der Grundlage des Vergleichs zwischen dem einen oder den mehreren Digitale-Identität-Tokens und den steuernden Richtlinien kann die Richtlinienauthentizitätskomponente 502 feststellen, welche Einschränkungen, sofern vorhanden, für die vorliegende Ausführung der einen oder der mehreren Anwendungen gelten. Somit kann die Schlüsselauthentizitätskomponente 402 feststellen, ob die vorliegende Anwendung berechtigt ist, auf durch die eine oder die mehreren Datenspeichereinheiten 108 verwaltete Daten zuzugreifen, und/oder die Richtlinienauthentizitätskomponente 502 kann feststellen, ob beliebige Datenzugriffsbeschränkungen für die vorliegende Ausführung der Anwendung gelten. In einer oder mehreren Ausführungsformen kann der Berechtigungsnachweisspeicher 106 einer berechtigten Anwendung auf der Grundlage der Feststellungen der Schlüsselauthentizitätskomponente 402 und der Richtlinienauthentizitätskomponente 502 einen oder mehrere Sicherheitsberechtigungs-nachweise zuordnen. In einigen Ausführungsformen kann der Berechtigungsnachweisspeicher 106 einer berechtigten Anwendung auf der Grundlage der Feststellungen der Schlüsselauthentizitätskomponente 402

oder der Richtlinienauthentizitätskomponente 502 einen oder mehrere Sicherheitsberechtigungsnachweise zuordnen. Die Sicherheitsberechtigungsnachweise können es der Anwendung ermöglichen, auf durch die eine oder die mehreren Datenspeichereinheiten 108 verwaltete Daten zuzugreifen. Auch können der eine oder die mehreren Sicherheitsberechtigungsnachweise einen Umfang und/oder eine Ebene des Zugriffs auf der Grundlage der Anwendung und/oder der Ausführung der Anwendung gemäß einer oder mehreren steuernden Richtlinien (die z.B. durch Eigner der Daten definiert werden können) einschränken.

[0046] Fig. 6 veranschaulicht ein Schaubild eines beispielhaften, nicht einschränkenden Computeranwendungsprozesses 600, der durch das System 100 gemäß einer oder mehreren hierin beschriebenen Ausführungsformen ausgeführt werden kann. Auf eine wiederholte Beschreibung von gleichen Elementen, die in weiteren hierin beschriebenen Ausführungsformen genutzt werden, wird der Einfachheit halber verzichtet. In verschiedenen Ausführungsformen können die mit Bezug auf Fig. 6 dargestellten und/oder beschriebenen Übertragungen durch das eine oder die mehreren Netzwerke 104 vereinfacht werden. Wie in Fig. 6 gezeigt ist, können eine oder mehrere Anwendungskomponenten 114 (z.B. ein Cluster von zwei Anwendungskomponenten 114) während des Computeranwendungsprozesses 600 eine Ausführung einer Anwendung vereinfachen. Zum Beispiel können die eine oder die mehreren Anwendungskomponenten 114 einen oder mehrere Sidecar-Container erzeugen, wie hierin beschrieben ist.

[0047] Bei 602 können der eine oder die mehreren Sidecar-Container einen oder mehrere Ansprüche in Bezug auf die Anwendung erfassen und die Ansprüche an die eine oder die mehreren TPM-Komponenten 202 senden. Zum Beispiel können die Ansprüche eine oder mehrere Arbeitslasten der Anwendung beschreiben. Bei 604 können die eine oder die mehreren TPM-Komponenten 202 ein oder mehrere Digitale-Identität-Tokens auf der Grundlage der Ansprüche und eines oder mehrerer privater Schlüssel, die durch die eine oder die mehreren TPM-Komponenten 202 vertraulich behandelt werden, erzeugen. Des Weiteren können die eine oder die mehreren TPM-Komponenten 202 das eine oder die mehreren Digitale-Identität-Tokens an den einen oder die mehreren Sidecar-Container senden. Bei 606 können der eine oder die mehreren Sidecar-Container das eine oder die mehreren Digitale-Identität-Tokens mit der einen oder den mehreren Anwendungen gemeinsam nutzen. In verschiedenen Ausführungsformen kann die Anwendung in Unkenntnis darüber bleiben, wie das eine oder die mehreren Digitale-Identität-Tokens gebildet wurden und/oder was das eine oder die mehreren Digitale-Identität-Tokens gebildet hat.

Somit benötigt das System 100 die Sicherheitskomponente 110 nicht zur Speicherung von einem oder mehreren Sicherheitsberechtigungsnachweisen für eine Authentifizierung mit dem einen oder den mehreren Berechtigungsnachweisspeichern; vielmehr kann die Sicherheitskomponente (z.B. über die Anwendungskomponente 114 und/oder die TPM-Komponente 202) das eine oder die mehreren Digitale-Identität-Tokens zur Authentifizierung bereitstellen, welche (z.B. über die TPM-Komponente 202) auf der Grundlage von einem oder mehreren, durch den einen oder die mehreren Sidecar-Container erfassten Ansprüchen (z.B. über die Anwendungskomponente 114) dynamisch erzeugt werden können.

[0048] Bei 608 kann die Anwendung das eine oder die mehreren Digitale-Identität-Tokens an den einen oder die mehreren Berechtigungsnachweisspeicher 106 senden, um einen oder mehrere Sicherheitsberechtigungsnachweise anzufordern. Bei 610 kann die Schlüsselauthentizitätskomponente 402 das eine oder die mehreren Digitale-Identität-Tokens mit einem oder mehreren öffentlichen Schlüsseln vergleichen, der bzw. die in einer oder mehreren Bibliotheken 122 mit öffentlichen Schlüsseln enthalten sind. In verschiedenen Ausführungsformen können die eine oder die mehreren Bibliotheken 122 mit öffentlichen Schlüsseln durch ein oder mehrere Administratoren des vertrauenswürdigen Systems 100 verwaltet werden. In einer oder mehreren Ausführungsformen können die eine oder die mehreren Bibliotheken 122 mit öffentlichen Schlüsseln durch eine oder mehrere Entitäten und/oder Systeme verwaltet werden, die durch einen oder mehrere Eigner der in der einen oder den mehreren Datenspeichereinheiten 108 gespeicherten vertraulichen Daten definiert werden. Eine vertrauenswürdige Verwaltung der einen oder der mehreren Bibliotheken 122 mit öffentlichen Schlüsseln kann die Identifizierung von gefälschten Digitale-Identität-Tokens ermöglichen, die versuchen, eine Berechtigung aus dem einen oder den mehreren Berechtigungsnachweisspeichern 106 zu erhalten. Als Reaktion darauf, dass das eine oder die mehreren Digitale-Identität-Tokens mit einem oder mehreren öffentlichen Schlüsseln abgeglichen wird/werden, kann die Schlüsselauthentizitätskomponente 402 feststellen, dass die Anwendung zum Empfang von einem oder mehreren Sicherheitsberechtigungsnachweisen berechtigt ist. Demgegenüber kann die Schlüsselauthentizitätskomponente 402 feststellen, dass die Anwendung als Reaktion darauf, dass das eine oder die mehreren Digitale-Identität-Tokens nicht mit einem oder mehreren öffentlichen Schlüsseln abgeglichen werden, nicht zum Empfang von einem oder mehreren Sicherheitsberechtigungsnachweisen berechtigt ist.

[0049] Wobei die Schlüsselauthentizitätskomponente 402 feststellt, dass es sich bei der Anwendung um eine berechtigte Anwendung handelt, kann die

Richtlinienauthentizitätskomponente 502 des Weiteren das eine oder die mehreren Digitale-Identität-Tokens mit einer oder mehreren in einer oder mehreren Richtlinienbibliotheken 504 enthaltenen Richtlinien vergleichen. Die eine oder die mehreren Richtlinien können eine oder mehrere Datenzugriffsbeschränkungen skizzieren, die für die Anwendung und/oder die vorliegende Ausführung der Anwendung gelten (wie z.B. hierin beschrieben ist). Auf der Grundlage des Vergleichs bei 612 kann die Richtlinienauthentizitätskomponente 502 feststellen, welche Datenzugriffsbeschränkungen, sofern vorhanden, für die vorliegende Ausführung der Anwendung gelten. Bei 614 kann der Berechtigungsnachweisspeicher 106 der Anwendung auf der Grundlage der Feststellungen der Schlüsselauthentizitätskomponente 402 und/oder der Richtlinienauthentizitätskomponente 502 einen oder mehrere Sicherheitsberechtigungs-nachweise zuordnen. Zum Beispiel können der eine oder die mehreren Sicherheitsberechtigungs-nachweise als Reaktion darauf zugeordnet werden, dass die Anwendung berechtigt ist, auf durch die eine oder die mehreren Datenspeichereinheiten 108 verwaltete Daten zuzugreifen, und/oder die Sicherheitsberechtigungs-nachweise können den Umfang und/oder die Ebene des der Anwendung gewährten Datenzugriffs festlegen.

[0050] Bei 616 kann die Anwendung den einen oder die mehreren zugeordneten Sicherheitsberechtigungs-nachweise verwenden, um auf die eine oder die mehreren Datenspeichereinheiten 108 zuzugreifen und/oder um gespeicherte Daten gemäß beliebigen, durch den einen oder die mehreren Sicherheitsberechtigungs-nachweise festgelegten Datenzugriffsbeschränkungen abzurufen. Die Anwendung kann daraufhin die abgerufenen Daten verwenden, um eine oder mehrere Aufgaben auszuführen und/oder den Computeranwendungsprozess 600 abzuschließen.

[0051] Fig. 7 veranschaulicht ein Schaubild des beispielhaften, nicht einschränkenden Systems 100, das mehrere Server 102 aufweist, die eine Ausführung einer Anwendung an mehreren Standorten gemäß einer oder mehreren hierin beschriebenen Ausführungsformen vereinfachen können. Auf eine wiederholte Beschreibung von gleichen Elementen, die in weiteren hierin beschriebenen Ausführungsformen genutzt werden, wird der Einfachheit halber verzichtet. Wie in Fig. 7 gezeigt ist, kann das System 100 zum Beispiel aufweisen: einen ersten Server 702, einen zweiten Server 704, einen dritten Server 706 und/oder einen vierten Server 708. Der erste Server 702, der zweite Server 704, der dritte Server 706 und/oder der vierte Server 708 können jeweils: eine oder mehrere der verschiedenen Komponenten aufweisen, die hierin mit Bezug auf den Server 102 beschrieben sind, an verschiedenen Standorten positioniert sein und/oder über ein oder mehrere

Netzwerke 104 (z.B. über eine Cloud-Computing-Umgebung) Daten austauschen. Zum Beispiel kann sich der erste Server 702 in London befinden, der zweite Server 704 kann sich in Dallas befinden, der dritte Server 706 kann sich in Berlin befinden und/oder der vierte Server 708 kann sich in Washington D.C. befinden.

[0052] Um eine oder mehrere der Funktionen des Systems 100 beispielhaft aufzuzeigen, betrachtet das folgende beispielhafte Szenario ein multinationales Unternehmen mit Standorten in Dallas und Berlin. Das Unternehmen kann das System 100 verwenden, um einen oder mehrere Computeranwendungsprozesse 600 auszuführen und/oder um die folgenden steuernden Richtlinien mit Bezug auf Mitarbeiterdaten zu definieren, die in einer oder mehreren Datenspeichereinheiten 108 gespeichert sind. Die erste Richtlinie kann skizzieren, dass es zwei Ebenen des Datenzugriffs gibt: einen uneingeschränkten Datenzugriff, der die folgenden Informationen in Bezug auf die Mitarbeiter des Unternehmens umfassen kann: Vorname, Nachname, Stellung, Sozialversicherungsnummern und/oder Telefonnummern; und/oder einen eingeschränkten Datenzugriff, der nur den Vornamen, den Nachnamen und Informationen zur Stellung umfassen kann. Eine zweite Richtlinie kann skizzieren, dass nur Anwendungen, die Anforderungen von dem Unternehmensserver in Berlin absenden und einen bestimmten vertrauenswürdigen, signierten Container verwenden, uneingeschränkter Datenzugriff gewährt werden kann; andernfalls kann Anwendungen, die Anforderungen von dem Unternehmensserver in Berlin absenden, eingeschränkter Datenzugriff gewährt werden. Eine dritte Richtlinie kann skizzieren, dass eine in Washington D.C. ansässige Prüfgesellschaft vorübergehend uneingeschränkter Datenzugriff anfordern kann, um eine Steuerprüfung durchzuführen. Eine vierte Richtlinie kann skizzieren, dass Anwendungen, die Anforderungen von dem Unternehmensserver in Dallas absenden, eingeschränkter Datenzugriff gewährt werden kann. Auch kann eine fünfte Richtlinie skizzieren, dass Anwendungen, die Anforderungen von anderen Standorten als Dallas und/oder Berlin absenden, nicht zum Zugriff auf die Mitarbeiterdaten berechtigt sind.

[0053] Der erste Server 702, der zweite Server 704, der dritte Server 706 und/oder der vierte Server 708 kann jeweils die gleiche Anwendung über einen oder mehrere Computeranwendungsprozesse 600 ausführen, aber einen anderen Zugriff auf die eine oder die mehreren Datenspeichereinheiten 108 erhalten. Zum Beispiel können die auf den verschiedenen Servern 102 erzeugten Digitale-Identität-Tokens mindestens aufgrund der abweichenden Standorte eines jeden Servers 102 unterschiedlich sein. Des Weiteren kann der Berechtigungsnachweisspeicher 106 auf der Grundlage des abweichenden Inhalts

der Digitale-Identität-Tokens und/oder der vorstehend definierten Richtlinien (die z.B. in der einen oder den mehreren Richtlinienbibliotheken 504 gespeichert sind) zu unterschiedlichen Feststellungen in Bezug auf die Ausführung der Anwendung auf der Mehrzahl der Server 102 kommen.

[0054] Zum Beispiel kann der Berechtigungsnachweisspeicher 106 feststellen, dass der Anwendung, wenn sie auf dem ersten Server 702 ausgeführt wird, gemäß der fünften Richtlinie mindestens aufgrund dessen, dass die Anforderung für den Sicherheitsberechtigungs-nachweis aus London stammte, kein Sicherheitsberechtigungs-nachweis zugeordnet wird (wie z.B. von dem durch eine TPM-Komponente 202 des ersten Servers 702 erzeugten Digitale-Identität-Token skizziert). In einem weiteren Fall kann der Berechtigungsnachweisspeicher 106 feststellen, dass der Anwendung, wenn sie auf dem zweiten Server 704 ausgeführt wird, gemäß der vierten Richtlinie mindestens aufgrund dessen, dass die Anforderung für den Sicherheitsberechtigungs-nachweis von einer berechtigten Anwendung in Dallas stammte, ein Sicherheitsberechtigungs-nachweis zugeordnet wird, der eingeschränkten Datenzugriff bietet (wie z.B. von dem durch eine TPM-Komponente 202 des zweiten Servers 704 erzeugten Digitale-Identität-Token skizziert). In einem weiteren Fall kann der Berechtigungsnachweisspeicher 106 feststellen, dass der Anwendung, wenn sie auf dem dritten Server 706 ausgeführt wird, mindestens aufgrund dessen, dass die Anforderung für den Sicherheitsberechtigungs-nachweis von einer berechtigten Anwendung in Berlin stammte, ein Sicherheitsberechtigungs-nachweis zugeordnet werden kann, der uneingeschränkten Datenzugriff bietet, wenn die Spezifikationen der zweiten Richtlinie erfüllt sind, und/oder ein Sicherheitsberechtigungs-nachweis zugeordnet werden kann, der eingeschränkten Datenzugriff bietet, wenn die Spezifikationen der zweiten Richtlinie nicht erfüllt sind (wie z.B. von dem durch eine TPM-Komponente 202 des dritten Servers 706 erzeugten Digitale-Identität-Token skizziert). In einem weiteren Fall kann der Berechtigungsnachweisspeicher 106 feststellen, dass der Anwendung, wenn sie auf dem vierten Server 708 ausgeführt wird, gemäß der dritten Richtlinie mindestens aufgrund dessen, dass die Anforderung für den Sicherheitsberechtigungs-nachweis von einer berechtigten Anwendung in Washington D.C. stammte, ein Sicherheitsberechtigungs-nachweis zugeordnet wird, der uneingeschränkten Datenzugriff bietet (wie z.B. von dem durch eine TPM-Komponente 202 des vierten Servers 708 erzeugten Digitale-Identität-Token skizziert).

[0055] Fig. 8 veranschaulicht einen Ablaufplan eines beispielhaften, nicht einschränkenden Verfahrens 800, das ein Einschränken des Zugriffs auf Berechtigungsnachweise für Serviceanbieter-Administratoren über ein Berechtigungsnachweis-Freiga-

besystem 100 auf der Grundlage einer Berechtigung von einer oder mehreren Computeranwendungsarbeitslasten gemäß einer oder mehreren hierin beschriebenen Ausführungsformen vereinfachen kann. Auf eine wiederholte Beschreibung von gleichen Elementen, die in weiteren hierin beschriebenen Ausführungsformen genutzt werden, wird der Einfachheit halber verzichtet.

[0056] Bei 802 kann das Verfahren ein Erzeugen (z.B. über die TPM-Komponente 202), durch ein mit einem oder mehreren Prozessoren 120 betriebsfähig verbundenes System, von einem oder mehreren Digitale-Identität-Tokens umfassen, die an einen Computeranwendungsprozess gebunden sein können (z.B. gemäß dem beispielhaften Computeranwendungsprozess 600). Des Weiteren können das eine oder die mehreren Digitale-Identität-Tokens in verschiedenen Ausführungsformen durch eine Vertrauenskette signiert sein, die Hardware (z.B. der TPM-Komponente 202) entstammen kann. Zum Beispiel können das eine oder die mehreren Digitale-Identität-Tokens auf der Grundlage von einem oder mehreren Ansprüchen erzeugt werden, die aus einer vorliegenden Anwendung und/oder einem oder mehreren privaten Schlüsseln erfasst werden, wie hierin beschrieben ist. Zum Beispiel können ein oder mehrere Sidecar-Container (die z.B. über die Anwendungskomponente 114 erzeugt wurden) eine oder mehrere vorliegende Anwendungen analysieren und/oder einen oder mehrere Messwerte erfassen, die eine oder mehrere Arbeitslasten der Anwendungen beschreiben. In verschiedenen Ausführungsformen können das eine oder die mehreren Digitale-Identität-Tokens durch die hierin beschriebene, beispielhafte Struktur 300 charakterisiert sein (z.B. können das eine oder die mehreren Digitale-Identität-Tokens JWTs sein). Auch können das eine oder die mehreren Digitale-Identität-Tokens in einer oder mehreren Ausführungsformen so gesetzt werden (z.B. über die TPM-Komponente 202), dass sie nach einem definierten Zeitraum (z.B. Bruchteilen einer Sekunde, Sekunden, Minuten usw.) ablaufen.

[0057] Bei 804 kann das Verfahren 800 ein Vergleichen (z.B. über die Schlüsselauthentizitätskomponente 402), durch das System 100, des einen oder der mehreren Digitale-Identität-Tokens mit einem oder mehreren Sicherheitsschlüsseln umfassen, um einen oder mehrere Sicherheitsberechtigungs-nachweise abzurufen (z.B. zur Ausführung des Computeranwendungsprozesses). Wie hierin beschrieben ist, kann es sich bei dem einen oder den mehreren Sicherheitsschlüsseln um öffentliche Schlüssel handeln, die in der einen oder den mehreren öffentlichen Bibliotheken 122 enthalten sind, welche durch einen oder mehrere vertrauenswürdige Administratoren des Systems 100 verwaltet werden. Des Weiteren können der eine oder die mehreren öffentlichen

Schlüssel mit einem oder mehreren privaten Schlüsseln korrelieren, die zum Erzeugen des einen oder der mehreren Digitale-Identität-Tokens verwendet werden, und/oder sie können dadurch ein Authentifizieren des einen oder der mehreren Digitale-Identität-Tokens vereinfachen.

[0058] Zum Beispiel kann der Vergleich bei 804 ein Feststellen umfassen, ob das eine oder die mehreren Digitale-Identität-Tokens mit einem oder mehreren der öffentlichen Schlüssel übereinstimmen oder anderweitig mit einem oder mehreren der öffentlichen Schlüssel korrelieren. Auf der Grundlage des Vergleichs bei 804 kann das System 100 (z.B. über die Schlüsselauthentizitätskomponente 402) feststellen, ob das analysierte Digitale-Identität-Token authentisch ist (z.B. durch das System 100 erzeugt wurde), und/oder ob der vorliegende Computeranwendungsprozess zum Empfang von einem oder mehreren Sicherheitsberechtigungs-nachweisen berechtigt ist. Zum Beispiel kann ein Digitale-Identität-Token, das konstruierte Daten (z.B. fiktive Nutzdaten) und/oder geänderte Daten (z.B. geänderte Nutzdaten) umfasst, durch das System 100 (z.B. über die Schlüsselauthentizitätskomponente 402) über den Vergleich bei 804 identifiziert werden (z.B. aufgrund von Abweichungen zwischen den Digitale-Identität-Tokens und den verfügbaren öffentlichen Schlüsseln). In einem weiteren Beispiel können eine oder mehrere Anwendungen, die nicht zum Empfang von Sicherheitsberechtigungs-nachweisen berechtigt sind, durch den Vergleich bei 804 identifiziert werden (z.B. aufgrund von Abweichungen zwischen den Digitale-Identität-Tokens und den verfügbaren öffentlichen Schlüsseln).

[0059] Bei 806 kann das Verfahren 800 des Weiteren ein Vergleichen (z.B. über die Richtlinienauthentizitätskomponente 502), durch das System 100, des einen oder der mehreren Digitale-Identität-Tokens mit einer oder mehreren definierten Richtlinien umfassen, die den vorliegenden Computeranwendungsprozess steuern können (z.B. gemäß dem beispielhaften Computeranwendungsprozess 600), wobei der Abruf des einen oder der mehreren Sicherheitsberechtigungs-nachweise des Weiteren auf dem Vergleich bei 806 beruhen kann. Wie hierin beschrieben ist, können die eine oder die mehreren Richtlinien in der einen oder den mehreren Richtlinienbibliotheken 504 enthalten sein und/oder durch einen oder mehrere Eigner von Daten definiert werden, welche über eine Verteilung der Sicherheitsberechtigungs-nachweise verwaltet werden. Das Vergleichen bei 806 kann ein Identifizieren von beliebigen, für den Computeranwendungsprozess geltenden Datenzugriffsbeschränkungen vereinfachen.

[0060] Zum Beispiel kann das Vergleichen bei 806 feststellen, ob die Berechtigung der Anwendung zum Zugriff auf vertraulich behandelte Daten einer

oder mehreren Einschränkungen unterliegt. Zum Beispiel können der eine oder die mehreren, dem vorliegenden Computeranwendungsprozess zugeordneten Sicherheitsberechtigungs-nachweise des Weiteren auf einer oder mehreren Arbeitslasten der vorliegenden Anwendung beruhen. Dadurch kann das System 100 in verschiedenen Ausführungsformen einen oder mehrere Sicherheitsberechtigungs-nachweise einer vorliegenden Anwendung zuordnen, um eine Ausführung des Computeranwendungsprozesses auf der Grundlage von: dem Berechtigungsstatus der vorliegenden Anwendung, der Authentizität des einen oder der mehreren Digitale-Identität-Tokens und/oder einer oder mehreren, durch eine oder mehrere steuernde Richtlinien definierten Datenzugriffsbeschränkungen zu vereinfachen.

[0061] Fig. 9 veranschaulicht einen Ablaufplan eines beispielhaften, nicht einschränkenden Verfahrens 900, das ein Einschränken des Zugriffs auf Berechtigungs-nachweise für Serviceanbieter-Administratoren über ein Berechtigungs-nachweis-Freigabesystem 100 auf der Grundlage einer Berechtigung von einer oder mehreren Computeranwendungsarbeitslasten gemäß einer oder mehreren hierin beschriebenen Ausführungsformen vereinfachen kann. Auf eine wiederholte Beschreibung von gleichen Elementen, die in weiteren hierin beschriebenen Ausführungsformen genutzt werden, wird der Einfachheit halber verzichtet.

[0062] Bei 902 kann das Verfahren 900 ein Erzeugen (z.B. über die Anwendungskomponente 114), durch ein mit einem oder mehreren Prozessoren 120 betriebsfähig verbundenes System, von einem oder mehreren Sidecar-Containern umfassen, die einen oder mehrere Ansprüche in Bezug auf eine Anwendung erfassen können. Zum Beispiel können der eine oder die mehreren Sidecar-Container einen oder mehrere Messwerte erfassen, die eine oder mehrere Arbeitslasten der Anwendungen beschreiben. In verschiedenen Ausführungsformen können die eine oder die mehreren Anwendungen aus einem oder mehreren Containern bestehen, die in einem oder mehreren Pods mit dem einen oder den mehreren Sidecar-Containern gekapselt sind.

[0063] Bei 904 kann das Verfahren 900 ein Erzeugen (z.B. über die TPM-Komponente 202), durch ein System 100, von einem oder mehreren Digitale-Identität-Tokens umfassen, die an einen Computeranwendungsprozess gebunden sein können (z.B. gemäß dem beispielhaften Computeranwendungsprozess 600). Des Weiteren können das eine oder die mehreren Digitale-Identität-Tokens in verschiedenen Ausführungsformen durch eine Vertrauenskette signiert sein, die Hardware (z.B. der TPM-Komponente 202) entstammen kann. Zum Beispiel können das eine oder die mehreren Digitale-Identität-Tokens

auf der Grundlage von einem oder mehreren Ansprüchen erzeugt werden, die durch den einen oder die mehreren Sidecar-Container und/oder einen oder mehrere private Schlüssel erfasst werden, wie hierin beschrieben ist. In verschiedenen Ausführungsformen können das eine oder die mehreren Digitale-Identität-Tokens durch die hierin beschriebene, beispielhafte Struktur 300 charakterisiert sein (z.B. können das eine oder die mehreren Digitale-Identität-Tokens JWTs sein). Auch können das eine oder die mehreren Digitale-Identität-Tokens in einer oder mehreren Ausführungsformen so gesetzt werden (z.B. über die TPM-Komponente 202), dass sie nach einem definierten Zeitraum (z.B. Bruchteilen einer Sekunde, Sekunden, Minuten usw.) ablaufen.

[0064] Bei 906 kann das Verfahren 900 ein Vergleichen (z.B. über die Schlüsselauthentizitätskomponente 402), durch das System 100, des einen oder der mehreren Digitale-Identität-Tokens mit einem oder mehreren Sicherheitsschlüsseln umfassen, um ein Abrufen von einem oder mehreren Sicherheitsberechtigungs-nachweisen (z.B. zur Ausführung des Computeranwendungsprozesses) zu vereinfachen. Wie hierin beschrieben ist, kann es sich bei dem einen oder den mehreren Sicherheitsschlüsseln um öffentliche Schlüssel handeln, die in der einen oder den mehreren Bibliotheken 122 mit öffentlichen Schlüsseln enthalten sind, welche durch einen oder mehrere vertrauenswürdige Administratoren des Systems 100 verwaltet werden. Des Weiteren können der eine oder die mehreren öffentlichen Schlüssel einem oder mehreren privaten Schlüsseln entsprechen, die zum Erzeugen des einen oder der mehreren Digitale-Identität-Tokens verwendet werden, und/oder sie können dadurch ein Authentifizieren des einen oder der mehreren Digitale-Identität-Tokens vereinfachen.

[0065] Zum Beispiel kann der Vergleich bei 906 ein Feststellen umfassen, ob das eine oder die mehreren Digitale-Identität-Tokens mit einem oder mehreren der öffentlichen Schlüssel übereinstimmen oder anderweitig mit einem oder mehreren der öffentlichen Schlüssel korrelieren. Auf der Grundlage des Vergleichs bei 906 kann das System 100 (z.B. über die Schlüsselauthentizitätskomponente 402) feststellen, ob das analysierte Digitale-Identität-Token authentisch ist (z.B. durch das System 100 erzeugt wurde), und/oder ob der vorliegende Computeranwendungsprozess zum Empfang von einem oder mehreren Sicherheitsberechtigungs-nachweisen berechtigt ist. Zum Beispiel kann ein Digitale-Identität-Token, das konstruierte Daten (z.B. fiktive Nutzdaten) und/oder geänderte Daten (z.B. geänderte Nutzdaten) umfasst, durch das System 100 (z.B. über die Schlüsselauthentizitätskomponente 402) über den Vergleich bei 906 identifiziert werden (z.B. aufgrund von Abweichungen zwischen den Digitale-Identität-Tokens und den verfügbaren öffentlichen

Schlüsseln). In einem weiteren Beispiel können eine oder mehrere Anwendungen, die nicht zum Empfang von Sicherheitsberechtigungs-nachweisen berechtigt sind, durch den Vergleich bei 906 identifiziert werden (z.B. aufgrund von Abweichungen zwischen den Digitale-Identität-Tokens und den verfügbaren öffentlichen Schlüsseln).

[0066] Bei 908 kann das Verfahren 900 des Weiteren ein Vergleichen (z.B. über die Richtlinienauthentizitätskomponente 502), durch das System 100, des einen oder der mehreren Digitale-Identität-Tokens mit einer oder mehreren definierten Richtlinien umfassen, die den vorliegenden Computeranwendungsprozess steuern können (z.B. gemäß dem beispielhaften Computeranwendungsprozess 600), wobei der Abruf des einen oder der mehreren Sicherheitsberechtigungs-nachweise des Weiteren auf dem Vergleich bei 806 beruhen kann. Wie hierin beschrieben ist, können die eine oder die mehreren Richtlinien in der einen oder den mehreren Richtlinienbibliotheken 504 enthalten sein und/oder durch einen oder mehrere Eigner von Daten definiert werden, welche über eine Verteilung der Sicherheitsberechtigungs-nachweise verwaltet werden. Das Vergleichen bei 908 kann ein Identifizieren von beliebigen, für den Computeranwendungsprozess geltenden Datenzugriffsbeschränkungen vereinfachen.

[0067] Zum Beispiel kann das Vergleichen bei 908 feststellen, ob die Berechtigung der Anwendung zum Zugriff auf vertraulich behandelte Daten einer oder mehreren Einschränkungen unterliegt. Zum Beispiel können der eine oder die mehreren, dem vorliegenden Computeranwendungsprozess zugeordneten Sicherheitsberechtigungs-nachweise des Weiteren auf einer oder mehreren Arbeitslasten der vorliegenden Anwendung beruhen. Dadurch kann das System 100 in verschiedenen Ausführungsformen einen oder mehrere Sicherheitsberechtigungs-nachweise einer vorliegenden Anwendung zuordnen, um eine Ausführung des Computeranwendungsprozesses auf der Grundlage von: dem Berechtigungsstatus der vorliegenden Anwendung, der Authentizität des einen oder der mehreren Digitale-Identität-Tokens und/oder einer oder mehreren, durch eine oder mehrere steuernde Richtlinien definierten Datenzugriffsbeschränkungen zu vereinfachen.

[0068] Bei 910 kann das Verfahren 900 auch ein Ausführen (z.B. über die Anwendungskomponente 114), durch das System 100, des Computeranwendungsprozesses umfassen, indem der eine oder die mehreren Sicherheitsberechtigungs-nachweise verwendet werden, um Daten aus einer oder mehreren Datenbanken (die z.B. durch eine oder mehrere Datenspeichereinheiten 108 verwaltet werden) abzurufen. Zum Beispiel können die eine oder die mehreren vorliegenden Anwendungen Daten aus einer

oder mehreren Datenspeichereinheiten 108 gemäß einer oder mehreren Zugriffsbeschränkungen abrufen, die durch den einen oder die mehreren Sicherheitsberechtigungsnachweise festgelegt werden.

[0069] Es sei von vornherein klargestellt, dass das Umsetzen der hierin angeführten Lehren nicht auf eine Cloud-Computing-Umgebung beschränkt ist, obwohl diese Offenbarung eine ausführliche Beschreibung von Cloud-Computing umfasst. Stattdessen können Ausführungsformen der vorliegenden Erfindung gemeinsam mit jeder beliebigen weiteren Art von jetzt bekannter oder später erfundener Datenverarbeitungsumgebung umgesetzt werden.

[0070] Cloud-Computing ist ein Servicebereitstellungsmodell zum Ermöglichen eines problemlosen bedarfsgesteuerten Netzwerkzugriffs auf einen gemeinsam genutzten Pool von konfigurierbaren Datenverarbeitungsressourcen (z.B. Netzwerken, Netzwerkbandbreite, Servern, Verarbeitung, Hauptspeichern, Speichern, Anwendungen, virtuellen Maschinen und Services), die mit minimalem Verwaltungsaufwand bzw. minimaler Interaktion mit einem Anbieter des Service schnell bereitgestellt und freigegeben werden können. Dieses Cloud-Modell kann mindestens fünf Eigenschaften umfassen, mindestens drei Dienstmodelle und mindestens vier Implementierungsmodelle.

Bei den Eigenschaften handelt es sich um die folgenden:

[0071] On-Demand Self-Service: Ein Cloud-Nutzer kann einseitig automatisch nach Bedarf für Datenverarbeitungsfunktionen wie Serverzeit und Netzwerkspeicher sorgen, ohne dass eine menschliche Interaktion mit dem Anbieter der Dienste erforderlich ist.

[0072] Broad Network Access: Es sind Funktionen über ein Netzwerk verfügbar, auf die durch Standardmechanismen zugegriffen wird, welche die Verwendung durch heterogene Thin- oder Thick-Client-Plattformen (z.B. Mobiltelefone, Laptops und PDAs) unterstützen.

[0073] Resource-Pooling: Die Datenverarbeitungsressourcen des Anbieters werden zusammengeschlossen, um mehreren Nutzern unter Verwendung eines Multi-Tenant-Modells zu dienen, wobei verschiedene physische und virtuelle Ressourcen dynamisch nach Bedarf zugewiesen und neu zugewiesen werden. Es gibt eine gefühlte Standortunabhängigkeit, da der Nutzer allgemein keine Kontrolle bzw. Kenntnis über den genauen Standort der bereitgestellten Ressourcen hat, aber in der Lage sein kann, einen Standort auf einer höheren Abstraktionsebene festzulegen (z.B. Land, Staat oder Rechenzentrum).

[0074] Rapid Elasticity: Funktionen können für eine schnelle horizontale Skalierung (scale out) schnell und elastisch bereitgestellt werden, in einigen Fällen auch automatisch, und für ein schnelles Scale-in schnell freigegeben werden. Für den Nutzer erscheinen die für das Bereitstellen verfügbaren Funktionen häufig unbegrenzt und sie können jederzeit in jeder beliebigen Menge gekauft werden.

[0075] Measured Service: Cloud-Systeme steuern und optimieren die Verwendung von Ressourcen automatisch, indem sie eine Messfunktion auf einer gewissen Abstraktionsebene nutzen, die für die Art von Dienst geeignet ist (z.B. Speicher, Verarbeitung, Bandbreite sowie aktive Benutzerkonten). Die Nutzung von Ressourcen kann überwacht, gesteuert und gemeldet werden, wodurch sowohl für den Anbieter als auch für den Nutzer des verwendeten Dienstes Transparenz geschaffen wird.

Bei den Dienstmodellen handelt es sich um die folgenden:

[0076] Software as a Service (SaaS): Die dem Nutzer bereitgestellte Funktion besteht darin, die in einer Cloud-Infrastruktur laufenden Anwendungen des Anbieters zu verwenden. Die Anwendungen sind über eine Thin-Client-Schnittstelle wie einen Web-Browser (z.B. auf dem Web beruhende E-Mail) von verschiedenen Client-Einheiten her zugänglich. Der Nutzer verwaltet bzw. steuert die zugrunde liegende Cloud-Infrastruktur nicht, darunter das Netzwerk, Server, Betriebssysteme, Speicher bzw. sogar einzelne Anwendungsfunktionen, mit der möglichen Ausnahme von eingeschränkten benutzerspezifischen Anwendungskonfigurationseinstellungen.

[0077] Platform as a Service (PaaS): Die dem Nutzer bereitgestellte Funktion besteht darin, durch einen Nutzer erstellte bzw. erhaltene Anwendungen, die unter Verwendung von durch den Anbieter unterstützten Programmiersprachen und Tools erstellt wurden, in der Cloud-Infrastruktur einzusetzen. Der Nutzer verwaltet bzw. steuert die zugrunde liegende Cloud-Infrastruktur nicht, darunter Netzwerke, Server, Betriebssysteme bzw. Speicher, hat aber die Kontrolle über die eingesetzten Anwendungen und möglicherweise über Konfigurationen des Application Hosting Environment.

[0078] Infrastructure as a Service (IaaS): Die dem Nutzer bereitgestellte Funktion besteht darin, das Verarbeiten, Speichern, Netzwerke und andere grundlegende Datenverarbeitungsressourcen bereitzustellen, wobei der Nutzer in der Lage ist, beliebige Software einzusetzen und auszuführen, zu der Betriebssysteme und Anwendungen gehören können. Der Nutzer verwaltet bzw. steuert die zugrunde liegende Cloud-Infrastruktur nicht, hat aber die Kontrolle über Betriebssysteme, Speicher, eingesetzte

Anwendungen und möglicherweise eine eingeschränkte Kontrolle über ausgewählte Netzwerkkomponenten (z.B. Host-Firewalls).

Bei den Einsatzmodellen handelt es sich um die folgenden:

[0079] Private Cloud: Die Cloud-Infrastruktur wird einzig und allein für eine Organisation betrieben.

[0080] Sie kann durch die Organisation oder einen Dritten verwaltet werden und kann sich in den eigenen Räumen oder in fremden Räumen befinden.

[0081] Community Cloud: Die Cloud-Infrastruktur wird von mehreren Organisationen gemeinsam genutzt und unterstützt eine spezielle Benutzergemeinschaft, die gemeinsame Angelegenheiten hat (z.B. Mission, Sicherheitsanforderungen, Richtlinien sowie Überlegungen bezüglich der Einhaltung von Vorschriften). Sie kann durch die Organisationen oder einen Dritten verwaltet werden und kann sich in den eigenen Räumen oder in fremden Räumen befinden.

[0082] Public Cloud: Die Cloud-Infrastruktur wird der allgemeinen Öffentlichkeit oder einer großen Industrie-Gruppe zur Verfügung gestellt und sie gehört einer Cloud-Dienste verkaufenden Organisation.

[0083] Hybrid Cloud: Die Cloud-Infrastruktur ist eine Zusammensetzung aus zwei oder mehreren Clouds (privat, Benutzergemeinschaft oder öffentlich), die zwar einzelne Einheiten bleiben, aber durch eine standardisierte oder proprietäre Technologie miteinander verbunden sind, die Daten- und Anwendungsportierbarkeit ermöglicht (z.B. Cloud-Zielgruppenverteilung für den Lastenausgleich zwischen Clouds).

[0084] Eine Cloud-Computing-Umgebung ist dienstorientiert mit Fokus auf Statusunabhängigkeit, geringer Kopplung, Modularität und semantischer Interoperabilität. Im Herzen von Cloud-Computing liegt eine Infrastruktur, die ein Netzwerk aus zusammengeschalteten Knoten umfasst.

[0085] Unter Bezugnahme auf **Fig. 10** ist eine veranschaulichende Cloud-Computing-Umgebung 1000 dargestellt. Wie gezeigt ist, enthält die Cloud-Computing-Umgebung 1000 einen oder mehrere Cloud-Computing-Knoten 1002, mit denen von Cloud-Nutzern verwendete lokale Datenverarbeitungseinheiten wie zum Beispiel ein elektronischer Assistent (PDA, personal digital assistant) oder ein Mobiltelefon 1004, ein Desktop-Computer 1006, ein Laptop-Computer 1008 und/oder ein Automobil-Computer-System 1010 Daten austauschen können. Die Knoten 1002 können miteinander Daten austauschen. Sie können physisch oder virtuell in ein oder

mehrere Netzwerke wie private, Benutzergemeinschafts-, öffentliche oder hybride Clouds gruppiert werden (nicht gezeigt), wie vorstehend beschrieben wurde, oder in eine Kombination daraus. Dies ermöglicht es der Cloud-Computing-Umgebung 1000, Infrastruktur, Plattformen und/oder Software als Dienst anzubieten, für die ein Cloud-Nutzer keine Ressourcen auf einer lokalen Datenverarbeitungseinheit vorhalten muss. Es sei darauf hingewiesen, dass die Arten von in **Fig. 10** gezeigten Datenverarbeitungseinheiten 1004 bis 1010 lediglich veranschaulichend sein sollen und dass die Datenverarbeitungsknoten 1002 und die Cloud-Computing-Umgebung 1000 über eine beliebige Art Netzwerk und/oder über eine beliebige Art von über ein Netzwerk aufrufbarer Verbindung (z.B. unter Verwendung eines Web-Browsers) mit einer beliebigen Art von computergestützter Einheit Daten austauschen können.

[0086] Unter Bezugnahme auf **Fig. 11** ist ein Satz von funktionalen Abstraktionsschichten gezeigt, die von der Cloud-Computing-Umgebung 1000 (**Fig. 10**) bereitgestellt werden. Auf eine wiederholte Beschreibung von gleichen Elementen, die in weiteren hierin beschriebenen Ausführungsformen genutzt werden, wird der Einfachheit halber verzichtet. Es sollte von vornherein klar sein, dass die in **Fig. 11** gezeigten Komponenten, Schichten und Funktionen lediglich veranschaulichend sein sollen und Ausführungsformen der Erfindung nicht darauf beschränkt sind. Wie dargestellt ist, werden die folgenden Schichten und entsprechenden Funktionen bereitgestellt:

[0087] Eine Hardware- und Softwareschicht 1102 umfasst Hardware- und Softwarekomponenten. Zu Beispielen für Hardwarekomponenten gehören:

Mainframe-Computer 1104; auf der RISC- (Reduced Instruction Set Computer) Architektur beruhende Server 1106; Server 1108; Blade-Server 1110;

Speichereinheiten 1112; und Netzwerke sowie Netzwerkkomponenten 1114. In einigen Ausführungsformen umfassen Softwarekomponenten eine Netzwerk-Anwendungsserver-Software 1116 und eine Datenbanksoftware 1118.

[0088] Die Virtualisierungsschicht 1120 stellt eine Abstraktionsschicht bereit, aus der die folgenden Beispiele für virtuelle Einheiten bereitgestellt werden können: virtuelle Server 1122; virtueller Speicher 1124; virtuelle Netzwerke 1126, darunter virtuelle private Netzwerke; virtuelle Anwendungen und Betriebssysteme 1128; und virtuelle Clients 1130.

[0089] In einem Beispiel kann eine Verwaltungsschicht 1132 die nachstehend beschriebenen Funktionen bereitstellen. Eine Ressourcen-Bereitstellung

1134 stellt die dynamische Beschaffung von Datenverarbeitungsressourcen sowie anderen Ressourcen bereit, die zum Durchführen von Aufgaben innerhalb der Cloud-Computing-Umgebung verwendet werden. Ein Messen und eine Preisfindung 1136 stellen die Kostenverfolgung beim Verwenden von Ressourcen innerhalb der Cloud-Computing-Umgebung sowie die Abrechnung oder Rechnungsstellung für den Verbrauch dieser Ressourcen bereit. In einem Beispiel können diese Ressourcen Anwendungssoftwarelizenzen umfassen. Die Sicherheit stellt die Identitätsüberprüfung für Cloud-Nutzer und Aufgaben sowie Schutz für Daten und andere Ressourcen bereit. Ein Benutzerportal 1138 stellt Nutzern und Systemadministratoren den Zugang zu der Cloud-Computing-Umgebung bereit. Eine Verwaltung des Dienstumfangs 1140 stellt die Zuordnung und Verwaltung von Cloud-Computing-Ressourcen bereit, so dass die benötigten Dienstziele erreicht werden. Ein Planen und Erfüllen von Vereinbarungen zum Dienstumfang (SLA, Service Level Agreement) 1142 stellt die Anordnung vorab und die Beschaffung von Cloud-Computing-Ressourcen, für die eine zukünftige Anforderung vorausgesehen wird, gemäß einem SLA bereit.

[0090] Eine Arbeitslastschicht 1144 stellt Beispiele für die Funktionalität bereit, für welche die Cloud-Computing-Umgebung verwendet werden kann. Zu Beispielen für Arbeitslasten und Funktionen, die von dieser Schicht bereitgestellt werden können, gehören: Abbildung und Navigation 1146; Software-Entwicklung und Lebenszyklusverwaltung 1148; Bereitstellung von Ausbildung in virtuellen Klassenzimmern 1150; Datenanalytikverarbeitung 1152; Transaktionsverarbeitung 1154; und Verwaltung von Sicherheitsberechtigungs-nachweisen 1156. Verschiedene Ausführungsformen der vorliegenden Erfindung können die unter Bezugnahme auf die **Fig. 10** und **11** beschriebene Cloud-Computing-Umgebung verwenden, um die Ausgabe von einem oder mehreren Sicherheitsberechtigungs-nachweisen zu vereinfachen, um eine Ausführung von einem oder mehreren Computeranwendungsprozessen zu vereinfachen.

[0091] Bei der vorliegenden Erfindung kann es sich um ein System, ein Verfahren und/oder ein Computerprogrammprodukt auf jeder möglichen Integrationsstufe technischer Details handeln. Das Computerprogrammprodukt kann ein durch einen Computer lesbares Speichermedium (oder -medien) mit durch einen Computer lesbaren Programmanweisungen darauf umfassen, um einen Prozessor dazu zu veranlassen, Aspekte der vorliegenden Erfindung auszuführen. Bei dem durch einen Computer lesbaren Speichermedium kann es sich um eine physische Einheit handeln, die Anweisungen zur Verwendung durch ein System zur Ausführung von Anweisungen behalten und speichern kann. Bei dem durch einen

Computer lesbaren Speichermedium kann es sich zum Beispiel um eine elektronische Speichereinheit, eine magnetische Speichereinheit, eine optische Speichereinheit, eine elektromagnetische Speichereinheit, eine Halbleiterspeichereinheit oder jede geeignete Kombination daraus handeln, ohne auf diese beschränkt zu sein. Zu einer nicht erschöpfenden Liste spezifischerer Beispiele des durch einen Computer lesbaren Speichermediums gehören die folgenden: eine auswechselbare 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 auswechselbarer Kompaktspeicherplatte-Nur-Lese-Speicher (CD-ROM), eine DVD (digital versatile disc), ein Speicher-Stick, eine Diskette, eine mechanisch kodierte Einheit wie zum Beispiel Lochkarten oder erhabene Strukturen in einer Rille, auf denen Anweisungen gespeichert sind, und jede geeignete Kombination daraus. Ein durch einen Computer lesbares Speichermedium soll in der Verwendung hierin 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 ein anderes Übertragungsmedium ausbreiten (z.B. Lichtwellenleiterkabel durchlaufende Lichtimpulse) oder durch einen Draht übermittelte elektrische Signale.

[0092] 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 Weitverkehrsnetz 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.

[0093] Bei durch einen Computer lesbaren Programmanweisungen zum Ausführen von Arbeitsschritten der vorliegenden Erfindung kann es sich um Assembler-Anweisungen, ISA-Anweisungen (Instruction-Set-Architecture), Maschinenanweisungen, maschinenabhängige Anweisungen, Mikrocode, Firmwareanweisungen, zustandssetzende

Daten, Konfigurationsdaten für eine integrierte Schaltung oder entweder Quellcode oder Objektcode handeln, die in einer beliebigen Kombination aus einer oder mehreren Programmiersprachen geschrieben werden, darunter objektorientierte Programmiersprachen wie Smalltalk, C++ o.ä. sowie 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 Softwarepaket, teilweise auf dem Computer des Benutzers und teilweise auf einem fernen Computer oder vollständig auf dem fernen Computer oder Server ausgeführt werden. In letzterem Fall kann der entfernt angeordnete Computer mit dem Computer des Benutzers durch eine beliebige Art Netzwerk verbunden sein, darunter ein lokales Netzwerk (LAN) oder ein Weitverkehrsnetz (WAN), oder die Verbindung kann mit einem externen Computer hergestellt werden (zum Beispiel über das Internet unter Verwendung eines Internet-Dienstansbieters). In einigen Ausführungsformen können elektronische Schaltungen, darunter zum Beispiel programmierbare Logikschaltungen, vor Ort programmierbare Gatter-Anordnungen (FPGA, field-programmable gate arrays) oder programmierbare Logikanordnungen (PLA, programmable logic arrays) die durch einen Computer lesbaren Programmanweisungen ausführen, indem sie Zustandsinformationen der durch einen Computer lesbaren Programmanweisungen nutzen, um die elektronischen Schaltungen zu personalisieren, um Aspekte der vorliegenden Erfindung durchzuführen.

[0094] Aspekte der vorliegenden Erfindung sind hierin unter Bezugnahme auf Ablaufpläne und/oder Blockschaltbilder bzw. Schaubilder von Verfahren, Vorrichtungen (Systemen) und Computerprogrammprodukten gemäß Ausführungsformen der Erfindung beschrieben. Es wird darauf hingewiesen, dass jeder Block der Ablaufpläne und/oder der Blockschaltbilder bzw. Schaubilder sowie Kombinationen von Blöcken in den Ablaufplänen und/oder den Blockschaltbildern bzw. Schaubildern mittels durch einen Computer lesbare Programmanweisungen ausgeführt werden können.

[0095] 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, so dass die über den Prozessor des Computers bzw. der anderen programmierbaren Datenverarbeitungsvorrichtung ausgeführten Anweisungen ein Mittel zur Umsetzung der in dem Block bzw. den Blöcken der Ablaufpläne und/oder der Blockschaltbilder bzw. Schaubilder festgelegten 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, so dass das durch einen Computer lesbare Speichermedium, auf dem Anweisungen gespeichert sind, ein Herstellungsprodukt aufweist, darunter Anweisungen, welche Aspekte der/des in dem Block bzw. den Blöcken des Ablaufplans und/oder der Blockschaltbilder bzw. Schaubilder angegebenen Funktion/Schritts umsetzen.

[0096] Die durch einen Computer lesbaren Programmanweisungen können auch auf einen Computer, eine andere programmierbare Datenverarbeitungsvorrichtung oder eine andere Einheit geladen werden, um das Ausführen einer Reihe von Prozessschritten auf dem Computer bzw. der anderen programmierbaren Vorrichtung oder anderen Einheit zu verursachen, um einen auf einem Computer ausgeführten Prozess zu erzeugen, so dass die auf dem Computer, einer anderen programmierbaren Vorrichtung oder einer anderen Einheit ausgeführten Anweisungen die in dem Block bzw. den Blöcken der Ablaufpläne und/oder der Blockschaltbilder bzw. Schaubilder festgelegten Funktionen/Schritte umsetzen.

[0097] Die Ablaufpläne und die Blockschaltbilder bzw. Schaubilder 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 dem Ablaufplan oder in den Blockschaltbildern bzw. Schaubildern ein Modul, ein Segment oder einen Teil von Anweisungen darstellen, das bzw. der eine oder mehrere ausführbare Anweisungen zur Ausführung der bestimmten logischen Funktion (en) aufweist. In einigen alternativen Ausführungen können die in dem Block angegebenen Funktionen in einer anderen Reihenfolge als in den Figuren gezeigt stattfinden. Zwei nacheinander gezeigte Blöcke können zum Beispiel in Wirklichkeit weitgehend gleichzeitig ausgeführt werden, oder die Blöcke können manchmal je nach entsprechender Funktionalität in umgekehrter Reihenfolge ausgeführt werden. Es ist ferner anzumerken, dass jeder Block der Blockschaltbilder bzw. Schaubilder und/oder der Ablaufpläne sowie Kombinationen aus Blöcken in den Blockschaltbildern bzw. Schaubildern und/oder den Ablaufplänen durch spezielle auf Hardware beruhende Systeme umgesetzt werden können, welche die festgelegten Funktionen oder Schritte durchführen, oder Kombinationen aus Spezial-Hardware und Computeranweisungen ausführen.

[0098] Um einen Kontext für die verschiedenen Aspekte des offenbaren Gegenstands bereitzustellen, sollen **Fig. 12** sowie die folgende Erläuterung eine allgemeine Beschreibung einer geeigneten Umgebung bereitstellen, in der die verschiedenen Aspekte des offenbaren Gegenstands ausgeführt werden können. **Fig. 12** veranschaulicht ein Blockschaubild einer beispielhaften, nicht einschränkenden Betriebsumgebung, in der eine oder mehrere hierin beschriebene Ausführungsformen ermöglicht werden können. Auf eine wiederholte Beschreibung von gleichen Elementen, die in weiteren hierin beschriebenen Ausführungsformen genutzt werden, wird der Einfachheit halber verzichtet. Unter Bezugnahme auf **Fig. 12** kann eine geeignete Betriebsumgebung 1200 zum Ausführen von verschiedenen Aspekten dieser Offenbarung einen Computer 1212 umfassen. Der Computer 1212 kann auch eine Verarbeitungseinheit 1214, einen Systemspeicher 1216 und einen Systembus 1218 umfassen. Der Systembus 1218 kann Systemkomponenten betriebsfähig verbinden, darunter, ohne darauf beschränkt zu sein, den Systemspeicher 1216 mit der Verarbeitungseinheit 1214. Bei der Verarbeitungseinheit 1214 kann es sich um einen beliebigen von verschiedenen verfügbaren Prozessoren handeln. Duale Mikroprozessoren und andere Multiprozessor-Architekturen können ebenfalls als Verarbeitungseinheit 1214 genutzt werden. Bei dem Systembus 1218 kann es sich um eine beliebige Busstruktur von mehreren Arten von Busstrukturen handeln, darunter den Speicherbus oder Speichercontroller, einen peripheren Bus oder externen Bus und/oder einen lokalen Bus, der eine beliebige Vielfalt an verfügbaren Busarchitekturen verwendet, darunter, ohne darauf beschränkt zu sein, Industrial Standard Architecture (ISA), Micro-Channel Architecture (MSA), Extended ISA (EISA), Intelligent Drive Electronics (IDE), VESA Local Bus (VLB), Peripheral Component Interconnect (PCI), Card Bus, Universal Serial Bus (USB), Advanced Graphics Port (AGP), Firewire und Small Computer Systems Interface (SCSI). Der Systemspeicher 1216 kann auch einen flüchtigen Speicher 1220 und einen nicht flüchtigen Speicher 1222 umfassen. Das Basic Input/Output System (BIOS), das die Basisroutinen zur Übertragung von Informationen zwischen Elementen innerhalb des Computers 1212 enthält, wie beispielsweise während des Starts, kann im nicht flüchtigen Speicher 1222 gespeichert werden. Zur Veranschaulichung und nicht als Einschränkung kann der nicht flüchtige Speicher 1222 einen Nur-Lese-Speicher (ROM), einen programmierbaren ROM (PROM), einen elektrisch programmierbaren ROM (EPROM), einen elektrisch löschbaren programmierbaren ROM (EEPROM), einen Flashspeicher oder einen nicht flüchtigen Direktzugriffsspeicher (RAM) (z.B. einen ferroelektrischen RAM (FeRAM)) umfassen. Der flüchtige Speicher 1220 kann auch einen Direktzugriffsspeicher (RAM) umfassen, der als externer

Cache dient. Zur Veranschaulichung und nicht als Einschränkung ist ein RAM in vielen Formen verfügbar, wie beispielsweise als statischer RAM (SRAM), dynamischer RAM (DRAM), synchroner DRAM (SDRAM), Double Data Rate SDRAM (DDR SDRAM), erweiterter SDRAM (ESDRAM), Synchlink-DRAM (SLDRAM), Direct Rambus RAM (DRRAM), Direct Rambus Dynamic RAM (DRDRAM) und Rambus Dynamic RAM.

[0099] Der Computer 1212 kann auch austauschbare/nicht austauschbare, flüchtige/nicht flüchtige Computerspeichermedien umfassen. **Fig. 12** veranschaulicht zum Beispiel einen Plattenspeicher 1224. Der Plattenspeicher 1224 kann auch, ohne darauf beschränkt zu sein, Einheiten wie ein Magnetplattenlaufwerk, ein Diskettenlaufwerk, ein Bandlaufwerk, ein Jaz-Laufwerk, ein Zip-Laufwerk, ein LS-100-Laufwerk, eine Flashspeicherkarte oder einen Speicher-Stick umfassen. Der Plattenspeicher 1224 kann Speichermedien auch separat oder in Kombination mit anderen Speichermedien umfassen, darunter, ohne darauf beschränkt zu sein, ein optisches Plattenlaufwerk wie beispielsweise eine Compact-Disk-ROM-Einheit (CD-ROM), ein CD-Recordable-Laufwerk (CD-R-Laufwerk), ein CD-Rewritable-Laufwerk (CD-RW-Laufwerk) oder ein Digital-Versatile-Disk-ROM-Laufwerk (DVD-ROM). Um eine Verbindung des Plattenspeichers 1224 mit dem Systembus 1218 zu vereinfachen, kann eine austauschbare oder nicht austauschbare Schnittstelle verwendet werden, wie beispielsweise eine Schnittstelle 1226. **Fig. 12** stellt auch Software dar, die als Vermittler zwischen Benutzern und den in der geeigneten Betriebsumgebung 1200 beschriebenen grundlegenden Computerressourcen dienen kann. Eine solche Software kann zum Beispiel auch ein Betriebssystem 1228 umfassen. Das Betriebssystem 1228, das auf dem Plattenspeicher 1224 gespeichert sein kann, dient zur Steuerung und Zuordnung von Ressourcen des Computers 1212. Systemanwendungen 1230 können von der Verwaltung von Ressourcen durch das Betriebssystem 1228 durch Programmmodule 1232 und Programmdateien 1234 profitieren, die z.B. entweder im Systemspeicher 1216 oder auf dem Plattenspeicher 1224 gespeichert sind. Man sollte verstehen, dass diese Offenbarung mit verschiedenen Betriebssystemen oder Kombinationen von Betriebssystemen ausgeführt werden kann. Ein Benutzer gibt Befehle oder Informationen in den Computer 1212 durch eine oder mehrere Eingabeeinheiten 1236 ein. Eingabeeinheiten 1236 können, ohne darauf beschränkt zu sein, eine Zeigereinheit wie beispielsweise eine Maus, eine Rollkugel, einen Stift, ein Touchpad, eine Tastatur, ein Mikrofon, einen Joystick, eine Spielesteuerung, eine Satellitenschüssel, einen Scanner, eine TV-Tunerkarte, eine Digitalkamera, eine digitale Videokamera, eine Webkamera und dergleichen umfassen. Diese und andere Eingabeeinheiten können durch den System-

bus 1218 über einen oder mehrere Schnittstellenanschlüsse 1238 mit der Verarbeitungseinheit 1214 verbunden sein. Die eine oder die mehreren Schnittstellenanschlüsse 1238 können zum Beispiel einen seriellen Anschluss, einen parallelen Anschluss, eine Spieleanschluss und einen Universal Serial Bus (USB) umfassen. Eine oder mehrere Ausgabeinheiten 1240 können einige Anschlüsse von der gleichen Art als Eingabeeinheit 1236 verwenden. Somit kann ein USB-Anschluss zum Beispiel verwendet werden, um dem Computer 1212 eine Eingabe bereitzustellen und um Informationen aus dem Computer 1212 an eine Ausgabeinheit 1240 auszugeben. Ein Ausgabeadapter 1242 kann bereitgestellt werden, um zu veranschaulichen, dass es einige Ausgabeinheiten 1240 wie Monitore, Lautsprecher und Drucker, unter anderen Ausgabeinheiten 1240 gibt, die spezielle Adapter erforderlich machen. Die Ausgabeadapter 1242 können, zur Veranschaulichung und nicht als Einschränkung, Video- und Soundkarten umfassen, die ein Verbindungsmittel zwischen der Ausgabeinheit 1240 und dem Systembus 1218 bereitstellen. Es sei angemerkt, dass andere Einheiten und/oder Systeme von Einheiten sowohl Eingabe- als auch Ausgabefunktionen wie beispielsweise einen oder mehrere ferne Computer 1244 bereitstellen.

[0100] Der Computer 1212 kann unter Verwendung von logischen Verbindungen zu einem oder mehreren fernen Computern, wie beispielsweise dem fernen Computer 1244, in einer vernetzten Umgebung betrieben werden. Bei dem fernen Computer 1244 kann es sich um einen Computer, einen Server, einen Leitwegrechner, einen Netzwerk-PC, eine Workstation, eine auf einem Mikroprozessor beruhende Vorrichtung, eine gleichgeordnete Einheit oder einen anderen gewöhnlichen Netzwerknoten und dergleichen handeln und er kann üblicherweise auch viele oder alle der in Bezug auf den Computer 1212 beschriebenen Elemente umfassen. Der Einfachheit halber ist nur eine Hauptspeichereinheit 1246 mit dem fernen Computer 1244 veranschaulicht. Der ferne Computer 1244 kann mit dem Computer 1212 durch eine Netzwerkschnittstelle 1248 logisch verbunden sein und dann über eine Übertragungsverbindung 1250 physisch verbunden werden. Des Weiteren kann der Betrieb über mehrere (lokale und ferne) Systeme verteilt sein. Die Netzwerkschnittstelle 1248 kann drahtgebundene und/oder drahtlose Übertragungsnetzwerke wie beispielsweise lokale Netze (LAN), Weitverkehrsnetze (WAN), Mobilfunknetze usw. umfassen. Zu LAN-Technologien gehören Fiber Distributed Data Interface (FDDI), Copper Distributed Data Interface (CDDI), Ethernet, Token Ring und dergleichen. Zu WAN-Technologien gehören, ohne darauf beschränkt zu sein, Punkt-zu-Punkt-Verbindungen, Leitungsvermittlungsnetze wie Integrated Services Digital Networks (ISDN) und Varianten davon, Paket-

vermittlungsnetze und Digital Subscriber Lines (DSL). Eine oder mehrere Übertragungsverbindungen 1250 beziehen sich auf die Hardware/Software, die zur Verbindung der Netzwerkschnittstelle 1248 mit dem Systembus 1218 genutzt wird. Zwar ist die Übertragungsverbindung 1250 zur veranschaulichenden Klarheit innerhalb des Computers 1212 gezeigt, doch kann sie sich auch außerhalb des Computers 1212 befinden. Die Hardware/Software zur Verbindung mit der Netzwerkschnittstelle 1248 kann lediglich zu Beispielzwecken auch interne und externe Technologien wie beispielsweise Modems umfassen, darunter reguläre Telefonmodems, Kabelmodems und DSL-Modems, ISDN-Adapter und Ethernet-Karten.

[0101] Bei Ausführungsformen der vorliegenden Erfindung kann es sich um ein System, ein Verfahren, eine Vorrichtung und/oder ein Computerprogrammprodukt auf jeder möglichen Integrationsstufe technischer Details handeln. Das Computerprogrammprodukt kann ein durch einen Computer lesbares Speichermedium (oder -medien) mit durch einen Computer lesbaren Programmanweisungen darauf umfassen, um einen Prozessor dazu zu veranlassen, Aspekte der vorliegenden Erfindung auszuführen. Bei dem durch einen Computer lesbaren Speichermedium kann es sich um eine greifbare Einheit handeln, die Anweisungen zur Verwendung durch ein System zur Ausführung von Anweisungen behalten und speichern kann. Bei dem durch einen Computer lesbaren Speichermedium kann es sich zum Beispiel, ohne darauf beschränkt zu sein, um eine elektronische Speichereinheit, eine magnetische Speichereinheit, eine optische Speichereinheit, eine elektromagnetische Speichereinheit, eine Halbleiterspeichereinheit oder eine beliebige geeignete Kombination des Vorstehenden handeln. Zu einer nicht erschöpfenden Liste spezifischerer Beispiele des durch einen Computer lesbaren Speichermediums können auch die folgenden gehören: eine auswechselbare Computerdiskette, eine Festplatte, ein Direktzugriffsspeicher (RAM), ein Nur-Lese-Speicher (ROM), ein löschbarer programmierbarer Nur-Lese-Speicher (EPROM oder Flashspeicher), ein statischer Direktzugriffsspeicher (SRAM), ein auswechselbarer Kompaktspeicherplatte-Nur-Lese-Speicher (CD-ROM), eine DVD (digital versatile disc), ein Speicher-Stick, eine Diskette, eine mechanisch kodierte Einheit wie zum Beispiel Lochkarten oder erhabene Strukturen in einer Rille, auf denen Anweisungen gespeichert sind, und eine beliebige geeignete Kombination des Vorstehenden. Ein durch einen Computer lesbares Speichermedium soll in der Verwendung hierin 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 ein anderes Übertragungsmedium ausbreiten (z.B. Lichtwellenleiterka-

bel durchlaufende Lichtimpulse) oder durch einen Draht übermittelte elektrische Signale.

[0102] 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 Weitverkehrsnetz 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 umfassen. 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. Bei durch einen Computer lesbaren Programmanweisungen zum Ausführen von verschiedenen Aspekten der vorliegenden Erfindung kann es sich um Assembler-Anweisungen, ISA-Anweisungen (Instruction-Set-Architecture), Maschinenanweisungen, maschinenabhängige Anweisungen, Mikrocode, Firmwareanweisungen, zustandssetzende Daten, Konfigurationsdaten für eine integrierte Schaltung oder entweder Quellcode oder Objektcode handeln, die in einer beliebigen Kombination aus einer oder mehreren Programmiersprachen geschrieben werden, darunter objektorientierte Programmiersprachen wie Smalltalk, C++ o.ä. sowie 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 fernen Computer oder vollständig auf dem fernen Computer oder Server ausgeführt werden. In letzterem Fall kann der entfernt angeordnete Computer mit dem Computer des Benutzers durch eine beliebige Art Netzwerk verbunden sein, darunter ein lokales Netzwerk (LAN) oder ein Weitverkehrsnetz (WAN), oder die Verbindung kann mit einem externen Computer hergestellt werden (zum Beispiel über das Internet unter Verwendung eines Internet-Diensteanbieters). In einigen Ausführungsformen können elektronische Schaltungen, darunter zum Beispiel programmierbare Logikschaltungen, vor Ort programmierbare Gatter-Anordnungen (FPGA, field-programmable gate arrays) oder programmierbare Logikanordnungen (PLA, programmable logic arrays) die durch einen Computer lesbaren Programmanweisungen

ausführen, indem sie Zustandsinformationen der durch einen Computer lesbaren Programmanweisungen nutzen, um die elektronischen Schaltungen zu personalisieren, um Aspekte der vorliegenden Erfindung durchzuführen.

[0103] Aspekte der vorliegenden Erfindung sind hierin unter Bezugnahme auf Ablaufpläne und/oder Blockschaltbilder bzw. Schaubilder von Verfahren, Vorrichtungen (Systemen) und Computerprogrammprodukten gemäß Ausführungsformen der Erfindung beschrieben. Es wird darauf hingewiesen, dass jeder Block der Ablaufpläne und/oder der Blockschaltbilder bzw. Schaubilder sowie Kombinationen von Blöcken in den Ablaufplänen und/oder den Blockschaltbildern bzw. Schaubildern mittels durch einen Computer lesbare Programmanweisungen ausgeführt werden können. 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, so dass die über den Prozessor des Computers bzw. der anderen programmierbaren Datenverarbeitungsvorrichtung ausgeführten Anweisungen ein Mittel zur Umsetzung der in dem Block bzw. den Blöcken der Ablaufpläne und/oder der Blockschaltbilder bzw. Schaubilder festgelegten 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, so dass das durch einen Computer lesbare Speichermedium, auf dem Anweisungen gespeichert sind, ein Herstellungsprodukt umfasst, darunter Anweisungen, welche Aspekte der/des in dem Block bzw. den Blöcken des Ablaufplans und/oder der Blockschaltbilder bzw. Schaubilder angegebenen Funktion/Schritts umsetzen. Die durch einen Computer lesbaren Programmanweisungen können auch auf einen Computer, eine andere programmierbare Datenverarbeitungsvorrichtung oder eine andere Einheit geladen werden, um das Ausführen einer Reihe von Prozessvorgängen auf dem Computer bzw. der anderen programmierbaren Vorrichtung oder anderen Einheit zu verursachen, um einen auf einem Computer ausgeführten Prozess zu erzeugen, so dass die auf dem Computer, einer anderen programmierbaren Vorrichtung oder einer anderen Einheit ausgeführten Anweisungen die in dem Block bzw. den Blöcken der Ablaufpläne und/oder der Blockschaltbilder bzw. Schaubilder festgelegten Funktionen/Schritte umsetzen.

[0104] Die Ablaufpläne und die Blockschaltbilder bzw. Schaubilder 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 dem Ablaufplan oder in den Blockschaltbildern bzw. Schaubildern ein Modul, ein Segment oder einen Teil von Anweisungen darstellen, das bzw. der eine oder mehrere ausführbare Anweisungen zur Ausführung der bestimmten logischen Funktion (en) umfasst. In einigen alternativen Ausführungen können die in den Blöcken angegebenen Funktionen in einer anderen Reihenfolge als in den Figuren gezeigt stattfinden. Zwei nacheinander gezeigte Blöcke können zum Beispiel in Wirklichkeit im Wesentlichen gleichzeitig ausgeführt werden, oder die Blöcke können manchmal je nach entsprechender Funktionalität in umgekehrter Reihenfolge ausgeführt werden. Es ist ferner anzumerken, dass jeder Block der Blockschaltbilder bzw. Schaubilder und/oder der Ablaufpläne sowie Kombinationen aus Blöcken in den Blockschaltbildern bzw. Schaubildern und/oder den Ablaufplänen durch spezielle auf Hardware beruhende Systeme umgesetzt werden können, welche die festgelegten Funktionen oder Schritte durchführen, oder Kombinationen aus Spezial-Hardware und Computeranweisungen ausführen.

[0105] Zwar wurde der Gegenstand vorstehend in dem allgemeinen Kontext von durch einen Computer ausführbaren Anweisungen eines Computerprogrammprodukts beschrieben, das auf einem Computer und/oder Computern ausgeführt wird, doch erkennt der Fachmann, dass diese Offenbarung auch in Kombination mit anderen Programmmodulen ausgeführt werden kann. Im Allgemeinen umfassen Programmmodule Routinen, Programme, Komponenten, Datenstrukturen usw., die bestimmte Aufgaben durchführen und/oder bestimmte abstrakte Datentypen ausführen. Überdies versteht der Fachmann, dass die erfindungsgemäßen, durch einen Computer ausgeführten Verfahren mit anderen Konfigurationen von Computersystemen in die Praxis umgesetzt werden können, darunter Einzelprozessor- oder Multiprozessor-Computersystemen, Mini-Datenverarbeitungseinheiten, Mainframe-Computern sowie Computern, tragbaren Datenverarbeitungseinheiten (z.B. PDA, Telefon), auf einem Mikroprozessor basierender oder programmierbarer Unterhaltungs- oder Industrieelektronik und dergleichen. Die veranschaulichten Aspekte können auch in verteilten Datenverarbeitungsumgebungen in die Praxis umgesetzt werden, in denen Aufgaben durch ferne Verarbeitungseinheiten durchgeführt werden, die durch ein Übertragungsnetzwerk verbunden sind. Jedoch können einige, wenn nicht alle Aspekte dieser Offenbarung auf eigenständigen Computern in die Praxis umgesetzt werden. In einer verteilten Datenverarbeitungsumgebung können sich Pro-

grammmodule sowohl in lokalen als auch in fernen Hauptspeichereinheiten befinden.

[0106] In der Verwendung in dieser Anwendung können sich die Begriffe „Komponente“, „System“, „Plattform“, „Schnittstelle“ und dergleichen auf eine computerbezogene Entität oder eine auf eine betriebsfähige Maschine mit einer oder mehreren bestimmten Funktionalitäten bezogene Entität beziehen und/oder eine solche umfassen. Bei den hierin offenbarten Entitäten kann es sich entweder um Hardware, eine Kombination aus Hardware und Software, Software oder in Ausführung befindliche Software handeln. Zum Beispiel kann es sich bei einer Komponente, ohne darauf beschränkt zu sein, um einen auf einem Prozessor ausgeführten Prozess, einen Prozessor, ein Objekt, eine ausführbare Datei, einen Ausführungsthread, ein Programm und/oder einen Computer handeln. Zur Veranschaulichung kann es sich sowohl bei einer auf einem Server ausgeführten Anwendung als auch bei dem Server um eine Komponente handeln. Eine oder mehrere Komponenten können sich innerhalb eines Prozesses und/oder eines Ausführungsthreads befinden und eine Komponente kann auf einem einzelnen Computer lokalisiert und/oder zwischen zwei oder mehreren Computern verteilt sein. In einem weiteren Beispiel können jeweilige Komponenten aus verschiedenen, durch einen Computer lesbaren Datenträgern heraus ausgeführt werden, die über verschiedene, darauf gespeicherte Datenstrukturen verfügen. Die Komponenten können über lokale und/oder ferne Prozesse wie beispielsweise gemäß einem Signal, das über ein oder mehrere Datenpakete verfügt (z.B. Daten aus einer Komponente, die mit einer anderen Komponente in einem lokalen System, einem verteilten System und/oder über ein Netzwerk wie beispielsweise das Internet mit anderen Systemen über das Signal interagiert), Daten austauschen. Als ein weiteres Beispiel kann es sich bei einer Komponente um eine Vorrichtung mit einer bestimmten, durch mechanische Teile bereitgestellten Funktionalität handeln, welche durch elektrische oder elektronische Schaltungen betrieben werden, die durch eine durch einen Prozessor ausgeführte Software- oder Firmware-Anwendung betrieben werden. In einem solchen Fall kann sich der Prozessor innerhalb oder außerhalb der Vorrichtung befinden und mindestens einen Teil der Software- oder Firmware-Anwendung ausführen. Als noch ein weiteres Beispiel kann es sich bei einer Komponente um eine Vorrichtung handeln, die eine bestimmte Funktionalität durch elektronische Komponenten ohne mechanische Teile bereitstellt, wobei die elektronischen Komponenten einen Prozessor oder ein anderes Mittel zur Ausführung von Software oder Firmware umfassen können, das die Funktionalität der elektronischen Komponenten mindestens zum Teil übernimmt. In einem Aspekt kann eine Komponente eine elektronische Komponente über eine vir-

tuelle Maschine, z.B. innerhalb eines Cloud-Verarbeitungssystems, emulieren.

[0107] Zudem soll der Begriff „oder“ ein einschließendes „oder“ und nicht ein ausschließendes „oder“ bedeuten. Das heißt, sofern nichts anderes angegeben ist oder aus dem Kontext hervorgeht, soll „X nutzt A oder B“ beliebige der natürlichen einschließenden Permutationen bedeuten. Das heißt, wenn X A nutzt; X B nutzt; oder X sowohl A als auch B nutzt, ist „X nutzt A oder B“ in beliebigen der vorstehenden Fälle erfüllt. Überdies sollten die Artikel „ein“ und „eine“ in der Verwendung in der vorliegenden Spezifikation und den beigefügten Zeichnungen generell in der Bedeutung von „ein(e) oder mehrere“ ausgelegt werden, sofern nichts anderes angegeben ist oder aus dem Kontext hervorgeht, dass es auf eine Singularform gerichtet sein soll. In der Verwendung hierin werden die Begriffe „Beispiel“ und/oder „beispielhaft“ in der Bedeutung von „als ein Beispiel, ein Fall oder eine Veranschaulichung dienend“ verwendet. Zur Vermeidung von Missverständnissen ist der hierin offenbarte Gegenstand nicht durch solche Beispiele beschränkt. Zudem ist ein beliebiger Aspekt oder Entwurf, der hierin als ein „Beispiel“ und/oder als „beispielhaft“ beschrieben ist, weder unbedingt als gegenüber anderen Aspekten oder Entwürfen bevorzugt oder vorteilhafter auszulegen, noch soll er gleichwertige beispielhafte Strukturen und Techniken ausschließen, die dem Fachmann bekannt sind.

[0108] In der in der vorliegenden Spezifikation verwendeten Weise kann sich der Begriff „Prozessor“ auf so gut wie jede Verarbeitungseinheit beziehen, darunter, ohne darauf beschränkt zu sein, Einzelkernprozessoren, Einzelprozessoren mit Software-Multithreadausführungsfunktion; Mehrkernprozessoren; Mehrkernprozessoren mit Software-Multithreadausführungsfunktion; Mehrkernprozessoren mit Hardware-Multithreadtechnologie; parallele Plattformen; und parallele Plattformen mit verteiltem, gemeinsam genutzten Speicher. Ferner kann sich ein Prozessor auf eine integrierte Schaltung, eine anwendungsspezifische integrierte Schaltung (ASIC, application specific integrated circuit), einen Digitalsignalprozessor (DSP), eine im Feld programmierbare Gatter-Anordnung (FPGA, field programmable gate array), einen programmierbaren Logikcontroller (PLC, programmable logic controller), eine komplexe programmierbare Logikeinheit (CPLD, complex programmable logic device), eine diskrete Gatter- oder Transistorlogik, diskrete Hardwarekomponenten oder eine beliebige Kombination daraus beziehen, die zur Durchführung der hierin beschriebenen Funktionen ausgelegt ist. Des Weiteren können Prozessoren Architekturen im Nanomaßstab wie beispielsweise, ohne darauf beschränkt zu sein, Molekular- und Quantenpunkttransistoren, Schalter und Gatter nutzen, um die Speicherbelegung zu optimieren oder die Leistung von Benutzer-

geräten zu verbessern. Ein Prozessor kann auch als eine Kombination aus Datenverarbeitungseinheiten ausgeführt sein. In dieser Offenbarung werden Begriffe wie beispielsweise „Speicher“, „Datenspeicher“, „Datenbank“ und so gut wie jede andere für den Betrieb und die Funktionalität einer Komponente relevante Informationsspeicherkomponente verwendet, um sich auf „Hauptspeicherkomponenten“, "in einem „Hauptspeicher“ verkörperte Entitäten oder einen Hauptspeicher umfassende Komponenten zu beziehen. Man sollte verstehen, dass es sich bei hierin beschriebenen Hauptspeicher und/oder hierin beschriebenen Hauptspeicherkomponenten entweder um flüchtigen Speicher oder nicht flüchtigen Speicher handeln kann oder sie sowohl flüchtigen als auch nicht flüchtigen Speicher umfassen können. Zur Veranschaulichung und nicht als Einschränkung kann der nicht flüchtige Speicher einen Nur-Lese-Speicher (ROM), einen programmierbaren ROM (PROM), einen elektrisch programmierbaren ROM (EPROM), einen elektrisch löschbaren programmierbaren ROM (EEPROM), einen Flashspeicher oder einen nicht flüchtigen Direktzugriffsspeicher (RAM) (z.B. einen ferroelektrischen RAM (FeRAM)) umfassen. Ein flüchtiger Speicher kann einen RAM umfassen, der zum Beispiel als externer Cache dienen kann. Zur Veranschaulichung und nicht als Einschränkung ist ein RAM in vielen Formen verfügbar, wie beispielsweise als synchroner RAM (SRAM), dynamischer RAM (DRAM), synchroner DRAM (SDRAM), Double Data Rate SDRAM (DDR SDRAM), erweiterter SDRAM (ESDRAM), Synchlink-DRAM (SLDRAM), Direct Rambus RAM (DRRAM), Direct Rambus Dynamic RAM (DRDRAM) und Rambus Dynamic RAM (RDRAM). Ferner sollen die offenbarten Hauptspeicherkomponenten von Systemen oder durch einen Computer ausgeführten Verfahren hierin diese und beliebige andere geeignete Arten von Hauptspeicher umfassen, ohne auf ein Umfassen beschränkt zu sein.

[0109] Das vorstehend Beschriebene umfasst bloße Beispiele von Systemen, Computerprogrammprodukten und durch einen Computer ausgeführten Verfahren. Es ist natürlich nicht möglich, jede vorstellbare Kombination aus Komponenten, Produkten und/oder durch einen Computer ausgeführten Verfahren zum Zweck der Beschreibung dieser Offenbarung zu beschreiben, jedoch kann der Fachmann erkennen, dass viele weitere Kombinationen und Permutationen dieser Offenbarung möglich sind. Darüber hinaus sollen, insoweit die Begriffe „umfasst“, „hat“, „besitzt“ und dergleichen in der ausführlichen Beschreibung, den Ansprüchen, Anhängen und Zeichnungen verwendet werden, diese Begriffe in einer Weise einschließend sein, die ähnlich dem Begriff „aufweisend“ bzw. „umfassend“ ist, da „aufweisend“ bzw. „umfassend“, wenn es genutzt wird, als ein Übergangswort in einem Anspruch verwendet wird. Die Beschreibungen der verschiedenen

Ausführungsformen erfolgten zum Zweck der Veranschaulichung, sollen jedoch nicht erschöpfend oder auf die offenbarten Ausführungsformen beschränkt sein. Viele Änderungen und Varianten sind für den Fachmann erkennbar, ohne vom Umfang der beschriebenen Ausführungsformen abzuweichen. Die hierin verwendete Terminologie wurde gewählt, um die Grundgedanken der Ausführungsformen, die praktische Anwendung oder technische Verbesserung gegenüber auf dem Markt befindlicher Technologien am besten zu erklären bzw. um anderen Fachleuten das Verständnis der hierin offenbarten Ausführungsformen zu ermöglichen.

Patentansprüche

1. System (100) zur Verteilung eines Sicherheitsberechtigungs nachweises, wobei das System (100) aufweist:
einen Hauptspeicher (116, 1216), der durch einen Computer ausführbare Komponenten speichert;
einen Prozessor (120, 1214), der mit dem Hauptspeicher (116, 1216) betriebsfähig verbunden ist und der die in dem Hauptspeicher (116, 1216) gespeicherten, durch einen Computer ausführbaren Komponenten ausführt, wobei die durch einen Computer ausführbaren Komponenten aufweisen:
eine vertrauenswürdige Plattformmodulkomponente (202), die ausführbar ist, um ein Digitale-Identität-Token (300) zu erzeugen (802, 904), das an einen Computeranwendungsprozess (600) gebunden ist, wobei das Erzeugen (802, 904) auf ein oder mehreren Messwerten basiert, die ein oder mehrere Arbeitslasten des Computeranwendungsprozesses (600) beschreiben; und
eine Authentizitätskomponente, die ausführbar ist, um das Digitale-Identität-Token (300) zu analysieren, um einen Sicherheitsberechtigungs nachweis abzurufen, wobei die Authentizitätskomponente eine Schlüsselauthentizitätskomponente (402) aufweist, um das Digitale-Identität-Token (300) mit einem Sicherheitsschlüssel zu vergleichen (804, 906), um auf der Grundlage des Vergleichs (804, 906) einen Sicherheitsberechtigungs nachweis abzurufen; und wobei die Authentizitätskomponente eine Richtlinienauthentizitätskomponente (502) aufweist, die ausführbar ist, um einen Vergleich (806, 908) des Digitale-Identität-Tokens (300) mit einer definierten Richtlinie durchzuführen, die den Computeranwendungsprozess (600) steuert, wobei ein Abrufen des Sicherheitsberechtigungs nachweises des Weiteren auf dem Vergleich (806, 908) beruht.

2. System (100) nach einem der vorhergehenden Ansprüche, wobei das Digitale-Identität-Token (300) durch eine Vertrauenskette signiert ist, die Hardware entstammt.

3. System (100) nach einem der vorhergehenden Ansprüche, des Weiteren aufweisend:

eine Anwendungskomponente (114), um den Sicherheitsberechtigungs nachweis zum Ausführen (910) des Computeranwendungsprozesses (600) zu verwenden, indem Daten aus einer Datenbank abgerufen werden.

4. System (100) nach einem der vorhergehenden Ansprüche, wobei das Digitale-Identität-Token (300) ausführbar ist, um nach einer definierten Zeitdauer abzulaufen.

5. Durch einen Computer ausgeführtes Verfahren (800, 900, 1156) zur Verteilung eines Sicherheitsberechtigungs nachweises, wobei das Verfahren (800, 900, 1156) umfasst:

Erzeugen (802, 904), durch ein mit einem Prozessor (120, 1214) betriebsfähig verbundenes System (100), eines Digitale-Identität-Tokens (300), das an einen Computeranwendungsprozess (600) gebunden ist, wobei das Erzeugen (802, 904) auf ein oder mehreren Messwerten basiert, die ein oder mehrere Arbeitslasten des Computeranwendungsprozesses (600) beschreiben; und
Analysieren, durch das System (100), des Digitale-Identität-Tokens (300), um einen Sicherheitsberechtigungs nachweis abzurufen, wobei ein Analysieren aufweist: ein Vergleichen (804, 906) des Digitale-Identität-Tokens (300) mit einem Sicherheitsschlüssel, um basierend auf dem Vergleichen (804, 906) einen Sicherheitsberechtigungs nachweis abzurufen, und ein Vergleichen (806, 908) des Digitale-Identität-Tokens (300) mit einer definierten Richtlinie aufweist, die den Computeranwendungsprozess (600) steuert, wobei der Abruf des Sicherheitsberechtigungs nachweises des Weiteren auf dem Vergleichen (806, 908) des Digitale-Identität-Tokens (300) mit der definierten Richtlinie beruht.

6. Durch einen Computer ausgeführtes Verfahren (800, 900, 1156) nach Anspruch 5, wobei der Sicherheitsschlüssel einen öffentlichen Schlüssel aufweist, wobei ein Abruf des Sicherheitsberechtigungs nachweises des Weiteren auf dem Vergleichen des Digitale-Identität-Tokens (300) und des öffentlichen Schlüssels beruht.

7. Durch einen Computer ausgeführtes Verfahren (800, 900, 1156) nach einem der Ansprüche 5 oder 6, wobei das Digitale-Identität-Token (300) durch eine Vertrauenskette signiert ist, die Hardware entstammt.

8. Durch einen Computer ausgeführtes Verfahren (800, 900, 1156) nach einem der Ansprüche 5 bis 7, des Weiteren umfassend:

Ausführen (910), durch das System (100), des Computeranwendungsprozesses (600), indem der Sicherheitsberechtigungs nachweis zum Abrufen von Daten aus einer Datenbank verwendet wird.

9. Durch einen Computer ausgeführtes Verfahren (800, 900, 1156) nach einem der Ansprüche 5 bis 8, wobei das Digitale-Identität-Token (300) nach einer definierten Zeitdauer abläuft.

10. Computerprogrammprodukt zur Verteilung eines Sicherheitsberechtigungs nachweises, wobei das Computerprogrammprodukt aufweist:
ein durch einen Computer lesbares Speichermedium, das durch eine Verarbeitungsschaltung lesbar ist und Anweisungen zur Ausführung durch die Verarbeitungsschaltung speichert, um ein Verfahren (800, 900, 1156) nach einem der Ansprüche 5 bis 9 durchzuführen.

11. Computerprogramm, das auf einem durch einen Computer lesbaren Datenträger gespeichert ist und in den internen Hauptspeicher (116, 1216) eines digitalen Computers ladbar ist, wobei das Computerprogramm Teile von Software-Code aufweist, wenn das Programm auf einem Computer (1212) ausgeführt wird, um das Verfahren (800, 900, 1156) nach einem der Ansprüche 5 bis 9 durchzuführen.

Es folgen 12 Seiten Zeichnungen

Anhängende Zeichnungen

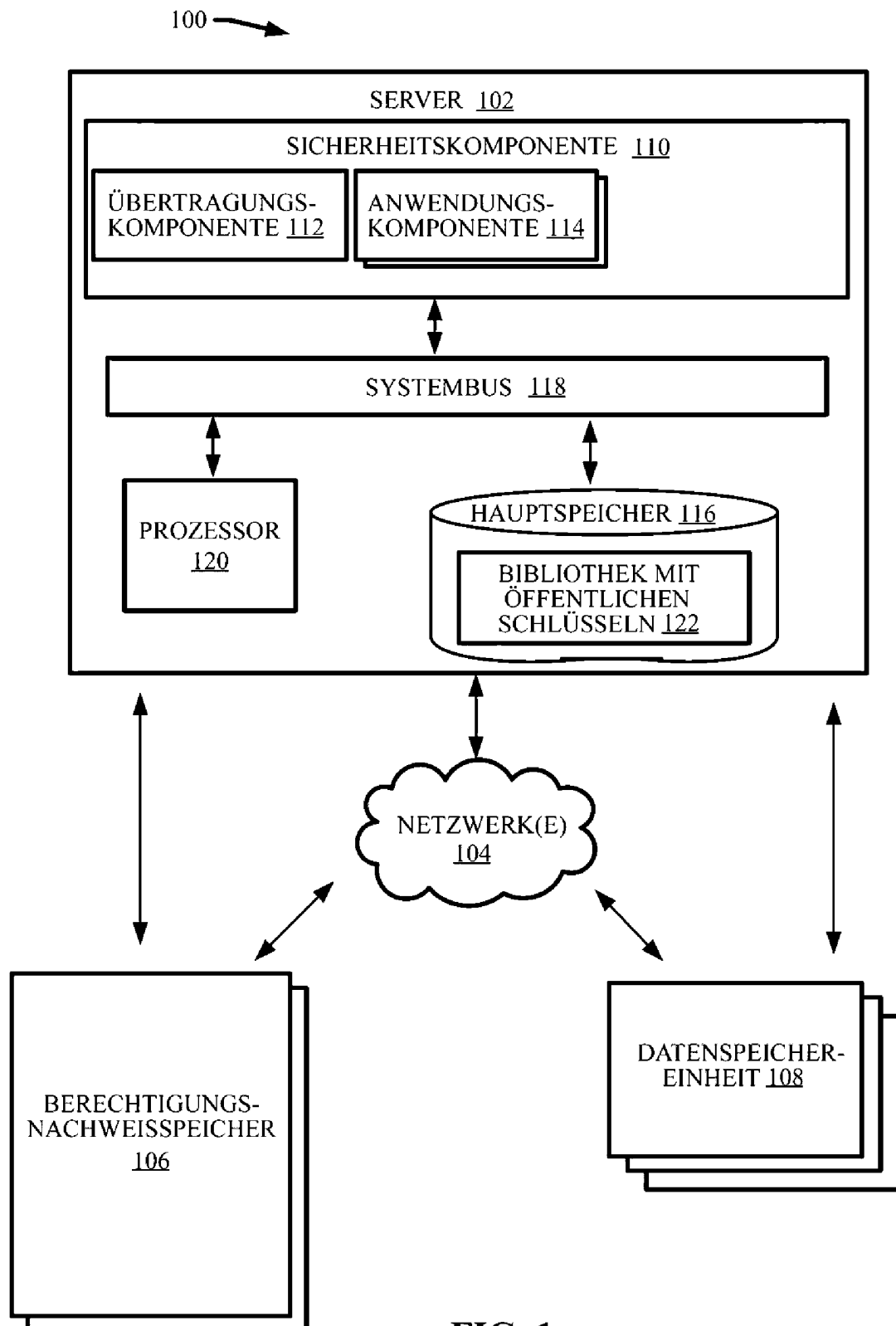


FIG. 1

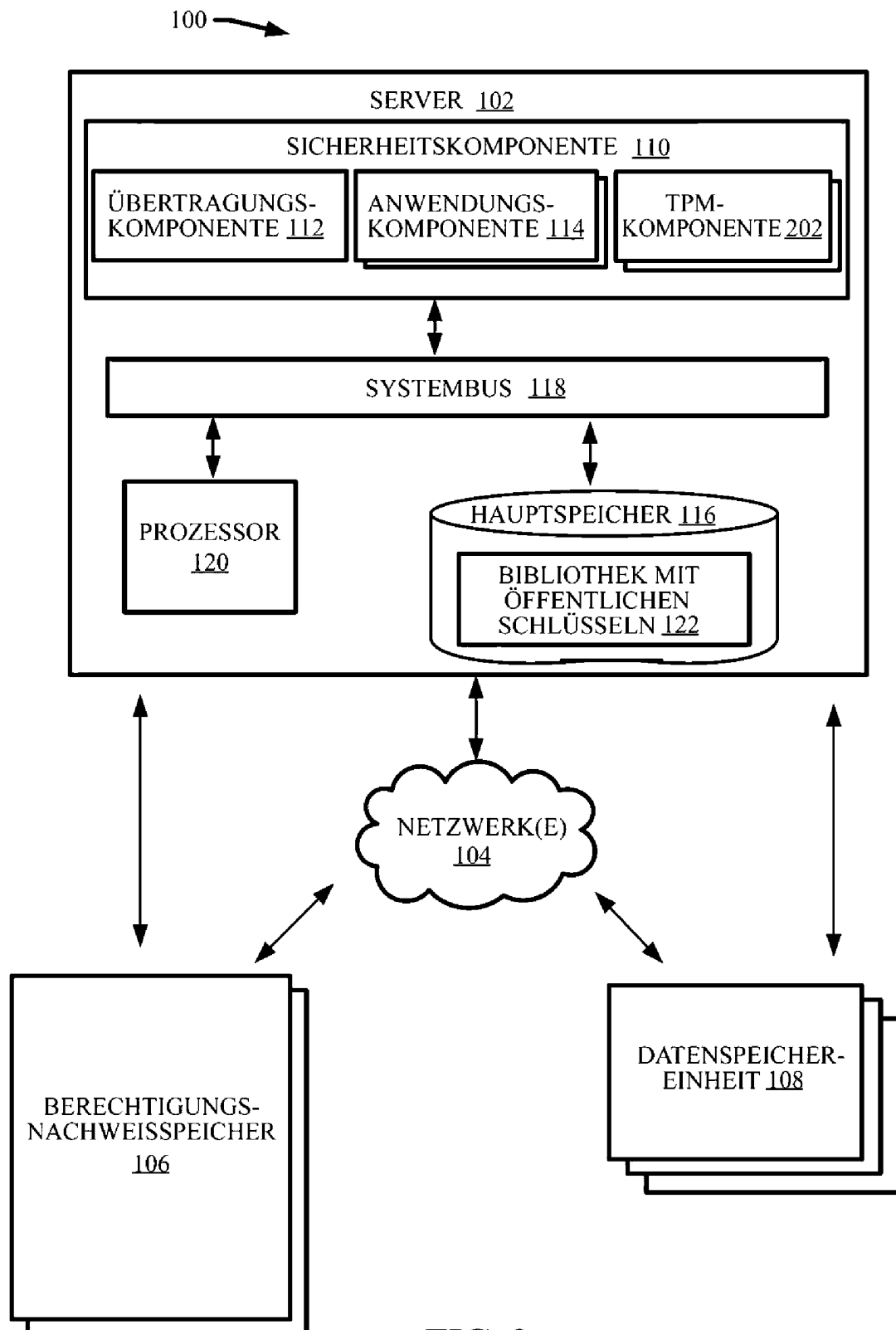


FIG. 2

300

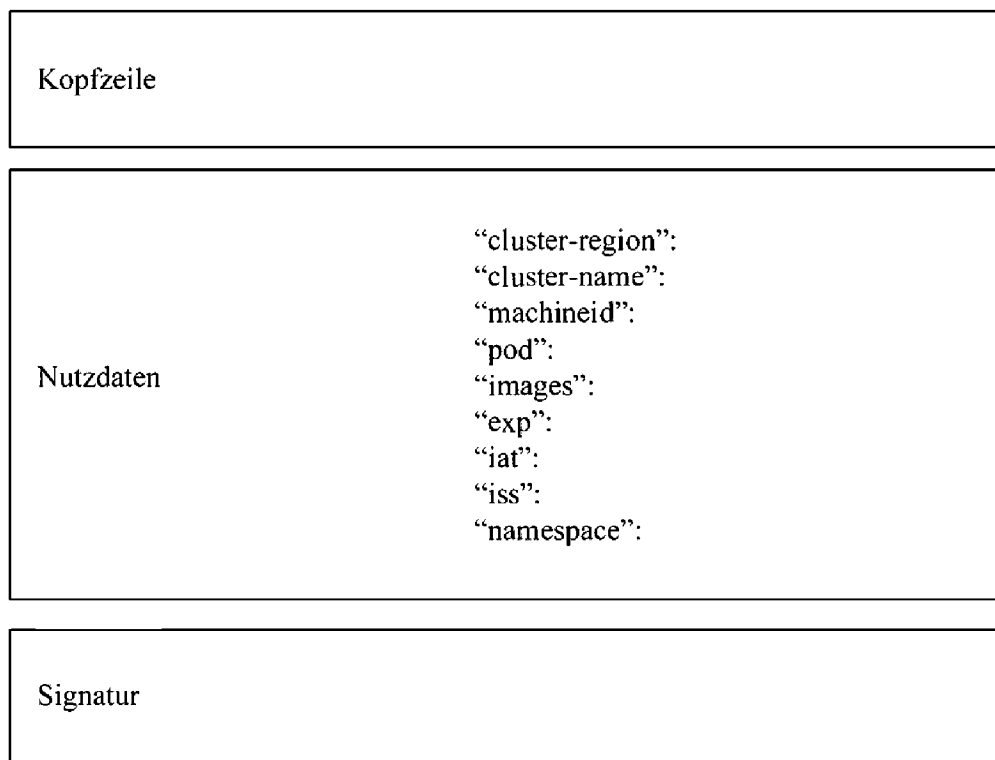


FIG. 3

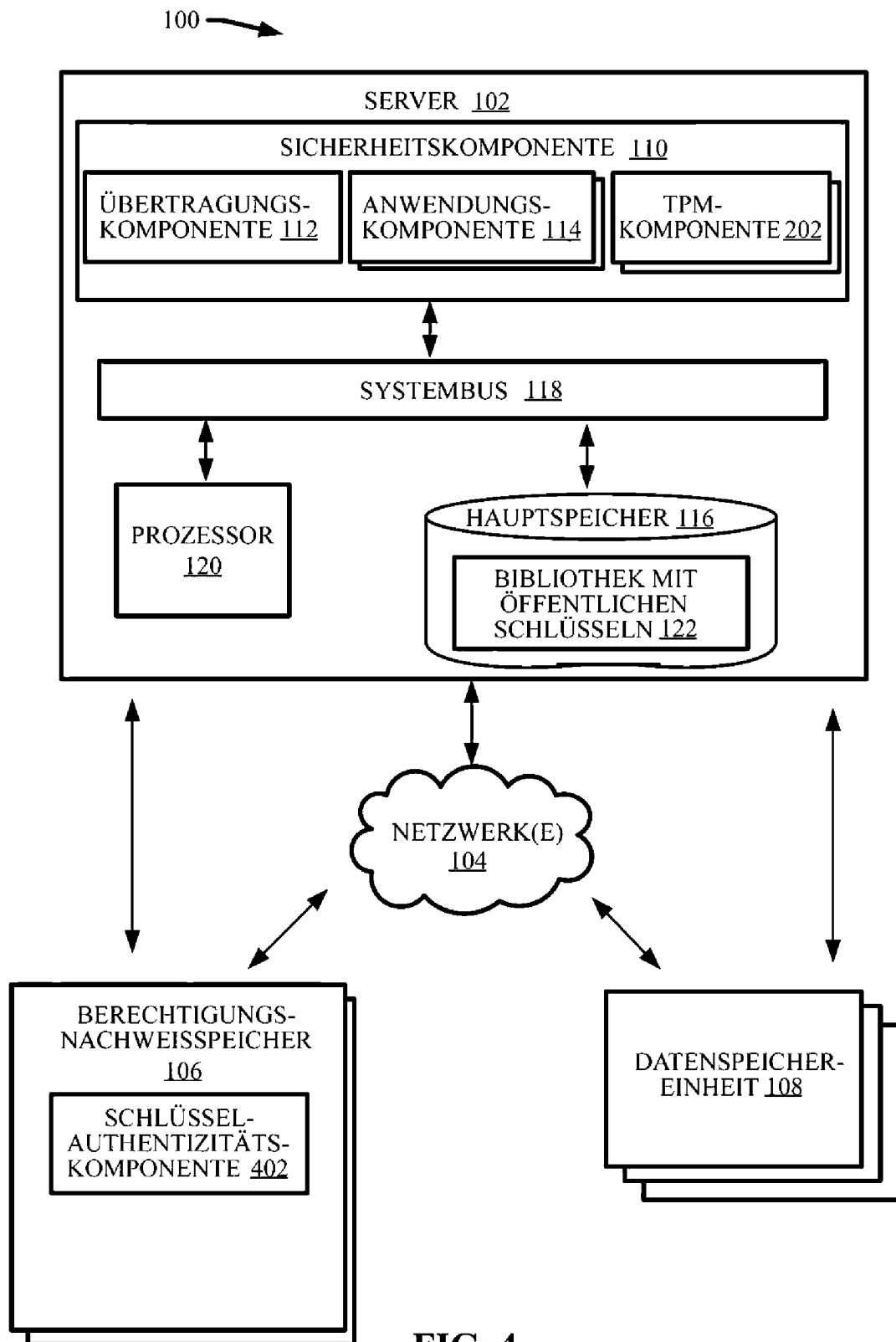
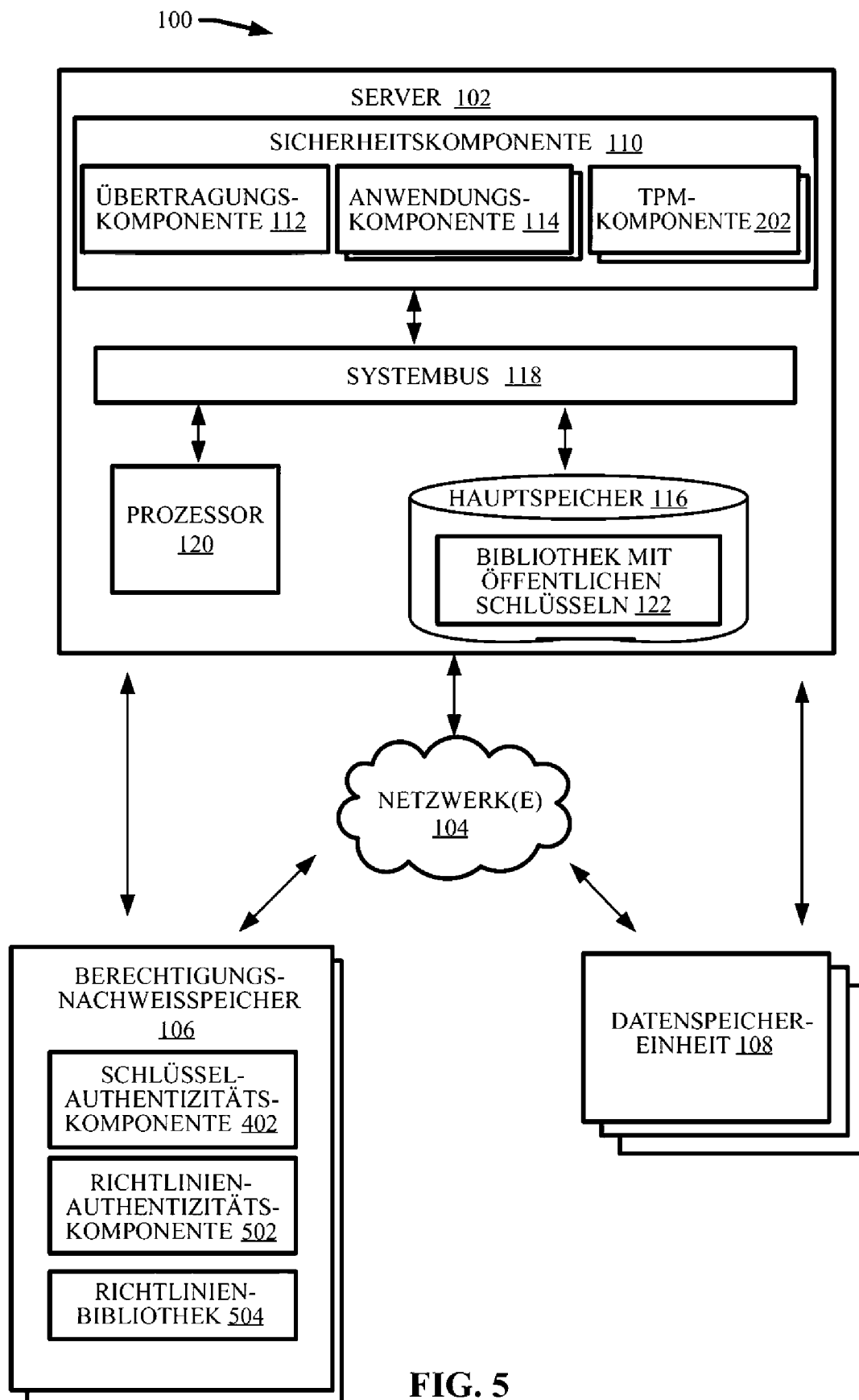


FIG. 4



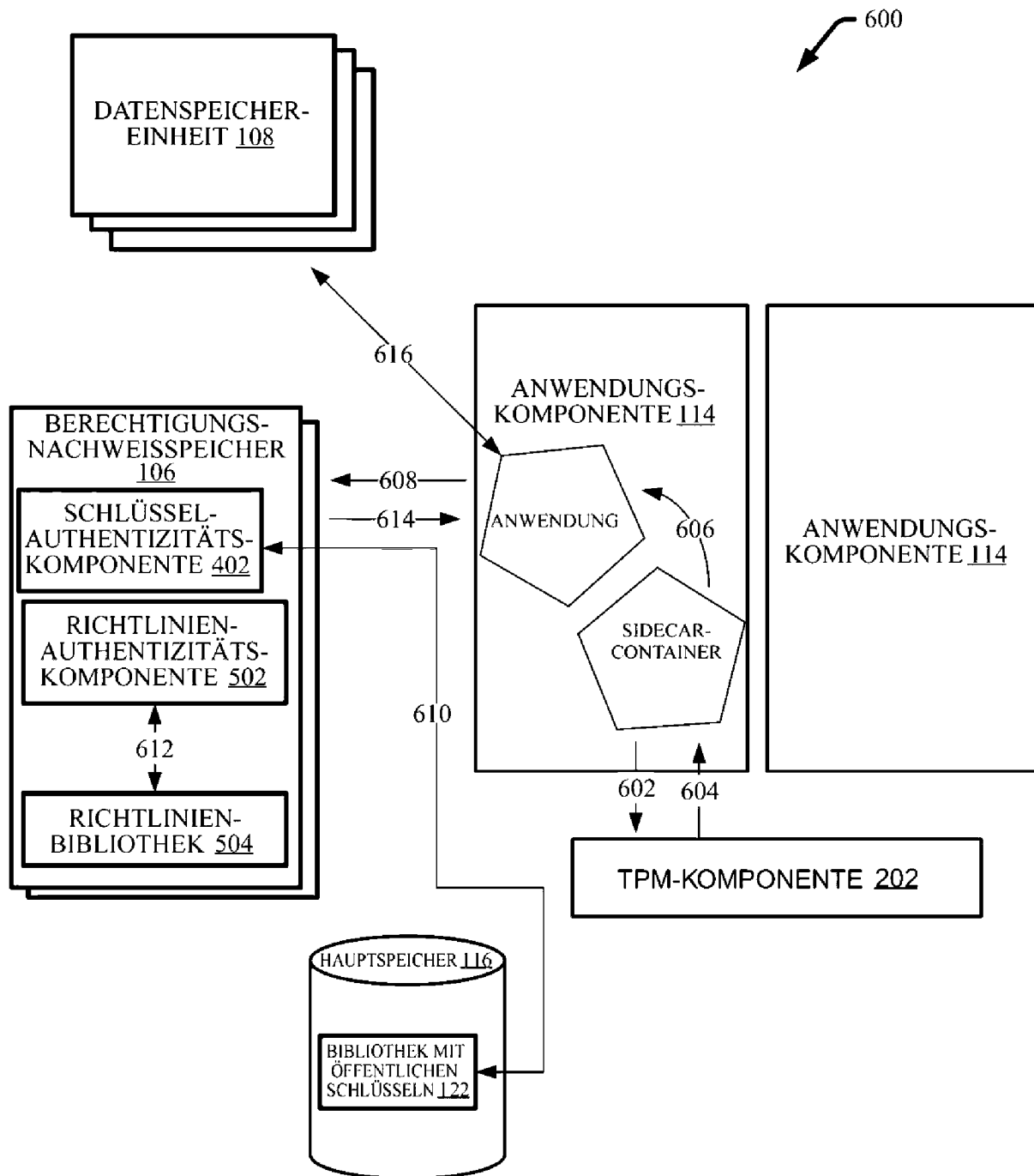


FIG. 6

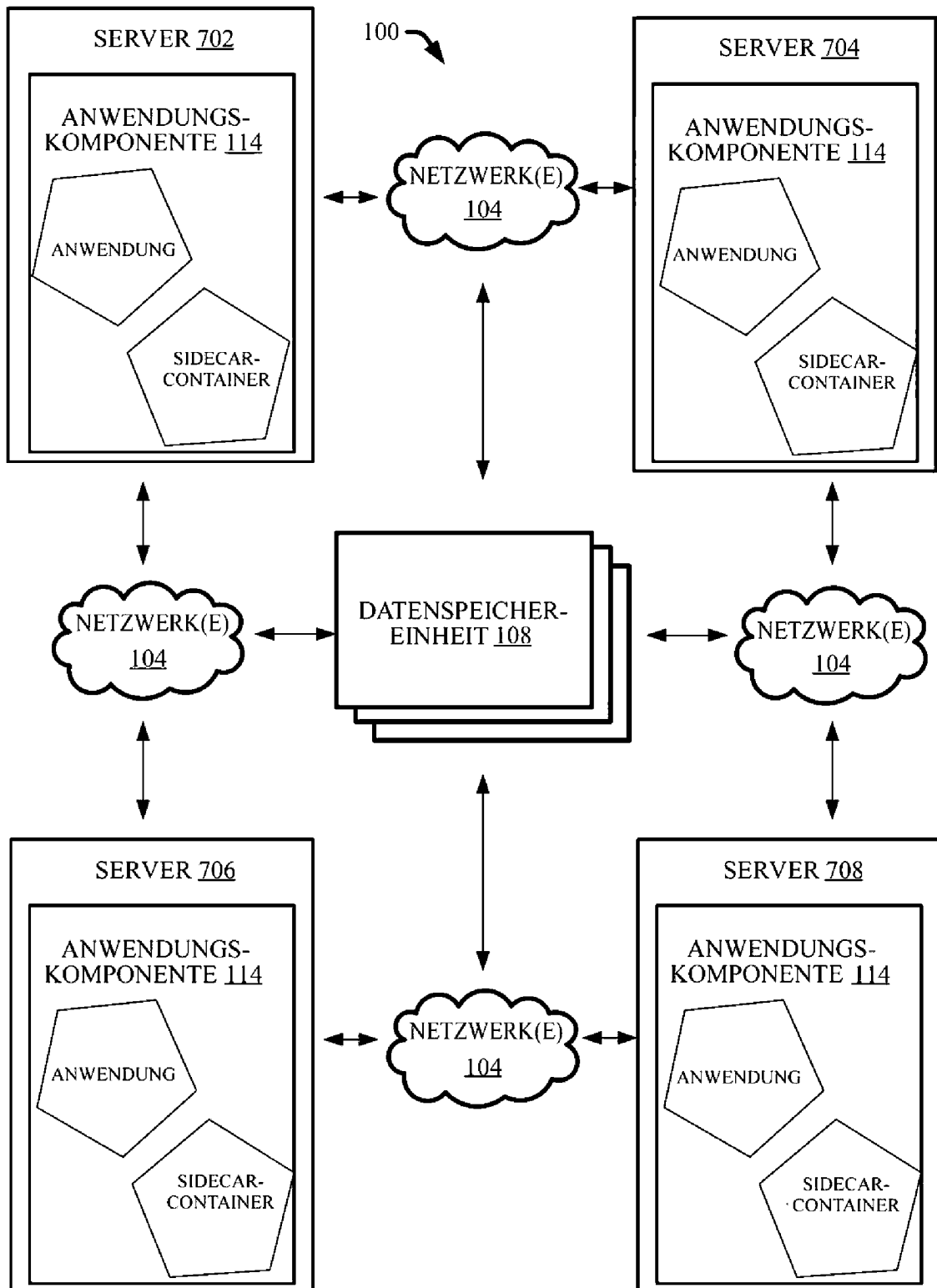
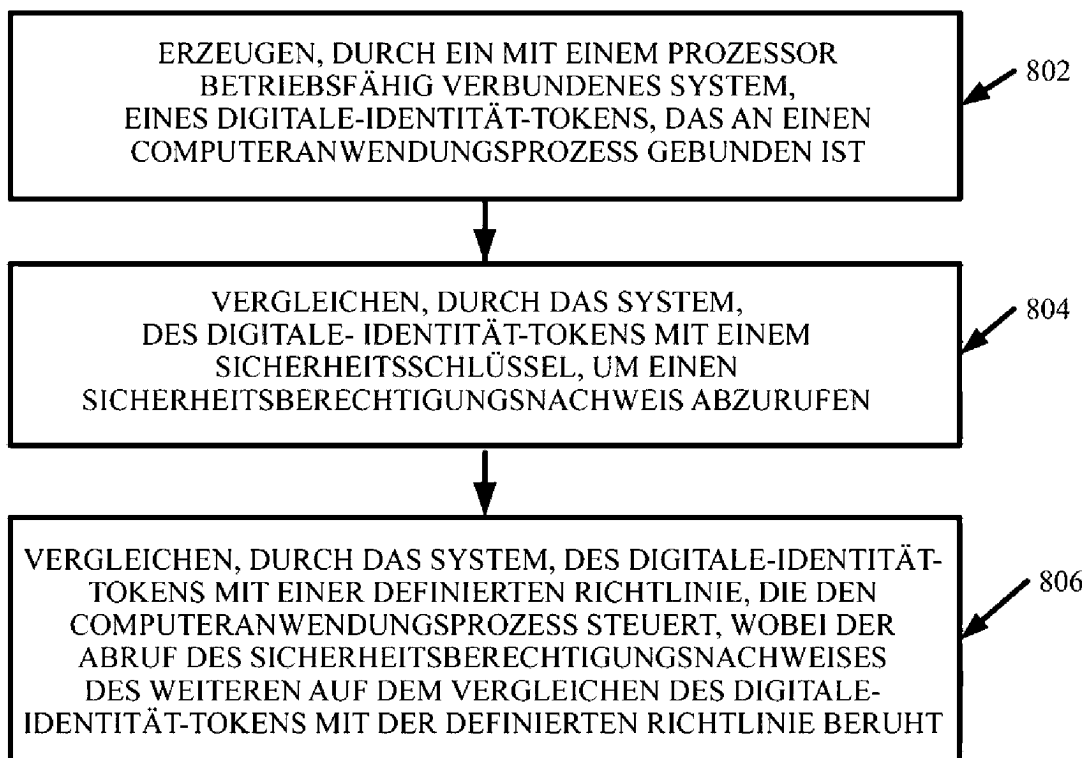


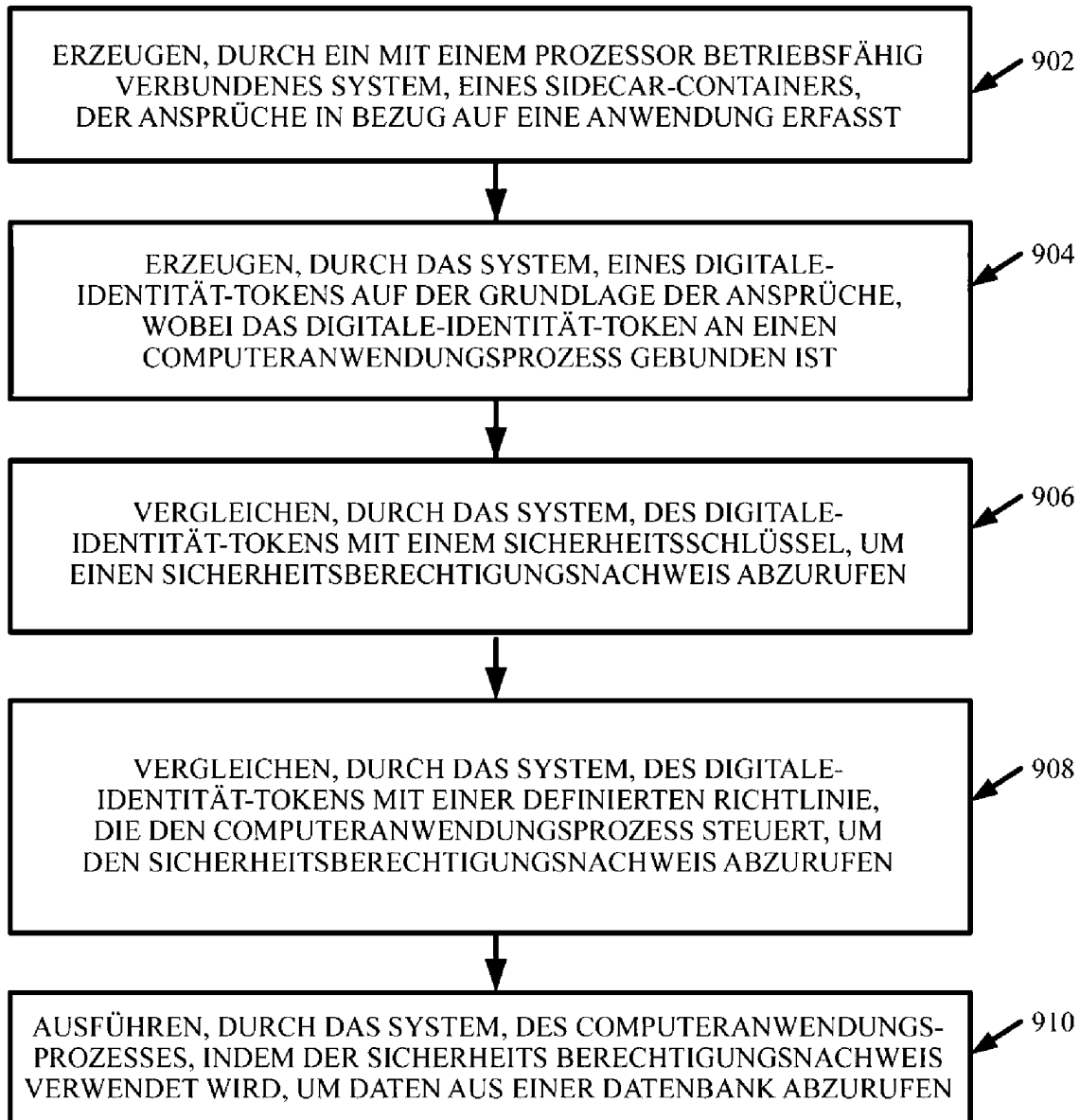
FIG. 7

800 →

FIG. 8



900

FIG. 9

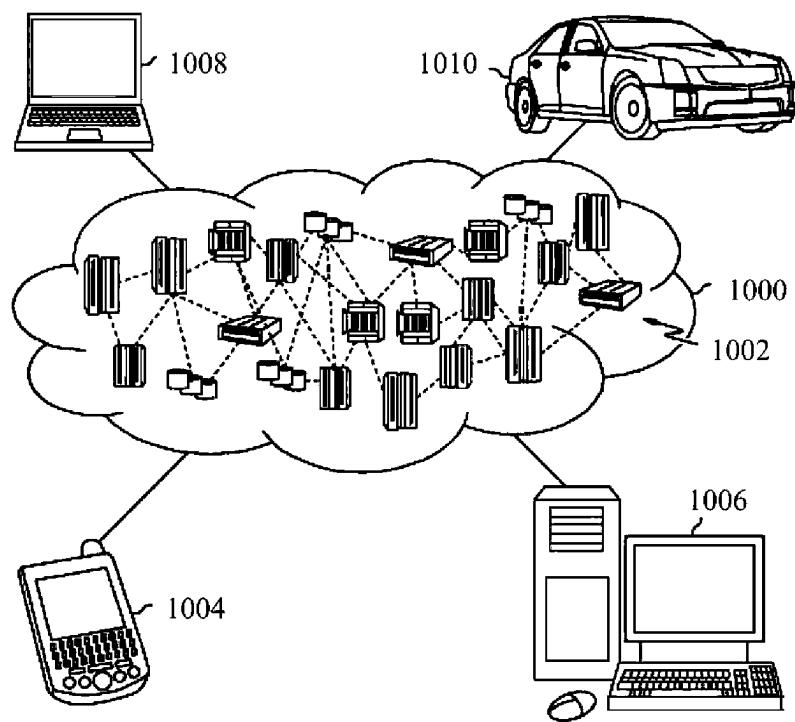


FIG. 10

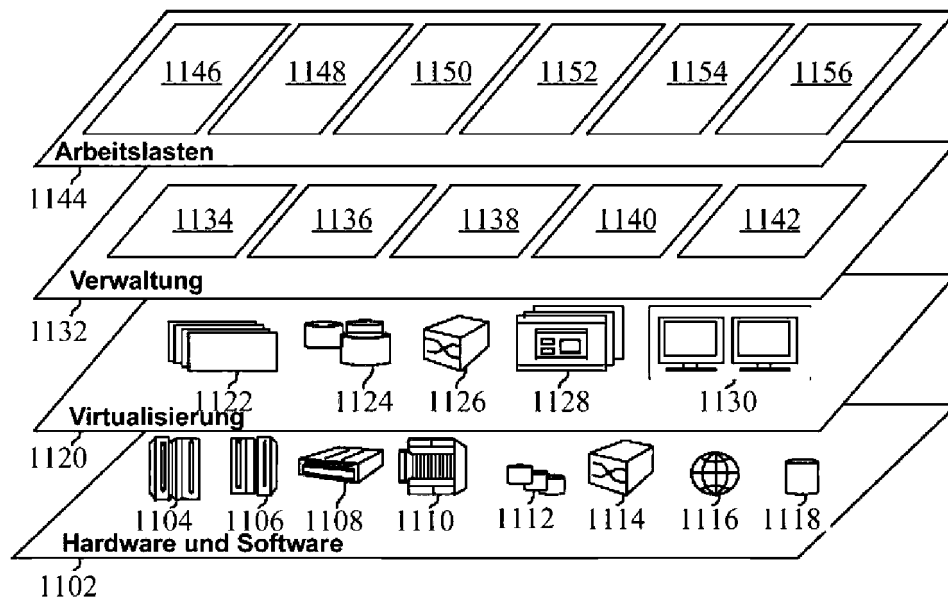
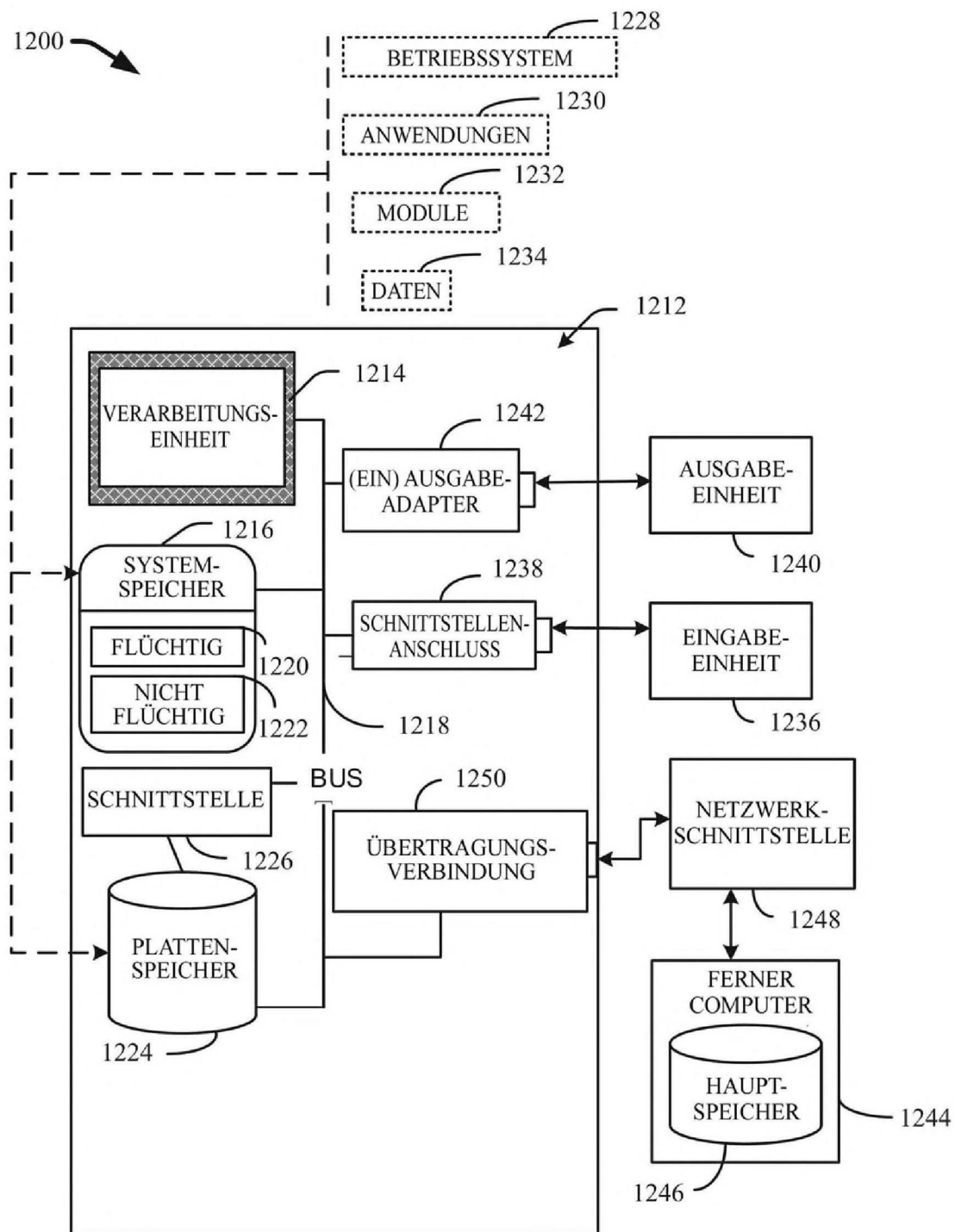


FIG. 11

**FIG. 12**