(19) Deutsches Patent- und Markenamt

(10) **DE 20 2016 107 487 U1** 2017.06.14

(12) # Gebrauchsmusterschrift

(21) Aktenzeichen: **20 2016 107 487.8**
(22) Anmeldetag: **29.12.2016**
(47) Eintragungstag: **04.05.2017**
(45) Bekanntmachungstag im Patentblatt: **14.06.2017**

(51) Int Cl.: ***G06F 21/30*** (2013.01)

(30) Unionspriorität:
62/288,960 **29.01.2016** **US**

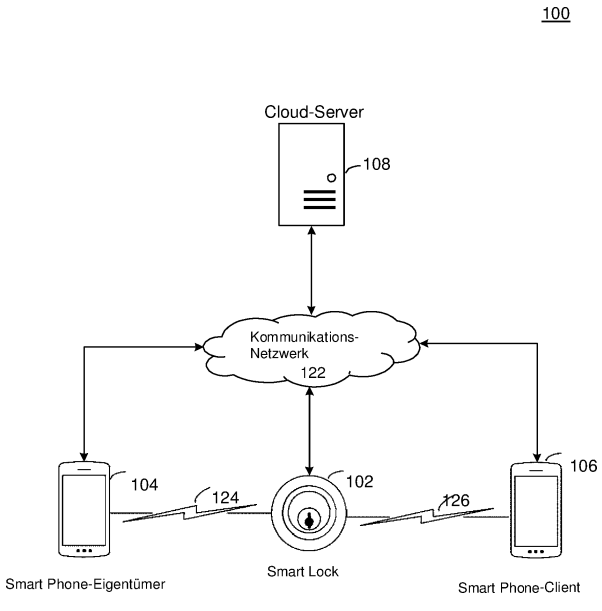
(73) Name und Wohnsitz des Inhabers:
GOOGLE INC., Mountain View, Calif., US

(74) Name und Wohnsitz des Vertreters:
Maikowski & Ninnemann Patentanwälte Partnerschaft mbB, 10707 Berlin, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Authentifizierung eines lokalen Gerätes**

(57) Hauptanspruch: Vorrichtung, umfassend:
mindestens einen Prozessor; und
einen Speicher, der ausführbare Anweisungen speichert, die bei Ausführung durch den mindestens einen Prozessor den mindestens einen Prozessor zum Durchführen der folgenden Schritte veranlassen:
das Erhalten eines Master-Zugrifftokens für ein Ressourcengerät;
das Identifizieren eines einem Client-Gerät zugeordneten Benutzers;
das Bestimmen, dass der Benutzer autorisiert wurde, beschränkten Zugriff auf das Ressourcengerät zu erhalten;
das Erzeugen, in Reaktion auf die Bestimmung, eines auf dem Master-Gerätetoken basierenden lokalen Zugriffstokens, wobei das lokale Zugriffstoken konfiguriert ist, Zugriff auf das Ressourcengerät zu gewähren, ohne dass eine Netzwerkverbindung des Ressourcengerätes erforderlich ist;
das Bereitstellen des lokalen Zugriffstokens für das Ressourcengerät an das Client-Gerät.



Beschreibung

GEBIET

[0001] Diese Beschreibung beschreibt Technologien bezüglich drahtloser Kommunikationen über Niedrigenergie-Netzwerke.

ALLGEMEINER STAND DER TECHNIK

[0002] Geräte mit geringem Energieverbrauch, beispielsweise Smart Locks, intelligente Haushaltsgeräte (z. B. Waschmaschinen, Herde, Kühlschränke, usw.), intelligente Thermostate, und andere Geräte, die zu Fernsteuerung, Fernsensorik und ferngesteuertem Betrieb in der Lage sind, sind in zunehmendem Maße üblich und stellen einen Teil des täglichen Lebens dar. Aufgrund der begrenzten Verarbeitungsfähigkeiten dieser Geräte, sowie Bandbreitenbeschränkungen der Datenübertragung bedingt durch die Niedrigenergie-Netzwerke, mit denen sie betrieben werden (z. B. Bluetooth™-Low-Energy(BLE)-Netzwerke), ist möglich, dass viele Niedrigenergie-Geräte nicht fähig sind, herkömmliche Zugriffskontrollverfahren zu implementieren.

KURZDARSTELLUNG

[0003] Die offenbarten Ausführungsformen beziehen sich auf computergestützte Verfahren, die Niedrigenergie-Geräte, beispielsweise Smart Locks, intelligente Haushaltsgeräte (z. B. Waschmaschinen, Herde, Kühlschränke, usw.), intelligente Thermostate, und andere Geräte, die zu ferngesteuertem Betrieb und Fernsteuerung in der Lage sind, befähigen, Zugriffskontrollentscheidungen an ein oder mehrere zusätzliche Geräte zu delegieren, beispielsweise Computersysteme, die Cloud-Netzwerke unterhalten. Anhand der offenbarten Ausführungsformen kann ein Niedrigenergie-Gerät (z. B. ein Ressourcengerät) ein oder mehrere Master-Tokens erzeugen und lokal speichern, beispielsweise ein Master-Gerätetoken, das anderen Geräten die Verifizierung der Identität des Niedrigenergie-Gerätes ermöglicht, und ein Master-Zugriffstoken, das andere Geräte befähigt, auf das Niedrigenergie-Gerät zuzugreifen. Das Ressourcengerät kann beispielsweise seine Zugriffskontrollentscheidungen an eines der Computersysteme delegieren, indem es sein(e) Master-Token(s) an das Computersystem überträgt. Das Computersystem kann die empfangenen Master-Tokens speichern und zugunsten des Ressourcengerätes eine Zugriffskontrollliste unterhalten zwecks Identifizierung von Geräten, die zum Zugriff auf das Ressourcengerät autorisiert sind, sowie verschiedener dem autorisierten Zugriff seitens des Eigentümers des Ressourcengerätes auferlegter Restriktionen und Beschränkungen.

[0004] Nach dem Empfang einer Anfrage von einem Client-Gerät auf Zugriff auf das Ressourcengerät, kann das Computersystem nach einigen Aspekten nicht nur bestimmen, dass der Eigentümer dem Client-Gerät beschränkten Zugriff auf das Ressourcengerät gewährt hat, sondern ebenfalls, dass der angeforderte Zugriff mit den verschiedenen seitens des Eigentümers des Ressourcengerätes auferlegten Restriktionen und Beschränkungen konsistent ist. Zwecks Ermöglichens des gewährten beschränkten Zugriffs kann das Computersystem ein auf dem Master-Gerätetoken basierendes lokales Gerätetoken, und ein auf dem Master-Zugriffstoken basierendes lokales Zugriffstoken erzeugen oder „prägen“. Das lokale Gerätetoken kann das Client-Gerät befähigen, eine sichere ausgerichtete Verbindung mit dem Ressourcengerät herzustellen, z. B. über eine direkte drahtlose Verbindung zwischen den Geräten, beispielsweise ein Niedrigenergie-BLE-Netzwerk, und das lokale Zugriffstoken kann ein „kurzlebiges“ Token sein, welches die verschiedenen auferlegten Restriktionen und Beschränkungen spezifiziert. Das Client-Gerät kann diese lokalen Token dem Ressourcengerät über ein Niedrigenergie-Netzwerk bereitstellen, sowie in Übereinstimmung mit den auferlegten Restriktionen und Beschränkungen über den Zugriff verhandeln, ohne mit dem Computergerät oder Netzwerkzugang zu kommunizieren.

[0005] In einem allgemeinen Aspekt beinhaltet ein computergestütztes Verfahren: Erhalten eines Master-Zugriffstokens für ein Ressourcengerät von einem oder mehreren Prozessoren einer Vorrichtung; Identifizieren, durch den einen oder die mehreren Prozessoren, eines einem Client-Gerät zugeordneten Benutzers; und Bestimmen, durch den einen oder die mehreren Prozessoren, dass der Benutzer autorisiert wurde, beschränkten Zugriff auf das Ressourcengerät zu erhalten. Als Reaktion auf die Bestimmung kann das Verfahren durch den einen oder die mehreren Prozessoren ein auf dem Master-Gerätetoken basierendes lokales Zugriffstoken erzeugen. In einigen Aspekten kann das lokale Zugriffstoken konfiguriert sein, Zugriff auf das Ressourcengerät zu gewähren, ohne dass eine Netzwerkverbindung des Ressourcengerätes erforderlich ist. Das Verfahren beinhaltet ebenfalls das Bereitstellen, durch den einen oder die mehreren Prozessoren, des lokalen Zugriffstokens für das Ressourcengerät an das Client-Gerät. Das Ressourcengerät kann ein Niedrigenergie-Ressourcengerät sein.

[0006] In einigen Implementierungen können die offenbarten Verfahren das Bestimmen beinhalten, dass der Benutzer mindestens entweder von einem Eigentümer des Ressourcengerätes oder einer zur Zugriffskontrolle des Ressourcengerätes befähigten Instanz autorisiert wurde, beschränkten Zugriff auf das Ressourcengerät zu erhalten.

[0007] In einigen Implementierungen können die offenbarten Verfahren das Empfangen einer Anfrage von einem Client-Gerät, beschränkten Zugriff auf das Ressourcengerät zu erhalten, und, in Reaktion auf die Anfrage, das Bereitstellen des lokalen Zugriffstokens für das Ressourcengerät an das Client-Gerät, beinhalten. In gewissen Aspekten kann die Anfrage mindestens eine Kennung des Benutzers oder eine Kennung des Client-Gerätes beinhalten. Das lokale Zugriffstoken für das Ressourcengerät kann dem Client-Gerät in Reaktion auf die Anfrage bereitgestellt werden.

[0008] In einigen Implementierungen können die offenbarten Verfahren das Identifizieren des Client-Gerätes, basierend auf mindestens einem Teil der empfangenen Anfrage, das Bestimmen, dass das Client-Gerät autorisiert wurde, beschränkten Zugriff auf das Ressourcengerät zu erhalten, und das Erzeugen des lokalen Zugriffstokens in Reaktion auf die Bestimmung, dass das Client-Gerät autorisiert wurde, beschränkten Zugriff zu erhalten, beinhalten.

[0009] In einigen Implementierungen können die offenbarten Verfahren das Erhalten einer Zugriffskontrollliste für das Ressourcengerät beinhalten. In einigen Aspekten kann die Zugriffskontrollliste einen oder mehrere Benutzer identifizieren, die autorisiert sind, entsprechende beschränkte Zugriffe auf das Ressourcengerät zu erhalten.

[0010] In einigen Implementierungen ist die Vorrichtung konfiguriert, die Zugriffskontrollliste in einem lokalen Speicher zu speichern.

[0011] In einigen Implementierungen können die offenbarten Verfahren das auf der Zugriffskontrollliste basierende Bestimmen, dass der eine oder die mehreren autorisierten Benutzer den Benutzer beinhalten, und, in Reaktion auf die Bestimmung, dass der eine oder die mehreren autorisierten Benutzer den Benutzer beinhalten, das Festlegen, dass der Benutzer des Client-Gerätes autorisiert wurde, beschränkten Zugriff zu erhalten, beinhalten.

[0012] In einigen Implementierungen können die offenbarten Verfahren das Empfangen von Zugriffskontrolldaten von einem dem Eigentümer des Ressourcengerätes zugeordneten Eigentümergerät, und das Modifizieren von mindestens einem Teil der Zugriffskontrollliste zwecks Identifizierens des Benutzers des Client-Gerätes als autorisierten Benutzer, beinhalten. In einigen Aspekten können die Zugriffskontrolldaten den Benutzer autorisieren, beschränkten Zugriff auf das Ressourcengerät zu erhalten.

[0013] In einigen Implementierungen können die Zugriffskontrolldaten Zugriffsparameter beinhalten, und die Zugriffsparameter können einen Umfang des dem Benutzer gewährten beschränkten Zugriffs festlegen. Die offenbarten Verfahren können ebenfalls das Modifizieren von mindestens einem Teil der Zugriffskontrollliste zwecks Einbeziehens der Zugriffsparameter beinhalten.

[0014] In einigen Implementierungen können die Zugriffsparameter mindestens, alternativ oder kumulativ, eine dem Benutzer zugeordnete Rolle, eine zeitliche Restriktion, eine Restriktion der Zugriffsart, eine Restriktion des Offline-Zugriffs oder eine Restriktion der Fähigkeit des Client-Gerätes zur Erzeugung von Tokens, beinhalten, und die Zugriffskontrollliste kann den einen oder die mehreren dem Benutzer zugeordneten Zugriffsparameter identifizieren.

[0015] In einigen Implementierungen kann das lokale Zugriffstoken ein Macaroon beinhalten, das einen oder mehrere Schutzvorbehalte und einen entsprechenden Schlüssel umfasst; die offenbarten Verfahren können, basierend auf der Zugriffskontrollliste, dem Benutzer zugeordnete Zugriffsparameter identifizieren, einen Ablaufzeitpunkt für das lokale Zugriffstoken festlegen, und Vorgänge durchführen, die den Ablaufzeitpunkt und die identifizierten Zugriffsparameter in den einen oder die mehreren Schutzvorbehalte des lokalen Zugriffstokens einbeziehen.

[0016] In einigen Implementierungen können die offenbarten Verfahren das Modifizieren von mindestens einem Teil der Zugriffskontrollliste zwecks Einbeziehens des für das lokale Zugriffstoken des Benutzers festgelegten Ablaufzeitpunktes beinhalten.

[0017] In einigen Implementierungen kann das lokale Zugriffstoken Daten zum Identifizieren mindestens des Benutzers oder des Client-Gerätes beinhalten, und das offenbarte Verfahren kann die Anwendung einer digitalen Signatur auf das lokale Zugriffstoken beinhalten.

[0018] In einigen Implementierungen kann das lokale Zugriffstoken beispielsweise ein Macaroon beinhalten, das einen oder mehrere Schutzvorbehalte und einen entsprechenden Schlüssel beinhaltet, wobei der entsprechende Schlüssel die angewandte digitale Signatur beinhalten kann, und das offenbarte Verfahren kann das Erzeugen der digitalen Signatur beinhalten, basierend auf einer Anwendung eines MAC-Algorithmus auf mindestens einen Teil des einen oder der mehreren Schutzvorbehalte.

[0019] In einigen Implementierungen können der eine oder die mehreren Schutzvorbehalte mindestens, alternativ oder kumulativ, ein Ablaufdatum des Tokens, eine dem Benutzer zugeordnete Rolle oder die Daten zum Identifizieren mindestens des Benutzers oder des Client-Gerätes beinhalten.

[0020] In einigen Implementierungen kann das lokale Zugriffstoken ein digitales Zertifikat beinhalten.

[0021] In einigen Implementierungen können die offenbarten Verfahren das Empfangen eines Master-Zugriffstokens vom Ressourcengerät, und das Erzeugen des lokalen Zugriffstokens, basierend auf mindestens einem Teil des Master-Zugriffstokens, beinhalten.

[0022] In einigen Implementierungen kann das Master-Clienttoken beispielsweise ein erstes Macaroon mit einem oder mehreren Schutzvorbehalten und einem entsprechenden ersten Schlüssel beinhalten, das lokale Zugriffstoken kann ein zweites Macaroon, welches einen oder mehrere Schutzvorbehalte und einen entsprechenden zweiten Schlüssel enthält, beinhalten.

[0023] In einigen Implementierungen können die zweiten Schutzvorbehalte die ersten Schutzvorbehalte, ein Ablaufdatum des lokalen Zugriffstokens, und einen oder mehrere dem beschränkten Zugriff des Benutzers zugeordnete Zugriffsparameter beinhalten, welche mindestens, alternativ oder kumulativ, eine dem Benutzer zugewiesene Rolle, eine zeitliche Restriktion, eine Restriktion der Zugriffsart, eine Restriktion des Offline-Zugriffs oder eine Restriktion der Fähigkeit des Client-Gerätes zur Erzeugung von Tokens, beinhalten können.

[0024] In einigen Implementierungen können die offenbarten Verfahren das Empfangen eines Master-Gerätetokens vom Ressourcengerät beinhalten, das Master-Gerätetoken das Client-Gerät befähigend, die Identität des Ressourcengerätes zu verifizieren, und, in Reaktion auf die Bestimmung, das Erzeugen eines lokalen Gerätetokens, basierend auf mindestens einem Teil des Master-Gerätetokens, und Bereitstellen des lokalen Gerätetokens an das Client-Gerät.

[0025] In einem weiteren allgemeinen Aspekt beinhaltet ein computerimplementiertes Verfahren: Herstellen, durch einen oder mehrere Prozessoren eines Ressourcengerätes, einer sicheren drahtlosen Verbindung mit einem Client-Gerät; Empfangen, durch den einen oder die mehreren Prozessoren, von Tokendaten, abgeleitet vom Zugriffstoken des Client-Gerätes, und einer Zugriffsanfrage auf das Ressourcengerät vom Client-Gerät; Bestimmen, durch den einen oder die mehreren Prozessoren, ohne über ein Netzwerk zu kommunizieren, dass die empfangenen Tokendaten abgeleitet sind von einem gültigen Token, welches den Zugriff auf das Ressourcengerät autorisiert; und Bestimmen, durch den einen oder die mehreren Prozessoren, ohne über ein Netzwerk zu kommunizieren, dass das Zugriffstoken eine Zugriffsstufe autorisiert, welche ausreichend ist, den vom Client-Gerät angeforderten Zugriff einzuräumen. Als Reaktion auf das Bestimmen, dass die empfangenen Tokendaten von einem gültigen Token abgeleitet sind, und das Bestimmen, dass das Zugriffstoken eine Zugriffsstufe autorisiert, welche ausreichend ist, den vom elektronischen Gerät angeforderten Zugriff einzuräumen, kann das Verfahren ebenfalls das Einräumen, durch den einen oder die mehreren Prozessoren, des vom Client-Gerät angeforderten Zugriffs auf das Ressourcengerät beinhalten.

[0026] In einigen Implementierungen kann die sichere drahtlose Verbindung eine direkte drahtlose Verbindung zwischen dem Client-Gerät und dem Ressourcengerät beinhalten.

[0027] In einigen Implementierungen kann die direkte drahtlose Verbindung eine Bluetooth-Low-Energy (BLE)-Verbindung beinhalten.

[0028] In einigen Implementierungen können die offenbarten Verfahren ebenfalls das Empfangen von Schutzvorbehaltsdaten und Zufallsdaten vom Client-Gerät beinhalten, wobei die Schutzvorbehaltsdaten durch das Client-Gerät von einem lokalen Gerätetoken extrahiert wurden, das Berechnen eines Schlüsselwertes, basierend auf mindestens einem Teil der empfangenen Schutzvorbehaltsdaten und Zufallsdaten, das Übertragen des berechneten Schlüsselwertes an das Client-Gerät, und das Herstellen der sicheren drahtlosen Verbindung mit dem Client-Gerät, basierend auf einer Übereinstimmung zwischen dem berechneten Schlüsselwert und einem zusätzlichen, durch das Client-Gerät basierend auf dem lokalen Gerätetoken berechneten Schlüsselwert.

[0029] In einigen Implementierungen können die offenbarten Verfahren das Festlegen des berechneten Schlüssels als Sitzungsschlüssel beinhalten.

[0030] In einigen Implementierungen können die Schutzvorbehaltsdaten und die Zufallsdaten unter Verwendung eines gemeinsamen symmetrischen Schlüssels verschlüsselt werden, und die offenbarten Verfahren beinhalten das Entschlüsseln der empfangenen Schutzvorbehaltsdaten und Zufallsdaten, das Verschlüsseln des berechneten Schlüsselwertes unter Verwendung des gemeinsamen symmetrischen Schlüssels, und das Übertragen des verschlüsselten Schlüsselwertes an das Client-Gerät.

[0031] In einigen Implementierungen kann das Ressourcengerät Zugriffskontrollentscheidungen an mindestens, alternativ oder kumulativ, ein einem Cloud-Server zugeordnetes Computersystem, einen Authentifizierungsdienst durch Dritte oder an ein Gerät eines Eigentümers des Ressourcengerätes delegieren, und mindestens das Computersystem, der Authentifizierungsdienst durch Dritte oder das Eigentümergerät erzeugten das Zugriffstoken und stellten das Zugriffstoken dem Client-Gerät bereit.

[0032] In einigen Implementierungen können die offenbarten Verfahren das Durchführen der Schritte des Festlegens, des Empfangens und des Bereitstel-

lens, ohne hierbei über das Netzwerk zu kommunizieren, beinhalten.

[0033] In einigen Implementierungen umfasst das Zugriffstoken ein Macaroon mit einem oder mehreren Schutzvorbehalten und einem entsprechenden Schlüssel.

[0034] In einigen Implementierungen kann der Schritt des Bestimmens, dass die empfangenen Tokendaten von einem gültigen Token abgeleitet sind, ohne über ein Netzwerk zu kommunizieren, ebenfalls das Extrahieren des einen oder der mehreren Schutzvorbehalte aus den empfangenen Tokendaten, das Berechnen einer Kopie der empfangenen Tokendaten basierend auf den extrahierten Schutzvorbehalten und einem vom Ressourcengerät unterhaltenen Master-Zugriffstoken, das Bestimmen, dass die empfangenen Tokendaten der berechneten Kopie entsprechen, und das Festlegen, dass die empfangenen Tokendaten von einem gültigen Token abgeleitet sind, wenn die empfangenen Tokendaten der berechneten Kopie entsprechen, beinhalten.

[0035] In einigen Implementierungen kann der Schritt des Bestimmens, dass die empfangenen Tokendaten von einem gültigen Token abgeleitet sind, ohne über ein Netzwerk zu kommunizieren, des Weiteren das Identifizieren einer Zugriffskette für das empfangene Zugriffstoken, basierend auf mindestens einem Teil der Schutzvorbehaltextrakte, und das Verifizieren der Zugriffskette für das empfangene Token, beinhalten.

[0036] In einigen Implementierungen können der eine oder die mehreren Schutzvorbehalte ein Ablaufdatum des Zugriffstokens, eine dem Client-Gerät durch den Eigentümer des Ressourcengerätes zugewiesene Rolle, und ein oder mehrere Zugriffsparameter beinhalten, wobei die Zugriffsparameter mindestens, alternativ oder kumulativ, eine zeitliche Restriktion, eine Restriktion einer Zugriffsart, eine Restriktion des Offline-Zugriffs oder eine Restriktion der Fähigkeit des Client-Gerätes zur Erzeugung von Tokens umfassen, und die Zugriffsanfrage an das Ressourcengerät identifiziert eine oder mehrere der vom Ressourcengerät angeforderten Funktionen.

[0037] In einigen Implementierungen kann der Schritt des Bestimmens, dass das Zugriffstoken die ausreichende Zugriffsstufe autorisiert, das Bestimmen, basierend auf dem Ablaufdatum, dass das Zugriffstoken nicht abgelaufen ist, das Identifizieren einer vom Client-Gerät erforderten Rolle zwecks Zugriffs auf die angeforderten Funktionen des Ressourcengerätes, das Bestimmen, dass die erforderte Rolle mit der zugewiesenen Rolle konsistent ist, das Bestimmen, dass die eine oder die mehreren angeforderten Funktionen mit dem einen oder den mehreren Zugriffsparametern konsistent sind, und, in Reaktion auf die Bestimmungen, dass (i) das Zugriffstoken nicht abgelaufen ist, (ii) die erforderte Rolle konsistent mit der zugewiesenen Rolle ist und (iii) eine oder mehrere angeforderte Funktionen mit dem einen oder den mehreren Zugriffsparametern konsistent sind, das Festlegen, dass das Zugriffstoken eine Zugriffsstufe autorisiert, welche ausreichend ist, den angeforderten Zugriff einzuräumen, beinhalten.

[0038] In einigen Implementierungen hat das Ressourcengerät die Zugriffskontrollentscheidungen mindestens an, alternativ oder kumulativ, ein einem Cloud-Server zugeordnetes Computersystem, einen Authentifizierungsdienst durch Dritte oder an ein Gerät des Eigentümers des Ressourcengerätes delegiert; und mindestens das Computersystem, der Authentifizierungsdienst durch Dritte oder das Eigentümergerät erzeugten das Zugriffstoken und stellten das Zugriffstoken dem Client-Gerät bereit.

[0039] In anderen Ausführungsformen können entsprechende Systeme, Geräte und Computerprogramme so konfiguriert sein, dass sie die Aktionen der auf den Computerspeichergeräten kodierten Verfahren ausführen. Ein Gerät mit einem oder mehreren Prozessoren kann demgemäß konfiguriert werden anhand von Software, Firmware oder einer Kombination dieser, welche, falls auf dem Gerät installiert, bei Betrieb des Gerätes die Durchführung der Aktionen veranlassen. Ein oder mehrere Computerprogramme können demgemäß konfiguriert werden anhand von Befehlen, die, bei Ausführung durch das Gerät, die Durchführung der Aktionen veranlassen.

[0040] Implementierungen der hierin offenbarten Technologie können einen oder mehrere der nachfolgenden Vorteile bereitstellen. Ein Gerät kann Zugriffskontrollentscheidungen an ein Remote-System delegieren. Dies ermöglicht einem Gerät anspruchsvolle Sicherheits- und Zugriffskontrolle, bei gleichzeitiger Senkung des Energiebedarfs, der Verarbeitungsbedürfnisse und des Netzwerkbandbreitenbedarfs des Gerätes. Das System kann eine optimierte Zugriffskontrolle ermöglichen, welche erlaubt, spezifische Erlaubnisse und Restriktionen zu gewähren. Zusätzlich kann das System autorisierten Benutzern ermöglichen, beschränkten Zugriff an Dritte zu delegieren, welcher unterschiedlichen Restriktionen und Beschränkungen unterliegen kann. Obwohl ein Remote-System Entscheidungen im Hinblick auf Erlaubnisgewährungen für Benutzer und Geräte trifft, ist das Sicherheitsschema zusätzlich dementsprechend eingerichtet, dass Kommunikation zwischen dem Remote-System und dem gesicherten Gerät nicht erforderlich ist. Dies bedeutet, dass das gesicherte System bei Eingang einer Zugriffsanfrage bestimmen kann, ob der Anfragende autorisiert ist, ohne dass hierbei eine nachfolgende Kommunikation mit dem Remote-System erfolgt. Auf diese Weise ist das Authentifizierungsschema selbst bei Nichtvorliegen ei-

ner Netzwerkverbindung effektiv. Die Fähigkeit, eine Authentifizierung ohne Vorliegen einer Netzwerkverbindung durchzuführen, kann ebenfalls den Energiebedarf senken, was für kleine oder batteriebetriebene Geräte besonders vorteilhaft ist.

[0041] Die Details einer oder mehrerer Ausführungsformen des Gegenstands, die in dieser Spezifikation beschrieben werden, sind in den zugehörigen Zeichnungen und der nachfolgenden Beschreibung dargelegt. Weitere potentielle Merkmale, Aspekte und Vorteile des Gegenstands werden anhand der Beschreibung, der Zeichnungen und der Patentansprüche offensichtlich.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0042] **Fig.** 1 ist ein Diagramm eines exemplarischen Computersystems.

[0043] **Fig.** 2 ist ein Diagramm, das einen exemplarischen Austausch von Daten veranschaulicht, welcher eine Delegierung von Zugriffskontrollentscheidungen zwischen Geräten ermöglicht.

[0044] **Fig.** 3 ist ein Flussdiagramm eines exemplarischen Verfahrens zur Delegierung von Zugriffskontrollentscheidungen von einem Ressourcengerät an ein oder mehrere Computergeräte.

[0045] **Fig.** 4 ist ein Diagramm, das einen exemplarischen Austausch von Daten veranschaulicht, welcher einen tokenbasierten Zugriff eines Client-Gerätes auf ein Ressourcengerät ermöglicht.

[0046] **Fig.** 5 ist ein Flussdiagramm eines exemplarischen Verfahrens zur Zugriffsgewährung auf ein Ressourcengerät.

[0047] **Fig.** 6 ist ein Blockdiagramm von Computergeräten, die zur Implementierung von in diesem Dokument beschriebenen Systemen und Verfahren verwendet werden können.

[0048] In den unterschiedlichen Zeichnungen werden gleiche Bezugszeichen und Bezeichnungen für gleiche Elemente verwendet.

DETAILLIERTE BESCHREIBUNG

[0049] **Fig.** 1 veranschaulicht ein exemplarisches System **100** zur Delegierung von Zugriffskontrollentscheidungen von einem Ressourcengerät an ein oder mehrere Geräte und/oder Computersysteme und zum Bereitstellen von gerätespezifischen Tokens, welche Zugriff auf das Ressourcengerät gewähren, ohne eines Netzwerkzugriffs zu bedürfen. Zum Beispiel kann System **100** ein Ressourcengerät **102**, ein Eigentümergerät **104**, ein Client-Gerät **106**, ein Computersystem **108** und ein Kommunikationsnetzwerk **122**, welches geeignet ist, eines oder mehrere der Komponenten des Systems **100** miteinander zu verbinden, beinhalten.

[0050] In gewissen Aspekten kann System **100** des Weiteren ebenfalls ein oder mehrere lokale drahtlose Kommunikationsnetzwerke (z. B. drahtlose Peer-to-Peer-Netzwerke, usw.) beinhalten, welche geeignet sind, eine oder mehrere Komponenten des Systems **100** direkt zu verbinden. In **Fig.** 1 kann System **100** beispielsweise ein lokales drahtloses Kommunikationsnetzwerk **124**, welches Ressourcengerät **102** und Eigentümergerät **104** direkt verbindet, beinhalten, und zusätzlich oder alternativ ein lokales drahtloses Kommunikationsnetzwerk **126**, welches Ressourcengerät **102** und Client-Gerät **106** direkt verbindet. Die offenbarten Ausführungsformen sind jedoch nicht auf diese exemplarischen lokalen drahtlosen Kommunikationsnetzwerke beschränkt, und in anderen Aspekten kann System **100** beliebige zusätzliche oder eine unterschiedliche Anzahl an für die Komponenten des Systems **100** geeigneten lokalen drahtlosen Kommunikationsnetzwerken beinhalten.

[0051] Im Allgemeinen kann ein Ressourcengerät **102** ein Geheimnis erzeugen oder unterhalten, z. B. einen Ursprungsschlüssel, der lediglich dem Ressourcengerät **102** bekannt ist. Das Ressourcengerät **102** erzeugt einen Master-Schlüssel oder Master-Token, der/das sich vom Ursprungsschlüssel ableitet. Das Ressourcengerät **102** sendet sodann das Master-Token an eine vertrauenswürdige Instanz, um die Zugriffsverwaltungsrechte an die vertrauenswürdige Instanz zu delegieren. In einigen Implementierungen ist die vertrauenswürdige Instanz ein über das Internet zugängliches Remote-Serversystem, beispielsweise Computersystem **108**. Nach Abschluss der Delegierung ist die vertrauenswürdige Instanz in der Lage, eine beliebige Anzahl an Zugriffsschlüsseln oder Zugriffstokens zwecks Zugriffs auf das Ressourcengerät **102** herzustellen, ohne das Ressourcengerät **102** zu kontaktieren. Das Ressourcengerät **102** kann zum Zeitpunkt des Erzeugens neuer Zugriffstokens sogar abgeschaltet oder offline sein.

[0052] Später, wenn eine andere Partei Zugriff auf das Ressourcengerät **102** anfordert, präsentiert die anfordernde Partei ein von der vertrauenswürdigen Instanz erhaltenes Zugriffstoken. Anhand des Zugriffstokens ist das Ressourcengerät **102** in der Lage, zu verifizieren, dass (i) das Zugriffstoken vom Ursprungsschlüssel des Gerätes abgeleitet wurde, und (ii) das Zugriffstoken von der zuständigen Zugriffsverwaltungsinstanz ausgegeben wurde. Zusätzlich ist das Ressourcengerät **102** in der Lage, der das Zugriffstoken präsentierenden Partei gewährte Zugriffsrechte, Privilegien und Restriktionen zu bestimmen. Dies ermöglicht dem Ressourcengerät **102**, basierend auf dem Zugriffstoken und ohne Kommunikation mit der vertrauenswürdigen Instanz, an wel-

che die Zugriffsverwaltungsrechte delegiert wurden, zu bestimmen, ob Zugriff eingeräumt wird und welcher Zugriffsumfang einzuräumen ist.

[0053] In einigen Aspekten kann Ressourcengerät **102** ein Niedrigenergie-Gerät (z. B. ein von einer Niedrigenergie-Mikrocontroller-Einheit (MCU) und/oder einem System-on-Chip (SoC) betriebenes) beinhalten, welches konfiguriert sein kann, Kommunikationen mit Komponenten des Systems **100** über Kommunikationsnetzwerk **122** herzustellen, und zusätzlich oder alternativ direkte Verbindungen über lokale drahtlose Kommunikationsnetzwerke **124** und **126** herzustellen. Das Niedrigenergie-Gerät kann beispielsweise ein batteriebetriebenes Gerät oder ein in anderer Form energiebeschränktes Gerät sein. Beispielhaft kann Ressourcengerät **122** in nicht einschränkender Form einen Satz drahtloser Lautsprecher, einen drahtlosen Drucker oder ein anderes elektronisches Gerät, ein Smart Lock, eine intelligente Anwendung (z. B. einen Kühlschrank, Herd und/oder eine Waschmaschine), ein intelligentes Thermostat oder einen anderen Sensor, und ein beliebiges zusätzliches oder anderes Gerät (z. B. ein Internet-der-Dinge (IOT) verbundenes Gerät), das, abgesehen von anderen Dingen, geeignet ist zur Herstellung von direkten Kommunikationen mit Computersystem **108** über Netzwerk **122**, direkten Kommunikationen mit Eigentümergerät **104** über das lokale drahtlose Kommunikationsnetzwerk **124**, und zusätzlich oder alternativ direkten Kommunikationen mit Client-Gerät **106** über das lokale drahtlose Kommunikationsnetzwerk **126**, beinhalten. In einigen Implementierungen kann Ressourcengerät **102** als „Server"-Gerät gemäß den Weave- oder µWeave-Protokollen dienen.

[0054] Eigentümergerät **104** und Client-Gerät **106** können in nicht einschränkender Form ein Mobiltelefon, ein Smartphone, einen Tablet-Computer, einen Desktop-Computer, einen Laptop-Computer, einen Tablet-Computer, einen tragbaren Computer, einen Music-Player, einen E-Book-Reader, ein Navigationssystem, oder jedes andere geeignete Computergerät, das geeignet ist zur Herstellung von Kommunikationen mit Komponenten des Systems **100** über Kommunikationsnetzwerk **122**, das lokale drahtlose Kommunikationsnetzwerk **124** und/oder das lokale drahtlose Kommunikationsnetzwerk **126**, beinhalten. Zusätzlich kann Computersystem **108** ein oder mehrere Computersysteme beinhalten, konfiguriert zum Ausführen von auf einem Speicher gespeicherten Softwarebefehlen, ein oder mehrere mit den offenbarten Ausführungsformen konsistente Verfahren durchführend, und zur Kommunikation mit einem oder mehreren Komponenten des Systems **100** über Netzwerk **122**.

[0055] Des Weiteren können die lokalen Netzwerke **124** und/oder **126** in gewissen Aspekten ein drahtloses Personal Area Network (PAN), beispielsweise ein Bluetooth™-Low-Energy(BLE)-Netzwerk, beinhalten. In anderen Aspekten, und konsistent mit den offenbarten Ausführungsformen, können Netzwerk **122** und zusätzlich oder alternativ ein oder mehrere der lokalen Netzwerke **124** und **126** in nicht einschränkender Form ein drahtloses lokales Netzwerk (LAN), z. B. ein „Wi-Fi"-Netzwerk, ein RF-Netzwerk, ein Nahbereichkommunikations(NFC)-Netzwerk, ein drahtloses Metropolitan-Area-Network (MAN), das eine Vielzahl drahtloser LANs verbindet und ein Großraumnetzwerk (WAN), z. B. das Internet, beinhalten.

[0056] In einigen Ausführungsformen können die Komponenten des Systems **100** Zugriffskontrollprotokolle implementieren, die dem Client-Gerät **106** Zugriffskontrollrechte gewähren, und die das Client-Gerät **106** befähigen, gemäß den gewährten Zugriffskontrollprivilegien auf Ressourcengerät **102** zuzugreifen. Beispielhaft können herkömmliche Zugriffskontrollverfahren erforderlich machen, dass ein zugängliches Gerät (z. B. Ressourcengerät **102**) eine Zugriffskontrollliste (z. B. eine ACL) unterhält, die eine oder mehrere autorisierte Geräte (z. B. Client-Gerät **106**) und eine diesen autorisierten Geräten eingeräumte Zugriffsstufe identifiziert. Nach dem Empfang einer Zugriffsanfrage eines Gerätes kann das zugängliche Gerät die ACL analysieren, um zu bestimmen, ob das anfragende Gerät ein autorisiertes Gerät ist, und, falls dies der Fall ist, eine dem anfragenden Gerät einzuräumende Zugriffsstufe und/oder Zugriffsart bestimmen.

[0057] Wie zuvor beschrieben kann das Ressourcengerät **102** jedoch von Niedrigenergie-MCUs und -SoCs betriebene Geräte beinhalten. Diese Niedrigenergie-MCUs und/oder -SoCs haben relativ niedrige Taktfrequenzen und verfügen über begrenzten lokalen Speicherplatz, wodurch sie ungeeignet sein können, ACLs für mehrere autorisierte Geräte zu unterhalten und Zugriffskontrollprotokolle bei solchen Frequenzen, die zum Verarbeiten und Authentifizieren individueller Anfragen (z. B. von Client-Gerät **106** oder von anderen Client-Geräten des Systems **100**) erforderlich sind, durchzuführen. Angesichts der durch die Niedrigenergie-MCUs und/oder -SoCs auferlegten Begrenzungen, können mit den offenbarten Ausführungsformen konsistente Zugriffskontrollprotokolle Zugriffskontrollentscheidungen von Ressourcengerät **102** an andere Komponenten des Systems **100** delegieren, welche zum Zugriff auf Ressourcengerät **102** autorisierte Geräte identifizieren können, und welche lokale Tokens erzeugen oder „prägen" können, die, nach Präsentation an das Ressourcengerät **102**, dem autorisierten Gerät ermöglichen, auf Funktionen des Ressourcengerätes **102** zuzugreifen.

[0058] Beispielhaft können Ressourcengerät **102**, Eigentümergerät **104** und Client-Gerät **106** jeweils zur Herstellung von Kommunikationen mit dem Com-

putersystem **108** über Netzwerk **122** befähigt sein, und mit den offenbarten Ausführungsformen konsistente Zugriffskontrollprotokolle können Ressourcengerät **102** befähigen, Zugriffskontrollentscheidungen an Computersystem **108** zu delegieren. In einigen hierin beschriebenen Aspekten kann das Computersystem **108** als Cloud-Server (z. B. ein von Google Cloud™ unterhaltener Server) dienen, und kann zugunsten des Ressourcengerätes **102** ACLs erzeugen und unterhalten, basierend auf von Eigentümergerät **104** empfangener Eingabe (und zusätzlich oder alternativ von jedem beliebigen anderen Gerät einer Einheit, die den Zugriff auf Ressourcengerät **102** kontrolliert oder verwaltet). Wie weiter unten beschrieben, kann das Computersystem **108** des Weiteren lokale Token erzeugen oder prägen, die ein autorisiertes Gerät (z. B. Client-Gerät **106**) befähigen, eine Identität des Ressourcengerätes **102** zu verifizieren und eine Stufe, Art und Dauer des Zugriffs von Client-Gerät **106** auf Ressourcengerät **102** zu spezifizieren.

[0059] Zum Starten der Zugriffskontrollprotokolle, die Zugriffskontrollentscheidungen des Ressourcengerätes **102** an Computersystem **108** delegieren, kann Eigentümergerät **104** (z. B. von einer Einheit unterhalten, die Eigentümerin von Ressourcengerät **102** ist oder den Zugriff auf dieses kontrolliert) in gewissen Aspekten ein oder mehrere Verfahren durchführen, die Ressourcengerät **102** über Netzwerk **124** erkennen. Beispielsweise kann Ressourcengerät **112** erkennbar sein für Geräte, die in Netzwerk **124** betrieben werden, und kann Anzeigedaten bezüglich seines erkennbaren Status an Geräte aussenden, die in Netzwerk **124** betrieben werden. In einem Fall kann Ressourcengerät **102** öffentlich erkennbar sein und die ausgesandten Anzeigedaten können eine Gerätekennung des Ressourcengerätes **102** (z. B. eine Media-Access-Control(MAC)-Adresse, eine IP-Adresse, usw.) beinhalten. Nach dem Empfang der Gerätekennung durch das Eigentümergerät **104**, kann Eigentümergerät **104** Ressourcengerät **102** erkennen und eine Paarbildung mit diesem vornehmen, sowie eine direkte drahtlose Verbindung mit Ressourcengerät **102** herstellen (z. B. über Netzwerk **124**).

[0060] In anderen Fällen kann Ressourcengerät **122** privat erkennbar sein, und kann flüchtige Kennungsdaten (EID) in den Anzeigedaten beinhalten, um seine Mitgliedschaft in einem oder mehreren in System **100** betriebenen privaten Netzwerken anzuzeigen. Beispielsweise kann Ressourcengerät **102**, falls es privat erkennbar ist, Anzeigedaten aussenden, die eine Zufallszahl spezifischer Länge (z. B. eine Zufallszahl mit einer Länge von **16** Bit) und eine digitale Signatur dieser Zufallsnummer, die unter Verwendung eines von den Mitgliedern des einen oder mehreren privaten Netzwerken geteilten privaten kryptographischen Schlüssels erzeugt wurde, beinhalten. In einigen Aspekten kann Ressourcengerät **102** die digitale Signatur durch Anwendung eines Message-Authentication-Code(MAC)-Algorithmus (z. B. eines HMAC-SHA256-Algorithmus mit einer Tag-Länge von sechzehn Bytes) auf die Zufallszahl und den gemeinsamen privaten kryptographischen Schlüssel erzeugen. Eigentümergerät **104** kann die Anzeigedaten empfangen, eine zusätzliche digitale Signatur der Zufallszahl unter Verwendung des gemeinsamen privaten kryptographischen Schlüssels erzeugen, Ressourcengerät **102** erkennen falls die empfangenen und erzeugten digitalen Signaturen übereinstimmen, und die direkte drahtlose Verbindung mit Ressourcengerät **102** über Netzwerk **124** herstellen.

[0061] Nach erfolgter Erkennung und Paarbildung kann Eigentümergerät **104** ein oder mehrere Verfahren (z. B. „Bootstrapping"-Verfahren) durchführen, um Ressourcengerät **102** bei Computersystem **108** zu registrieren und mit den offenbarten Ausführungsformen konsistente Zugriffskontrollverfahren zu implementieren. Beispielhaft kann Eigentümergerät **104** Kommunikationen mit Computersystem **108** über Netzwerk **122** herstellen und kann Computersystem **108** ein oder mehrere Authentifizierungsreferenzen (z. B. Clouddienst-Konten zugeordnete Logins, Passwörter, biometrische Daten, Tokens, digitale Zertifikate, usw.) bereitstellen. Computersystem **108** kann in einigen Aspekten die empfangenen Authentifizierungsreferenzen mit den gespeicherten Clouddienst-Kontendaten (z. B. Daten, die anzeigen, dass Benutzer Konten des Clouddienstes haben, beispielsweise Google Cloud™, oder Benutzer, die GAIA™-Konten haben), um einen Benutzer von Eigentümergerät **104** zu authentifizieren (z. B. der Eigentümer von Eigentümergerät **104** und/oder die den Zugriff auf Eigentümergerät **104** kontrollierende Einheit).

[0062] Nach erfolgter Authentifizierung kann Eigentümergerät **104** eine Registrierungsvorlage erzeugen und diese dem Benutzer über eine grafische Benutzeroberfläche (z. B. über eine ausgeführte mobile Anwendung und/oder eine mit dem Clouddienst verbundene Webseite) präsentieren. In einigen Aspekten kann die Registrierungsvorlage eine Absicht des Benutzers anzeigen, Ressourcengerät **102** für ein oder mehrere mit den offenbarten Ausführungsformen konsistente Zugriffskontrollverfahren zu registrieren. Beispielhaft kann Eigentümergerät **104** des Weiteren die Eingabe von Registrierungsdaten durch den Benutzer in die präsentierte Registrierungsvorlage empfangen, welche in nicht einschränkender Form Daten zum Identifizieren des Ressourcengerätes **102**, Eigentümergerätes **104** und/oder des Clouddienst-Kontos des Benutzers beinhalten können, und Eigentümergerät **104** kann die Registrierungsdaten unter Verwendung eines oder mehrerer sicherer Kommunikationsprotokolle (z. B. Secure Hypertext Transfer Protocol (HTTPS), usw.) über Netzwerk **122** an Computersystem **108** übertragen.

[0063] Computersystem **108** kann die empfangenen Registrierungsdaten verarbeiten und eine mit Eigentümergerät **104**, einem Clouddienst-Konto des Benutzers (z. B. das GAIA™-Konto des Benutzers, das Konto des Benutzers bei Google Cloud™) und Ressourcengerät **102** verlinkte eindeutige Registrierungsticketkennung erzeugen. In einigen Fällen kann Computersystem **108** die erzeugte Registrierungsticketkennung in einem lokalen Speicher oder Datenpool speichern und kann die erzeugte Registrierungsticketkennung unter Verwendung eines oder mehrerer sicherer Kommunikationsprotokolle (z. B. Secure Hypertext Transfer Protocol (HTTPS), usw.) über Netzwerk **122** an Eigentümergerät **104** übertragen.

[0064] Eigentümergerät **104** kann die Registrierungsticketkennung von Computersystem **108** empfangen, und kann in einigen Aspekten die Registrierungsticketkennung unter Verwendung des gemeinsamen privaten kryptographischen Schlüssels verschlüsseln, und die verschlüsselte Registrierungsticketkennung über Netzwerk **124** an Ressourcengerät **102** übertragen. Ressourcengerät **102** kann die verschlüsselte Registrierungsticketkennung empfangen und entschlüsseln, welche in einem lokalen Speicher oder Datenpool gespeichert werden kann. Des Weiteren kann Ressourcengerät **102** in gewissen Aspekten die Registrierungsticketkennung dem Computersystem **108** bereitstellen (z. B. mittels eines Aufrufs an eine geeignete Anwendungsprogrammierung-Schnittstelle (API), beispielsweise eine mit den Weave-Protokollen konsistente Privet API), um das Registrierungsverfahren abzuschließen.

[0065] Computersystem **108** kann die Registrierungsticketkennung mittels der API empfangen, und kann basierend auf der Registrierungsticketkennung Eigentümergerät **104** und das Clouddienst-Konto identifizieren. Als Reaktion auf die Bestimmung kann Computersystem **108** eine oder mehrere Authentifizierungsreferenzen für Ressourcengerät **102** erzeugen, und kann ein oder mehrere Zugriffskontrolllisten (z. B. ACLs) für Ressourcengerät **102** erzeugen und lokal speichern. Wie weiter unten beschrieben, können die erzeugten und gespeicherten ACLs unter anderem zum Zugriff auf Ressourcengerät **102** autorisierte Geräte identifizieren, sowie einen oder mehrere Zugriffsparameter, die einen Umfang des autorisierten Zugriffs definieren, beschränken und/oder begrenzen, identifizieren. Computersystem **108** kann die erzeugten Authentifizierungsreferenzen unter Verwendung eines beliebigen der zuvor beschriebenen sicheren Kommunikationsprotokolle über Netzwerk **122** an Ressourcengerät **102** übertragen. Ressourcengerät **102** kann die ausgestellten Authentifizierungsreferenzen empfangen und in einem lokalen Speicher oder Datenpool speichern, und in gewissen Aspekten kann Computersystem **108** basierend auf den ausgegebenen Authentifizierungsreferenzen sichere Kommunikationssitzungen mit Ressourcengerät **102** herstellen.

[0066] Nach erfolgter Registrierung können Ressourcengerät **102**, Eigentümergerät **104**, Client-Gerät **106** und Computersystem **108** kollektiv Vorgänge durchführen, die eine oder mehrere mit den offenbarten Ausführungsformen konsistente Zugriffskontrollprotokolle implementieren. Beispielsweise können die offenbarten Verfahren Ressourcengerät **102** befähigen, Zugriffskontrollentscheidungen an Computersystem **108** zu delegieren (z. B. einen Cloud-Server, beispielsweise einen von Google Cloud™ unterhaltenen Server), welches ein oder mehrere Tokens erzeugen kann, die Client-Gerät **106** in Übereinstimmung mit einer oder mehreren von Eigentümergerät **104** auferlegten Beschränkungen oder Restriktionen Zugriff auf Ressourcengerät **102** einräumen.

[0067] Um diese und andere Zugriffskontrollverfahren zu implementieren, können Ressourcengerät **102**, Eigentümergerät **104**, Client-Gerät **106** und/oder Computersystem **108** konfiguriert sein, ein(en) oder mehrere kryptographische Schlüssel und Tokens zu erzeugen, zu empfangen und/oder zu speichern. Beispielsweise kann während der hierin beschriebenen Erkennungsverfahren Ressourcengerät **102** einen kryptographischen Ursprungsschlüssel erzeugen, welchen Ressourcengerät **102** in einem lokalen Speicher oder Datenpool speichern kann und welcher von Ressourcengerät **102** vertraulich gehalten werden kann.

[0068] Zusätzlich können in gewissen Aspekten Ressourcengerät **102**, Eigentümergerät **104** und/oder Client-Gerät **106** lokale Kopien eines gemeinsamen privaten kryptographischen Schlüssels speichern, welcher Kommunikationen zwischen dem Ressourcengerät und Eigentümergerät **104** über Netzwerk **124** (sowie ebenfalls mit Client-Gerät **106** über Netzwerk **126**) während des anfänglichen Handshake-Verfahrens verschlüsseln kann, um gerätespezifische Informationen vor Passivempfängern zu verbergen. In gewissen Aspekten kann der gemeinsame private kryptographische Schlüssel von Ressourcengerät **102** unter Verwendung des gespeicherten kryptographischen Ursprungsschlüssels erzeugt werden, und Ressourcengerät **102** kann den gemeinsamen privaten kryptographischen Schlüssel Eigentümergerät **104** und/oder Client-Gerät **106** über das entsprechende Netzwerk, **124** beziehungsweise **126**, bereitstellen. In anderen Aspekten kann Ressourcengerät **112** den gemeinsamen privaten kryptographischen Schlüssel einem zusätzlichen Gerät (z. B. einem Gerät des Eigentümers von Ressourcengerät **112**) und/oder Computersystem **108** (z. B. einem Cloud-Server, beispielsweise einem von Google Cloud™ unterhaltenen Server) während eines Erstregistrierungs- und/oder Bootstrapping-Verfahrens bereitstellen. Das zusätzliche Gerät und/oder Com-

putersystem **108** kann den gemeinsamen privaten kryptographischen Schlüssel sodann dem Client-Gerät **106** als Teil eines oder mehrerer lokaler Zugriffstokens, wie weiter unten beschrieben, bereitstellen.

[0069] Geräte- und Zugriffstokens, welche mit den offenbarten Ausführungsformen konsistent sind, können als Macaroons formatiert werden, welche eine Bytestring-Sequenz (z. B. Schutzvorbehalte) und ein Authentifizierungs-Tag (z. B. eine digitale Signatur) beinhalten, rekursiv berechnet durch Anwendung eines Message-Authentication-Code(MAC)-Algorithmus auf jeden Schutzvorbehalt in verschachtelter Form. Wie weiter unten beschrieben, können die Schutzvorbehalte in nicht einschränkender Form Gerätekennungen, Kennungen gerätespezifischer kryptographischer Schlüssel, und/oder Zugriffsrestriktionen (z. B. Ablaufdaten, zeitliche Restriktionen, Privilegienstufen, Restriktionen von resharing, sitzungsbasierende Restriktionen, zeitliche Restriktionen, usw.) beinhalten. In weiter unten beschriebenen zusätzlichen Aspekten kann des Weiteren ein zuvor erzeugtes Macaroon erweitert werden (z. B. durch Ressourcengerät **102**, Eigentümergerät **104**, Computersystem **108**, usw.), indem zusätzliche Schutzvorbehalte hinzugefügt werden und durch rekursive Anwendung eines MAC-Algorithmus auf die zusätzlichen Schutzvorbehalte, wobei das vorherige Tag als Schlüssel verwendet wird. Mit den offenbarten Ausführungsformen konsistente MAC-Algorithmen können in nicht einschränkender Form einen HMAC-SHA256-Algorithmus mit einer Tag-Länge von sechzehn Bytes, und andere für das Client-Gerät **106** und Ressourcengerät **112** geeignete Algorithmen beinhalten.

[0070] Beispielsweise kann Ressourcengerät **102** ein Master-Gerätetoken und ein Master-Zugriffstoken erzeugen, welche, wie zuvor beschrieben, als Macaroons formatiert werden können. Die Schutzvorbehalte des Master-Gerätetokens können in nicht einschränkender Weise eine Kennung von Ressourcengerät **102** (z. B. eine MAC-Adresse, usw.) und Zufallsdaten (z. B. eine Zufalls-Nonce), die von Ressourcengerät **102** erzeugt wurden, beinhalten. In weiteren Fällen können die Schutzvorbehalte des Master-Zugriffstokens unter anderem eine dem Eigentümer von Ressourcengerät **102** zugeordnete Rolle oder Privilegienstufe (z. B. ein höchstmögliches Privileg), sowie die Zufalls-Nonce, beinhalten. Ressourcengerät **102** kann ebenfalls digitale Signaturen für die Master-Geräte- und Zugriffstokens erzeugen, basierend beispielsweise auf dem gespeicherten kryptographischen Ursprungsschlüssel und den entsprechenden Schutzvorbehalten der Master-Geräte- und Zugriffstokens (z. B. unter Verwendung eines geeigneten MAC-Algorithmus). Die erzeugten digitalen Signaturen (welche z. B. als Authentifizierungs-Tags für ihnen entsprechende Pendants der Macaroons dienen können) können in einigen Fällen die Wahrscheinlichkeit senken, dass eine böswillige Drittpartei eines oder mehrere der Tokens während der Übertragung zwischen Ressourcengerät **102** und anderen Komponenten des Systems **100** abfangen und modifizieren könnte.

[0071] Wie zuvor beschrieben können mit den offenbarten Ausführungsformen konsistente Zugriffskontrollprotokolle Ressourcengerät **102** befähigen, seine Zugriffskontrollentscheidungen an Computersystem **108** zu delegieren (z. B. einen Cloud-Server, beispielsweise einen von Google Cloud™ unterhaltenen Server), welches in Übereinstimmung mit einer oder mehreren von Eigentümergerät **104** auferlegten Beschränkungen und Restriktionen Zugriffsprivilegien auf ein oder mehrere zusätzliche Geräte (z. B. Client-Gerät **106**) einräumen kann. Zwecks Ermöglichens dieser Delegierung kann Ressourcengerät **102** die Master-Geräte- und Zugriffstokens über Netzwerk **122** an Computersystem **108** übertragen (z. B. unter Verwendung beliebiger der zuvor dargelegten sicheren Kommunikationsprotokolle).

[0072] Computersystem **108** kann in einigen Aspekten die Master-Geräte- und Zugriffstokens von Ressourcengerät **102** empfangen, kann die Master-Geräte- und Zugriffstokens Eigentümergerät **104** (und zusätzlich oder alternativ einem Clouddienst-Konto des Benutzers von Eigentümergerät **104**) zuordnen, und kann die Master-Geräte- und Zugriffstokens in einem lokalen Speicher oder Datenpool speichern. In gewissen Aspekten und wie unter Bezugnahme auf **Fig.** 2 beschrieben, kann Computersystem **108** Lokalgerät- und Zugriffstokens erzeugen, welche in Übereinstimmung mit einer oder mehreren von Eigentümergerät **104** auferlegten Beschränkungen und/oder Restriktionen Client-Gerät **106** Zugriffsprivilegien auf ein oder mehrere Funktionen von Ressourcengerät **102** einräumen kann.

[0073] **Fig.** 2 ist ein schematisches Diagramm, das einen exemplarischen Austausch von Daten **200** veranschaulicht, welcher eine Delegierung von Zugriffskontrollentscheidungen von Ressourcengerät **102** an Computersystem **108** ermöglicht, in Übereinstimmung mit offenbarten Ausführungsformen. Beispielhaft, und unter Verwendung beliebiger der zuvor beschriebenen exemplarischen Techniken, kann Ressourcengerät **102** Master-Geräte- und Zugriffstokens erzeugen, welche als Macaroons formatiert werden können, und welche von Ressourcengerät **102** an Computersystem **108** übertragen werden können. Jedoch sind die offenbarten Ausführungsformen nicht auf vom Ressourcengerät **102** erzeugte Master-Geräte- und Zugriffstokens beschränkt, und in anderen Aspekten können mit den offenbarten Ausführungsformen konsistente Master-Geräte- und Zugriffstokens von Eigentümergerät **104**, einem anderen der Ressourcengerät **102** kontrollierenden Einheit zugeordneten Gerät (in **Fig.** 1 nicht abgebildet),

sowie des Weiteren jedem beliebigen zusätzlichen oder anderen innerhalb Systems **100** betreibbaren und delegiertem Zugriff geeigneten Gerät erzeugt werden.

[0074] In einigen Aspekten, wie zuvor beschrieben, kann Computersystem **108** eine Zugriffskontrollliste (z. B. eine ACL) erzeugen oder unterhalten, welche ein oder mehrere zum Zugriff auf Ressourcengerät **102** autorisierte Geräte identifiziert, sowie des Weiteren einen oder mehrere Zugriffsparameter, die einen Umfang des autorisierten Zugriffs definieren, beschränken und/oder begrenzen. In gewissen Aspekten können die Zugriffsparameter in nicht einschränkender Form ein Ablaufdatum, sitzungsbasierende Restriktionen (z. B. Begrenzung des delegierten Zugriffs auf eine einzige, festgelegte Kommunikationseinstellung), zeitliche Restriktionen (z. B. Gültigkeitsdauer, gültige Daten und Uhrzeiten, usw.), Restriktionen bezüglich der Arten des autorisierten Zugriffs (z. B. Verwendung von Funktionen, Modifizierung von Einstellungen, usw.), dem autorisierten Gerät zugeordnete Rollen (z. B. Eigentümer, Manager, Benutzer, usw.), die Fähigkeit der autorisierten Geräte, Zugriff weiter zu delegieren (z. B. zusätzliche Tokens zu prägen) und/oder die Fähigkeit der autorisierten Geräte, auf Ressourcengerät **102** offline zuzugreifen (z. B. ohne Zugriff auf Netzwerk **122**), beinhalten. Jedoch sind die offenbarten Ausführungsformen nicht auf diese exemplarischen Zugriffsparameter beschränkt, und in weiteren Aspekten können mit den offenbarten Ausführungsformen konsistente ACLs beliebige zusätzliche oder andere Zugriffsparameter beinhalten, die für Computersystem **108**, Ressourcengerät **102** und die autorisierten Geräte (z. B. Client-Gerät **106**) geeignet sind. Des Weiteren können einer oder mehrere der Zugriffsparameter von Eigentümergerät **104** festgelegt werden (z. B. basierend auf von einem entsprechenden Benutzer empfangener Eingabe), welche zusätzlich oder alternativ von Computersystem **108** festgelegte Default-Parameter aufweisen können, basierend auf Eigenschaften des Ressourcengerätes **102** und/oder der autorisierten Geräte (z. B. Client-Gerät **106**).

[0075] In einer Ausführungsform kann ein Benutzer von Eigentümergerät **104** auf eine dem Computersystem **108** zugeordnete grafische Benutzeroberfläche (GUI) zugreifen (z. B. von einer durch Eigentümergerät **104** ausgeführten mobilen Anwendung erzeugte und/oder eine Webseite, auf die zugegriffen wurde und welche von Eigentümergerät **104** präsentiert wurde). In einigen Aspekten kann die präsentierte GUI ein oder mehrere zum Zugriff auf Ressourcengerät **102** autorisierte Geräte identifizieren (z. B. in der einen oder den mehreren ACLs), kann den einen oder die mehreren Zugriffsparameter für jedes der autorisierten Geräte identifizieren und kann des Weiteren den Benutzer befähigen, der ACL ein zusätzliches autorisiertes Gerät hinzuzufügen und die Zugriffsparameter für das zusätzliche autorisierte Gerät zu spezifizieren.

[0076] Beispielsweise kann der Benutzer, in Form von Eingaben in die von Eigentümergerät **104** präsentierte GUI, Informationen bereitstellen, die (i) Client-Gerät **106** als ein zum Zugriff auf Ressourcengerät **102** autorisiertes Gerät identifizieren und (ii) einen oder mehrere Zugriffsparameter spezifizieren, die einen Umfang des autorisierten Zugriffs durch Client-Gerät **106** definieren, beschränken und/oder begrenzen. In einigen Fällen kann die Client-Gerät **106** identifizierende Information eine Gerätekennung und/oder eine Kennung eines Benutzers, welcher Client-Gerät **106** bedient, beinhalten. Des Weiteren, wie zuvor beschrieben, kann die Information Zugriffsparameter spezifizieren, welche in nicht einschränkender Form Ablaufdaten, sitzungsbasierende Restriktionen, zeitliche Restriktionen, Arten des autorisierten Zugriffs, Rollen, Restriktionen subsequenter Delegierung, und seitens Eigentümergerät **104** auferlegte Offline-Zugriffsrestriktionen, beinhalten. In einigen Fällen, und konsistent mit den offenbarten Ausführungsformen, muss die spezifizierte Rolle einer Eigentümergerät **104** zugeordneten vergleichbaren Rolle gleichwertig, oder geringer als diese sein.

[0077] Wie in **Fig.** 2 veranschaulicht, kann Eigentümergerät **104** die Informationseingabe des Benutzers empfangen und zu Zugriffskontrolldaten **201** bündeln, welche unter Verwendung beliebiger der zuvor dargelegten sicheren Kommunikationsprotokolle über Netzwerk **122** an Computersystem **108** übertragen werden können. In gewissen Aspekten können die Zugriffskontrolldaten **201** ebenfalls eine oder mehrere Authentifizierungsreferenzen beinhalten (z. B. einen Benutzernamen des Benutzers für ein Clouddienst-Konto, ein Passwort, biometrische Daten, usw.), welche Computersystem **108** befähigen, Eigentümergerät **104** und/oder den Benutzer von Eigentümergerät **104** zu authentifizieren.

[0078] Computersystem **108** kann Zugriffskontrolldaten **201** von Eigentümergerät **104** empfangen, und kann Eigentümergerät **104** und/oder den Benutzer von Eigentümergerät **104** basierend auf einer oder mehreren Authentifizierungsreferenzen authentifizieren. Des Weiteren kann Computersystem **108** in einigen Aspekten die Zugriffskontrolldaten **201** analysieren zwecks Erhaltens von Daten, die das neu autorisierte Gerät (z. B. Client-Gerät **106**) und den einen oder die mehreren Zugriffsparameter, welche den Umfang autorisierten Zugriffs von Client-Gerät **106** definieren, identifizieren. In gewissen Ausführungsformen kann Computersystem **108** auf Teile der Ressourcengerät **102** entsprechenden gespeicherten ACL zugreifen und den Teil der ACL, auf den zugegriffen wurde, aktualisieren, um Daten einzubeziehen, welche Client-Gerät **106** identifizieren und des Weiteren die Zugriffsparameter, welche die Fähigkeit

des Zugriffs von Client-Gerät **106** auf Ressourcengerät **102** definieren, beschränken und/oder begrenzen (z. B. das Erzeugen einer aktualisierten ACL **202**).

[0079] Zusätzlich kann in einigen Ausführungsformen ein Benutzer von Client-Gerät **106** einem Clouddienst-Konto (z. B. Google Cloud™ oder anderen von Computersystem **108** unterhaltenen Clouddiensten) zugeordnet werden, und Client-Gerät **106** kann eine oder mehrere von Computersystem **108** ausgegebene Authentifizierungsreferenzen lokal speichern. In gewissen Aspekten kann Client-Gerät **106** die Authentifizierungsdaten **203** an Computersystem **108** übertragen (z. B. über Netzwerk **122**, unter Verwendung beliebiger der zuvor dargelegten sicheren Kommunikationsprotokolle). Die Authentifizierungsdaten **203** können unter anderem die eine oder mehreren an Client-Gerät **106** ausgegebene Authentifizierungsreferenzen beinhalten, und Computersystem **108** kann Client-Gerät **106** basierend auf einem Vergleich der empfangenen Authentifizierungsreferenzen und gespeicherten Clouddienst-Kontodaten (z. B. Daten, die gültige GAIA™-Konten identifizieren, Daten, die gültige Google Cloud™-Konten identifizieren, usw.) authentifizieren.

[0080] Falls die empfangenen Authentifizierungsreferenzen nicht mit den gespeicherten Clouddienst-Kontodaten übereinstimmen, kann Computersystem **108** den fehlgeschlagenen Authentifizierungsversuch anzeigende Outcome-Daten **204** erzeugen und diese an Client-Gerät **104** übertragen. Falls Computersystem **108** jedoch feststellt, dass die empfangenen Authentifizierungsreferenzen mit Teilen der gespeicherten Clouddienst-Kontodaten übereinstimmen, kann Computersystem **108** das Authentifizierungsverfahren als erfolgreich erachten und kann die erfolgreiche Authentifizierung bestätigende Outcome-Daten **204** an Client-Gerät **106** übertragen.

[0081] Als Reaktion auf die erfolgreiche Authentifizierung kann Client-Gerät **106** eine Anfrage auf Zugriff auf Ressourcengerät **102** (z. B. Zugriffsanfrage **205**) erzeugen und diese an Computersystem **108** übertragen (z. B. über Netzwerk **122**, unter Verwendung beliebiger der zuvor dargelegten sicheren Kommunikationsprotokolle). Die Zugriffsanfrage **205** kann in gewissen Aspekten eine Kennung von Ressourcengerät **102** beinhalten (z. B. eine MAC-Adresse, eine IP-Adresse, usw.). In anderen Aspekten, konsistent mit den offenbarten Ausführungsformen, ist es möglich, dass Zugriffsanfrage **205** nicht gerätespezifisch ist, sondern stattdessen Zugriff auf sämtliche Geräte anfordert, für die Eigentümergerät **104** Client-Gerät **106** Zugriffsprivilegien eingeräumt hat. Wie zuvor beschrieben kann Client-Gerät **106** die Zugriffsanfrage **205** über Netzwerk **122**, unter Verwendung beliebiger der zuvor dargelegten sicheren Kommunikationsprotokolle, an Computersystem **108** übertragen.

[0082] Computersystem **108** kann die Zugriffsanfrage **205** empfangen und kann bestimmen, ob der angeforderte Zugriff auf Ressourcengerät **102** mit der von Eigentümergerät **104** auf Client-Gerät **106** eingeräumten Zugriffsstufe konsistent ist. Beispielsweise kann Computersystem **108** die Zugriffsanfrage **205** analysieren, um Ressourcengerät **102** zu identifizieren, sowie zusätzlich oder alternativ Client-Gerät **106**. In gewissen Aspekten kann Computersystem **108** auf eine lokal gespeicherte Kopie der Ressourcengerät **102** entsprechenden ACL zugreifen, und, basierend auf Einträgen in der ACL, bestimmen, ob Eigentümergerät **104** Client-Gerät **106** Zugriff auf Ressourcengerät **102** eingeräumt hat.

[0083] Falls Computersystem **108** basierend auf Einträgen in der ACL bestimmt, dass Eigentümergerät **104** Client-Gerät **106** (und/oder einem Benutzer von Client-Gerät **106**) keinen Zugriff auf Ressourcengerät **102** eingeräumt hat, kann Computersystem **108** eine das Ausbleiben der Einräumung von Zugriff anzeigende Fehlermeldung erzeugen, und diese Fehlermeldung an Client-Gerät **106** übertragen (in **Fig.** 2 nicht abgebildet). Falls Computersystem **108** jedoch feststellt, dass Eigentümergerät **104** Client-Gerät **106** (und/oder einem Benutzer von Client-Gerät **106**) Zugriff auf Ressourcengerät **102** eingeräumt hat, kann Computersystem **108** ein lokales Gerätetoken und ein lokales Zugriffstoken (z. B. lokale Tokendaten **206** der **Fig.** 2) erzeugen, welche kollektiv Client-Gerät **106** ermöglichen, auf eine oder mehrere Funktionen von Ressourcengerät **102** zuzugreifen.

[0084] In gewissen Aspekten kann Computersystem **108** auf gespeicherte Kopien von Master-Geräte- und Zugriffstokens (z. B. von Ressourcengerät **102** erzeugte und von diesem nach erfolgreichem Abschluss des Registrierungsverfahrens empfangene) zugreifen, und kann das lokale Gerätetoken erzeugen oder „prägen“, basierend auf Erweiterungen zu entsprechenden der Master-Geräte- und Zugriffstokens. Beispielhaft, wie zuvor beschrieben, kann das Master-Gerätetoken als Macaroon formatiert werden, dessen Schutzvorbehalte in nicht einschränkender Form eine Kennung des Ressourcengerätes **102** (z. B. eine MAC-Adresse, usw.) und Zufallsdaten (z. B. eine gerätespezifische Zufalls-Nonce) beinhalten können, die von Ressourcengerät **102** erzeugt wurden. Zur Erzeugung des lokalen Gerätetokens kann Computersystem **108** das Master-Gerätetoken durch Hinzufügen eines oder mehrerer zusätzlicher Schutzvorbehalte (z. B. eine Gerätekennung von Client-Gerät **106**, zusätzliche Zufallsdaten in Form von Zufalls-Noncen usw.) erweitern und durch rekursive Anwendung eines MAC-Algorithmus auf die zusätzlichen Schutzvorbehalte, wobei das vorherige Tag als Schlüssel verwendet wird.

[0085] Beispielhaft kann des Weiteren das Master-Zugriffstoken ebenfalls als Macaroon formatiert wer-

den, dessen Schutzvorbehalte in nicht einschränkender Form eine dem Eigentümer des Ressourcengerätes zugeordnete Rolle (z. B. ein höchstmögliches Privileg) und/oder Zufallsdaten (z. B. eine gerätespezifische Zufalls-Nonce), die von Ressourcengerät **102** erzeugt wurden, beinhalten können. Zur Erzeugung des lokalen Zugriffstokens kann Computersystem **108** in gewissen Aspekten das Master-Gerätetoken erweitern durch Hinzufügen eines oder mehrerer zusätzlicher Schutzvorbehalte, welche die eine oder die mehreren dem Zugriff von Client-Gerät **106** auf Ressourcengerät **102** seitens Eigentümergerät **104** auferlegten Beschränkungen und/oder Restriktionen (z. B. den einen oder die mehreren in der ACL gespeicherten Zugriffsparameter), sowie zusätzliche Zufallsdaten (z. B. Zufalls-Noncen), identifizieren.

[0086] Zum Beispiel kann Computersystem **108** die dem Ressourcengerät **102** entsprechende ACL verarbeiten, um Zugriffsparameter zu extrahieren, welche seitens Eigentümergerät **104** der Fähigkeit von Client-Gerät **106** auferlegte Beschränkungen und/oder Restriktionen des Zugriffs auf Ressourcengerät **102** anzeigen. Wie zuvor erwähnt können die auferlegten Beschränkungen und Restriktionen in nicht einschränkender Form ein Ablaufdatum, eine zeitliche Beschränkung (z. B. gültige Daten und Uhrzeiten), eine sitzungsbasierende Restriktion (z. B. Begrenzung des delegierten Zugriffs auf eine einzige, festgelegte Kommunikationssitzung), Restriktionen der Zugriffsarten (z. B. Verwendung von Funktionen, Modifizierung von Einstellungen, usw.), eine Rolle des Client-Gerätes **106** (z. B. Eigentümer, Manager, Benutzer, usw.), eine Fähigkeit des Client-Gerätes **106** zur weiteren Delegierung von Zugriff (z. B. zusätzliche Tokens zu prägen) und/oder eine Fähigkeit des Client-Gerätes **106**, auf Ressourcengerät **102** offline zuzugreifen (z. B. ohne Zugriff auf Netzwerk **122**), beinhalten. Computersystem **108** kann sodann einen neuen Tag für das lokale Zugriffstoken erzeugen, indem ein geeigneter MAC-Algorithmus auf die zusätzlichen Schutzvorbehalte angewandt wird, den vorherigen Tag (z. B. des Master-Zugriffstokens) als Schlüssel verwendend.

[0087] In einigen Aspekten können die erzeugten lokalen Geräte- und Zugriffstokens „kurzlebig“ (d. h. gültig für eine Stunde, einen Tag, usw.) sein, und Computersystem **108** kann die erzeugten lokalen Geräte- und Zugriffstokens in einem lokalen Speicher oder Datenpool speichern. Zusätzlich können mit den offenbarten Ausführungsformen konsistente MAC-Algorithmen in nicht einschränkender Form einen HMAC-SHA256-Algorithmus mit einer Tag-Länge von sechzehn Bytes, und andere für das Client-Gerät **106**, Ressourcengerät **112** und Netzwerk **122** geeignete Algorithmen beinhalten. Computersystem **108** kann sodann Daten erzeugen, welche die erzeugten lokalen Geräte- und Zugriffstokens (z. B. lokale Tokendaten **206**) beinhalten, und die lokalen Tokendaten **206** unter Verwendung beliebiger der zuvor dargelegten sicheren Kommunikationsprotokolle über Netzwerk **122** an Client-Gerät **106** übertragen. In einigen Aspekten kann Client-Gerät **106** lokale Tokendaten **206** von Computersystem **108** über Netzwerk **122** empfangen, und kann die Kopien der lokalen Geräte- und Zugriffstokens in einem lokalen Speicher oder Datenpool speichern.

[0088] **Fig.** 3 ist ein Flussdiagramm eines exemplarischen Verfahrens **300** zur Delegierung von Zugriffskontrollentscheidungen von einem Ressourcengerät an ein oder mehrere Computergeräte, in Übereinstimmung mit den offenbarten Ausführungsformen. In gewissen Aspekten kann ein als Cloud-Server betriebenes Computersystem (z. B. Computersystem **108**) die Schritte des exemplarischen Verfahrens **300** durchführen, welche ein Ressourcengerät (z. B. Ressourcengerät **102**) befähigen können, Zugriffskontrollentscheidungen an Computersystem **108** zu übertragen, und welche einem oder mehreren durch ein Gerät eines Eigentümers von Ressourcengerät **102** (z. B. Eigentümergerät **104**) designierten Client-Geräten (z. B. Client-Gerät **106**) Zugriffsrechte auf Ressourcengerät **102** einräumen.

[0089] In einigen Aspekten, konsistent mit den offenbarten Ausführungsformen, kann Eigentümergerät **104** Vorgänge durchführen, welche Ressourcengerät **102** beim Betrieb über Netzwerk **124** erkennen. Beispielsweise kann Ressourcengerät **102** erkennbar sein für Geräte, die in Netzwerk **124** betrieben werden, und kann Anzeigedaten bezüglich seines erkennbaren Status an Geräte aussenden, die in Netzwerk **124** betrieben werden. In gewissen Aspekten kann Ressourcengerät **102** öffentlich oder privat erkennbar sein, und Eigentümergerät **104** kann Ressourcengerät **102**, sowohl in einem öffentlich als auch privat erkennbaren Status, unter Verwendung beliebiger der zuvor beschriebenen exemplarischen Techniken, entdecken.

[0090] Als Reaktion auf die erfolgreiche Erkennung von Ressourcengerät **102** durch Eigentümergerät **104** kann Computersystem **108** Vorgänge durchführen, die Ressourcengerät **102** registrieren und Ressourcengerät **102** einem Clouddienst-Konto des Eigentümers von Ressourcengerät **102** zuordnen (z. B. einem GAIA™-Konto, einem Google Cloud™-Konto, usw.), sowie zusätzlich oder alternativ mit Eigentümergerät **104** (z. B. in Schritt **302**). Beispielsweise kann Eigentümergerät **104** Kommunikationen mit Computersystem **108** über Netzwerk **122** herstellen, und kann Computersystem **108** eine oder mehrere Authentifizierungsreferenzen bereitstellen (z. B. Benutzernamen, Passwörter, biometrische Daten, Tokens, digitale Zertifikate, usw.). Computersystem **108** kann in einigen Aspekten die empfangenen Authentifizierungsreferenzen mit gespeicherten Authentifizierungsdaten (z. B. gespeicherte GAIA™-Kontodaten,

gespeicherte Google Cloud™-Kontodaten, usw.) vergleichen, um Eigentümergerät **104** zu authentifizieren.

[0091] Wie zuvor beschrieben kann Eigentümergerät **104** Daten erzeugen, welche die Registrierung von Ressourcengerät **102** bei Computersystem **108** unterstützen (z. B. basierend auf Dateneingabe durch einen Benutzer des Eigentümergerätes in eine präsentierte Registrierungsvorlage), und Eigentümergerät **104** kann die erzeugten Registrierungsdaten über Netzwerk **122** an Computersystem **108** übertragen (unter Verwendung beliebiger der zuvor beschriebenen sicheren Kommunikationsprotokolle). Die erzeugten Registrierungsdaten können in nicht einschränkender Form Daten zum Identifizieren des Ressourcengerätes **102**, Eigentümergerätes **104** und/oder des dem Eigentümer von Ressourcengerät **102** zugeordneten Clouddienst-Kontos beinhalten.

[0092] Computersystem **108** kann die Registrierungsdaten in Schritt **302** empfangen, und kann eine mit Eigentümergerät **104**, dem Clouddienst-Konto des Benutzers und Ressourcengerät **102** verlinkte eindeutige Registrierungsticketkennung erzeugen. In einigen Fällen kann Computersystem **108** die erzeugte Registrierungsticketkennung in einem lokalen Speicher oder Datenpool speichern und kann die erzeugte Registrierungsticketkennung unter Verwendung eines oder mehrerer sicherer Kommunikationsprotokolle (z. B. Secure Hypertext Transfer Protocol (HTTPS), usw.) über Netzwerk **122** an Eigentümergerät **104** übertragen.

[0093] Eigentümergerät **104** kann die Registrierungsticketkennung von Computersystem **108** empfangen, und kann in einigen Aspekten die Registrierungsticketkennung unter Verwendung des gemeinsamen privaten kryptographischen Schlüssels verschlüsseln, bevor die verschlüsselte Registrierungsticketkennung über Netzwerk **124** an Ressourcengerät **102** übertragen wird. Ressourcengerät **102** kann die verschlüsselte Registrierungsticketkennung empfangen (und gegebenenfalls entschlüsseln), welche in einem lokalen Speicher oder Datenpool gespeichert werden kann. Des Weiteren kann Ressourcengerät **102** in gewissen Aspekten die Registrierungsticketkennung Computersystem **108** bereitstellen (z. B. mittels eines Aufrufs an eine geeignete Anwendungsprogrammierung-Schnittstelle (API), beispielsweise eine mit den Weave-Protokollen konsistente Privet API), um das Registrierungsverfahren abzuschließen.

[0094] Computersystem **108** kann die Registrierungsticketkennung mittels der API empfangen und, basierend auf der Registrierungsticketkennung, ein oder mehrere Authentifizierungsreferenzen erzeugen und diese an Ressourcengerät **102** ausgeben (z. B. in Schritt **302**). Computersystem **108** kann die erzeugten und ausgegebenen Authentifizierungsreferenzen über Netzwerk **122** an Ressourcengerät **102** übertragen, welches die ausgegebenen Authentifizierungsreferenzen empfangen und in einem lokalen Speicher oder Datenpool speichern kann. Des Weiteren kann Ressourcengerät **102** basierend auf den ausgegebenen Authentifizierungsreferenzen eine gesicherte Kommunikationssitzung mit Computersystem **108** über Netzwerk **122** herstellen.

[0095] In zusätzlichen Aspekten, und in Reaktion auf die Registrierung von Ressourcengerät **102**, kann Computersystem **108** eine Zugriffskontrollliste (z. B. ACL) für Ressourcengerät **102** erzeugen und lokal speichern (z. B. in Schritt **304**). Die erzeugte und gespeicherte ACL kann unter anderem ein oder mehrere zum Zugriff auf Ressourcengerät **102** autorisierte Geräte und ein oder mehrere Zugriffsparameter, welche von Eigentümergerät **104** dem autorisierten Zugriff auferlegte Beschränkungen und Restriktionen definieren, identifizieren. In gewissen Aspekten können die Zugriffsparameter in nicht einschränkender Form ein Token-Ablaufdatum, eine sitzungsbasierende Restriktion (z. B. Begrenzung des delegierten Zugriffs auf eine einzige, festgelegte Kommunikationseinstellung), eine zeitliche Restriktion (z. B. Gültigkeitsdauer, usw.), eine Restriktion bezüglich der Art des autorisierten Zugriffs (z. B. Verwendung spezifischer Funktionen, Modifizierung von Einstellungen, usw.), eine einem autorisierten Gerät zugewiesene Rolle oder Privilegienstufe (z. B. Eigentümer, Manager, Benutzer, usw.), eine Fähigkeit des autorisierten Gerätes, Zugriff weiter zu delegieren (z. B. Zugriff erneut zu teilen) und/oder eine Fähigkeit eines autorisierten Gerätes, auf Ressourcengerät **102** offline zuzugreifen (z. B. ohne Zugriff auf Netzwerk **122**), beinhalten. In einigen Fällen kann Computersystem **108** die erzeugte und gespeicherte ACL dem Eigentümergerät **104** und/oder einem dem Eigentümergerät **104** zugeordneten Clouddienst-Konto zuordnen, und, wie weiter unten beschrieben, Computersystem **108** kann Verfahren zum Zugriff und zur Modifizierung der gespeicherten ACL durchführen, in Reaktion auf von Eigentümergerät **104** empfangene Zugriffskontrolldaten.

[0096] In gewissen Aspekten kann Ressourcengerät **102** seine Zugriffskontrollentscheidungen an Computersystem **108** delegieren, welches in Übereinstimmung mit von Eigentümergerät **104** auferlegten Restriktionen und Beschränkungen Zugriffsprivilegien mit einem oder mehreren zusätzlichen Geräten (z. B. Client-Gerät **106**) teilen kann. Zwecks Ermöglichens dieser Delegierung kann Ressourcengerät **102** eine sichere Kommunikationssitzung mit Computersystem **108** herstellen (z. B. basierend auf den ausgegebenen Authentifizierungsreferenzen), und kann Kopien eines Master-Gerätetokens und eines Master-Zugriffstokens über Netzwerk **122** an Computersystem **108** übertragen (z. B. unter Verwendung be-

liebiger der zuvor dargelegten sicheren Kommunikationsprotokolle). In einigen Aspekten kann Computersystem **108** die Master-Geräte- und Zugriffstokens von Ressourcengerät **102** empfangen (z. B. in Schritt **306**), und kann die empfangenen Master-Geräte- und Zugriffstokens in einem lokalen Speicher oder Datenpool speichern. Wie weiter unten beschrieben kann Computersystem **108** die Struktur der Master-Geräte- und/oder Zugriffstokens modifizieren, um lokale Token zu erzeugen, welche einem oder mehreren Client-Gerät(en) (z. B. Client-Gerät **106**) Zugriff auf Ressourcengerät **102** einräumen.

[0097] Beispielhaft, wie zuvor beschrieben, können die Master-Geräte- und Zugriffstokens als Macaroons formatiert werden, welche eine Bytestring-Sequenz (z. B. Schutzvorbehalte) und ein Authentifizierungs-Tag (z. B. eine digitale Signatur) aufweisen, rekursiv berechnet durch Anwendung eines Message-Authentication-Code(MAC)-Algorithmus auf jeden Schutzvorbehalt in verschachtelter Form. Die Schutzvorbehalte des Master-Gerätetokens können in nicht einschränkender Form eine Kennung des Ressourcengerätes **102** (z. B. eine MAC-Adresse, usw.) und Zufallsdaten (z. B. eine gerätespezifische Zufalls-Nonce), die von Ressourcengerät **102** erzeugt wurden, beinhalten. In weiteren Fällen können die Schutzvorbehalte des Master-Zugriffstokens unter anderem eine dem Eigentümer von Ressourcengerät zugeordnete Rolle oder Privilegienstufe (z. B. ein höchstmögliches Privileg), sowie die gerätespezifische Zufalls-Nonce, beinhalten. Des Weiteren kann die auf die Tokens angewandte digitale Signatur in einigen Fällen die Wahrscheinlichkeit senken, dass eine böswillige Drittpartei Teile der Schutzvorbehaltsdaten abfangen könnte und nicht-autorisierte Modifizierungen an diesen vornehmen könnte.

[0098] In gewissen Aspekten kann Computersystem **108** konfiguriert sein, Zugriffskontrolldaten (z. B. Zugriffskontrolldaten **201** der **Fig.** 2) von Eigentümergerät **104** zu empfangen (z. B. in Schritt **308**). Die empfangenen Zugriffskontrolldaten können beispielsweise Information beinhalten, die (i) ein zum Zugriff auf Ressourcengerät **102** autorisiertes Gerät (z. B. Client-Gerät **106**) identifiziert und (ii) einen oder mehrere Zugriffsparameter spezifiziert, die den autorisierten Zugriff des Client-Gerätes **106** definieren, beschränken und/oder begrenzen. In einigen Fällen kann ein Benutzer von Eigentümergerät **104** mindestens einen Teil der empfangenen Zugriffskontrolldaten als Eingabe für eine Computersystem **108** zugeordnete grafische Benutzeroberfläche (GUI) bereitstellen (z. B. von einer durch Eigentümergerät **104** ausgeführten mobilen Anwendung erzeugte und/oder eine Webseite, auf die zugegriffen wurde und von Eigentümergerät **104** präsentiert wurde).

[0099] Beispielhaft können die empfangenen Zugriffskontrolldaten eine Kennung von Client-Gerät **106** und/oder eine Kennung eines Benutzers, welcher Client-Gerät **106** bedient, beinhalten. Des Weiteren, wie zuvor beschrieben, können die empfangenen Zugriffskontrolldaten Zugriffsparameter spezifizieren, welche in nicht einschränkender Form sitzungsbasierende Restriktionen, zeitliche Restriktionen, Restriktionen bezüglich der Art des autorisierten Zugriffs, Rollen oder Privilegienstufen, Restriktionen subsequenter Delegierung und Offline-Zugriffsrestriktionen, welche seitens Eigentümergerät **104** der Fähigkeit von Client-Gerät **106** auferlegt wurden, auf Ressourcengerät **102** zuzugreifen, beinhalten. In einigen Fällen, und konsistent mit den offenbarten Ausführungsformen, muss die seitens des Benutzers von Eigentümergerät **104** spezifizierte Rolle oder Privilegienstufe einer vergleichbaren Privilegienstufe des Eigentümergerätes **104** gleichwertig, oder geringer als diese sein. In zusätzlichen Aspekten können die empfangenen Zugriffskontrolldaten eine oder mehrere Authentifizierungsreferenzen (z. B. einen Login-Namen eines dem Eigentümergerät **104** zugeordneten Clouddienst-Kontos, ein Passwort, biometrische Daten, usw.) beinhalten, welche Computersystem **108** befähigen, Eigentümergerät **104** und/oder den Benutzer von Eigentümergerät **104** zu authentifizieren.

[0100] In Schritt **310** kann Computersystem **108** konfiguriert sein, Eigentümergerät **104** zu authentifizieren (z. B. basierend auf einem Vergleich der empfangenen Authentifizierungsreferenzen mit gespeicherten Clouddienst-Kontodaten), sowie des Weiteren, die empfangenen Zugriffskontrolldaten zu analysieren, um das neu autorisierte Gerät (z. B. Client-Gerät **106**) und den einen oder die mehreren Zugriffsparameter die den Zugriff von Client-Gerät **106** auf Ressourcengerät **102** definieren, beschränken und/oder begrenzen, zu identifizieren. Computersystem **108** kann ebenfalls auf die lokal gespeicherte ACL zugreifen, und, in Schritt **312**, mindestens einen Teil der ACL, auf welche zugegriffen wurde, modifizieren, um Daten einzubeziehen, die Client-Gerät **106** und den einen oder die mehreren Zugriffsparameter (z. B. die aktualisierte ACL **202** der **Fig.** 2) identifizieren.

[0101] In einigen Aspekten kann ein Benutzer von Client-Gerät **106** einem Clouddienst-Konto (z. B. Google Cloud™ oder anderen von Computersystem **108** unterhaltenen Clouddiensten) zugeordnet werden, und Client-Gerät **106** kann eine oder mehrere von Computersystem **108** ausgegebene Authentifizierungsreferenzen lokal speichern. In einigen Fällen kann Client-Gerät **106** die Authentifizierungsdaten (z. B. die Authentifizierungsdaten **203** der **Fig.** 2) unter Verwendung beliebiger der zuvor dargelegten sicheren Kommunikationsprotokolle über Netzwerk **122** an Computersystem **108** übertragen. Computersystem **108** kann die Authentifizierungsdaten von Client-Gerät **106** empfangen (z. B. in Schritt **314**), und kann Client-Gerät **106** basierend auf einem Ver-

gleich der empfangenen Authentifizierungsdaten und gespeicherten Clouddienst-Kontodaten authentifizieren, unter Verwendung beliebiger der hierin beschriebenen exemplarischen Techniken (z. B. in Schritt **316**).

[0102] Falls Computersystem **108** feststellt, dass die Authentifizierungsreferenzen von Client-Gerät **106** nicht mit den gespeicherten Clouddienst-Kontodaten übereinstimmen (z. B. Schritt **316**; NEIN), kann Computersystem **108** die fehlgeschlagene Authentifizierung anzeigende Fehlerdaten erzeugen, und diese Fehlerdaten über Netzwerk **122** an Client-Gerät **106** übertragen (z. B. in Schritt **318**). Das exemplarische Verfahren **300** endet dann in Schritt **320**.

[0103] Falls Computersystem **108** jedoch feststellt, dass die Authentifizierungsreferenzen des Client-Gerätes mit einem Teil der gespeicherten Clouddienst-Kontodaten übereinstimmen (z. B. Schritt **316**; JA), kann Computersystem **108** eine Bestätigung der erfolgreichen Authentifizierung erzeugen, und diese über Netzwerk **122** an Client-Gerät **106** übertragen (z. B. in Schritt **322**).

[0104] Als Reaktion auf die erfolgreiche Authentifizierung kann Client-Gerät **106** eine Anfrage auf lokalen Zugriff auf Ressourcengerät **102** erzeugen (z. B. Zugriffsanfrage **205**), und diese an Computersystem **108** übertragen. Zugriffsanfrage **205** kann in gewissen Aspekten Kennungen von Ressourcengerät **102** und Client-Gerät **106** beinhalten (z. B. eine MAC-Adresse, eine IP-Adresse, usw.)

[0105] Computersystem **108** kann die Zugriffsanfrage von Client-Gerät **106** empfangen (z. B. in Schritt **324**), und kann bestimmen, ob der angeforderte Zugriff mit dem seitens Eigentümergerät **104** Client-Gerät **106** eingeräumten Zugriff konsistent ist (z. B. in Schritt **326**). Beispielsweise kann in Schritt **326** Computersystem **108** die empfangene Zugriffsanfrage analysieren, um Ressourcengerät **102**, sowie zusätzlich oder alternativ Client-Gerät **106**, zu identifizieren. Computersystem **108** kann ebenfalls auf die lokal gespeicherte Kopie der Ressourcengerät **102** entsprechenden ACL zugreifen, und, basierend auf den Einträgen der ACL, bestimmen, ob Eigentümergerät **104** Client-Gerät **106** Zugriff auf Ressourcengerät **102** gewährt hat.

[0106] Falls Eigentümergerät **104** Client-Gerät **106** keinen Zugriff gewährt hat (z. B. Schritt **326**; NEIN), kann Computersystem **108** zu Schritt **318** zurückgehen und das Ausbleiben der Gewährung von Zugriff anzeigende Fehlerdaten erzeugen, und diese Fehlerdaten über Netzwerk **122** an Client-Gerät **106** übertragen. Das exemplarische Verfahren **300** endet dann in Schritt **320**.

[0107] Alternativ hierzu, falls Computersystem **108** feststellt, dass Eigentümergerät **104** Client-Gerät **106** Zugriff auf Ressourcengerät **102** eingeräumt hat (z. B. Schritt **326**; JA), kann Computergerät **108** ein lokales Gerätetoken und ein lokales Zugriffstoken (z. B. lokale Tokens **206** der **Fig.** 2) erzeugen, welche kollektiv den Zugriff von Client-Gerät **106** auf Ressourcengerät **102** ermöglichen (z. B. in Schritt **328**). In gewissen Aspekten kann Computersystem **108** in Schritt **328** auf gespeicherte Kopien von Master-Geräte- und Zugriffstokens (z. B. von Ressourcengerät **102** erzeugte und von diesem nach erfolgreichem Abschluss des Registrierungsverfahrens empfangene) zugreifen, und kann das lokale Gerätetoken erzeugen oder „prägen“, basierend auf Erweiterungen zu entsprechenden der Master-Geräte- und Zugriffstokens.

[0108] Beispielhaft, wie zuvor beschrieben, kann das Master-Gerätetoken als Macaroon formatiert werden, dessen Schutzvorbehalte in nicht einschränkender Form eine Kennung des Ressourcengerätes **102** (z. B. eine MAC-Adresse, usw.) und Zufallsdaten (z. B. eine Zufalls-Nonce) beinhalten können, die von Ressourcengerät **102** erzeugt wurden. Zur Erzeugung des lokalen Gerätetokens in Schritt **328** kann Computersystem **108** das Master-Gerätetoken durch Hinzufügen eines oder mehrerer zusätzlicher Schutzvorbehalte (z. B. eine Gerätekennung von Client-Gerät **106**, zusätzliche Zufallsdaten in Form von Zufalls-Noncen, usw.) erweitern und durch rekursive Anwendung eines MAC-Algorithmus auf die zusätzlichen Schutzvorbehalte, wobei das vorherige Tag als Schlüssel verwendet wird.

[0109] Beispielhaft kann des Weiteren das Master-Zugriffstoken ebenfalls als Macaroon formatiert werden, dessen Schutzvorbehalte in nicht einschränkender Form eine dem Eigentümer des Ressourcengerätes zugeordnete Rolle oder Privilegienstufe (z. B. ein höchstmögliches Privileg) und/oder Zufallsdaten (z. B. eine Zufalls-Nonce), die von Ressourcengerät **102** erzeugt wurden, beinhalten können. In gewissen Aspekten kann Computersystem **108** zwecks Erzeugens des lokalen Zugriffstokens in Schritt **328** das Master-Zugriffstoken erweitern, indem diesem ein oder mehrere zusätzliche Schutzvorbehalte hinzugefügt werden, welche die eine oder die mehreren dem Zugriff von Client-Gerät **106** auf Ressourcengerät **102** seitens Eigentümergerät **104** auferlegten Beschränkungen und/oder Restriktionen (z. B. der eine oder die mehreren in der ACL gespeicherten Zugriffsparameter), sowie zusätzliche Zufallsdaten (z. B. Zufalls-Noncen), identifizieren.

[0110] Zum Beispiel kann Computersystem **108** die lokal gespeicherte ACL analysieren, um Zugriffsparameter zu extrahieren, welche die seitens Eigentümergerät **104** der Fähigkeit von Client-Gerät **106** auferlegten Beschränkungen und/oder Restriktionen

des Zugriffs auf Ressourcengerät **102** anzeigen. Wie zuvor erwähnt, können die auferlegten Beschränkungen und Restriktionen in nicht einschränkender Form ein Ablaufdatum, eine zeitliche Beschränkung (z. B. gültige Daten und Uhrzeiten für den Zugriff), eine sitzungsbasierende Restriktion (z. B. Begrenzung des delegierten Zugriffs auf eine einzige, festgelegte Kommunikationssitzung), Restriktionen der Zugriffsarten (z. B. Verwendung von Funktionen, Modifizierung von Einstellungen, usw.), eine Rolle des Client-Gerätes **106** (z. B. Eigentümer, Manager, Benutzer, usw.), eine Fähigkeit des Client-Gerätes **106** zur weiteren Delegierung von Zugriff (z. B. zusätzliche Tokens zu prägen) und/oder eine Fähigkeit des Client-Gerätes **106**, auf Ressourcengerät **102** offline zuzugreifen (z. B. ohne Zugriff auf Netzwerk **122**), beinhalten. Computersystem **108** kann sodann ein neuer Tag für das lokale Zugriffstoken erzeugen, indem ein geeigneter MAC-Algorithmus auf die zusätzlichen Schutzvorbehalte angewandt wird, das vorherige Tag (z. B. des Master-Zugriffstokens) als Schlüssel verwendend.

[0111] Computersystem **108** kann sodann die erzeugten lokalen Geräte- und Zugriffstokens (z. B. die lokalen Tokendaten **206** der **Fig.** 2) unter Verwendung beliebiger der zuvor dargelegten sicheren Kommunikationsprotokolle über Netzwerk **122** an Client-Gerät **106** übertragen (z. B. in Schritt **330**). Das exemplarische Verfahren **300** endet dann in Schritt **320**.

[0112] In den zuvor beschriebenen Ausführungsformen kann Computersystem **108** konfiguriert sein, die lokalen Geräte- und/oder Zugriffstokens in Reaktion auf eine von Client-Gerät **106** empfangene Zugriffsanfrage zu erzeugen. In einigen Fällen, und konsistent mit den offenbarten Ausführungsformen, kann Computersystem **108** stattdessen Verfahren durchführen, welche die lokalen Geräte- und/oder Zugriffstokens in spezifizierten und vorbestimmten Intervallen (z. B. stündlich, täglich, usw.), oder in Reaktion auf das detektierte Auftreten einer oder mehrerer Ereignisse (z. B. eine Modifizierung einer ACL in Reaktion auf eine Anfrage von Eigentümergerät **104**), prägen und speichern. In zusätzlichen Aspekten kann Computersystem **108** ebenfalls Vorgänge durchführen zum „Puschen“ zusätzlicher Versionen der lokalen Geräte- und/oder Zugriffstokens zu spezifischen oder vorbestimmten Zeiten, oder in Reaktion auf beliebige der zuvor beschriebenen Ereignisse, an Client-Gerät **106** (z. B. über Netzwerk **122**, unter Verwendung beliebiger der zuvor beschriebenen sicheren Kommunikationsprotokolle).

[0113] In gewissen Ausführungsformen können die zuvor beschriebenen exemplarischen Verfahren Ressourcengerät **102** befähigen, Zugriffskontrollentscheidungen an Computersystem **108** zu delegieren (z. B. einen Cloud-Server, beispielsweise einen von Google Cloud™ unterhaltenen Server), welches in Übereinstimmung mit einer oder mehreren von Eigentümergerät **104** auferlegten Beschränkungen Client-Gerät **106** Zugriff auf Ressourcengerät **102** einräumen kann. Beispielsweise kann Computersystem **108**, wie zuvor beschrieben, Client-Gerät **106** ein lokales Gerätetoken und einen lokalen Client bereitstellen. In zusätzlichen Ausführungsformen, weiter unten dargelegt, können die lokalen Geräte- und Zugriffstokens Client-Gerät **106** ermöglichen, eine direkte drahtlose Verbindung mit Ressourcengerät **102** herzustellen (z. B. über Netzwerk **126**), und auf Ressourcengerät **102** in Übereinstimmung mit seitens des Eigentümergerätes auferlegten Beschränkungen und/oder Restriktionen zuzugreifen, ohne zusätzliche Netzwerkkommunikation mit Eigentümergerät **104** oder Computersystem **108** zu benötigen.

[0114] In einigen Aspekten, konsistent mit den offenbarten Ausführungsformen, kann Client-Gerät **106** Vorgänge durchführen, welche Ressourcengerät **102** beim Betrieb über Netzwerk **126** erkennen. Beispielsweise kann Ressourcengerät **102** erkennbar sein für Geräte, die in Netzwerk **126** betrieben werden, und kann Anzeigedaten bezüglich seines erkennbaren Status an Geräte aussenden, die in Netzwerk **126** betrieben werden. In gewissen Aspekten kann Ressourcengerät **102** öffentlich oder privat erkennbar sein, und Client-Gerät **106** kann Ressourcengerät **102**, sowohl in einem öffentlich als auch privat erkennbaren Status, unter Verwendung beliebiger der zuvor beschriebenen exemplarischen Techniken, erkennen.

[0115] Nach Erkennung von Ressourcengerät **102** durch Client-Gerät **106**, können Client-Gerät **106** und Ressourcengerät **102** Verfahren einleiten zwecks Herstellens einer sicheren direkten Verbindung über Netzwerk **126**, beispielsweise das zuvor beschriebene Low-Energy(BLE)-Netzwerk. Beispielsweise kann Client-Gerät **106** nach Empfang und Speicherung des lokalen Gerätetokens (z. B. von Computersystem **108** empfangen) Zufallsdaten erzeugen (z. B. eine Client-spezifische Zufalls-Nonce), und kann eine Schutzvorbehalt-Sequenz aus dem gespeicherten lokalen Token extrahieren. Die extrahierte Schutzvorbehalt-Sequenz kann in nicht einschränkender Form eine Kennung des Ressourcengerätes **102** (z. B. eine MAC-Adresse, usw.) und Zufallsdaten (z. B. eine gerätespezifische Zufalls-Nonce), die von Ressourcengerät **102** erzeugt wurden, beinhalten.

[0116] In gewissen Aspekten kann Client-Gerät **106** konfiguriert sein, einen ersten Wert (z. B. einen ersten Hash) eines symmetrischen kryptographischen Schlüssels zu berechnen, basierend auf der Anwendung eines MAC-Algorithmus (z. B. eines HMAC-SHA256-Algorithmus mit einer Tag-Länge von sechzehn Bytes) auf das gespeicherte lokale Gerätetoken und die erzeugte Client-spezifische Zufalls-Nonce. Des Weiteren, wie weiter unten unter Bezugnahme auf **Fig.** 4 beschrieben, kann Client-Gerät **106**

anfordern, dass Ressourcengerät **102** einen zweiten Wert des symmetrischen kryptographischen Schlüssels berechnet, basierend auf der rekursiven Anwendung eines MAC-Algorithmus auf einen kryptographischen Ursprungsschlüssel (z. B. von Ressourcengerät **102** unterhaltenen), die extrahierten Schutzvorbehalt-Sequenz und die erzeugte Client-spezifische Zufalls-Nonce, und kann des Weiteren eine Identität des Ressourcengerätes **102** verifizieren, basierend auf einem Vergleich des ersten und zweiten symmetrischen kryptographischen Schlüssels.

[0117] **Fig.** 4 ist ein schematisches Diagramm, das einen exemplarischen Austausch von Daten **400** veranschaulicht, welcher einen tokenbasierten Zugriff auf Ressourcengerät **102** durch Client-Gerät **106** ermöglicht, in Übereinstimmung mit offenbarten Ausführungsformen. Zum Beispiel kann Client-Gerät **106** über Netzwerk **126** an Ressourcengerät **102** Daten (z. B. Schlüssel-Anforderungsdaten **401**) übertragen, anfordernd, dass das Ressourcengerät den zweiten Wert des symmetrischen kryptographischen Schlüssels berechne. Schlüssel-Anforderungsdaten **401** können in nicht einschränkender Form die extrahierten Schutzvorbehalt-Sequenzen und die Client-spezifischen Zufalls-Noncen beinhalten, und in gewissen Aspekten kann Client-Gerät **106** Schlüssel-Anforderungsdaten **401** unter Verwendung eines gemeinsamen privaten kryptographischen Schlüssels, wie zuvor beschrieben, verschlüsseln. Die offenbarten Ausführungsformen sind jedoch nicht auf diese exemplarischen Verschlüsselungsschemen beschränkt, und in anderen Aspekten kann Client-Gerät **106** Schlüssel-Anforderungsdaten **401** unter Verwendung beliebiger zusätzlicher oder anderer Verschlüsselungsschemen, welche für Schlüssel-Anforderungsdaten **401**, Client-Gerät **106** und Ressourcengerät **102** geeignet sind, verschlüsseln (oder kann Schlüssel-Anforderungsdaten **401** alternativ unverschlüsselt übertragen).

[0118] In einigen Aspekten kann Ressourcengerät **102** Schlüssel-Anforderungsdaten **401** empfangen (und gegebenenfalls entschlüsseln), und kann den angeforderten zweiten Wert des symmetrischen kryptographischen Schlüssels berechnen, basierend auf einer rekursiven Anwendung des MAC-Algorithmus auf den kryptographischen Ursprungsschlüssel, die extrahierte Schutzvorbehalt-Sequenz und die erzeugte Client-spezifische Zufalls-Nonce. Beispielsweise kann der MAC-Algorithmus einen HMAC-SHA 256-Algorithmus mit einer Tag-Länge von sechzehn Bytes beinhalten. Ressourcengerät **102** kann in einigen Fällen einen Hash-Wert berechnen, basierend auf einer ersten Anwendung des MAC-Algorithmus auf den kryptographischen Ursprungsschlüssels und die extrahierten Schutzvorbehalt-Sequenzen, und kann den zweiten Wert des symmetrischen kryptographischen Schlüssels basierend auf einer zweiten Anwendung des MAC-Algorithmus auf den berechneten Hash-Wert und die Client-spezifischen Zufalls-Nonce berechnen. Ressourcengerät **102** kann in einigen Aspekten Schlüsseldaten, welche den zweiten kryptographischen Schlüssel (z. B. Schlüsselwertdaten **402**) beinhalten, über Netzwerk **126** an Client-Gerät **106** übertragen. In einigen Fällen, wie zuvor beschrieben, kann Ressourcengerät **102** Schlüsseldaten unter Verwendung des gemeinsamen privaten kryptographischen Schlüssels und zusätzlich oder alternativ beliebiger anderer Verschlüsselungsschemen, welche für Schlüsselwertdaten **402**, Ressourcengerät **102** und Client-Gerät **106** geeignet sind, verschlüsseln (oder kann Schlüssel-Anforderungsdaten **401** alternativ unverschlüsselt übertragen).

[0119] Client-Gerät **106** kann Schlüsselwertdaten **402** empfangen (und gegebenenfalls entschlüsseln), um den zweiten Wert des symmetrischen kryptographischen Schlüssels zu erhalten, welchen Client-Gerät **106** mit dem berechneten ersten Wert vergleichen kann. Falls Client-Gerät **106** feststellt, dass die ersten und zweiten Werte nicht übereinstimmen, kann Client-Gerät **106** eine einen fehlgeschlagenen Verbindungsversuch anzeigende Antwort an Ressourcengerät **102** übertragen (in **Fig.** 4 nicht dargestellt), welche das Verbindungsverfahren mit Client-Gerät **106** abbrechen kann und Ressourcengerät **102** veranlassen kann, zusätzliche Anzeigedaten auszusenden, um Erkennungsverfahren mit anderen über Netzwerk **126** betriebenen Geräten einzuleiten.

[0120] Alternativ hierzu, falls Client-Gerät **106** feststellt, dass die ersten und zweiten Werte der symmetrischen kryptographischen Schlüssel übereinstimmen, kann Client-Gerät **106** eine Identität des Ressourcengerätes **102** verifizieren, und kann eine sichere direkte Verbindung mit Ressourcengerät **102** über Netzwerk **126** herstellen. Anhand des Verifizierens der Identität von Ressourcengerät **102** (z. B., dass Client-Gerät **106** eine Verbindung mit dem richtigen Gerät herstellt), kann Client-Gerät **106** in gewissen Aspekten gewährleisten, dass kein Angreifer oder böswillige Drittpartei einen Mann-in-the-Middle-Angriff versucht. Des Weiteren können die von Client-Gerät **106** und Ressourcengerät **102** berechneten ersten und zweiten Werte der symmetrischen kryptographischen Schlüssel in einigen Aspekten Sitzungsschlüssel **403** aufweisen, welche zukünftige Kommunikationen zwischen Client-Gerät **106** und Ressourcengerät **102** über die hergestellte direkte drahtlose Verbindung verschlüsseln können, einschließlich derjenigen Kommunikationen, welche Client-Gerät **106** befähigen, in Übereinstimmung mit dem gespeicherten lokalen Zugriffstoken auf eine oder mehrere Funktionen des Ressourcengerätes **102** zuzugreifen.

[0121] In gewissen Aspekten kann Client-Gerät **106** über die hergestellte drahtlose Verbindung eine Anfrage, auf eine oder mehrere Funktionen von Res-

sourcengerät **102** zuzugreifen (z. B. lokale Lokalzugriffsanfragedaten **404**) an Ressourcengerät **102** übertragen. Client-Gerät **106** kann zum Beispiel Daten beinhalten, die den angeforderten lokalen Zugriff identifizieren (z. B. Umfang, Art und/oder Dauer des Zugriffs), und kann des Weiteren eine Kopie des gespeicherten lokalen Zugriffstokens beinhalten. Ressourcengerät **102** kann Lokalzugriffsanfragedaten **404** empfangen (und gegebenenfalls entschlüsseln), und kann Lokalzugriffsanfragedaten **404** analysieren, um das lokale Zugriffstoken und die den angeforderten Zugriff identifizierenden Daten zu erhalten. In einigen Aspekten kann Ressourcengerät **102** die Gültigkeit des lokalen Zugriffstokens und seiner angezeigten Autorisierungskette feststellen, und kann des Weiteren bestimmen, ob der angeforderte lokale Zugriff mit den in den lokalen Zugriffstokens inbegriffenen Zugriffsparametern (z. B. in einen oder mehrere Schutzvorbehalte des lokalen Zugriffstokens durch Computersystem **108** integriert) konsistent ist.

[0122] Beispielsweise, wie zuvor beschrieben, kann Computersystem **108** das lokale Zugriffstoken basierend auf einer Erweiterung eines von Ressourcengerät **102** erzeugten und unterhaltenen Master-Zugriffstokens erzeugen. In gewissen Aspekten kann Ressourcengerät **102** eine Schutzvorbehalt-Sequenz aus der empfangenen Kopie des lokalen Zugriffstokens (welches z. B. die Zugriffsparameter definieren kann, die die lokalen Zugriffsprivilegien von Client-Gerät **106** definieren) extrahieren, und einen MAC-Algorithmus auf die extrahierte Schutzvorbehalt-Sequenz und das Master-Zugriffstoken (z. B. von Ressourcengerät **102** erzeugt und gespeichert) anwenden, um eine gerätespezifische Kopie des lokalen Zugriffstokens zu erzeugen.

[0123] Falls die empfangenen und gerätespezifischen Kopien der lokalen Zugriffstoken übereinstimmen (z. B. die Tags der empfangenen und gerätespezifischen Kopien der lokalen Zugriffstoken stimmen überein), kann Ressourcengerät **102** die Gültigkeit der empfangenen Kopie des lokalen Zugrifftokens feststellen. In gewissen Aspekten, und in Reaktion auf die festgestellte Gültigkeit, kann Ressourcengerät **102** bestimmen, ob der von Client-Gerät **106** angeforderte Zugriff mit dem von Eigentümergerät **104** gewährten Zugriff konsistent ist, beispielsweise wie in den Zugriffsparametern der extrahierten Schutzvorbehalt-Sequenzen spezifiziert.

[0124] Beispielsweise kann Ressourcengerät **102** die von Client-Gerät **106** empfangene Zugriffsanfrage analysieren, um die eine oder die mehreren angeforderten Funktionen zu identifizieren, sowie des Weiteren eine von Client-Gerät **106** erforderte Rolle zwecks Zugriffs auf die angeforderten Funktionen zu bestimmen oder zu identifizieren. Des Weiteren, wie zuvor beschrieben, kann Ressourcengerät **102** basierend auf der extrahierten Schutzvorbehalt-Sequenz bestimmen, dass das lokale Zugriffstoken noch nicht abgelaufen ist (z. B. dass das in den Zugriffsparametern spezifizierte Ablaufdatum noch nicht eingetreten ist). Ressourcengerät **102** kann ebenfalls eine Client-Gerät **106** zugewiesene Rolle oder Privilegienstufe identifizieren (z. B. basierend auf einer in den Zugriffsparametern spezifizierten Rolle), und kann eine oder mehrere Client-Gerät **106** seitens Eigentümergerät **104** auferlegte zusätzliche Restriktionen identifizieren (z. B. zeitliche Restriktionen, Restriktionen der Zugriffsart, Restriktionen des Offline-Gebrauchs und der subsequenten Delegierung, usw.).

[0125] In gewissen Aspekten kann Ressourcengerät **102** bestimmen, ob die seitens Client-Gerät **106** erforderte Rolle zwecks Zugriffs auf die angeforderten Funktionen mit der Client-Gerät **106** zugewiesenen Rolle (z. B. von Eigentümergerät **104**) konsistent ist, und des Weiteren, ob die angeforderten Funktionen mit der einen oder den mehreren von Eigentümergerät **104** auferlegten Restriktionen konsistent ist. Falls der angeforderte Zugriff mit der zugewiesenen Rolle und den auferlegten Restriktionen konsistent ist, kann Ressourcengerät **102** die festgestellte Konsistenz anzeigende Daten und eine Bestätigung des angeforderten Zugriffs erzeugen (z. B. Zugriffsbestätigungsdaten **405**) und diese über Netzwerk **126** an Client-Gerät **106** übertragen, und Ressourcengerät **102** kann Client-Gerät **106** den angeforderten Zugriff gewähren (z. B. gewährter Zugriff **406**). Alternativ hierzu, falls Ressourcengerät **102** den angeforderten Zugriff als inkonsistent mit der zugewiesenen Rolle und/oder den auferlegten Restriktionen erachtet, kann Ressourcengerät **102** eine Fehlermeldung (in **Fig.** 4 nicht abgebildet) erzeugen und über Netzwerk **126** an Client-Gerät **106** übertragen (z. B. welche Client-Gerät **106** veranlassen kann, den angeforderten Zugriff zu modifizieren). Client-Gerät **106** und Ressourcengerät **102** können sodann zusätzliche Daten austauschen, die den Zugriff von Client-Gerät **106** auf Ressourcengerät **102** ermöglichen.

[0126] **Fig.** 5 ist ein Flussdiagramm eines exemplarischen Verfahrens **500** zur Zugriffsgewährung auf ein Ressourcengerät, in Übereinstimmung mit den offenbarten Ausführungsformen. In gewissen Aspekten kann ein Ressourcengerät (z. B. Ressourcengerät **102**) die Schritte des exemplarischen Verfahrens **500** durchführen, welches Ressourcengerät **102** befähigen kann, eine sichere und direkte drahtlose Verbindung mit einem Zugriff anfordernden Client-Gerät (z. B. Client-Gerät **106**) herzustellen, und Client-Gerät **106**, basierend auf einem lokalen Zugriffstoken (z. B. ein lokales Zugriffstoken), welches Ressourcengerät **102** seitens Client-Gerät **106** über eine direkte drahtlose Verbindung präsentiert wurde, Zugriff gewähren.

[0127] In einigen Aspekten kann Ressourcengerät **102** Vorgänge durchführen, welche, in Verbindung mit von Client-Gerät **106** durchgeführten Verifizierungsvorgängen, unter Verwendung beliebiger der zuvor beschriebenen exemplarischen Techniken eine sichere und direkte drahtlose Verbindung zwischen Ressourcengerät **102** und Client-Gerät **106** über Netzwerk **126** herstellen kann (z. B. in Schritt **502**). Falls beispielsweise, wie zuvor beschrieben, ein Client-spezifischer Wert eines symmetrischen kryptographischen Schlüssels (z. B. ein von Client-Gerät **106** berechneter) einem gerätespezifischen Wert des symmetrischen kryptographischen Schlüssels (z. B. einem von Ressourcengerät **102** berechneten) entspricht, können Client-Gerät **106** und Ressourcengerät **102** kollektiv die sichere und direkte drahtlose Verbindung über Netzwerk **126** herstellen (z. B. in Schritt **502**). Des Weiteren können Client-Gerät **106** und Ressourcengerät **102** ebenfalls kollektiv Client-spezifische und gerätespezifische Werte des symmetrischen kryptographischen Schlüssels als Sitzungsschlüssel (z. B. Sitzungsschlüssel **403** der **Fig.** 4) festlegen, mit denen Client-Gerät **106** und Ressourcengerät **102** subsequente Kommunikationen über die sichere direkte drahtlose Verbindung verschlüsseln können (z. B. wie in Schritt **502** festgelegt).

[0128] In einigen Aspekten kann Ressourcengerät **102** über die hergestellte drahtlose Verbindung von Client-Gerät **106** eine Anfrage auf Zugriff auf eine oder mehrere Funktionen von Ressourcengerät **102** (z. B. Lokalzugriffsanfragedaten **404** der **Fig.** 4) empfangen (z. B. in Schritt **504**). In einigen Aspekten kann die empfangene Anfrage Daten beinhalten, die den angeforderten lokalen Zugriff identifizieren (z. B. Umfang, Art und/oder Dauer des Zugriffs), und kann des Weiteren eine Kopie des gespeicherten lokalen Zugriffstokens beinhalten.

[0129] Ressourcengerät **102** kann die empfangene Anfrage analysieren, um mindestens einen Teil des lokalen Zugriffstokens und der den angeforderten Zugriff identifizierenden Daten zu erhalten, und kann in einigen Aspekten die Gültigkeit des lokalen Zugriffstokens und seiner angezeigten Autorisierungskette bestimmen (z. B. in Schritt **506**). Beispielsweise, wie zuvor beschrieben, kann Computersystem **108** das lokale Zugriffstoken basierend auf einer Erweiterung eines von Ressourcengerät **102** erzeugten und unterhaltenen Master-Zugriffstokens erzeugen. Ressourcengerät **102** kann in gewissen Aspekten eine Schutzvorbehalt-Sequenz aus dem empfangenen Teil des lokalen Zugriffstokens (z. B. welches die Zugriffsparameter definieren kann, die die lokalen Zugriffsprivilegien von Client-Gerät **106** definieren können) extrahieren, und einen MAC-Algorithmus auf die extrahierten Schutzvorbehalt-Sequenz und das Master-Zugriffstoken (z. B. von Ressourcengerät **102** erzeugte und gespeicherte) anwenden, um eine gerätespezifische Kopie des lokalen Zugriffstokens zu berechnen. Des Weiteren kann Ressourcengerät **102** die Gültigkeit des lokalen Zugriffstokens bestimmen (und somit bestimmen, dass der empfangene Teil von einem gültigen Token abgeleitet ist, welches Zugriff auf Ressourcengerät **102** autorisiert), basierend auf einem Vergleich der empfangenen und berechneten Kopien des lokalen Zugriffstokens (z. B. ein Vergleich der Tags der empfangenen und berechneten Kopien des lokalen Zugriffstokens in Macaroon-Form). In gewissen Aspekten kann Ressourcengerät **102** konfiguriert sein, die Gültigkeit des empfangenen lokalen Zugriffstokens basierend auf lokal gespeicherten Daten, ohne Kommunikation mit Computersystem **108** über Netzwerk **122**, zu bestimmen.

[0130] Falls Ressourcengerät **102** bestimmt, dass die empfangene Kopie des lokalen Zugriffstokens mit der berechneten Kopie des lokalen Zugriffstokens nicht übereinstimmt (z. B. Schritt **506**; NEIN) kann Ressourcengerät **102** die Ungültigkeit des lokalen Zugriffstokens anzeigende Fehlerdaten erzeugen, und diese Fehlerdaten an Client-Gerät **106** übertragen (z. B. in Schritt **508**). Das exemplarische Verfahren **500** endet dann in Schritt **510**.

[0131] Falls das Ressourcengerät jedoch eine Übereinstimmung zwischen den empfangenen und berechneten Kopien des lokalen Zugriffstokens feststellt (z. B. Schritt **506**; JA), kann Ressourcengerät **102** festlegen, dass der empfangene Teil des lokalen Zugriffstokens von einem gültigen Token abgeleitet ist, und somit die Gültigkeit des lokalen Zugriffstokens festlegen (z. B. in Schritt **512**). In gewissen Aspekten, und in Reaktion auf die festgestellte Gültigkeit, kann Ressourcengerät **102** bestimmen, ob der von Client-Gerät **106** angeforderte Zugriff mit dem von Eigentümergerät **104** gewährten Zugriff konsistent ist, z. B. wie in den Zugriffsparametern der extrahierten Schutzvorbehalt-Sequenz definiert (z. B. in Schritt **514**).

[0132] Beispielsweise kann in Schritt **514** Ressourcengerät **102** die von Client-Gerät **106** empfangene Zugriffsanfrage analysieren, um die eine oder die mehreren angeforderten Funktionen zu identifizieren, sowie des Weiteren eine von Client-Gerät **106** erforderte Rolle zwecks Zugriffs auf die angeforderten Funktionen zu bestimmen oder zu identifizieren. Des Weiteren kann Ressourcengerät **102** basierend auf Teilen der Schutzvorbehalt-Sequenz bestimmen, dass das lokale Zugriffstoken noch nicht abgelaufen ist (z. B. dass das in den Zugriffsparametern spezifizierte Ablaufdatum noch nicht eingetreten ist). In Schritt **514** kann Ressourcengerät **102** ebenfalls eine Client-Gerät **106** zugewiesene Rolle oder Privilegienstufe identifizieren (z. B. basierend auf einer in den Zugriffsparametern spezifizierten Rolle), und kann eine oder mehrere Client-Gerät **106** seitens Eigentümergerät **104** auferlegte zusätzliche Restriktionen

identifizieren (z. B. zeitliche Restriktionen, Restriktionen der Zugriffsart, Restriktionen des Offline-Gebrauchs und der subsequenten Delegierung, usw.).

[0133] In gewissen Aspekten kann Ressourcengerät **102** in Schritt **516** bestimmen, ob die seitens Client-Gerät **106** erforderte Rolle zwecks Zugriffs auf die angeforderten Funktionen mit der Client-Gerät **106** zugewiesenen Rolle konsistent ist (z. B. von Eigentümergerät **104**), und des Weiteren, ob die angeforderten Funktionen mit den zusätzlichen von Eigentümergerät **104** auferlegten Beschränkungen oder Restriktionen konsistent sind (z. B. innerhalb der Zugriffsparameter). Falls Ressourcengerät **102** bestimmt, dass die erforderte Rolle mit der zugewiesenen Rolle inkonsistent ist (z. B. erfordern die angeforderten Funktionen eine „Manager"-Rolle, das Eigentümergerät wies Client-Gerät **106** die Rolle eines „Benutzers" zu) und/oder die angeforderten Funktionen mit den auferlegten Beschränkungen und Restriktionen inkonsistent sind (z. B. Schritt **516**; NEIN), kann Ressourcengerät **102** zu Schritt **518** zurückgehen, und kann eine Fehlermeldung erzeugen und diese über Netzwerk **126** an Client-Gerät **106** übertragen. Das exemplarische Verfahren **500** endet dann in Schritt **510**.

[0134] Alternativ hierzu, falls Ressourcengerät **102** feststellt, dass die erforderte Rolle mit der zugewiesenen Rolle konsistent ist, und dass die angeforderten Funktionen mit den auferlegten Beschränkungen und Restriktionen konsistent sind (z. B. Schritt **516**; JA), kann Ressourcengerät **102** die festgestellte Konsistenz anzeigende Daten und eine Bestätigung des angeforderten Zugriffs erzeugen (z. B. Zugriffsbestätigungsdaten **405** der **Fig.** 4) und diese über Netzwerk **126** an Client-Gerät **106** übertragen (z. B. in Schritt **518**). Ressourcengerät **102** kann Client-Gerät **106** den angeforderten Zugriff gewähren, und kann zusätzliche Daten austauschen, welche den Zugriff von Client-Gerät **106** auf die angeforderten Funktionen ermöglichen (z. B. in Schritt **520**). Das exemplarische Verfahren **500** endet dann in Schritt **510**.

[0135] Eine oder mehrere der offenbarten Ausführungsformen verwendend, kann ein Gerät oder eine Einheit, das/die Eigentümer(in) von Ressourcengerät **102** ist oder dieses kontrolliert (z. B. Eigentümergerät **104**), den Zugriff auf Ressourcengerät **102** mit einem oder mehreren Client-Geräten teilen (z. B. über Client-Gerät **106**). Wie zuvor beschrieben, kann Eigentümergerät **104** über Netzwerk **122** Kommunikationen mit Computersystem **108** herstellen, und kann Daten bereitstellen, welche die eine oder die mehreren Einheiten mit Zugriffsprivilegien identifizieren (z. B. eine Gerätekennung von Client-Gerät **106**), sowie die diese Zugriffsprivilegien definierenden Beschränkungen und/oder Restriktionen spezifizieren. Die offenbarten Ausführungsformen erfordern jedoch weder eine direkte drahtlose Verbindung zwischen Eigentümergerät **104** und Client-Gerät **106** zwecks Ermöglichens einer Einräumung von Zugriffsrechten an Client-Gerät **106**, noch ist erforderlich, dass Client-Gerät **106** seine Identität gegenüber Eigentümergerät **104** verifiziert oder beweist. Des Weiteren kann Eigentümergerät **104** in gewissen zuvor beschriebenen Ausführungsformen sich selbst authentifizieren und Computersystem **108** gemeinsame Zugriffsprivilegien anzeigende Daten bereitstellen, unabhängig von Ressourcengerät **102** und Client-Gerät **106**, welche offline und/oder abgeschaltet sein können.

[0136] Des Weiteren, wie zuvor beschrieben, kann sich Client-Gerät **106** selbst gegenüber Computersystem **108** über Netzwerk **122** authentifizieren und Lokalgerät- und Zugriffstokens erhalten, welche den Zugriff von Client-Gerät **106** auf Ressourcengerät **102** ermöglichen (z. B. in Übereinstimmung mit den seitens Eigentümergerät **104** auferlegten Beschränkungen und/oder Restriktionen, die in eine von Computersystem **108** unterhaltene Zugriffskontrollliste (ACL) aufgenommen wurden). Obwohl Client-Gerät **106** zwecks Anforderns und Erhaltens dieser Tokens Kommunikationen mit Computersystem **108** über Netzwerk **122** herstellen kann, legen die offenbarten Ausführungsformen keine Erfordernisse bezüglich Ressourcengerät **102** und Eigentümergerät **104** fest, welche offline und ohne Verbindung zu Netzwerk **122** sein können, während Client-Gerät **106** Verfahren zum Anfordern und Erhalten dieser Token durchführt.

[0137] In zusätzlichen Aspekten können Client-Gerät **106** und Ressourcengerät **102** über Netzwerk **126** (z. B. ein Low-Energy(BLE)-Netzwerk) Daten austauschen, um den Zugriff von Client-Gerät **106** auf eine oder mehrere Funktionen von Ressourcengerät **102** zu verifizieren und herzustellen. Die offenbarten Ausführungsformen legen keinerlei Erfordernisse fest, dass Client-Gerät **106** und/oder Ressourcengerät **102** während der zuvor beschriebenen exemplarischen Verhandlungsverfahren mit Netzwerk **122** verbunden sein müssten; des Weiteren kann Ressourcengerät **102** die Gültigkeit des lokalen Zugriffstokens (z. B. wie von Client-Gerät **106** bereitgestellt) offline und ohne Kommunikationen mit Client-Gerät **106**, Eigentümergerät **104** und/oder Computersystem **108** bestimmen.

[0138] Des Weiteren, wie zuvor beschrieben, können das lokale Gerätauthentifizierungstoken und das lokale Zugriffstoken „kurzlebige" Token aufweisen, welche kurz nach Erzeugung durch Computergerät **108** ablaufen (z. B. Ablauf von dreißig Minuten, einer Stunde, einem Tag, usw. nach Erzeugung oder Prägung). In anderen Aspekten, und konsistent mit den offenbarten Ausführungsformen, kann Eigentümergerät **104** einem autorisierten Gerät (z. B. Client-Gerät **106**) Erlaubnis des Zugriffs auf Ressourcengerät **102** gewähren, während es offline und ohne Verbindung mit Netzwerk **122** ist. Beispielsweise

kann Computersystem **108** den Client-Gerät **106** gewährten Offline-Zugriff in einem Teil der Schutzvorbehaltsdaten eines entsprechenden lokalen Zugriffstokens spezifizieren (z. B. unter Verwendung beliebiger der zuvor beschriebenen exemplarischen Techniken). Zusätzlich kann Computersystem **108** in gewissen Ausführungsformen ein Ablaufdatum eines entsprechenden lokalen Zugriffstokens hinausschieben (z. B. Erzeugen eines „langlebigen" Tokens, welches Tage, Wochen oder Monate nach seiner Erzeugung durch Computersystem **108** abläuft), um den Zugriff von Client-Gerät **106** auf Ressourcengerät **102** zu ermöglichen.

[0139] In gewissen exemplarischen Ausführungsformen kann zusätzlich ein Benutzer eines Gerätes, dem von Eigentümergerät **104** Zugriff auf Ressourcengerät **102** gewährt wurde (z. B. ein Benutzer von Client-Gerät **106**), Inhaber eines Kontos eines von Computersystem **108** unterhaltenen Clouddienstes sein (z. B. ein GAIA™-Konto und/oder ein Google Cloud™-Konto), und eine Ressourcengerät **102** entsprechende Zugriffskontrollliste (ACL) kann den eingeräumten Zugriffsprivilegien des Clouddienst-Kontos zugeordnet werden. Die offenbarten Ausführungsformen sind jedoch nicht auf Verfahren zur Zugriffsgewährung für Inhaber von Clouddienst-Konten beschränkt, und in weiteren Ausführungsformen kann Eigentümergerät **104** Zugriffskontrolldaten übertragen, die einem autorisierten Gerät Zugriffsprivilegien gewähren und einen Out-of-Band-Kommunikationsmechanismus identifizieren, seitens eines Benutzers des autorisierten Geräts, welcher auf die Lokalgerät- und Zugriffstokens zugreifen kann, wie zuvor beschrieben. Beispielsweise kann ein Out-of-Band-Kommunikationsmechanismus in nicht einschränkender Form eine Email-Adresse oder -konto, ein Handle in einem Social-Media-Netzwerk (z. B. Facebook™, Twitter™, Google+™, usw.), ein Handle in einem Chat-Netzwerk oder Messaging-Dienst (z. B. einen WhatsApp™-Benutzernamen) und eine Telefonnummer, die zum Empfangen von SMS- und MMS-Textnachrichten geeignet ist, beinhalten.

[0140] In gewissen Aspekten, konsistent mit den offenbarten Ausführungsformen, kann Computersystem **108** Daten aufnehmen, die den Out-of-Band-Kommunikationsmechanismus identifizieren, im Teil der entsprechenden ACL. Nach Erzeugung der lokalen Geräte- und/oder Zugriffstokens (z.B. unter Verwendung beliebiger der zuvor beschriebenen exemplarischen Techniken), kann Computersystem **108** den Out-of-Band-Kommunikationsmechanismus anhand des Teils der ACL identifizieren, kann eine URL erzeugen, die Client-Gerät **106** befähigt, auf die lokalen Geräte- und/oder Zugriffstokens zuzugreifen und diese lokal zu speichern, und kann die URL in Übereinstimmung mit dem Out-of-Band-Kommunikationsmechanismus an Client-Gerät **106** übertragen.

[0141] Zum Beispiel kann der Benutzer von Client-Gerät **106** die URL aktivieren (z. B. durch Berühren, Anklicken, usw. auf einer Anzeigeeinheit von Client-Gerät **106**), und Client-Gerät **106** kann Kopien der lokalen Geräte- und/oder Zugriffstokens erhalten. In anderen Fällen können von Client-Gerät **106** ausgeführte Anwendungsprogramme (z. B. Croissant™ für Android™) die empfangene URL automatisch erkennen und die lokalen Geräte- und/oder Zugriffstokens ohne Benutzereingriff in den Hintergrund holen. In einigen Aspekten kann Computersystem **108** über Out-of-Band-Kommunikationsmechanismen abgerufenen lokalen Geräte- und/oder Zugriffstokens zusätzliche Restriktionen auferlegen, einschließlich kürzerer Gültigkeitsdauer und Begrenzungen auf eine bestimmte Anzahl an Zugriffsversuchen durch Client-Gerät **106**.

[0142] Des Weiteren kann Ressourcengerät **102** in gewissen Aspekten nicht über Netzwerk **122** mit Computersystem **108** verbunden sein (z. B. beruhend auf einer Abmeldung des Eigentümers), und kann zusätzlich oder alternativ nicht in der Lage sein, auf Netzwerk **122** zuzugreifen (was z. B. bei Niedrigenergie-Geräten wie Smart Locks usw. auftreten kann). Ohne Zugriff auf Netzwerk **122** kann Ressourcengerät **102** unfähig sein, Zugriffskontrollentscheidungen an Computersystem **108** zu delegieren, und kann des Weiteren unfähig sein, Master-Geräte- und/oder Zugriffstokens in System **1908** zu speichern oder anzufordern, das Computersystem **108** zusätzliche auf den Master-Geräte- und/oder Zugriffstokens basierende lokale Tokens prägt.

[0143] In zusätzlichen Ausführungsformen, ohne Zugriff auf Netzwerk **122**, kann Ressourcengerät **102** Zugriffskontrollentscheidungen an Eigentümergerät **104** delegieren (und zusätzlich oder alternativ an ein weiteres von Eigentümergerät **104** spezifiziertes Gerät), und Eigentümergerät **104** kann Kopien der Master-Geräte- und/oder Zugriffstokens unterhalten (z. B. über Netzwerk **124** übertragen, im Anschluss an die zuvor beschriebenen Erkennungsverfahren). In zusätzlichen Aspekten kann Eigentümergerät **104** Zugriffskontrolllisten festlegen, unterhalten und/oder aktualisieren, Anfragen von Client-Gerät **106** auf Zugriff auf das Ressourcengerät empfangen, und des Weiteren unter Verwendung beliebiger der zuvor beschriebenen exemplarischen Verfahren lokale Geräte- und/oder Zugriffstokens erzeugen oder prägen.

[0144] Die offenbarten Ausführungsformen können beispielsweise Eigentümergerät **104** befähigen, die geprägten lokalen Geräte- und/oder Zugriffstokens mit autorisierten Geräten (z. B. Client-Gerät **106**) unter Verwendung beliebiger geeigneter Out-of-Band-Kommunikationsmechanismen zu teilen. Zum Beispiel kann Eigentümergerät **104** die gespeicherten lokalen Geräte- und/oder Zugriffstokens repräsentierende BLOBs und/oder URLs erzeugen, und kann die

BLOBs und/oder URLs unter Verwendung beliebiger Out-of-Band-Kommunikationskanäle (z. B. Textnachricht, Email-Nachricht, direkte Chat-Nachricht, Social-Media-Messaging, usw.) übertragen. Client-Gerät **106** kann die BLOBs und/oder URLs empfangen, und kann die empfangenen BLOBs und/oder URLs verarbeiten, um die Lokalgerät- und/oder Zugriffstokens zu erhalten und in einem lokalen Speicher oder Datenpool zu speichern (z. B. mittels Benutzereingriffs oder programmgesteuert). Die offenbarten Ausführungsformen können die BLOBs und/oder URLs über unverschlüsselte Out-of-Band-Kommunikationskanäle übertragen, und somit dem zugrundeliegenden Transportmechanismus implizit vertrauen.

[0145] Des Weiteren, in gewissen zuvor beschriebenen Ausführungsformen, delegiert Ressourcengerät **102** Zugriffskontrollentscheidungen an Computersystem **108** (welches z. B. einen Clouddienst unterhält, beispielsweise Google Cloud™), welches auf starke Cloud-basierte Authentifizierung zurückgreift. In anderen Aspekten, und konsistent mit den offenbarten Ausführungsformen, kann Ressourcengerät **102** diese Zugriffskontrollentscheidungen an eine Drittpartei delegieren, welche die Master-Geräte- und/oder Zugriffstokens (z. B. von Ressourcengerät **102** empfangene) speichern kann, und welche neue beschränktere Tokens erzeugen kann und diese über verschiedene Transporte, unter Verwendung beliebiger der zuvor beschriebenen exemplarischen Verfahren, teilen kann. In gewissen Aspekten kann die Drittpartei-Authentifizierungsinstanz Kontrolle über Tokenerzeugung, Token-Lebensdauer und Token-Umfang ausüben.

[0146] Eine Anzahl exemplarischer Ausführungsformen wurde beschrieben. Dennoch ist zu verstehen, dass unterschiedliche Modifikationen vorgenommen werden können, ohne vom Gedanken und Umfang der Offenbarung abzuweichen. Beispielsweise können verschiedene Formen der dargestellten Abläufe verwendet werden, wobei Schritte in anderer Reihenfolge stattfinden, hinzugefügt oder entfernt werden können.

[0147] Ausführungsformen und sämtliche in dieser Beschreibung beschriebenen funktionsfähigen Operationen können in einer digitalen elektronischen Schaltung, oder in Computer-Software, Computer-Firmware, oder Computer-Hardware, darunter auch in aus dieser Beschreibung hervorgehenden Strukturen und deren strukturellen Äquivalenten, oder in Kombinationen einer oder mehrerer derselben, implementiert werden. Ausführungsformen können als ein oder mehrere Computerprogramm-Produkte implementiert werden, d. h. als ein oder mehrere Module mit Computerprogrammbefehlen, die auf einem computerlesbaren Medium kodiert sind, um dann von einem Datenverarbeitungsgerät ausgeführt zu werden, bzw. den Betrieb desselben zu steuern. Das computerlesbare Medium kann ein maschinenlesbares Speichergerät, ein maschinenlesbares Speichersubstrat, ein Speichergerät, eine ein maschinenlesbares propagiertes Signal betreffende Zusammensetzung, oder eine Kombination aus einem oder mehreren dieser sein. Das computerlesbare Medium kann ein nicht-flüchtiges computerlesbares Medium sein. Der Begriff „Datenverarbeitungsgerät“ umfasst sämtliche Geräte, Apparate und Maschinen zur Verarbeitung von Daten, wie z. B. einen programmierbaren Prozessor, einen Computer oder mehrere Prozessoren oder Computer. Das Gerät kann, zusätzlich zur Hardware, Code enthalten, der eine Ausführungsumgebung für das entsprechende Computerprogramm, wie z. B. Maschinencode in Prozessorfirmware, einen Protokollstapel, ein Datenbankverwaltungssystem, ein Betriebssystem oder eine Kombination aus einem oder mehrerer derselben, erstellt. Ein propagiertes Signal ist ein künstlich erzeugtes Signal, wie beispielsweise ein maschinenerzeugtes elektrisches, optisches oder elektromagnetisches Signal, welches erzeugt wird, um Informationen zur Übertragung an ein geeignetes Empfängergerät zu kodieren.

[0148] Ein Computerprogramm (das auch als Programm, Software, Softwareanwendung, Modul, Softwareanwendung, Script oder Code bezeichnet oder beschrieben werden kann) kann in jeder Form von Programmiersprache, darunter auch in kompilierten oder interpretierten Sprachen geschrieben, und in beliebiger Form, wie z. B. als allein lauffähiges Programm oder als Modul, Komponente, Subroutine, oder als eine andere, für den Einsatz in einer Computerumgebung geeignete Einheit bereitgestellt werden. Ein Computerprogramm entspricht nicht zwangsläufig einer Datei in einem Dateisystem. Ein Programm kann in einem Teil einer Datei gespeichert werden, das andere Programme oder Daten enthält (wie z. B. eine oder mehrere Skripte, die in einem Auszeichnungssprachen-Dokument gespeichert werden), in einer einzelnen dem betreffenden Programm gewidmeten Datei, oder in mehreren koordinierten Dateien (wie beispielsweise Dateien, die ein oder mehrere Module, Teilprogramme oder Maschinencode-Abschnitte enthalten), gespeichert werden. Ein Computerprogramm kann auf einem Computer oder auf mehreren Computern bereitgestellt und ausgeführt werden, die sich an einem Standort befinden oder über mehrere Standorte verteilt und durch ein Kommunikationsnetzwerk miteinander verbunden sind.

[0149] Die in dieser Beschreibung beschriebenen Prozesse und Logikabläufe können von einem oder mehreren programmierbaren Prozessoren ausgeführt werden, die ein oder mehrere Computerprogramme ausführen, die durch den auf Eingabedaten basierenden Betrieb und das Erzeugen von Ausgabedaten bestimmte Funktionen aktivieren. Die Pro-

zesse und Logikabläufe können auch durch eine vorhabensgebundene Logikschaltung, wie z.B. einen FPGA (Universalschaltkreis) oder einen ASIC (anwendungs-spezifischen integrierten Schaltkreis) ausgeführt und das Gerät in Form derselben implementiert werden.

[0150] Die für die Ausführung eines Computerprogramms geeigneten Prozessoren können beispielsweise allgemeine oder spezielle Mikroprozessoren oder jegliche andere Art Prozessoren von jeglicher Art von digitalem Computer beinhalten. In der Regel empfängt eine zentrale Verarbeitungseinheit Befehle und Daten von einem Nur-Lese-Speicher oder einem Direktzugriffsspeicher oder auch von beiden. Die wesentlichen Bestandteile eines Computers sind ein Prozessor zum Durchführen von Befehlen, sowie eine oder mehrere Speichergeräte zum Speichern von Befehlen und Daten. In der Regel enthält ein Computer eine oder mehrere Massenspeichergeräte zum Speichern von Daten, wie z. B: magnetische, magneto-optische oder optische Festplatten bzw. wird operativ gekoppelt, um Daten von denselben zu empfangen oder auf dieselben zu übertragen. Ein Computer muss jedoch nicht über solche Geräte verfügen. Darüber hinaus kann ein Computer in ein anderes Gerät, wie beispielsweise einen Tablet-Computer, ein Mobiltelefon, einen persönlichen digitalen Assistenten (PDA), einen mobilen Audio-Player, einen globalen Positionsbestimmungssystem(GPS)-Empfänger, um nur einige zu nennen, integriert sein. Zu den computerlesbaren zum Speichern von Computerprogrammbefehlen und Daten geeigneten Medien gehören sämtliche Arten von nichtflüchtigen Speichern, Medien und Speichergeräten, einschließlich Halbleiterspeicherelemente, wie beispielsweise EPROM, EEPROM und Flash-Speichergeräte; magnetische Festplatten, wie z.B. interne Festplatten oder Wechselplatten; magneto optische Festplatten; und CD-ROM- und DVD-ROM-Laufwerke. Der Prozessor und der Speicher können durch eine vorhabensgebundene Logikschaltung ergänzt oder in dieselbe integriert werden.

[0151] Um die Interaktion mit einem Benutzer zu ermöglichen, können Ausführungsformen zum Anzeigen von Informationen auf einem Computer mit einem Anzeigegerät, wie z. B. einem CRT-(Kathodenstrahlröhren), einem LCD-(Flüssigkristallanzeige)-Monitor, einer Touchscreen-Anzeige, einschließlich einer Tastatur und einem Zeigegerät, wie z. B. einer Maus oder einem Trackball implementiert werden, mit denen der Benutzer den Computer bedienen kann. Es können auch andere Gerätearten verwendet werden, um die Interaktion mit einem Benutzer zu ermöglichen; zum Beispiel kann es sich bei der Rückmeldung an den Benutzer um jegliche Art von sensorischer Rückmeldung, wie z.B. eine visuelle, akustische, oder taktile Rückmeldung handeln; auch die Eingabe des Benutzers kann in beliebiger Form, also auch akustisch, sprachlich oder taktil empfangen werden.

[0152] Die Ausführungsformen können in einem Computersystem implementiert werden, das eine Back-End-Komponente, wie z. B. einen Datenserver oder eine Middleware-Komponente, wie z. B. einen Anwendungsserver oder eine Front-End-Komponente, wie z. B. einen Client-Computer mit einer grafischen Benutzeroberfläche oder eine beliebige Kombination einer oder mehrerer der besagten Back-End-, Middleware- oder Front-End-Komponenten oder einen Web-Browser enthält, durch den ein Benutzer mit einer Ausführungsform der offenbarten Techniken interagieren kann. Die Komponenten des Systems können durch eine beliebige Form oder ein beliebiges Medium digitaler Datenkommunikation, wie z.B. ein Kommunikationsnetzwerk miteinander verbunden werden. Zu Kommunikationsnetzwerken zählen beispielsweise lokale Netzwerke („LAN“) und Großraumnetzwerke („WAN“), wie z.B. das Internet.

[0153] Das Computersystem kann aus Clients und Servern bestehen. Client und Server sind generell voneinander entfernt und interagieren in der Regel über ein Kommunikationsnetzwerk. Die Beziehung von Client und Server ergibt sich durch Computerprogramme, die auf den jeweiligen Computern ausgeführt werden und eine Client-Server-Beziehung zueinander haben.

[0154] Des Weiteren, für Situationen, in denen die hier erörterten Systeme persönliche Informationen über Benutzer sammeln oder persönliche Informationen nutzen können, kann den Benutzern die Möglichkeit eingeräumt werden, zu kontrollieren, ob Programme oder Merkmale Benutzerinformationen sammeln (z. B. Informationen über das soziale Netzwerk eines Benutzers, soziale Aktionen oder Aktivitäten, Beruf, Präferenzen eines Benutzers oder der aktuelle Standort eines Benutzers), oder um zu steuern, ob und/oder wie man Inhalte vom Content-Server empfängt, die für den Benutzer relevanter sein können. Außerdem können bestimmte Daten auf eine oder mehrere Arten anonymisiert werden, bevor sie gespeichert oder verwendet werden, sodass persönlich identifizierbare Informationen entfernt werden. Beispielsweise kann die Identität eines Benutzers so anonymisiert werden, dass keine persönlich identifizierbaren Informationen für den Benutzer bestimmt werden können, oder ein geografischer Standort eines Benutzers kann verallgemeinert werden, wo Standortinformationen empfangen werden, beispielsweise für eine Stadt, eine Postleitzahl oder eine Landesebene, sodass ein bestimmter Standort eines Benutzers nicht bestimmt werden kann. Somit kann der Benutzer Kontrolle darüber haben, wie Informationen über ihn oder sie gesammelt und von einem Content-Server verwendet werden.

[0155] Obwohl diese Beschreibung viele Details enthält, sollten diese nicht als Einschränkungen, sondern vielmehr als Beschreibungen von spezifischen Merkmalen bestimmter Ausführungsformen ausgelegt werden. Bestimmte Merkmale, die innerhalb dieser Beschreibung im Zusammenhang mit separaten Ausführungsformen beschrieben werden, können auch in Kombination in einer einzelnen Ausführungsform implementiert werden. Umgekehrt können verschiedene Merkmale, die im Zusammenhang mit einer einzelnen Ausführungsform beschrieben werden, auch in mehreren Ausführungsformen separat oder in einer geeigneten Teilkombination implementiert werden. Außerdem können, auch wenn die Merkmale weiter oben gegebenenfalls als in bestimmten Kombinationen wirkend beschrieben und sogar zunächst als solche beansprucht werden, in einigen Fällen ein oder mehrere Merkmale einer beanspruchten Kombination aus der Kombination herausgeschnitten und die beanspruchte Kombination auf eine Teilkombination oder eine Variante einer Teilkombination gerichtet werden.

[0156] Gleichermaßen sollte, obwohl die Vorgänge in den Zeichnungen in einer bestimmten Reihenfolge dargestellt sind, dies nicht so verstanden werden, dass die besagten Vorgänge in der dargestellten Reihenfolge oder in fortlaufender Reihenfolge durchgeführt werden müssen, oder dass alle veranschaulichten Vorgänge durchgeführt werden, um die erwünschten Ergebnisse zu erzielen. Unter bestimmten Umständen können Multitasking und Parallelverarbeitung von Vorteil sein. Darüber hinaus sollte die Trennung verschiedener Systemkomponenten in den oben beschriebenen Ausführungsformen nicht als erforderlich ausgelegt werden, auch gilt es zu verstehen, dass die beschriebenen Programmkomponenten und Systeme im Allgemeinen in einem einzelnen Softwareprodukt oder in mehreren Softwareprodukten gebündelt integriert werden können.

[0157] Somit wurden bestimmte Ausführungsformen beschrieben. Weitere Ausführungsformen liegen innerhalb des Schutzumfangs der folgenden Patentansprüche. So können beispielsweise die in den Patentansprüchen angegebenen Aktionen in einer anderen Reihenfolge durchgeführt werden und dennoch die erwünschten Ergebnisse erzielen.

[0158] **Fig.** 6 ist ein Blockdiagramm von Computergeräten **600**, **650**, die zur Implementierung von in diesem Dokument beschriebenen Systemen und Verfahren verwendet werden können, sowohl als Client, als auch als Server, oder als Vielzahl von Servern. Computergerät **600** soll verschiedene Formen digitaler Computer darstellen, wie z. B. Laptops, Desktops, Workstations, persönliche digitale Assistenten, Server, Blade-Server, Großrechner und sonstige geeignete Computer. Computergerät **650** soll verschiedene Formen mobiler Geräte darstellen, z. B. persönliche digitale Assistenten, Mobiltelefone, Smartphones und sonstige, ähnliche Computer. Zusätzlich kann Computergerät **600** oder **650** Universal-Serial-Bus(USB)-Speichermedien beinhalten. Die USB-Speichermedien können Betriebssysteme und andere Anwendungen speichern. Die USB-Speichermedien können Eingabe/Ausgabekomponenten beinhalten, beispielsweise einen Drahtlossender oder einen USB-Anschluss, der in den USB-Port eines anderen Computergerätes eingefügt werden kann. Die hierin dargestellten Komponenten, ihre Verbindungen und Beziehungen und ihre Funktionen haben lediglich exemplarischen Charakter und sind nicht dazu bestimmt, die Implementierungen der in diesem Dokument beschriebenen und/oder beanspruchten Erfindungen zu beschränken.

[0159] Computergerät **600** beinhaltet einen Prozessor **602**, einen Speicher **604**, ein Speichergerät **606**, eine Hochgeschwindigkeitsschnittstelle **608**, die mit dem Speicher **604** verbunden ist, sowie Hochgeschwindigkeits-Erweiterungsports **610** und eine langsame Schnittstelle **612**, die mit einem langsamen Bus **614** und dem Speichergerät **606** verbunden ist. Jede der Komponenten **602**, **604**, **606**, **608**, **610** und **612** sind unter Verwendung mehrerer Busse miteinander verbunden und können auf einem gemeinsamen Motherboard oder auf andere Weise entsprechend montiert werden. Der Prozessor **602** kann Anweisungen zur Ausführung innerhalb des Computergeräts **600** verarbeiten, einschließlich Anweisungen, die im Speicher **604** oder auf dem Speichergerät **606** gespeichert sind, um graphische Informationen für eine GUI auf einem externen Eingabe-/Ausgabegerät, wie beispielsweise die an Hochgeschwindigkeitsschnittstelle **608** gekoppelte Anzeige **616**, anzuzeigen. In anderen Ausführungen können, je nach Eignung, mehrere Prozessoren bzw. mehrere Busse gemeinsam mit mehreren Speichern und Speichertypen verwendet werden. Außerdem können mehrere Computergeräte **600** verbunden sein, wobei jedes Gerät Teile der notwendigen Operationen bereitstellt (z. B. als Serverbank, eine Gruppe von Blade-Servern oder ein Mehrprozessorsystem).

[0160] Der Speicher **604** speichert Informationen im Computer **600**. In einer Implementierung ist der Speicher **604** eine flüchtige Speichereinheit oder Einheiten. In einer Implementierung ist der Speicher **604** eine nicht-flüchtige Speichereinheit oder Einheiten. Der Speicher **604** kann auch eine andere Form von computerlesbarem Medium sein, wie z. B. eine magnetische oder optische Platte.

[0161] Das Speichergerät **606** ist dazu geeignet, Massenspeicherung für das Computergerät **600** bereitzustellen. In einer Implementierung kann das Speichergerät **606** ein computerlesbares Medium sein oder ein solches enthalten, wie z. B. ein Diskettenlaufwerk, eine Festplatte, ein optisches Lauf-

werk oder ein Bandlaufwerk, einen Flash-Speicher oder sonstige ähnliche Festspeichergeräte oder eine Anordnung solcher Geräte, darunter auch Geräte in einem Speichernetzwerk (Storage Area Network) oder sonstige Konfigurationen. Ein Computerprogrammprodukt kann konkret in einem Informationsträger ausgeführt sein. Das Computerprogrammprodukt kann auch Anweisungen enthalten die, wenn sie ausgeführt werden, eine oder mehrere Methoden wie die oben beschriebene ausführen. Der Informationsträger ist ein computer- oder maschinenlesbares Medium, beispielsweise der Speicher **604**, das Speichergerät **606** oder der Speicher auf dem Prozessor **602**.

[0162] Der Hochgeschwindigkeits-Controller **608** verwaltet bandbreitenintensive Operationen für den Computer **600**, während der langsame Controller **612** Operationen verwaltet, die weniger bandbreitenintensiv sind. Diese Zuweisung von Funktionen ist lediglich exemplarisch. In einigen Implementierungen ist die Hochgeschwindigkeitssteuerung **608** mit dem Speicher **604**, der Anzeige **616** (z. B. durch einen Grafikprozessor oder Beschleuniger) und die Hochgeschwindigkeits-Erweiterungsports **610** verbunden, die verschiedene Erweiterungskarten (nicht gezeigt) aufnehmen können. In der Implementierung ist der langsame Controller **612** mit Speichergerät **606** und dem langsamen Erweiterungsport **614** verbunden. Der langsame Erweiterungsport, der verschiedene Kommunikationsports einschließen kann (z. B. USB, Bluetooth, Ethernet, Wireless Ethernet), kann mit einem oder mehreren Eingabe-/ Ausgabegeräten verbunden sein, wie z. B. einer Tastatur, einem Zeigegerät, einem Scanner oder einem Netzwerkgerät, wie z. B. einem Switch oder Router, z. B. über einen Netzwerkadapter.

[0163] Der Computer **600** kann in einer Vielzahl verschiedener Formen ausgeführt werden, wie in der Abbildung gezeigt. So kann er beispielsweise als ein Standardserver **620** oder mehrfach in einer Gruppe derartiger Server implementiert werden. Er kann auch als Teil eines Rack-Serversystems **624** implementiert werden. Außerdem kann er in einem Personal Computer ausgeführt werden, z. B. in einem Laptopcomputer **622**. Alternativ können Komponenten des Computergerätes **600** mit anderen Komponenten in einem mobilen Gerät (nicht gezeigt) kombiniert werden, beispielsweise Gerät **650**. Jedes dieser Geräte kann eines oder mehrere der Computergeräte **600**, **650** enthalten, und es kann ein ganzes System aus mehreren miteinander kommunizierenden Computergeräten **600**, **650** aufgebaut werden.

[0164] Computergerät **650** beinhaltet einen Prozessor **652**, einen Speicher **664**, ein Eingabe-/Ausgabegerät, wie z. B. eine Anzeige **654**, eine Kommunikationsschnittstelle **666** und einen Transceiver **668**, neben anderen Komponenten. Das Gerät **650** kann auch mit einem Speichergerät ausgestattet sein, beispielsweise einem Micro-Drive oder sonstigem Gerät, um zusätzliche Speichermöglichkeiten zu bieten. Jede der Komponenten **650**, **652**, **664**, **654**, **666** und **668** sind unter Verwendung mehrerer Busse miteinander verbunden, und mehrere der Komponenten können auf einem gemeinsamen Motherboard oder auf andere Weise entsprechend montiert werden.

[0165] Der Prozessor **652** kann Anweisungen in Computergerät **650** ausführen, einschließlich solcher Anweisungen, die im Speicher **664** gespeichert sind. Der Prozessor kann als Chipset aus Chips implementiert werden, die separate und mehrere analoge und digitale Prozessoren enthalten. Zusätzlich kann der Prozessor unter Verwendung einer beliebigen Anzahl an Architekturen implementiert werden. Beispielsweise kann der Prozessor **410** ein CISC(Complex Instruction Set Computers)-Prozessor, ein RISC (Reduced Instruction Set Computer)-Prozessor, oder ein MISC(Minimal Instruction Set Computer)-Prozessor sein. Der Prozessor kann zum Beispiel die anderen Komponenten des Gerätes **650** koordinieren, beispielsweise die Steuerung der Benutzeroberflächen, Anwendungen, die auf Gerät **650** ausgeführt werden, und Drahtloskommunikation durch Gerät **650**.

[0166] Prozessor **652** kann mit einem Benutzer durch eine Kontrollschnittstelle **658** und eine Anzeigeschnittstelle **656**, die mit der Anzeige **654** verbunden ist, kommunizieren. Die Anzeige **654** kann z. B. eine TFT (Thin-Film-Transistor Liquid Crystal Display) Anzeige oder eine OLED (Organic Light Emitting Diode) Anzeige oder eine sonstige geeignete Anzeigetechnologie sein. Die Anzeigeschnittstelle **656** kann geeignete Schaltungen zum Betrieb der Anzeige **654** enthalten, damit dem Benutzer grafische und sonstige Informationen angezeigt werden können. Die Kontrollschnittstelle **658** kann Befehle von einem Benutzer entgegennehmen, und diese in Anweisungen für den Prozessor **652** übersetzen. Außerdem kann eine externe Schnittstelle **662** die Kommunikation mit Prozessor **652** ermöglichen, damit Gerät **650** mit anderen Geräten in seiner unmittelbaren Umgebung kommunizieren kann. Die externe Schnittstelle **662** kann beispielsweise in einigen Implementierungen die drahtgebundene Kommunikation ermöglichen, oder in anderen Implementierungen die drahtlose Kommunikation, und es können auch mehrere Schnittstellen verwendet werden.

[0167] Der Speicher **664** speichert Informationen im Computer **650**. Der Speicher **664** kann in Form eines oder mehrerer computerlesbarer Medien, einer oder mehrerer flüchtiger Speichereinheiten oder einer oder mehrerer nicht-flüchtiger Speichereinheiten ausgeführt werden. Es kann auch Erweiterungsspeicher **674** bereitgestellt und mit Gerät **650** über Erweiterungsschnittstelle **672** verbunden werden, die zum Beispiel eine Schnittstelle für SIMM-Karten (Single In

Line Memory Module) enthalten kann. Besagter Erweiterungsspeicher **674** kann zusätzlichen Speicherplatz für Gerät **650** bereitstellen, oder auch Anwendungen oder sonstige Informationen für Gerät **650** speichern. Insbesondere kann Erweiterungsspeicher **674** Anweisungen enthalten, die die oben beschriebenen Verfahren ausführen oder ergänzen, und kann darüber hinaus auch sichere Informationen enthalten. Somit kann Erweiterungsspeicher **674** beispielsweise als Sicherheitsmodul für Gerät **650** ausgeführt sein, und kann mit Anweisungen programmiert werden, die den sicheren Gebrauch des Computergerätes **650** ermöglichen. Außerdem können über die SIMM-Karten sichere Anwendungen bereitgestellt werden, zusammen mit zusätzlichen Informationen, wie z. B. die Ablage von Informationen zur Identifizierung auf der SIMM-Karte in einer Weise, die nicht gehackt werden kann.

[0168] Der Speicher kann beispielsweise Flash-Speicher und NVRAM-Speicher beinhalten, wie weiter unten dargelegt. In einer Implementierung kann ein Computerprogrammprodukt konkret in einem Informationsträger ausgeführt sein. Das Computerprogrammprodukt enthält Anweisungen die, wenn sie ausgeführt werden, eine oder mehrere Methoden ausführen, wie z. B. die oben beschriebenen. Der Informationsträger ist ein computer- oder maschinenlesbares Medium, beispielsweise der Speicher **664**, der Erweiterungsspeicher **674** oder der Speicher auf Prozessor **652**, welche zum Beispiel über Transceiver **668** oder externe Schnittstelle **662** empfangen werden können.

[0169] Gerät **650** kann drahtlos über Kommunikationsschnittstelle **666** kommunizieren, die gegebenenfalls eine digitale Signalverarbeitungsschaltung beinhalten kann. Kommunikationsschnittstelle **666** kann Kommunikationen in verschiedenen Modi und Protokollen ermöglichen, unter anderem beispielsweise GSM-Sprachanrufe, SMS, EMS oder MMS-Messaging, CDMA, TDMA, PDC, WCDMA, CDMA2000 oder GPRS. Solche Kommunikation kann beispielsweise über den Radiofrequenz-Transceiver **668** erfolgen. Außerdem kann die Kommunikation auf kurze Distanz erfolgen, beispielsweise mithilfe eines Bluetooth-, WiFi- oder sonstigen Transceivers (nicht gezeigt). Außerdem kann GPS(Global Positioning System)-Empfängermodul **670** drahtlos zusätzliche Navigations- und Ortungsdaten an Gerät **650** senden, die je nach Eignung durch Anwendungen verwendet werden können, die auf Gerät **650** ausgeführt werden.

[0170] Gerät **650** kann mithilfe eines Audio-Codecs **660** auch akustisch kommunizieren, das gesprochene Informationen von einem Benutzer empfangen und diese in nutzbare digitale Informationen umwandeln kann. Audio-Codec **660** kann auch für einen Benutzer hörbare Signale erzeugen, beispielsweise über einen Lautsprecher, z. B. in einem Hörer des Gerätes **650**. Solche Tonsignale können Tonsignale von Sprachanrufen sein, Tonaufnahmen (z. B. Sprachnachrichten, Musikdateien, usw.) und können darüber hinaus Tonsignale enthalten, die von Anwendungen erzeugt werden, die auf Gerät **650** ausgeführt werden.

[0171] Der Computer **650** kann in einer Vielzahl verschiedener Formen ausgeführt werden, wie in der Abbildung gezeigt. Zum Beispiel kann er als Mobiltelefon **680** ausgeführt werden. Er kann auch als Teil eines Smartphones **682**, eines persönlichen digitalen Assistenten oder eines sonstigen, ähnlichen mobilen Gerätes ausgeführt werden.

[0172] Verschiedene Ausführungen der hier beschriebenen Systeme und Techniken können in digitalen elektronischen Schaltungen, integrierten Schaltkreisen, speziell konstruierten ASICs (Application Specific Integrated Circuits), Computerhardware, Firmware, Software und/oder in Kombinationen davon ausgeführt werden. Diese verschiedenen Ausführungen können die Ausführung in einem oder mehreren Computerprogrammen beinhalten, die auf einem programmierbaren System mit mindestens einem programmierbaren Prozessor ausgeführt bzw. interpretiert werden können, der entweder speziell oder für allgemeine Zwecke bestimmt ist, und der mit einem Speichersystem verbunden ist, um von dort Daten und Anweisungen zu empfangen und sie dorthin zu senden, mit mindestens einem Eingabegerät und mindestens einem Ausgabegerät.

[0173] Diese Computerprogramme (die auch als Programme, Software, Softwareanwendungen oder Code bezeichnet werden) beinhalten Maschinenanweisungen für einen programmierbaren Prozessor, und können in einer prozeduralen und/oder objektorientierten Programmiersprache auf hohem Niveau und/oder in Assembly-/Maschinensprache ausgeführt werden. Die hier verwendeten Begriffe „maschinenlesbares Medium“ „computerlesbares Medium“ beziehen sich auf jedes Computerprogrammprodukt, jeden Apparat und/oder jedes Gerät (z. B. Magnetplatten, optische Platten, Speicher, programmierbare Logic Devices (PLDs)), die dazu verwendet werden, Maschinenanweisungen und/oder Daten an einen programmierbaren Prozessor zu senden, einschließlich eines maschinenlesbaren Mediums, das Maschinenanweisungen als maschinenlesbares Signal entgegennimmt. Der Begriff „maschinenlesbares Signal“ bezieht sich auf jedes Signal, das dazu verwendet wird, Maschinenanweisungen und/oder Daten an einen programmierbaren Prozessor zu senden.

[0174] Um die Interaktion mit einem Benutzer zu ermöglichen, können die hier dargestellten Systeme und Techniken auf einem Computer mit einem Anzei-

gegerät umgesetzt werden (z. B. einem CRT-(Kathodenstrahlröhren) oder LCD-(Flüssigkristallanzeige)-Monitor, einschließlich einer Tastatur und eines Zeigegerätes (z. B. einer Maus oder eines Trackballs), mit denen der Benutzer Eingaben in den Computer vornehmen kann. Es können auch andere Geräte verwendet werden, um die Interaktion mit einem Benutzer zu ermöglichen; zum Beispiel kann es sich bei der Rückmeldung an den Benutzer um jegliche Art von sensorischer Rückmeldung handeln (z. B. visuelle, akustische oder taktile Rückmeldung); auch die Eingaben des Benutzers können in beliebiger Form empfangen werden, d. h. auch akustisch, sprachlich oder taktil.

[0175] Die hier beschriebenen Systeme und Techniken können in einem Computersystem umgesetzt werden, das eine Backend-Komponente enthält (z. B. einen Datenserver) oder eine Middleware-Komponente (z. B. einen Anwendungsserver) oder eine Frontend-Komponente (z. B. einen Client-Computer mit einer grafischen Benutzeroberfläche oder einen Web-Browser, durch den der Benutzer mit einer hier dargestellten Umsetzung des Gegenstandes interagieren kann), oder eine beliebige Kombination solcher Backend-, Middleware- oder Frontend-Komponenten. Die Komponenten des Systems können durch eine beliebige Form oder ein beliebiges Medium digitaler Datenkommunikation verbunden sein (z. B. ein Kommunikationsnetzwerk). Zu Kommunikationsnetzwerken zählen beispielsweise lokale Netzwerke („LAN“), Großraumnetzwerke („WAN“), Peer-to-Peer-Netzwerke (mit Ad-Hoc- oder statischen Mitgliedern), Netzrechnerinfrastrukturen und das Internet.

[0176] Das Computersystem kann aus Clients und Servern bestehen. Client und Server sind generell voneinander entfernt und interagieren in der Regel über ein Kommunikationsnetzwerk. Die Beziehung von Client und Server ergibt sich durch Computerprogramme, die auf den jeweiligen Computern ausgeführt werden und eine Client-Server-Beziehung zueinander haben.

[0177] Eine Anzahl an Ausführungsformen der Erfindung wurde beschrieben. Dennoch ist zu verstehen, dass unterschiedliche Modifikationen vorgenommen werden können, ohne vom Gedanken und Umfang der Erfindung abzuweichen. Beispielsweise können verschiedene Formen der dargestellten Abläufe verwendet werden, wobei Schritte in anderer Reihenfolge stattfinden, hinzugefügt oder entfernt werden können. Ebenfalls sollte erkannt werden, dass, obwohl mehrere Anwendungen zur Authentifizierung eines lokalen Gerätes beschrieben wurden, zahlreiche andere Anwendungen vorgesehen sind. Dementsprechend liegen weitere Ausführungsformen innerhalb des Schutzumfangs der folgenden Patentansprüche.

Schutzansprüche

1. Vorrichtung, umfassend:
mindestens einen Prozessor; und
einen Speicher, der ausführbare Anweisungen speichert, die bei Ausführung durch den mindestens einen Prozessor den mindestens einen Prozessor zum Durchführen der folgenden Schritte veranlassen:
das Erhalten eines Master-Zugrifftokens für ein Ressourcengerät;
das Identifizieren eines einem Client-Gerät zugeordneten Benutzers;
das Bestimmen, dass der Benutzer autorisiert wurde, beschränkten Zugriff auf das Ressourcengerät zu erhalten;
das Erzeugen, in Reaktion auf die Bestimmung, eines auf dem Master-Gerätetoken basierenden lokalen Zugriffstokens, wobei das lokale Zugriffstoken konfiguriert ist, Zugriff auf das Ressourcengerät zu gewähren, ohne dass eine Netzwerkverbindung des Ressourcengerätes erforderlich ist;
das Bereitstellen des lokalen Zugriffstokens für das Ressourcengerät an das Client-Gerät.

2. Vorrichtung nach Anspruch 1, wobei der mindestens eine Prozessor des Weiteren den Schritt des Bestimmens durchführt, dass der Benutzer mindestens entweder von einem Eigentümer des Ressourcengerätes oder einer zur Zugriffskontrolle des Ressourcengerätes befähigten Instanz autorisiert wurde, beschränkten Zugriff auf das Ressourcengerät zu erhalten.

3. Vorrichtung nach Anspruch 1 oder Anspruch 2, wobei der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Empfangen einer Anfrage vom Client-Gerät, beschränkten Zugriff auf das Ressourcengerät zu erhalten, die Anfrage mindestens eine Kennung des Benutzers oder eine Kennung des Client-Gerätes umfassend; und
das Bereitstellen, in Reaktion auf die Anfrage, des lokalen Zugriffstokens für das Ressourcengerät an das Client-Gerät.

4. Vorrichtung nach Anspruch 3, wobei der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Identifizieren des Client-Gerätes, basierend auf mindestens einem Teil der empfangenen Anfrage;
das Bestimmen, dass das Client-Gerät autorisiert wurde, den beschränkten Zugriff auf das Ressourcengerät zu erhalten; und
das Erzeugen des lokalen Zugriffstokens in Reaktion auf die Bestimmung, dass das Client-Gerät autorisiert wurde, beschränkten Zugriff zu erhalten.

5. Vorrichtung nach Anspruch 1, wobei der mindestens eine Prozessor des Weiteren den Schritt des Erhaltens einer Zugriffskontrollliste für das Ressourcengerät durchführt, wobei die Zugriffskontrollliste einen oder mehreren Benutzer identifiziert, die autorisiert sind, entsprechende beschränkte Zugriffe auf das Ressourcengerät zu erhalten.

6. Vorrichtung nach Anspruch 5, wobei die Vorrichtung konfiguriert ist, die Zugriffskontrollliste in einem lokalen Speicher zu speichern.

7. Vorrichtung nach Anspruch 5 oder Anspruch 6, wobei der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Bestimmen, basierend auf der Zugriffskontrollliste, dass der eine oder die mehreren autorisierten Benutzer den dem Client-Gerät zugeordneten Benutzer beinhalten; und
das Festlegen, in Reaktion auf das Bestimmen, dass der eine oder die mehreren autorisierten Benutzer den Benutzer beinhalten, dass der Benutzer des Client-Gerätes autorisiert wurde, beschränkten Zugriff zu erhalten.

8. Vorrichtung nach irgendeinem der Ansprüche 5 bis 7, wobei der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Empfangen von Zugriffskontrolldaten von einem Eigentümergerät, wobei das Eigentümergerät einem Eigentümer des Ressourcengerätes zugeordnet ist und die Zugriffskontrolldaten den Benutzer autorisieren, den beschränkten Zugriff auf das Ressourcengerät zu erhalten; und
das Modifizieren von mindestens einem Teil der Zugriffskontrollliste, um den Benutzer des Client-Gerätes als autorisierten Benutzer zu identifizieren.

9. Vorrichtung nach Anspruch 8, wobei:
die Zugriffskontrolldaten Zugriffskontrollparameter umfassen, und die Zugriffsparameter einen Umfang des dem Benutzer gewährten beschränkten Zugriffs festlegen; und
der mindestens eine Prozessor des Weiteren den Schritt des Modifizierens von mindestens einem Teil der Zugriffskontrollliste zwecks Einbeziehens der Zugriffsparameter durchführt.

10. Vorrichtung nach Anspruch 9, wobei die Zugriffsparameter mindestens, alternativ oder kumulativ, eine dem Benutzer zugewiesene Rolle, eine zeitliche Restriktion, eine Restriktion einer Zugriffsart, eine Restriktion des Offline-Zugriffs oder eine Restriktion der Fähigkeit des Client-Gerätes zur Erzeugung von Tokens umfassen.

11. Vorrichtung nach Anspruch 5, wobei die Zugriffskontrollliste mindestens einen oder mehrere dem Benutzer zugeordnete Zugriffsparameter identifiziert, und die Zugriffsparameter mindestens, alternativ oder kumulativ, eine dem Benutzer zugewiesene Rolle, eine zeitliche Restriktion, eine Restriktion einer Zugriffsart, eine Restriktion des Offline-Zugriffs oder eine Restriktion der Fähigkeit des Client-Gerätes zur Erzeugung von Tokens umfassen.

12. Vorrichtung nach Anspruch 11, wobei:
das lokale Zugriffstoken ein Macaroon umfasst, und das Macaroon einen oder mehrere Schutzvorbehalte und einen entsprechenden Schlüssel umfasst; und
der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Identifizieren, basierend auf der Zugriffskontrollliste, der dem Benutzer zugeordneten Zugriffsparameter;
das Festlegen eines Ablaufzeitpunktes für das lokale Zugriffstoken; und
das Durchführen von Vorgängen, die den Ablaufzeitpunkt und die identifizierten Zugriffsparameter in den einen oder die mehreren Schutzvorbehalte des lokalen Zugriffstokens einbeziehen.

13. Vorrichtung nach Anspruch 12, wobei der mindestens eine Prozessor des Weiteren den Schritt des Modifizierens von mindestens einem Teil der Zugriffskontrollliste zwecks Einbeziehens des für das lokale Zugriffstoken des Benutzers festgelegten Ablaufzeitpunktes durchführt.

14. Vorrichtung nach irgendeinem der Ansprüche 1 bis 7, wobei:
das lokale Zugriffstoken Daten zum Identifizieren mindestens des dem Client-Gerät zugeordneten Benutzers oder des Client-Gerätes umfasst; und
der mindestens eine Prozessor des Weiteren den Schritt des Anwendens einer digitalen Signatur auf das lokale Zugriffstoken umfasst.

15. Vorrichtung nach Anspruch 14 wobei:
das lokale Zugriffstoken ein Macaroon umfasst, und das Macaroon einen oder mehrere Schutzvorbehalte und einen entsprechenden Schlüssel umfasst;
der entsprechende Schlüssel die angewandte digitale Signatur umfasst; und
der mindestens eine Prozessor des Weiteren den Schritt des Erzeugens der digitalen Signatur, basierend auf einer Anwendung eines MAC-Algorithmus auf mindestens einen Teil des einen oder der mehreren Schutzvorbehalte, durchführt.

16. Vorrichtung nach Anspruch 15, wobei der eine oder die mehreren Schutzvorbehalte mindestens, alternativ oder kumulativ, ein Ablaufdatum des Tokens, eine dem Benutzer zugewiesene Rolle oder die Daten zum Identifizieren mindestens des Benutzers oder des Client-Gerätes umfassen.

17. Vorrichtung nach irgendeinem der Ansprüche 22 bis 35, wobei das lokale Zugriffstoken ein digitales Zertifikat umfasst.

18. Vorrichtung nach irgendeinem der Ansprüche 1 bis 7, wobei der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Empfangen des Master-Zugriffstokens vom Ressourcengerät; und
das Erzeugen des lokalen Zugriffstokens, basierend auf mindestens einem Teil des empfangenen Master-Zugriffstokens.

19. Vorrichtung nach Anspruch 18, wobei:
das Master-Zugriffstoken ein erstes Macaroon umfasst, und das erste Macaroon einen oder mehrere erste Schutzvorbehalte und einen entsprechenden Schlüssel umfasst; und
das lokale Zugriffstoken ein zweites Macaroon umfasst, und das zweite Macaroon einen oder mehrere zweite Schutzvorbehalte und einen entsprechenden Schlüssel umfasst; und
das mindestens eine Verfahren des Weiteren den Schritt des Erzeugens des einen oder der mehreren zweiten Schutzvorbehalte durchführt, ein erster Teil der zweiten Schutzvorbehalte die ersten Schutzvorbehalte umfassend, ein zweiter Teil der zweiten Schutzvorbehalte ein Ablaufdatum des lokalen Zugriffstokens, und einen oder mehrere dem beschränkten Zugriff des Benutzers zugeordnete Zugriffsparameter umfassen, wobei die Zugriffsparemeter mindestens, alternativ oder kumulativ, eine dem Benutzer zugewiesene Rolle, eine zeitliche Restriktion, eine Restriktion einer Zugriffsart, eine Restriktion des Offline-Zugriffs oder eine Restriktion der Fähigkeit des Client-Gerätes zur Erzeugung von Tokens umfassen.

20. Vorrichtung nach Anspruch 1, wobei der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Empfangen eines Master-Gerätetokens vom Ressourcengerät, das Master-Gerätetoken das Client-Gerät befähigend, die Identität des Ressourcengerätes zu verifizieren;
das Erzeugen, in Reaktion auf das Bestimmen, eines lokalen Gerätetokens, basierend auf mindestens einem Teil des Master-Gerätetokens; und
das Bereitstellen des lokalen Gerätetokens an das Client-Gerät.

21. Konkretes, nicht-flüchtiges, computerlesbares Medium, welches Anweisungen speichert, die, bei Ausführung durch mindestens einen Prozessor einer Vorrichtung, ein Verfahren durchführen, das Verfahren umfassend:
das Erhalten eines Master-Zugrifftokens für ein Ressourcengerät;
das Identifizieren eines einem Client-Gerät zugeordneten Benutzers;
das Bestimmen, dass der Benutzer autorisiert wurde, beschränkten Zugriff auf das Ressourcengerät zu erhalten;
das Erzeugen, in Reaktion auf die Bestimmung, eines auf dem Master-Gerätetoken basierenden lokalen Zugriffstokens, wobei das lokale Zugriffstoken konfiguriert ist, Zugriff auf das Ressourcengerät zu gewähren, ohne dass eine Netzwerkverbindung des Ressourcengerätes zur Validierung des lokalen Zugriffstokens erforderlich ist;
das Bereitstellen des lokalen Zugriffstokens für das Ressourcengerät an das Client-Gerät.

22. Ressourcengerät, umfassend:
mindestens einen Prozessor; und
einen Speicher, der ausführbare Anweisungen speichert, die, bei Ausführung durch den mindestens einen Prozessor, den mindestens einen Prozessor zur Durchführung folgender Schritte veranlassen:
das Herstellen einer sicheren drahtlosen Verbindung mit einem Client-Gerät;
das Empfangen von Tokendaten, abgeleitet von einem Zugriffstoken des Client-Gerätes, und einer Zugriffsanfrage auf das Ressourcengerät vom Client-Gerät;
das Bestimmen, ohne über ein Netzwerk zu kommunizieren, dass die empfangenen Tokendaten abgeleitet sind von einem gültigen Token, welches den Zugriff auf das Ressourcengerät autorisiert;
das Bestimmen, ohne über das Netzwerk zu kommunizieren, dass das Zugriffstoken eine Zugriffsstufe autorisiert, welche ausreichend ist, den vom Client-Gerät angeforderten Zugriff einzuräumen; und
das Einräumen, in Reaktion auf das Bestimmen, dass die empfangenen Tokendaten von einem gültigen Token abgeleitet sind, und das Bestimmen, dass das Zugriffstoken eine Zugriffsstufe autorisiert, welche ausreichend ist, den vom elektronischen Gerät angeforderten Zugriff einzuräumen, des vom Client-Gerät angeforderten Zugriffs auf das Ressourcengerät.

23. Ressourcengerät nach Anspruch 22, wobei die sichere drahtlose Verbindung eine direkte drahtlose Verbindung zwischen dem Client-Gerät und dem Ressourcengerät umfasst.

24. Ressourcengerät nach Anspruch 23, wobei die direkte drahtlose Verbindung eine Bluetooth-Low-Energy(BLE)-Verbindung umfasst.

25. Ressourcengerät nach irgendeinem der Ansprüche 22 bis 24, wobei der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Empfangen von Schutzvorbehaltsdaten und Zufallsdaten vom Client-Gerät, wobei die Schutzvorbehaltsdaten durch das Client-Gerät von einem lokalen Gerätetoken extrahiert wurden;
das Berechnen eines Schlüsselwertes, basierend auf mindestens einem Teil der empfangenen Schutzvorbehaltsdaten und Zufallsdaten;
das Übertragen des ermittelten Schlüsselwertes an das Client-Gerät; und

das Herstellen der sicheren drahtlosen Verbindung mit dem Client-Gerät, basierend auf einer Übereinstimmung zwischen dem berechneten Schlüsselwert und einem zusätzlichen, durch das Client-Gerät basierend auf dem lokalen Gerätetoken berechneten Schlüsselwert.

26. Ressourcengerät nach Anspruch 25, wobei der mindestens eine Prozessor des Weiteren den Schritt des Festlegens des berechneten Schlüsselwertes als Sitzungsschlüssel durchführt.

27. Ressourcengerät nach Anspruch 25 oder Anspruch 26 wobei:
die Schutzvorbehaltsdaten und Zufallsdaten unter Verwendung eines gemeinsamen symmetrischen Schlüssels verschlüsselt werden; und
wobei der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Entschlüsseln der empfangenen Schutzvorbehaltsdaten und Zufallsdaten;
das Verschlüsseln des berechneten Schlüsselwertes unter Verwendung des gemeinsamen symmetrischen Schlüssels; und
das Übertragen des verschlüsselten Schlüsselwertes an das Client-Gerät.

28. Ressourcengerät nach irgendeinem der Ansprüche 22 bis 24, wobei das Zugriffstoken ein Macaroon umfasst, und das Macaroon einen oder mehrere Schutzvorbehalte und einen entsprechenden Schlüssel umfasst.

29. Ressourcengerät nach Anspruch 28, wobei der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Identifizieren des einen oder der mehreren Schutzvorbehalte vom Zugriffstoken;
das Berechnen einer Kopie der empfangenen Tokendaten basierend auf den extrahierten Schutzvorbehalten und einem vom Ressourcengerät unterhaltenen Master-Zugriffstoken;
das Bestimmen, dass die empfangenen Tokendaten der berechneten Kopie entsprechen; und
das Festlegen, dass die empfangenen Tokendaten von einem gültigen Token abgeleitet sind, wenn die empfangenen Tokendaten der berechneten Kopie entsprechen.

30. Ressourcengerät nach Anspruch 29, wobei der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Identifizieren einer Zugriffskette für das Zugriffstoken, basierend auf mindestens einem Teil Schutzvorbehaltextrakte; und
das Verifizieren der Zugriffskette für das empfangene Token.

31. Ressourcengerät nach irgendeinem der Ansprüche 28 bis 30, wobei:
der eine oder die mehreren Schutzvorbehalte ein Ablaufdatum des Zugriffstokens, eine dem Client-Gerät durch den Eigentümer des Ressourcengerätes zugewiesene Rolle, und ein oder mehrere Zugriffsparameter umfassen;
die Zugriffsparameter mindestens, alternativ oder kumulativ, eine zeitliche Restriktion, eine Restriktion einer Zugriffsart, eine Restriktion des Offline-Zugriffs oder eine Restriktion der Fähigkeit des Client-Gerätes zur Erzeugung von Tokens umfassen; und
die Zugriffsanfrage an das Ressourcengerät eine oder mehrere der vom Ressourcengerät angeforderten Funktionen identifiziert.

32. Ressourcengerät nach Anspruch 31. wobei der mindestens eine Prozessor des Weiteren folgende Schritte durchführt:
das Bestimmen, basierend auf dem Ablaufdatum, dass das Zugriffstoken nicht abgelaufen ist;
das Identifizieren einer vom Client-Gerät erforderten Rolle zwecks Zugriffs auf die angeforderten Funktionen des Ressourcengerätes;
das Bestimmen, dass die erforderte Rolle mit der zugewiesenen Rolle konsistent ist;
das Bestimmen, dass die eine oder die mehreren angeforderten Funktionen mit dem einen oder den mehreren Zugriffsparametern konsistent sind; und
das Festlegen, in Reaktion auf die Bestimmungen, dass (i) das Zugriffstoken nicht abgelaufen ist, (ii) die erforderte Rolle konsistent mit der zugewiesenen Rolle ist und (iii) eine oder mehrere angeforderte Funktionen mit dem einen oder den mehreren Zugriffsparametern konsistent sind, dass das Zugriffstoken eine Zugriffsstufe autorisiert, welche ausreichend ist, den angeforderten Zugriff einzuräumen

33. Ressourcengerät nach irgendeinem der Ansprüche 22 bis 32, wobei:
das Ressourcengerät die Zugriffskontrollentscheidungen mindestens an, alternativ oder kumulativ, ein einem Cloud-Server zugeordnetes Computersystem, einen Authentifizierungsdienst durch Dritte oder an ein Gerät des Eigentümers des Ressourcengerätes delegiert hat; und
mindestens das Computersystem, der Authentifizierungsdienst durch Dritte oder das Eigentümergerät erzeugten das Zugriffstoken und stellten das Zugriffstoken dem Client-Gerät bereit.

34. Ressourcengerät nach irgendeinem der Ansprüche 22 bis 33, wobei der mindestens eine Prozessor des Weiteren das Durchführen der Schritte des Festlegens, des Empfangens und des Bereitstellens, ohne hierbei über das Netzwerk zu kommunizieren, durchführt.

35. Konkretes, nicht-flüchtiges, computerlesbares Medium, welches Anweisungen speichert, die, bei Ausführung durch mindestens einen Prozessor einer

Vorrichtung, ein Verfahren durchführen, das Verfahren umfassend:
das Herstellen einer sicheren drahtlosen Verbindung mit einem Client-Gerät;
das Empfangen von Tokendaten, abgeleitet von einem Zugriffstoken des Client-Gerätes, und einer Zugriffsanfrage auf das Ressourcengerät vom Client-Gerät;
das Bestimmen, ohne über ein Netzwerk zu kommunizieren, dass die empfangenen Tokendaten abgeleitet sind von einem gültigen Token, welches den Zugriff auf das Ressourcengerät autorisiert;
das Bestimmen, ohne über das Netzwerk zu kommunizieren, dass das Zugriffstoken eine Zugriffsstufe autorisiert, welche ausreichend ist, den vom Client-Gerät angeforderten Zugriff einzuräumen; und
das Einräumen, in Reaktion auf das Bestimmen, dass die empfangenen Tokendaten von einem gültigen Token abgeleitet sind, und das Bestimmen, dass das Zugriffstoken eine Zugriffsstufe autorisiert, welche ausreichend ist, den vom Client-Gerät angeforderten Zugriff einzuräumen, des vom Client-Gerät angeforderten Zugriffs auf das Ressourcengerät.

Es folgen 6 Seiten Zeichnungen

Anhängende Zeichnungen

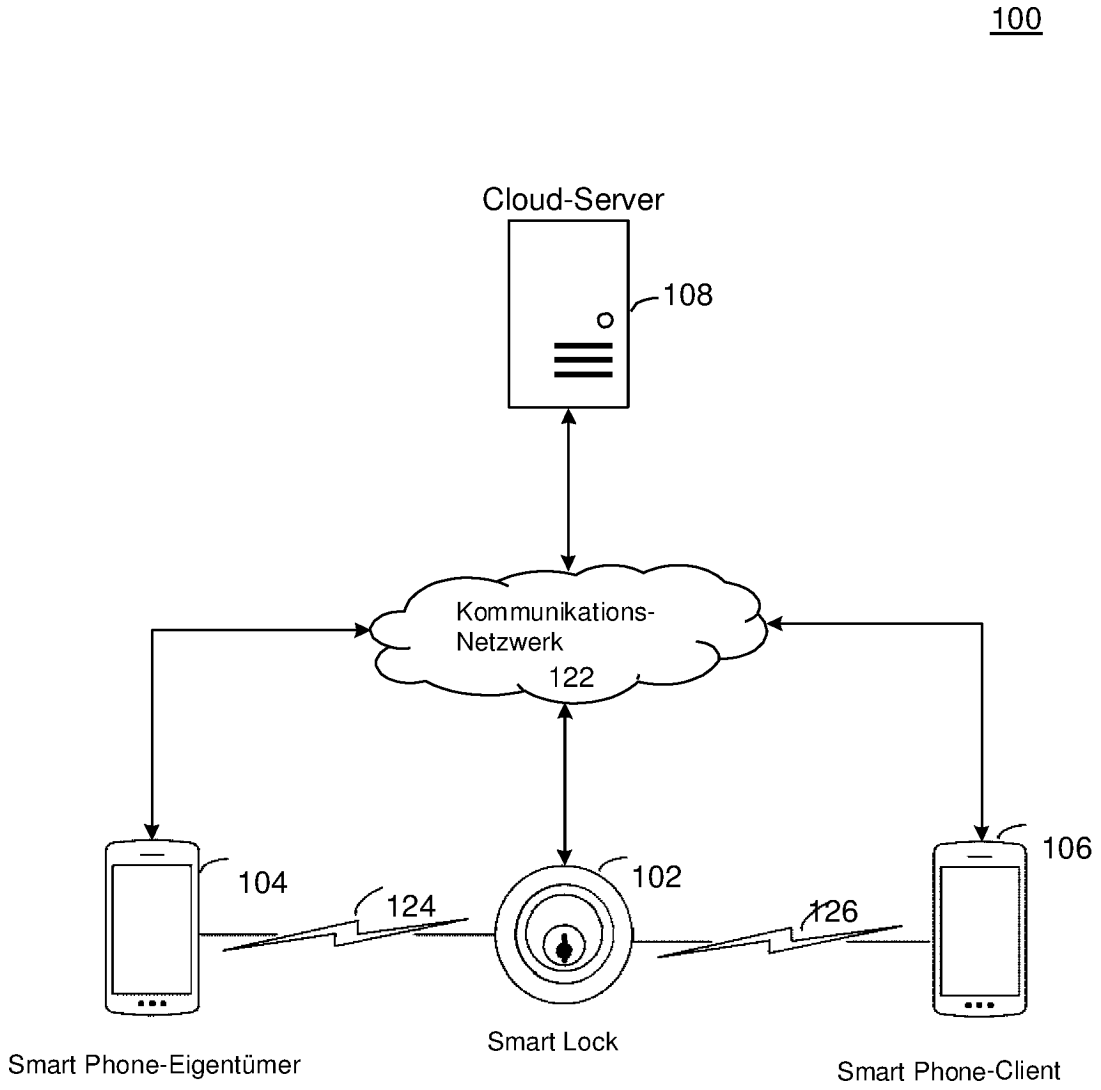


FIG. 1

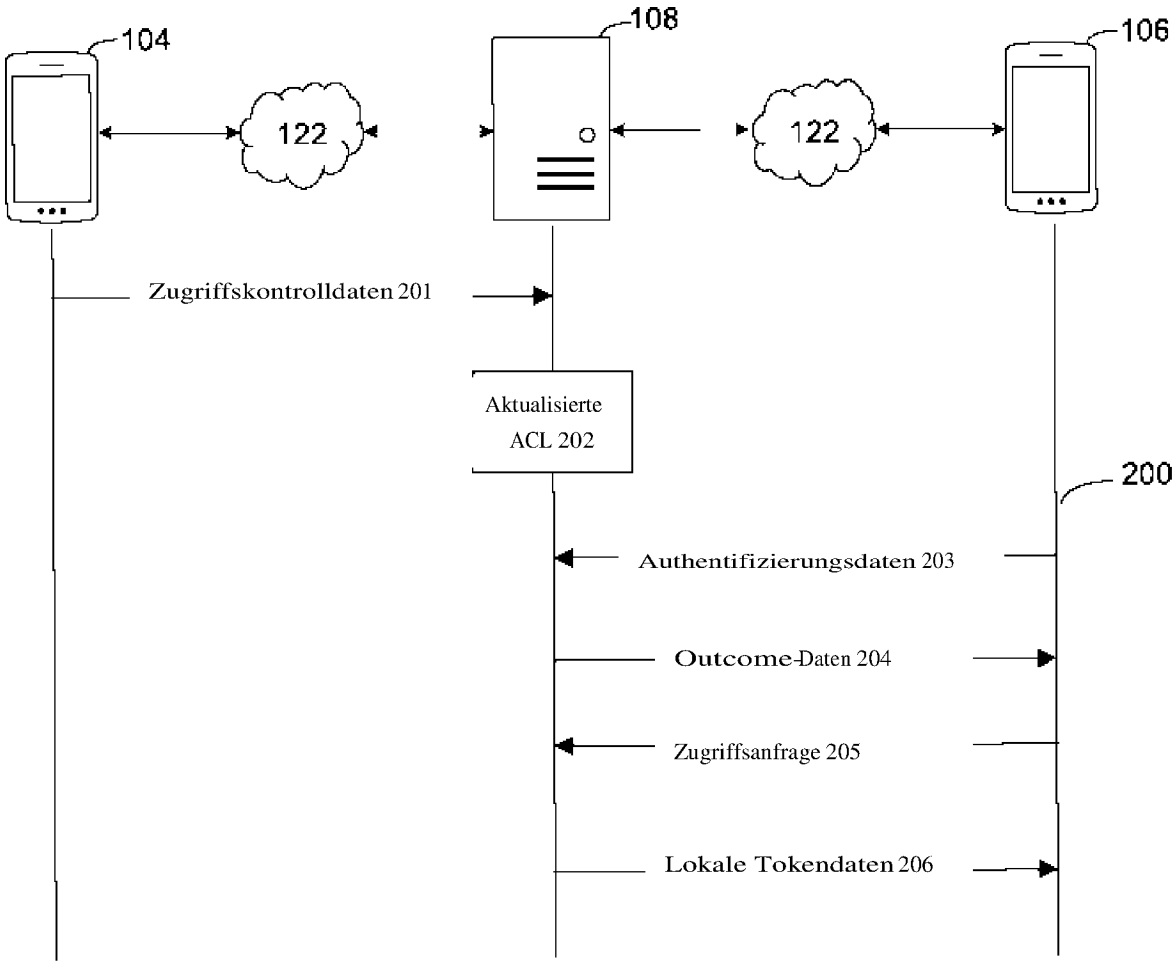

104
122
108
122
106
Zugriffskontrolldaten 201
Aktualisierte ACL 202
200
Authentifizierungsdaten 203
Outcome-Daten 204
Zugriffsanfrage 205
Lokale Tokendaten 206

FIG. 2

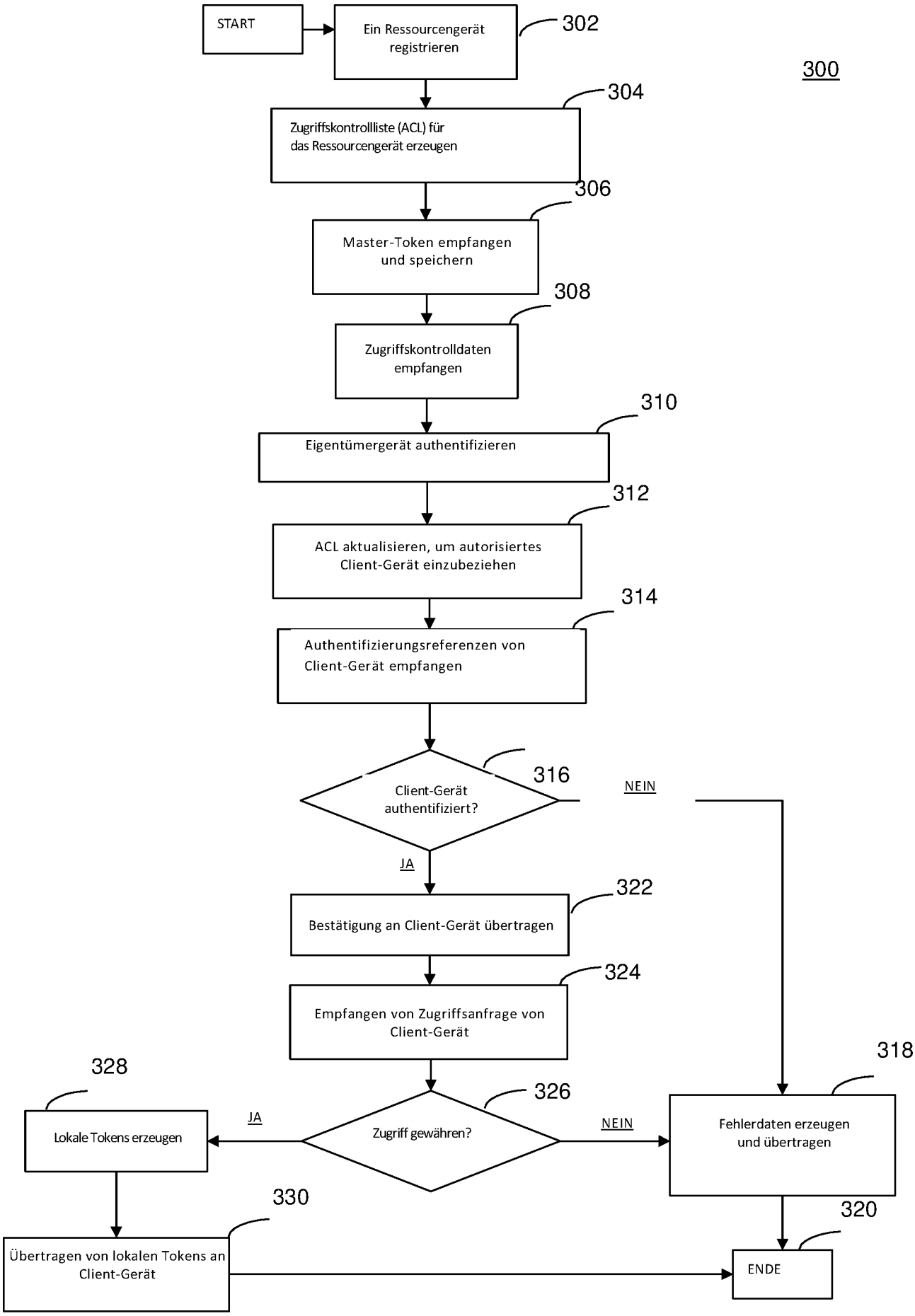

300
START
Ein Ressourcengerät registrieren
302
Zugriffskontrollliste (ACL) für das Ressourcengerät erzeugen
304
Master-Token empfangen und speichern
306
Zugriffskontrolldaten empfangen
308
Eigentümergerät authentifizieren
310
ACL aktualisieren, um autorisiertes Client-Gerät einzubeziehen
312
Authentifizierungsreferenzen von Client-Gerät empfangen
314
Client-Gerät authentifiziert?
316
NEIN
JA
Bestätigung an Client-Gerät übertragen
322
Empfangen von Zugriffsanfrage von Client-Gerät
324
Zugriff gewähren?
326
JA
NEIN
Lokale Tokens erzeugen
328
Fehlerdaten erzeugen und übertragen
318
Übertragen von lokalen Tokens an Client-Gerät
330
ENDE
320

FIG. 3

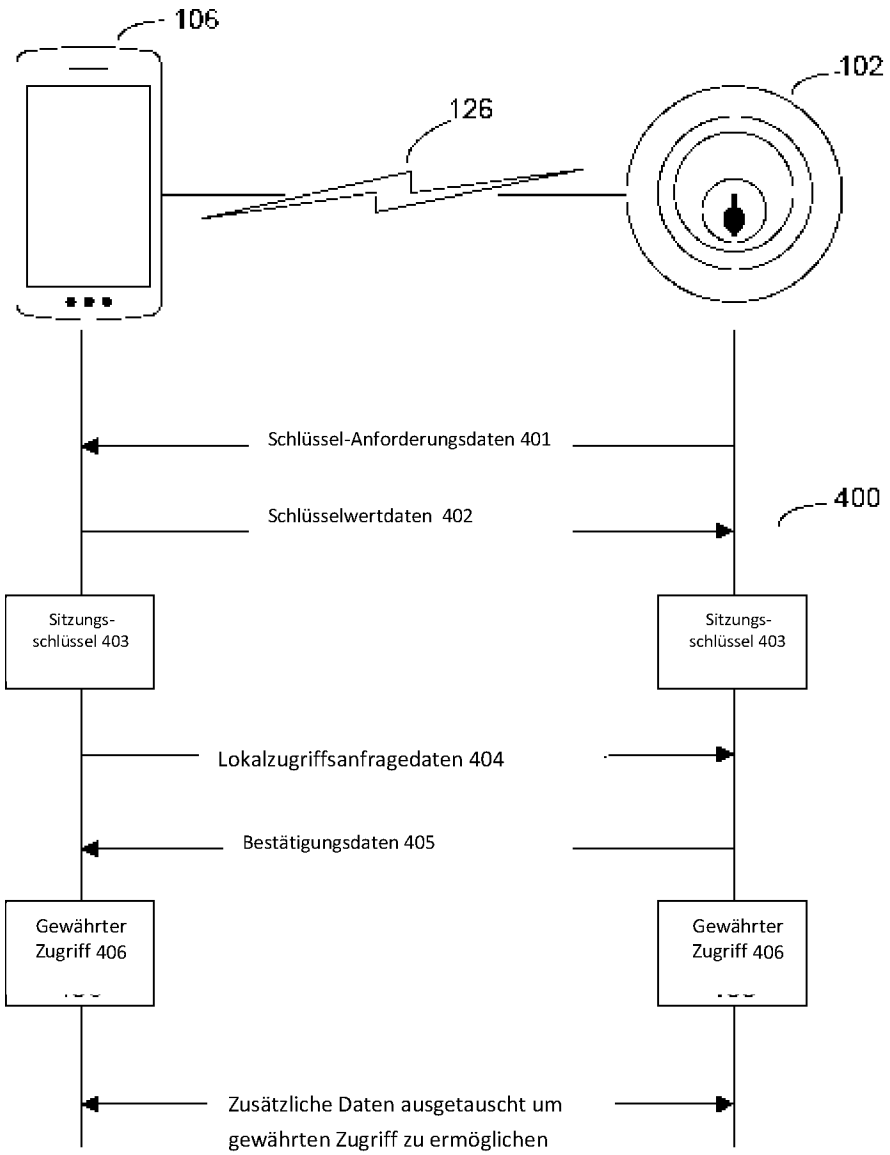

106
102
126
Schlüssel-Anforderungsdaten 401
Schlüsselwertdaten 402
400
Sitzungs-schlüssel 403
Sitzungs-schlüssel 403
Lokalzugriffsanfragedaten 404
Bestätigungsdaten 405
Gewährter Zugriff 406
Gewährter Zugriff 406
Zusätzliche Daten ausgetauscht um gewährten Zugriff zu ermöglichen

FIG. 4

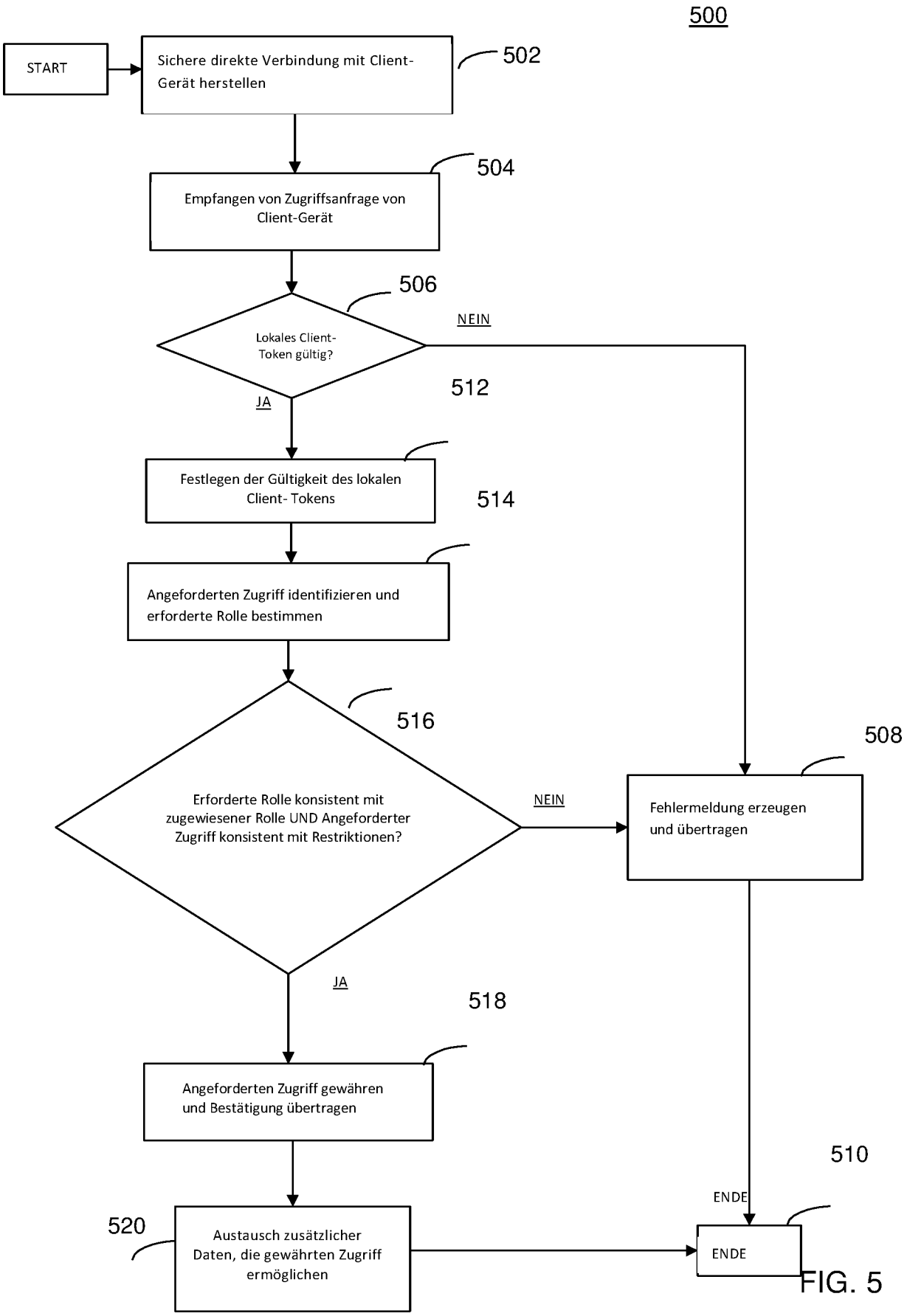

500
START
Sichere direkte Verbindung mit Client-Gerät herstellen
502
Empfangen von Zugriffsanfrage von Client-Gerät
504
Lokales Client-Token gültig?
506
NEIN
512
JA
Festlegen der Gültigkeit des lokalen Client- Tokens
514
Angeforderten Zugriff identifizieren und erforderte Rolle bestimmen
Erforderte Rolle konsistent mit zugewiesener Rolle UND Angeforderter Zugriff konsistent mit Restriktionen?
516
NEIN
Fehlermeldung erzeugen und übertragen
508
JA
518
Angeforderten Zugriff gewähren und Bestätigung übertragen
Austausch zusätzlicher Daten, die gewährten Zugriff ermöglichen
520
ENDE
510
ENDE

FIG. 5

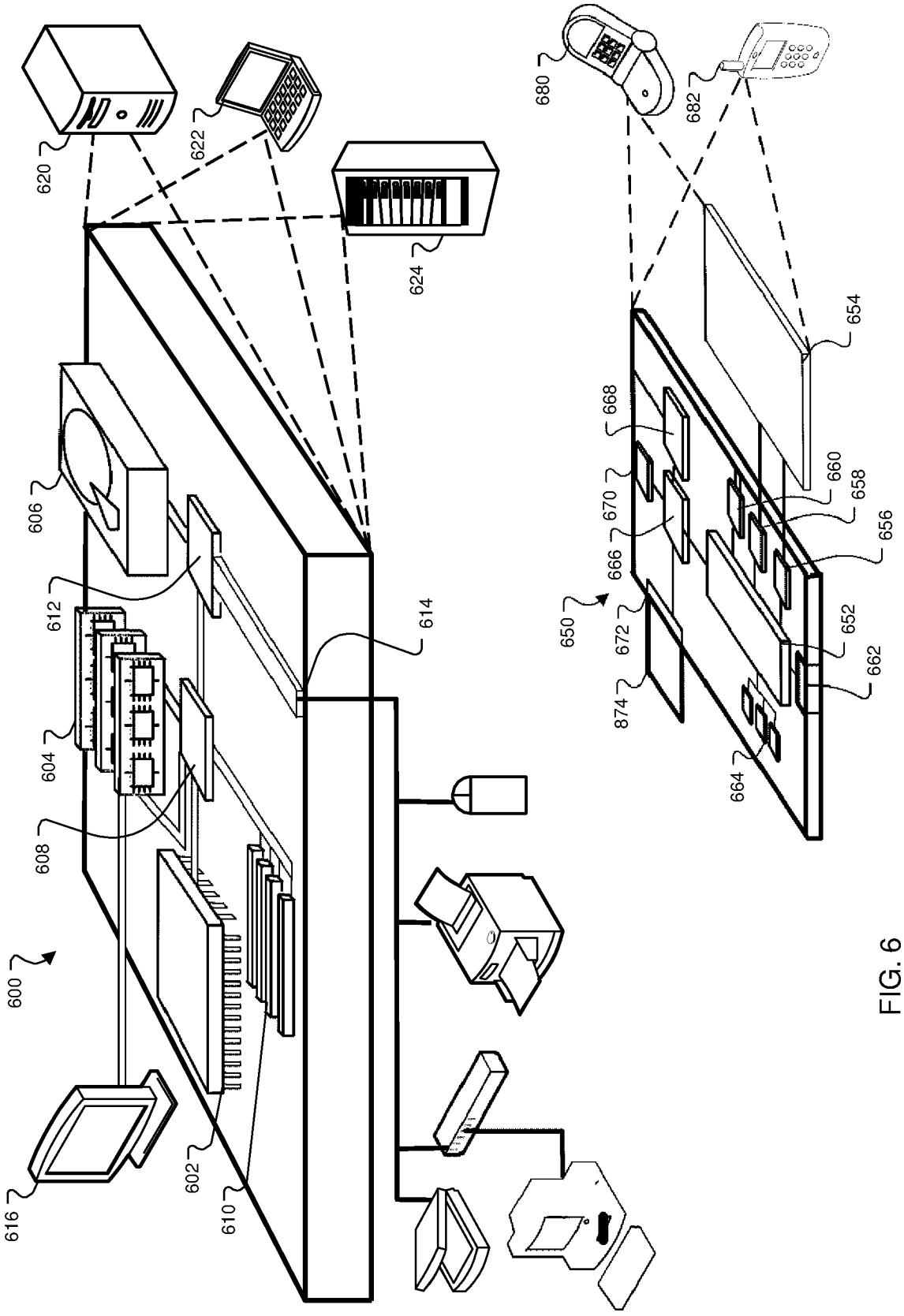

600
602
604
606
608
610
612
614
616
620
622
624
650
652
654
656
658
660
662
664
666
668
670
672
680
682
874

FIG. 6