(19) Deutsches Patent- und Markenamt

(10) **DE 11 2010 003 464 B4** 2019.05.16

(12) # Patentschrift

(21) Deutsches Aktenzeichen: **11 2010 003 464.8**
(86) PCT-Aktenzeichen: **PCT/EP2010/062007**
(87) PCT-Veröffentlichungs-Nr.: **WO 2011/023606**
(86) PCT-Anmeldetag: **18.08.2010**
(87) PCT-Veröffentlichungstag: **03.03.2011**
(43) Veröffentlichungstag der PCT Anmeldung in deutscher Übersetzung: **14.06.2012**
(45) Veröffentlichungstag der Patenterteilung: **16.05.2019**

(51) Int Cl.: ***G06F 21/62*** (2013.01)
G06F 21/30 (2013.01)

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

(30) Unionspriorität:
12/549,955 **28.08.2009** **US**

(73) Patentinhaber:
International Business Machines Corporation, Armonk, N.Y., US

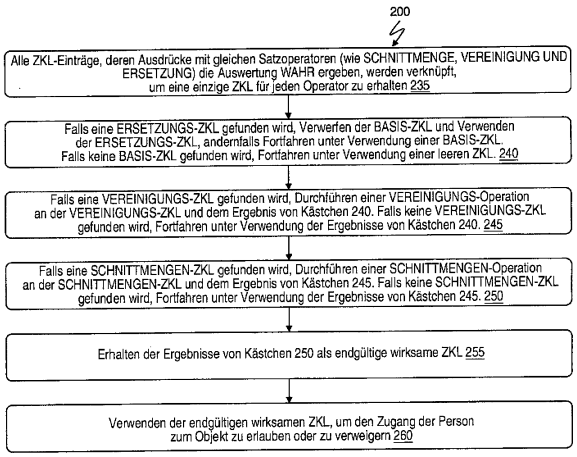
(74) Vertreter:
Richardt Patentanwälte PartG mbB, 65185 Wiesbaden, DE

(72) Erfinder:
Granados, Saheem, Poughkeepsie, N.Y., US; Brodfuehrer, Richard Joseph, Endicott, N.Y., US; Bryant, Corey, Poughkeepsie, N.Y., US; Yan, Stanley, Endicott, N.Y., US

(56) Ermittelter Stand der Technik:
siehe Folgeseiten

(54) Bezeichnung: **Modifikation von Zugangskontrolllisten**

(57) Hauptanspruch: Verfahren zur Modifikation von Basisberechtigungen von Zugangskontrolllisten durch Auswerten logischer Ausdrücke auf einem Server, wobei das Verfahren Folgendes umfasst:
Ermitteln von Basisberechtigungen für eine Person (subject) durch einen Server, indem ein Name der Person mit Zugangskontrolllisteneinträgen für ein Objekt verglichen werden;
Ermitteln der logische Ausdrücke umfassenden Zugangskontrolllisteneinträge für das Objekt durch einen Server;
Auswerten der Einträge logischer Ausdrücke der Zugangskontrolllisteneinträge für das Objekt mit logischen Ausdrucksattributen der Person durch einen Server, wobei die logischen Ausdruckseinträge so ausgewertet werden, dass festgestellt wird, welche Einträge logischer Ausdrücke für die logischen Ausdrucksattribute der Person wahr sind;
für logische Ausdrucksattribute, die wahr sind, Verknüpfen von Satzoperatoren der Einträge logischer Ausdrücke durch den Server dergestalt, dass eine einzige Vereinigungs-Zugangskontrollliste, eine einzige Schnittmengen-Zugangskontrollliste und eine einzige Ersetzungs-Zugangskontrollliste vorhanden ist;
wobei die Vereinigungs-Zugangskontrollliste eine Verknüpfung von Einträgen logischer Ausdrücke ist, die einen Vereinigungs-Operator verwenden;
wobei die Schnittmengen-Zugangskontrollliste eine Verknüpfung von Einträgen logischer Ausdrücke ist, die einen Schnittmengen-Operator verwenden, und
wobei die Ersetzungs-Zugangskontrollliste eine Verknüpfung von Einträgen ...



(56) Ermittelter Stand der Technik:

US	**2003 / 0 200 467**	**A1**
US	**2005 / 0 259 654**	**A1**
US	**2007 / 0 261 102**	**A1**
US	**2009 / 0 055 397**	**A1**
US	**2009 / 0 064 342**	**A1**

ZHANG, Guangsen; PARASHAR, Manish: Context-aware Dynamic Access Control for Pervasive Applications. Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004), 2004. URL: http://nsfcac.rutgers.edu/TASSL/Papers/automate-sesame-cnds-04.pdf [abgerufen am 8. Januar 2016]

Beschreibung

HINTERGRUND

[0001] Die vorliegende Offenbarung bezieht sich auf ein Verfahren zur Modifikation von Basisberechtigungen von Zugangskontrolllisten durch Auswerten logischer Ausdrücke auf einem Server, einen Server mit einem Prozessor und Speicher zur Speicherung eines Programms, wobei das Programm eingerichtet ist um das Verfahren zur Modifikation von Basisberechtigungen von Zugangskontrolllisten durch Auswerten logischer Ausdrücke durchzuführen sowie ein Computerprogramm, das materiell auf einem computerlesbaren Datenträger enthalten ist, wobei das Computerprogramm Anweisungen enthält, um einen Computer zu veranlassen, die das Verfahren zur Modifikation von Basisberechtigungen von Zugangskontrolllisten durch Auswerten logischer Ausdrücke durchzuführen.

[0002] Mit dem Fortschreiten verschiedener Technologien haben sich immer mehr Unternehmen dazu entschlossen, verteilte Technologien einzusetzen, um ihre Geschäftsprozesse zu verbessern. Oftmals werden diese Technologien dazu eingesetzt, die Reichweite von Unternehmen zu vergrößern und über die örtlichen Bereiche hinaus auszudehnen. Das Internet und andere Netzwerke können für diese Expansion die Infrastruktur bereitstellen. Ein grundlegender und äußerst notwendiger Punkt, der bei der Nutzung von Informationstechnologie als Rückgrat aller geschäftlichen Vorgänge beachtet werden muss, ist die Zugangskontrolle. Konzeptionell umfasst die Zugangskontrolle das Sicherstellen, dass eine Person/eine Personengruppe (subject entity) über ausreichende Rechte verfügt, um Vorgänge auf Objekten durchzuführen. Sowohl das ordnungsgemäße Einrichten der Zugangskontrolle als auch das Errichten ausreichender Sicherheitsprozesse werden bereits gut beherrscht, es sollten jedoch zusätzliche Funktionen verfügbar sein.

[0003] Die US 2009 / 0 055 397 A1 offenbart Verfahren und Vorrichtungen zur Zugangskontrolle für Objekte in einem Computer System. Offenbart wird ferner eine Zugangskontrollliste von Subjekten, wobei jedes Subjekt mit einer Menge von Operationen assoziiert ist, die dieses Subjekt auf einem Objekt ausführen kann, und mit einem Satz von Regeln, die Bedingungen spezifizieren, unter denen eine andere Menge von Operationen mit einem Subjekt assoziiert werden soll. Falls mindestens eine dieser Bedingungen erfüllt ist, wird die Zugangskontrollliste nach Maßgabe der Regel(n), deren Bedingung(en) erfüllt ist bzw. sind, von einem ersten Zustand in einen zweiten Zustand überführt.

[0004] Zhang und Parashar („Context-aware Dynamic Access Control for Pervasive Applications“, CNDS Conference 2004, URL: http://nsfcac.rutgers.edu/TASSL/Papers/automate-sesame-cnds-04.pdf) offenbaren Zugriffskontrollmechanismen, bei denen die Zugriffsentscheidungen für die Zugriffskontrolle von der Kombination erforderlicher Anmeldeinformationen der Benutzer sowie vom Kontext und Zustand des Systems abhängen. Die US 2005 / 0 259 654 A1 offenbart ein Verfahren, das den Zugriff eines Benutzers auf ein Netzwerk steuert, wobei das Netzwerk eine Vielzahl von Hosts beinhaltet, die über einen Netzwerkswitch miteinander verbunden sind. Das Verfahren beinhaltet das Speichern einer erweiterten Zugriffskontrollliste in einem Netzwerk-Switch, der Daten enthält, die sich auf mindestens den Benutzernamen, DNS-Namen, Domänennamen oder die physikalische Adressen beziehen. Aus der erweiterten Zugriffskontrollliste wird eine dynamische Zugriffskontrollliste erzeugt, wobei die dynamische Zugriffskontrollliste eine Vielzahl von IP-Adressen enthält, die den Zugriff des Benutzers auf das Netzwerk einschränken.

[0005] Die offenbart ein System und Verfahren zum Autorisieren des Zugriffs auf eine Entität durch einen Benutzer durch Binden einer Zugriffskontrollliste an jede Entität, Spezifizieren eines Satzes von Benutzerprivilegien für den Benutzer, Überkreuzen der Zugriffskontrollliste und des Satzes von Benutzerprivilegien in einer kompilierten ACL-Tabelle, stufenweises Aktualisieren der kompilierten ACL-Tabelle als Reaktion auf Laufzeitänderungen relevanter Tabellen, die die Zugriffskontrollliste und den Satz von Benutzerprivilegien enthalten und Referenzieren der kompilierten Zugriffskontrollliste zum Autorisieren einer Benutzeranforderung zum Zugriff auf eine Entität.

[0006] Die US 2009 / 0 064 342 A1 offenbart Vorrichtungen, Verfahren und Computerprogrammprodukte, die Rechte an einem Unternehmen festlegen. Die offenbarte Technologie verwaltet Datenstrukturen, die eine Reihe von Einheiten darstellen. Zu diesen Einheiten gehören geschützte Einheiten und Sensibilitätseinheiten. Jede der Sensitivitätseinheiten ist mit einer entsprechenden Sensitivitätszugriffskontrollliste verknüpft. Die Sensitivitätseinheiten beinhalten eine erste Sensitivitätseinheit, die mit einer ersten Sensitivitätszugriffskontrollliste verbunden ist. Eine erste geschützte Einheit, die eine von einer oder mehreren der geschützten Einheiten ist, die mit der ersten Empfindlichkeitseinheit verbunden sind. Die Technologie bewertet die Rechte an der ersten geschützten Einheit in Bezug auf die erste Sensitivitätszugriffskontrollliste und ermöglicht den Zugriff auf die erste geschützte Einheit als Reaktion auf die Rechtebewertung und präsentiert die erste geschützte Einheit, wenn der Zugriff freigegeben ist.

[0007] Die US 2007 / 0 261 102 A1 offenbart Verfahren und Systeme zur Steuerung des Zugriffs auf Objekte einer verteilten Computerumgebung. In ei-

ner Konfiguration empfängt eine Computervorrichtung eine Anforderung eines Auftraggebers, auf ein geschütztes Objekt zuzugreifen und das transitive Schließen der Liste der Gruppenidentifikatoren zu bewerten. Das geschützte Objekt ist einer Zugriffskontrollliste zugeordnet und verfügt über eine zeitinvariante Liste von Gruppenkennungen. Die Liste der Gruppenidentifikatoren beinhaltet die Zugriffsliste, die dem geschützten Objekt zugeordnet ist, um mindestens einen Hauptverantwortlichen zu identifizieren, der zum Zugriff auf das geschützte Objekt berechtigt ist.

[0008] Es ist daher die Aufgabe der Erfindung, den administrativen Aufwand bei der Einrichtung und Pflege von Zugangskontrollsystemen zu verringern.

[0009] Beispielhafte Ausführungsformen beziehen sich auf Zugangskontrolllisten und genauer auf dynamische Vergrößerung, Verringerung und/oder Ersetzen von Zugangskontrolllisten durch Auswertung von den Zugangskontrolllisten zugeordneten logischen Ausdrücken.

ZUSAMMENFASSUNG

[0010] Gemäß einer beispielhaften Ausführungsform wird ein Verfahren zur Modifikation von Basisberechtigungen von Zugangskontrolllisten durch Auswerten logischer Ausdrücke auf einem Server bereitgestellt. Ein Server legt Basisberechtigungen für eine Person fest, indem ein Name der Person mit Zugangskontrolllisteneinträgen für ein Objekt verglichen wird. Der Server unterhält die Basiseinträge und logische Ausdrücke umfassenden Zugangskontrolllisteneinträge für das Objekt. Die Zugangskontrolllisteneinträge logischer Ausdrücke schließen zudem einen der folgenden Satzoperatoren ein: Vereinigung (union), Schnittmenge (intersect) oder Ersetzung (replace). Zusätzlich zur Festlegung, welche Basiseinträge auf die Person anwendbar sind, bestimmt der Server die Einträge logischer Ausdrücke der Zugangskontrolllisteneinträge für das Objekt mit logischen Ausdrucksattributen der Person. Die Einträge logischer Ausdrücke werden ausgewertet, um festzustellen, welche Einträge logischer Ausdrücke für logische Ausdrucksattribute der Person wahr sind. Für logische Ausdrucksattribute, die wahr sind, verknüpft der Server Satzoperatoren der Einträge logischer Ausdrücke so, dass eine einzige Vereinigungs-Zugangskontrollliste, eine einzige Schnittmengen-Zugangskontrollliste und eine einzige Ersetzungs-Zugangskontrollliste vorhanden ist. Als Reaktion auf das Vorhandensein der Ersetzungs-Zugangskontrollliste führt der Server eine Ersetzungs-Operation durch, um die durch die Basiseinträge festgelegten Basisberechtigungen durch die Ersetzungs-Zugangskontrollliste zu ersetzen, und ein Ergebnis der Ersetzungs-Operation ist eine erste Ausgabe. Als Reaktion auf das Vorhandensein keiner Ersetzungs-Zugangskontrollliste sind die Basisberechtigungen die erste Ausgabe. Als Reaktion auf das Vorhandensein der Vereinigungs-Zugangskontrollliste führt der Server eine Vereinigungs-Operation an der ersten Ausgabe und der Vereinigungs-Zugangskontrollliste durch, und ein Ergebnis der Vereinigungs-Operation ist eine zweite Ausgabe. Als Reaktion auf das Vorhandensein keiner Vereinigungs-Zugangskontrollliste ist die erste Ausgabe die zweite Ausgabe. Als Reaktion auf das Vorhandensein der Schnittmengen-Zugangskontrollliste führt der Server eine Schnittmengen-Operation an der zweiten Ausgabe und der Schnittmengen-Zugangskontrollliste durch, und das Ergebnis der Schnittmengen-Operation ist eine dritte Ausgabe. Als Reaktion auf das Vorhandensein keiner Schnittmengen-Zugangskontrollliste ist die zweite Ausgabe die dritte Ausgabe. Der Server stellt die dritte Ausgabe als wirksame Rechte für die Person bereit.

Figurenliste

[0011] Nachfolgend werden in beispielhafter Weise Ausführungsformen der Erfindung unter Bezugnahme auf die begleitenden Zeichnungen beschrieben, in denen:

Fig. 1 ein Blockdiagramm gemäß beispielhafter Ausführungsformen zeigt;

Fig. 2 und **Fig. 3** einen Ablaufplan gemäß beispielhafter Ausführungsformen zeigt;

Fig. 4 eine konzeptionelle Darstellung eines Personenzugangs-Schaubildes gemäß beispielhafter Ausführungsformen zeigt;

Fig. 5 ein Venn-Diagram gemäß beispielhafter Ausführungsformen zeigt;

Fig. 6 ein Beispiel eines Computers mit Fähigkeiten zeigt, die Teil beispielhafter Ausführungsformen sein können.

DETAILLIERTE BESCHREIBUNG

[0012] Bei der Zugangskontrolle ist die Berücksichtigung des Standorts von anfragenden Personen oder Personengruppen (entities) üblicherweise nicht so einfach wie die Berücksichtigung der Namen der Personen oder Personengruppen. Internationale und örtliche Gesetze können Auswirkungen auf geschäftliche Vorgänge haben, wenn sie sich über den lokalen Standort hinaus erstrecken. Intranet- and Firewall-Technologien können ebenfalls eigene Standorte mit sich bringen, von denen aus Personen oder Personengruppen Berechtigungen erfragen. Die Zugangskontrolle sollte in der Lage sein, bei gegebenem Standort die Rechte einer Person wie in den beispielhaften Ausführungsformen beschrieben umzuwandeln. Weiterhin sollte der Anfragezeitpunkt ebenso eine Rolle bei der Festlegung der Rechte einer Person in beispielhaften Ausführungsformen sein.

[0013] Wie hieraus ersichtlich werden wird, sind Zeit und Standort lediglich Beispiel von Personenattributen, die während der Berechtigungserteilung als Faktoren berücksichtigt werden können. Diese Attribute sind es, die logische Ausdrucksattribute bilden, wie sie in den beispielhaften Ausführungsformen erläutert werden. Logische Ausdrucksattribute können beispielsweise den Satz von 1-N Personennamen, 0-N Gruppennamen, der IP-Adresse der Person, Tageszeit, Verbindungstyp der Person, Identitätsnachweis-Mechanismus usw. umfassen. Darüber hinausgehend kann ein Administrator, der die logischen Ausdrucksattribute einführt, nach Wunsch weitere logische Ausdrucksattribute aufnehmen.

[0014] In **Fig. 1** sind Kommunikationseinheiten **15** in der Lage, mit einem oder mehreren Servern **20** über ein Netzwerk **30** Daten auszutauschen. Bei den Kommunikationseinheiten **15** kann es sich beispielhaft, und ohne auf diese beschränkt zu sein, um Mobiltelefone, Festnetztelefone, Smartphones, Software-Telefone (soft telephones), persönliche digitale Assistenten (personal digital assistants), Decoder (set top boxes STB), Fernseher (TV), Spielekonsolen, MP3-Spieler, Computer und Server handeln.

[0015] Das Netzwerk **30** wiederum kann leitungsvermittelte und/oder paketvermittelte Technik und Einheiten wie Leitwegrechner (router), Vermittlungsstellen (switches), Netzknoten (hubs), Netzverbindungsschnittstellen (gateways) usw. zur Erleichterung der Datenübertragung umfassen. Das Netzwerk **30** kann kabelgebundene und/oder drahtlose Komponenten verwenden wie z.B. die IEEE-Standards **802.11** zur Bereitstellung der Datenübertragung über Funk. Das Netzwerk **30** kann IP-gestützte Netzwerke für die Datenübertragung zwischen einem Kundendienstzentrum und Kunden/Benutzern sein. Das Netzwerk **30** kann mehrere von bestimmten Benutzern eingerichtete Konten verwalten. Diese Konten können dann dazu verwendet werden, Zugang zu hierin beschriebenen Diensten bereitzustellen. Das Netzwerk **30** kann kabelgebundene und/oder drahtlose Komponenten umfassen, die Standards wie beispielsweise Multimedianachrichtendienste (multimedia messaging services, MMS) verwenden. Das Netzwerk **30** kann ein MMS-Zentrum (multimedia messaging center, MMC) einschließen, das die Netzwerkseite des Multimedianachrichtendienstes (MMS) umsetzt und es einem Betreiber ermöglicht, den Benutzern mobiler Kommunikationseinheiten Multimedianachrichten anzubieten. Das Netzwerk **30** kann ein verwaltetes IP-Netzwerk und/oder drahtloses Netzwerk einschließen, das durch einen Dienstanbieter verwaltet wird, der die Bandbreite und Dienstgüte (quality of service) für die hierin erläuterte Datenübertragungen steuern kann. Das Netzwerk **30** kann in drahtloser Weise ausgeführt sein, z.B. unter Verwendung drahtloser Protokolle und Technologien wie Wi-Fi®, WiMAX™, Bluetooth® usw. Bei dem Netzwerk **30** kann es sich auch um ein paketvermitteltes Netzwerk wie ein Nahbereichsnetzwerk (local area network), ein Weitbereichsnetzwerk (wide area network), ein Stadtnetz (metropolitan area network), ein Internet-Netzwerk oder ähnliche Arten von Netzwerken handeln. Das Netzwerk **30** kann ein mobiles Datenübertragungsnetzwerk, ein festes drahtloses Netzwerk, ein drahtloses Nahbereichsnetzwerk (wireless local area network LAN), ein drahtloses Weitbereichsnetzwerk (wireless wide area network (WAN), ein Netzwerk für den persönlichen Bereich (personal area network PAN), ein virtuelles privates Netzwerk (virtual private network VPN), ein Intranet oder ein beliebiges anderes geeignetes Netzwerk sein, und das Netzwerk **30** kann Geräte zum Empfangen oder Senden von Signalen wie einen Mobilfunkmast, eine Mobilfunkvermittlungsstelle, eine Basisstation oder einen drahtlosen Zugangspunkt umfassen.

[0016] Ein Zugangskontrollmodul **130** auf dem Arbeitsplatzrechner (workstation) **10** und/oder auf dem Server **20** kann gemäß der beispielhaften Ausführungsbeispiele zum Programmieren, Festlegen von Berechtigungen und Rechten und zum Eingeben von Daten auf den Servern **20** verwendet werden. Der Arbeitsplatzrechner **10** kann direkt mit den Servern **20** verbunden, in die Server **20** integriert und/oder funktionsmäßig mit den Servern **20** über das Netzwerk **30** verbunden sein. Weiterhin kann der Server **20** das Zugangskontrollmodul **130** im Ganzen und/oder in Teilen einschließen und über eine Schnittstelle mit dem Zugangskontrollmodul **130** verbunden sein.

[0017] Ein Administrator, der beispielsweise das Zugangskontrollmodul **130** auf dem Arbeitsplatzrechner **10** und/oder dem Server **20** verwendet, kann eine Zugangskontrolle für ein Objekt **120** festlegen. Zum Zweck der Erläuterung ist das Objekt **120** auf dem Server **20** abgebildet. Das Objekt **120** kann sich jedoch auch auf weiteren Servern **20** befinden. Das Objekt **120** kann ebenso für vielfältige Anwendungen, Programme, Datenbanken, Server usw. stehen, zu denen eine Person **5**, die die Kommunikationseinheit **15** verwendet, möglicherweise Zugang erlangen möchte. Es versteht sich, dass für das auf dem Server **20** abgebildete Objekt **120** keine Einschränkungen gelten sollen und es nur zum Zwecke der Veranschaulichung auf dem Server **20** abgebildet ist. Zum Zweck der Veranschaulichung sind das Zugangskontrollmodul **130**, das Objekt **120** und die Datenbanken **115** mit Speicher **30** des Servers **20** verbunden. Der Speicher **30** ist ein computerlesbarer Datenträger mit auf einem Computer ausführbaren Anweisungen, die durch einen Prozessor ausgeführt werden können.

[0018] In den beispielhaften Ausführungsformen können die Person **5** und die Kommunikationseinheit **15** austauschbar verwendet werden, da die Person **5** mithilfe der Kommunikationseinheit **15** versucht, Zugang zum Objekt **120** zu erhalten. Dementsprechend

kann im Falle, dass die Person **5** betrachtet wird, die Person **5** sowohl als Person **5** als auch als Kommunikationseinheit **15** stehen. Gleichermaßen kann im Falle, dass die Kommunikationseinheit **15** verwendet wird, die Kommunikationseinheit **15** sowohl für die Person **5** als auch für die Kommunikationseinheit **15** stehen, da die Person **5** die Kommunikationseinheit **15** dazu verwendet, Zugang zum Objekt **120** zu erhalten. Der Administrator, der das Zugangskontrollmodul **130** verwendet, muss beispielsweise im Voraus Rechte für die Person **5** einrichten. Für diese Verwaltungsaufgabe können Einrichtungen wie Platzhalter (wildcards) verwendet werden, um Anforderungen an Standorte, Zugangsdaten und/oder Zeit und weitere logische Ausdrucksattribute für Sätze von Rechten einzurichten. Dann bietet die anfragende Einheit wie beispielsweise die Person **5** von einem entfernten Standort wie z.B. dem Standort der Kommunikationseinheit **15** aus zu einer bestimmten Zeit ihre Zugangsdaten zur Prüfung der Identität an. Nach dem Feststellen der Identität werden die Zugangsdaten, die Zeit und der Standort der Einheit bei der Berechtigungserteilung einer Anfrage nach Zugang zum Objekt **120** gemäß der beispielhaften Ausführungsformen verwendet.

[0019] Die beispielhaften Ausführungsformen stellen einen neuartigen Ansatz bei der Festlegung von Rechten einer anfragenden Einheit wie der Person **5** bereit. Dieser Ansatz bietet Administratoren mehr Flexibilität und vereinfacht für den Administrator den Prozess zur Einrichtung der Rechte der Person **5** unter Berücksichtigung beispielsweise von Zeit und Standort. Der Prozess der Festlegung von Rechten bietet die hierin erläuterte Flexibilität.

[0020] Vor der Festlegung von Rechten für Berechtigungsprüfungen kann der Administrator unter Verwendung des Zugangskontrollmoduls **130** mit zugehörigen datenbankartigen Filtern und Rechenoperatoren Sätze von Rechten einrichten. Diese Filter können mittels Standort-, Zugangsdaten- und Zeitattributen sowie weiteren LAAs (Logische Ausdrucks-Attribute) festgelegt werden. Es ist für den Fachmann ersichtlich, dass komplexere Filter verwendet werden können und die hierin bereitgestellten Beispiele nur dem Zwecke der Erläuterung dienen. Weiterhin können diese Filter des Zugangskontrollmoduls **130** Prädikate des Vergleichstyps und logische Operatoren wie UND (AND), ODER (OR) und NICHT (NOT) beinhalten.

[0021] Zum Beispiel IP=192.* UND SUBJEKT=loginl UND TAG>= 27. Mai UND TAG< 28. Mai.

[0022] Die Rechenoperatoren werden vom Zugangskontrollmodul **130** bei der Durchführung von Berechtigungsprüfungen verwendet, um den endgültigen wirksamen Satz von Rechten zu ermitteln, der für die Person **5**, die nach Zugang zum Objekt **120** anfragt, zu dieser (bestimmten) Zeit, gültig ist. Angesichts dieser Flexibilität der beispielhaften Ausführungsformen ist der Prozess des Ermittelns von Rechten der Person **5** kein einfacher schlüsselwortgestützter Nachschlageprozess, wie dies in Systemen nach dem Stand der Technik der Fall ist, um einen aktiven Satz von Rechten abzurufen. Stattdessen lässt sich der Prozess des Zugangskontrollmoduls **130** in den folgenden Vorgängen beschreiben:

1. Ermitteln von Basisrechten, z.B. unter Verwendung eines schlüsselwortartigen Nachschlagens.

2. Sammeln aller anwendbaren Sätze von Rechten, deren Filter bei gegebenem Standort, gegebener Person und Tageszeit und anderen LAAs den Wert WAHR (true) ergeben.

3. Mittels der den Ergebnissen von Schritt **1** zugehörigen Operatoren inkrementelles Verknüpfen aller Ergebnisse von Schritt **1**, um die gewährten Rechte für die Person, den Standort und die Zeit und andere LAAs einzurichten. Mit diesen gewährten Rechten werden dann die Berechtigungserteilung und/oder Verweigerung der Anfrage nach Zugang durchgeführt.

[0023] Anders als bei Systemen nach dem Stand der Technik, die auf tabellenartigem Nachschlagen beruhen, führen die beispielhaften Ausführungsformen die Ermittlung von Rechten über das Zugangskontrollmodul **130** als inkrementellen Prozess durch. Der inkrementelle Prozess erfolgt dynamisch auf der Grundlage der vom Kontrollmodul **103** festgelegten aktuellen logischen Ausdrucksattribute der Person **5**. Durch diesen inkrementellen Prozess können Administratoren die Zahl von Spezifikationen verringern, die sie festlegen müssen, um die für Berechtigungsprüfungen benötigten Rechte einzurichten.

[0024] Als Beispiel kann der Fall dienen, dass die Zugangskontrolle für ein gegebenes Objekt **120** viele sehr granulare Spezifikationen von Rechten erfordert. Die vielen granularen Spezifikationen würden in Verbindung mit einer großen Domäne möglicher Personen und zugeordneter LAAs die explizite Spezifizierung wirksamer Sätze für jede mögliche Permutation des Satzes von Personen und LAAs erfordern. Oftmals weisen die unterschiedlichen Sätze wirksamer Rechte nur geringfügige Unterschiede auf. Analog einer mathematischen Funktion, die eine Regel zur Abbildung (mapping) einer sehr großen Domäne auf einen sehr großen Bereich definiert, ermöglicht es der inkrementelle Prozess des Zugangskontrollmoduls **130** einem Administrator, ein breites Spektrum von Subjekten und LAAs auf wirksame Rechte abzubilden, ohne jede Abbildung explizit angeben zu müssen. Durch die Verwendung des Zugangskontrollmoduls **130** kann ein Administrator zum Beispiel eine neue LA-ZKL (Zugangskontrollliste logischer Ausdrücke) für IP=1.2.3.* einrichten, anstatt jede einzelne

vorhandene Personen- und Gruppen-ZKL mit der IP-Adresse IP=1.2.3.* zu aktualisieren.

[0025] Zum Zwecke der Erklärung wird angenommen, dass die Server **20** beispielsweise das Lightweight Directory Access Protocol (LDAP) verwendet. LDAP-Server bieten ein deutliches Beispiel, wie die Zugangskontrolle von einer verteilten Anwendung verwaltet wird. Beispielhafte Ausführungsformen können durch LDAP-Serverprodukte umgesetzt sein, sind jedoch nicht auf LDAP-Server beschränkt. Im LDAP-Server **20** der beispielhaften Ausführungsformen wird die Person **5** durch einen Zugangsdatensatz vertreten. Zugangsdaten werden durch die Einheit (Person und Kommunikationseinheit **15**) vorgelegt, die zur Bindungszeit Zugang erfragt. Die Person **5** an der Kommunikationseinheit **15** kann mit dem Server **20** Daten austauschen, um die Berechtigung zum Zugang zum Objekt **120** zu erfragen, und auch das Zugangskontrollmodul **130** ist über eine Schnittstelle mit der Kommunikationseinheit **15** der Person **5** verbunden, um Zugangsdaten zu erhalten. Zum Beispiel können die vom Zugangskontrollmodul **130** des Servers **20** erhaltenen Zugangsdaten einen unterscheidbaren Verbindungsnamen (Bind Distinguished Name DN) (oder einen Personennamen) und ein Passwort, ein X.509-Zertifikat und/oder ein Kerberos-Ticket beinhalten. Diese Zugangsdaten können Mitglieder von Gruppen sein. Die Zugangsdaten der Person **5** können beispielsweise vom Zugangskontrollmodul **130** als Teil einer oder mehrerer Gruppen erkannt werden. Als Mitglied können die Zugangsdaten der Person **5** die der Gruppe verliehenen Rechte erben. Diese Rechte sind Berechtigung(en) von Zugangskontrolllisten (ZKL), und die Objekte (z.B. Objekt **120**) sind LDAP-Einträge z.B. in einer Datenbank **115**. Entsprechend kann die Person **5** einen oder mehrere Personennamen und/oder Gruppennamen besitzen. Ein LDAP-Administrator muss explizite ZKL-Berechtigungen für Einträge und/oder Sätze von Einträgen in der Datenbank **115** einrichten. Der Administrator muss ZKLs für alle zulässigen Zugangsdaten und/oder für Gruppen mit Mitgliedern einrichten.

[0026] Das folgende Beispiel zeigt einen LDAP-Eintrag (z.B. Objekt **120**) mit 2 Basis(base)-ZKL-Einträgen (wie beispielsweise Basis-ZKL-Einträge **150**) und 1 ZKL-Eintrag mit einem ZKL-Filter (wie beispielsweise ein ZKL-Eintrag logischer Ausdrücke **170**, **175** und/oder **180**). In diesem Beispiel können die LAAs folgendermaßen aussehen:

ibm-filterMechanismus, ibm-filterTageszeit, ibm-filterIP.

dn: ou=Zweite Ebene, ou=Männliche Olympier, o=Olympier, o=Olympia, o=Probe

objectclass: organizationalunit

ou: Zweite Ebene

description: Olympier zweiter Ebene

aclentry: access-id:CN=DIONYSOS, OU=ZWEITE EBENE, OU=MANNLICHE OLYMPIER, O=OLYMPIER, o=Olympia, o=sample: normal:rsc:object:ad

aclentry: access-id:CN=HERMES, OU=ZWEITE EBENE, OU=MANNLICHE OLYMPIER, O=OLYMPIER, o=Olympia, o=sample:normal:rsc aclentry: access-id:CN=HERA, OU=WEIBLICHE OLYMPIER, O=OLYMPIER, o=Olympia, o=sample:object:ad:normal: rwsc:sensitive:rwsc:critical:rwsc

aclentry: aclFilter:(&(&(ibm-filterMechanismus=EINFACH) (ibmfilterIP=127.0.0.1)) (&(ibm-filterWochentag<=6) (ibmfilterTageszeit>=00:00))) :intersect:normal:rwsc:at.cn:deny :w:restricted:rs

[0027] Durch Verwendung von Zugangsdaten, wie sie von der Person **5** auf der Kommunikationseinheit **15** erhalten werden, kann das Zugangskontrollmodul **130** Basis-ZKL-Einträge **150** von der Datenbank **115** einrichten. Basis-ZKL-Einträge **150** können eingerichtet werden, indem Attribute der Person **5** in der Datenbank **115** verglichen werden. Betrachten wir den Fall, in dem der Zugangsdatensatz von äußerst unterschiedlichen IP-Adressen verwendet werden kann. In einem derartigen Fall führen bei Systemen nach dem Stand der Technik die unterschiedlichen IP-Adressen zur Notwendigkeit vieler unterschiedlicher ZKL-Berechtigungseinträge, so dass es für einen Administrator mühsam sein kann sicherzustellen, dass alle IP-Adressen für einen Zugangsdatensatz den Sicherheitsanforderungen genügen.

[0028] Die beispielhaften Ausführungsformen können hingegen die ZKL-Vergleichsattribute verwenden, allerdings ist das Zugangskontrollmodul **130** zur Einrichtung einer spezifischen ZKL bei gegebenen Attributen zusätzlich so eingerichtet, dass es inkrementelle Aktualisierungen an den Basis-ZKL-Berechtigungen **155** auf der Grundlage logischer Ausdrucksattribute (darunter die IP-Adresse der Kommunikationseinheit **15**, der Identitätsnachweis-Mechanismus, Zugangsdaten und/oder der Zugangstag der Kommunikationseinheit **15**) ermöglicht. Gemäß den beispielhaften Ausführungsformen gehören zu den inkrementellen Aktualisierungen durch das Zugangskontrollmodul **130** die folgenden:

1. Erweiterung der Basis-ZKL-Berechtigungen **150** bei Verwendung eines Vereinigungs-Schlüsselwortes;

2. Eine Erweiterung der Basis-ZKL-Berechtigungen **150** bei Verwendung eines Schnittmengen-Schlüsselwortes;

3. Ersetzen der Basis-ZKL-Berechtigungen **150** bei Verwendung eines Ersetzungs-Schlüsselwortes.

[0029] Zeitweise können zu Erläuterungszwecken Beispiele nur im Hinblick auf IP-Adressen beschrieben sein, wobei der Fachmann erkennt, dass die beispielhaften Ausführungsformen nicht auf IP-Adressen beschränkt sind.

[0030] In beispielhaften Ausführungsformen entsprechen und/oder beziehen sich Basis-ZKL-Einträge **150** auf Basis-ZKL-Rechte/Berechtigungen für die Person **5**, die versucht, Zugang zum Objekt **120** zu erhalten. Ebenso entsprechen und/oder beziehen sich ZKL-Einträge logischer Ausdrücke (LA) **160** auf ZKL-Rechte/Berechtigungen logischer Ausdrücke (LA).

[0031] Gleichermaßen entsprechen und/oder beziehen sich Vereinigungs-ZKL-Gesamteinträge **170**, Schnittmengen-ZKL-Gesamteinträge **175** und Ersetzungs-ZKL-Gesamteinträge **180** auf Vereinigungs-ZKL-Gesamtrechte/-berechtigungen **170**, Schnittmengen-ZKL-Gesamtrechte/-berechtigungen **175** und Ersetzungs-ZKL-Gesamtrechte/-berechtigungen **180**. Wie für den Fachmann ersichtlich ist, können die obigen Begriffe in der Beschreibung austauschbar verwendet werden.

[0032] In beispielhaften Ausführungsformen ermöglicht es das Vereinigungs-Schlüsselwort des Zugangskontrollmoduls **130** einem Administrator, bei gegebenen LAAs wie beispielsweise IP-Adresse, Zugangsdatensatz, Berechtigungserteilungs-Mechanismus und/oder Zugangszeit einen Minimalsatz von Berechtigungen zu gewährleisten. Das Schnittmengen-Schlüsselwort ermöglicht es einem Administrator, einen Satz von Berechtigungen zu verringern und dabei sicherzustellen, dass nur eine oder mehrere bestimmte Berechtigung(en) verfügbar sind, wenn (und nur dann) die Basis-ZKL-Berechtigung(en) **150** die Berechtigung erteilen.

[0033] Durch Verwendung des Zugangskontrollmoduls **130** kann die aktuelle ZKL-Spezifikation so erweitert werden, dass sie einen als Suchfilterfeld festgelegten logischen Ausdruck und ein zusätzliches Satzoperationsfeld (z.B. in der Datenbank **115**) gemäß den beispielhaften Ausführungsformen beinhaltet. Das Zugangskontrollmodul **130** vergleicht die Suchfilterfelder mit dem Subjekt und seinen LAAs und den zusätzlichen Satzoperationsfeldern der Datenbank **115**, um inkrementell ZKL-Einträge logischer Ausdrücke (LA) **160** zu erstellen. Das Zugangskontrollmodul **130** ermittelt mithilfe der LA-ZKL-Einträge **160** die LA-Berechtigungen **160**. Die Spezifikation kann beispielsweise so aktualisiert werden, dass sie folgendermaßen aussieht:

> aclEntry: [access-id:|group:|role:] subject_DN: granted_rights | aclFilter:filter:operation:granted rights (rechteckige Klammern stehen für optionale Elemente)
> wobei:
>
> operation :- union (Vereinigung) | intersect (Schnittmenge) | replace (Ersetzung)
>
> filter :- ein grundlegender LDAP-Suchfilter, der Prädikate enthält, die Attribute verwenden können, die für Personen-LAAs stehen. Zum Beispiel können folgende Attribute verwendet werden:
>
> ibm-filterIP
>
> ibm-filterWochentag
>
> ibm-filterTageszeit
>
> rights (Rechte):- Standard-ZKL-Spezifikation, d.h. ein Satz von Berechtigungen für bestimmte Arten von LDAP-Objektspezifikationen; können explizite Verweigerungen von Berechtigungen beinhalten,

[0034] Fig. 4 zeigt eine konzeptionelle Darstellung eines Personenzugangsschaubilds **400** gemäß der beispielhaften Ausführungsformen. Konzeptionell lässt sich der ZKL-Festlegungsprozess wie folgt beschreiben:

[0035] Das Zugangskontrollmodul **130** legt bei gegebenen auf den Zugangsdatensatz anwendbaren Basis-ZKL-Einträgen **150** den Basis-Satz von ZKL-Berechtigungen **150** fest. Die Basis-ZKL-Berechtigungen **150** bei gegebenen Basis-ZKL-Einträgen **150** stellen Systeme nach dem Stand der Technik dar.

[0036] Es ist zu beachten, dass die Basis-ZKL-Berechtigungen **150** bei gegebenen Basis-ZKL-Einträgen **150** die neuen Filterfelder in der ZKL und die neuen Vergleichsattribute in der Datenbank **115** gemäß der beispielhaften Ausführungsformen nicht berücksichtigen. Die beispielhaften Ausführungsformen erlauben das Migrieren (zusätzlicher) Installationen, damit keine Modifikationen vorhandener Basis-ZKL-Einträge **150** von ZKL-Spezifikationen erforderlich sind. Das Zugangskontrollmodul **130** sammelt alle Einträge logischer Ausdrücke (LA) **150**, deren Filter bei den gegebenen logischen Ausdrucksattributen Zugangsdaten, Zugangszeit, IP-Adressen, Identitätsnachweis-Mechanismus usw. den Wert WAHR (true) ergeben. Hierzu sind folgende Beispiele zu beachten:

[0037] Als Erstes versucht die Person **5**, zwischen Samstag (durch die Zahl **6** dargestellt), Sonntag (durch die Zahl 0 dargestellt) Zugang zu erhalten, reduce rights aclentry: aclFilter:(|(ibmfilterWochentag=0) (ibm-filterWochentag=6)) :intersect:critical:rwsc:restricted:rwsc

[0038] Als Zweites versucht die Person **5**, Montag bis Freitag Zugang zum selben Computer (z.B. Kommunikationseinheit **15**) zu erhalten, guarantee a minimal set of rights aclentry: aclFilter: (&(ibmfilterIP=127.0.0.1) (ibmfilterWochentag>=1)) (ibm-

filterWochentag<=5)) :UNION:critical:rwsc:restricted: rwsc

[0039] Wenn mehrere ZKL-Eintragsfilter den Wert WAHR (true) ergeben, vereinigt das Zugangskontrollmodul **130** alle Rechte desselben Operationstyps und richtet einen eigenen repräsentativen ZLK-Eintrag für die Operationstypen Schnittmenge, Vereinigung und Ersetzung für die Person **5** ein. Dies bedeutet, dass das Zugangskontrollmodul **130** für jede Operation Vereinigungs-ZKL-Gesamteinträge **170**, Schnittmengen-ZKL-Gesamteinträge **175** und Ersetzungs-ZLK-Gesamteinträge **180** für die Person **5** festlegt und gruppiert. Wie in **Fig. 1** gezeigt beinhalten die LA-ZKL-Einträge **160** die Vereinigungs-ZKL-Gesamteinträge **170**, die Schnittmengen-ZKL-Gesamteinträge **175** und die Ersetzungs-ZLK-Gesamteinträge **180** für die Person **5**.

[0040] Das Zugangskontrollmodul **130** kann jeden der repräsentativen Schnittmengen-ZKL-Gesamteinträge **175**, der repräsentativen Vereinigungs-ZKL-Gesamteinträge **170** und der repräsentativen Ersetzungs-ZKL-Gesamteinträge **180** auf die Basis-ZKL-Einträge **150** in der folgenden Reihenfolge anwenden:

1. Wenn die Ersetzungs-ZKL-Gesamteinträge **180** durch das Zugangskontrollmodul **130** von der Datenbank **115** erhalten werden, ist das Zugangskontrollmodul **130** in der Lage, die Basis-ZKL-Einträge **150** durch die Berechtigungen der Ersetzungs-ZKL-Gesamteinträge **180** für die Person **5** zu ersetzen.

2. Wenn die Vereinigungs-ZKL-Gesamteinträge **170** durch das Zugangskontrollmodul **130** von der Datenbank **115** erhalten werden, ist das Zugangskontrollmodul **130** in der Lage, die Berechtigungen der Vereinigungs-ZKL-Gesamteinträge **170** mit dem sich aus Vorgang **1** ergebenden Satz von Berechtigungen oder den Basis-ZKL-Einträgen **150** zusammenzuführen, wenn es keine Ersetzungs-ZKL-Gesamteinträge **180** gibt.

3. Wenn die Schnittmengen-ZKL-Gesamteinträge **175** durch das Zugangskontrollmodul **130** von der Datenbank **115** erhalten werden, ist das Zugangskontrollmodul **130** in der Lage, die Schnittmenge der Schnittmengen-ZKL-Gesamteinträge **175** und dem sich aus Vorgang **2** ergebenden Satz von Berechtigungen zu bilden. Wenn es in Vorgang **2** keinen sich ergebenden Satz von Berechtigungen gibt, bildet das Zugangskontrollmodul **130** die Schnittmenge aus den Schnittmengen-ZKL-Gesamtberechtigungen **175** und dem sich aus Vorgang **1** ergebenden Satz von Berechtigungen. Wenn es keine Ersetzungs-ZKL-Gesamteinträge **180** und/oder Vereinigungs-ZKL-Gesamteinträge **170** gibt, bildet das Zugangskontrollmodul **130** die Schnittmenge aus den Schnittmengen-ZKL-Gesamteinträgen **175** und den Basis-ZKL-Einträgen.

[0041] Das Ergebnis von Vorgang **3** ist eine endgültige wirksame ZKL. Während des inkrementellen Berechnungsprozesses des Zugangskontrollmoduls **130** werden alle explizite Verweigerungen von Berechtigungen nicht beseitigt. Letztendlich wird die explizite Verweigerungsberechtigung in der endgültigen wirksamen ZKL eingerichtet und hat somit Auswirkungen auf die Berechtigungserteilung.

[0042] Die Festlegung der Rechte/Berechtigungen der endgültigen wirksamen ZKL der Person **5** auf der Kommunikationseinheit **15** für das Objekt **120** veranschaulicht das folgende Beispiel (in **Fig. 4** nicht abgebildet):

Objekt → Zugangskontrollliste (ZKL) = {{ Alle Basis-ZKL-Einträge} U { Alle ZKL-Einträge logischer Ausdrücke }}.

[0043] Gemäß beispielhaften Ausführungsformen vereinfacht dieser inkrementelle Ansatz die Arbeit eines Administrators bei der Durchsetzung von Sicherheitsanforderungen. Das Einrichten von Basis-ZKLs und die Verwendung neuer Schlüsselwörter kann die Notwendigkeit der Festlegung mehrerer redundanter ZKL-Spezifikationen verringern.

[0044] **Fig. 2** and 3 zeigen einen Ablaufplan **200** gemäß beispielhaften Ausführungsformen.

[0045] Durch einen Datenaustausch mit den Zugangskontrollmodul **130**, sucht und erbittet die Person **5** bei **205** mithilfe der Kommunikationseinheit **15** Zugang zum Objekt **120** des Servers **20**. Die Person **5** kann vielfältige Zugangsdaten wie beispielsweise einen unterscheidbaren Namen (distinguished name DN) beim Zugangskontrollmodul **130** eingeben.

[0046] Das Zugangskontrollmodul **130** ist bei **210** in der Lage, die unterscheidbaren Namen (DN) der Person **5** mit allen ZKL-Einträgen in der Datenbanken **15** zu vergleichen, und im Falle, dass eine Übereinstimmung gefunden wird, ist das Zugangskontrollmodul **130** in der Lage, DN = Satz aller übereinstimmenden Subjekt-DNs zu bestimmen.

[0047] Wenn keine DNs des Subjekts **5** übereinstimmen, ist das Zugangskontrollmodul **130** unter **215** in der Lage, alle DNs von Gruppen, zu denen die Person **5** gehört, mit allen ZKL-Einträgen in der Datenbank **115** zu vergleichen, und im Falle, dass eine Übereinstimmung gefunden wird, ist das Zugangskontrollmodul **130** in der Lage, DN = Satz aller übereinstimmenden Gruppen-DNs zu bestimmen.

[0048] Das Zugangskontrollmodul **130** ist bei **220** in der Lage, eine Basis-ZKL = VEREINIGUNG aller übereinstimmenden ZKL-Einträge aus Vorgang **210** oder Vorgang **215** zu ermitteln. Das Ergebnis von Vorgang **220** sind die Basis-ZKL-Einträge **150**.

[0049] Das Zugangskontrollmodul **130** ist bei **225** in der Lage, alle ZKL-Einträge mit logischen Ausdrücken für das Objekt **120** zu ermitteln. Das Ergebnis von Vorgang **225** sind die ZKL-Einträge logischer Ausdrücke **160**.

[0050] Das Zugangskontrollmodul **130** ist bei **230** in der Lage, alle LA-ZKL-Einträge **160** für das Objekt **120** mit logischen Ausdrücken auszuwerten, indem der Satz auf die die Person **5** anwendbarer logischer Ausdrucksattribute verwendet wird. Zu den durch das Zugangskontrollmodul **130** für die Person **5** ausgewerteten logischen Ausdrucksattribute gehören die IP-Adresse der Kommunikationseinheit **15**, den Tag, an dem die Person **5** versucht, Zugang zum Objekt **120** zu erhalten, die Art der Verbindung der Kommunikationseinheit **15** mit dem Server **20** und/oder der Identitätsnachweis-Mechanismus. Es ist zu beachten, dass sich ein Administrator gemäß der beispielhaften Ausführungsformen für einen abweichenden Satz von LAAs entscheiden kann. Das Zugangskontrollmodul **130** ist beispielsweise in der Lage festzustellen, ob der folgende logische Ausdruck wahr ist und die die darin enthaltenen Rechte gewähren: (IP=192.5.1.2 UND Zeit > 5 UND Tag= Montag): SCHNITTMENGE → {Schreiben, Löschen}

[0051] Das Zugangskontrollmodul **130** ist bei **235** in der Lage, über VEREINIGUNG alle ZKL-Einträge zu verknüpfen, deren Ausdrücke bei gleichen Satzoperatoren (wie SCHNITTMENGE (intersect), VEREINIGUNG (union) und ERSETZUNG (replace)) die Auswertung WAHR (true) ergeben, um eine einzige ZKL für jeden Operator zu erhalten. Zum Beispiel werden alle ZKL-Einträge in der Datenbank **115** für das Objekt **120** mit Vereinigungs-Operatoren in den LA-ZKL-Einträgen **160**, die die Auswertung WAHR ergeben, durch das Zugangskontrollmodul **130** verknüpft, um die Vereinigungs-ZKL-Gesamteinträge **170** zu erhalten. In ähnlicher Weise werden die ZKL-Einträge mit Schnittmengen-Operatoren in den LA-ZKL-Einträgen **160**, die die Auswertung „wahr“ ergeben, verknüpft, um die Schnittmengen-ZKL-Gesamteinträge **175** zu erhalten. Gleichermaßen werden die ZKL-Einträge mit Ersetzungs-Operatoren in den LA-ZKL-Einträgen **160**, die die Auswertung „wahr“ ergeben, verknüpft, um die Ersetzungs-ZKL-Gesamteinträge **180** zu erhalten.

[0052] Zusätzlich zu den **Fig. 2** und **Fig. 3** wird auch auf **Fig. 5** Bezug genommen. **Fig. 5** zeigt ein Venn-Diagram gemäß beispielhafter Ausführungsformen. In **Fig. 5** zeigt das Kästchen **500** die Basis-ZKL-Einträge **150**, die Vereinigungs-ZKL-Gesamteinträge logischer Ausdrücke **170**, die Schnittmengen-ZKL-Gesamteinträge logischer Ausdrücke **175** und/oder die Ersetzungs-ZKL-Gesamteinträge logischer Ausdrücke **180**.

[0053] Nach Ermitteln der den Wert WAHR (true) ergebenden LA-ZKL-Einträge **160**, welche die Vereinigungs-Gesamteinträge **170**, die Schnittmengen-Gesamteinträge **175** und/oder die Ersetzungs-Gesamteinträge **180** einschließen, fährt das Zugangskontrollmodul **130** unter Verwendung der Gesamteinträge **170**, **175** und **180** mit der inkrementellen Ermitteln der Rechte für die Person **5** fort. Das Zugangskontrollmodul **130** ist in der Lage, den folgenden Ausdruck auszuwerten: Falls bei **240** eine ERSETZUNGS-ZKL (replace ACL) gefunden wird, Verwerfen nur der BASIS-ZKL (base ACL) und Verwenden der ERSETZUNGS-ZKL; andernfalls Fortfahren unter Verwendung einer BASIS-ZKL; und falls keine BASIS-ZKL gefunden wird, Fortfahren unter Verwendung einer leeren ZKL. Kästchen **505** in **Fig. 5** zeigt das Zugangskontrollmodul **130**, das in der Lage ist, die Ersetzungs-Operation zum Ersetzen der Basis-ZKL-Einträge **150** durch die Ersetzungs-ZKL-Gesamteinträge logischer Ausdrücke **180** durchzuführen.

[0054] Das Zugangskontrollmodul **130** ist in der Lage, den folgenden Ausdruck auszuwerten: Falls unter **245** eine VEREINIGUNGS-ZKL (UNION ACL) gefunden wird, Durchführen einer VEREINIGUNGS-Operation an der VEREINIGUNGS-ZKL und dem Ergebnis des Vorgangs **240**; und falls keine VEREINIGUNGS-ZKL gefunden wird, Fortfahren unter Verwendung der Ergebnisse des Vorgangs **240**. Kästchen **510** in **Fig. 5** zeigt das Zugangskontrollmodul **130**, das in der Lage ist, die Vereinigungs-Operation zum Vereinigen der Ergebnisse von Kästchen **505** mit den Vereinigungs-ZKL-Gesamteinträgen logischer Ausdrücke **170** durchzuführen.

[0055] Das Zugangskontrollmodul **130** ist in der Lage, den folgenden Ausdruck auszuwerten: Falls unter **250** eine SCHNITTMENGEN-ZKL (INTERSECT ACL) gefunden wird, Durchführen einer SCHNITTMENGEN-Operation an der SCHNITTMENGEN-ZKL und dem Ergebnis des Vorgangs **245**; und falls keine SCHNITTMENGEN-ZKL gefunden wird, Fortfahren unter Verwendung der Ergebnisse des Vorgangs **245**. Kästchen **515** in **Fig. 5** zeigt das Zugangskontrollmodul **130**, das in der Lage ist, die Schnittmengen-Operation zur Bildung der Schnittmenge aus den Ergebnissen des Kästchens **510** und den Schnittmengen-ZKL-Gesamteinträgen logischer Ausdrücke **175** durchzuführen.

[0056] Das Zugangskontrollmodul **130** ist bei **255** in der Lage, die Ergebnisse des Vorgangs **250** als die endgültige wirksame ZKL zu erhalten. Das Kästchen **520** in **Fig. 5** zeigt die Einträge der endgültigen wirksamen ZKL für die Person, die die Kommunikations-

einheit **15** verwendet. Die Einträge der endgültigen wirksamen ZKL sind die Rechte/Berechtigungen für die Person **5**.

[0057] Das Zugangskontrollmodul **130** ist bei **260** in der Lage, die endgültige wirksame ZKL zu verwenden, um der Person den Zugang zum Objekt **120** auf dem Sever **20** zu erlauben oder zu verweigern. Zum Beispiel führt der Prozess des Ersetzens, Vereinigens und/oder der Schnittmengenbildung bei einer gegebenen Person **5** und ihren logischen Ausdrucksattributen zu einem Satz von dem Objekt **120** eigenen Rechten. Diese Rechte legen fest, was der Person **5** erlaubt ist und was nicht.

[0058] In beispielhaften Ausführungsformen ist das Objekt **120** die Ressource, die über die Zugangskontrollliste geschützt wird. Bei dem Objekt **120** kann es sich beispielsweise um verschiedene Internetseiten handeln, die auf dem Server **20** beherbergt werden (hosted), und die Person **5** erbittet Zugang zu den Internetseiten des Servers **20**. Eine Person wie die Person **5** und/oder die Kommunikationseinheit **15** ist die Einheit, die Zugang zu dem Objekt sucht. Die Person besitzt einen Satz von N Identitäten und/oder unterscheidbaren Namen (DN). Eine Gruppe ist ein Satz von N Personen, und die Gruppe wird mit ihrem eigenen DN bestimmt.

[0059] Rechte sind gewährte oder verweigerte Berechtigungen. Ein Satzoperator ist einer der Operatoren Schnittmenge, Vereinigung, und/oder Ersetzung. Die Zugangskontrollliste (ZKL) ist eine Liste von N eindeutigen Personen-/Gruppen-DN für Rechte, die Einträge abbilden, und/oder logische Ausdrücke + Satzoperator für Rechte, die Einträge abbilden. Zum Beispiel:

> Subj1 → {Lesen, Schreiben, Kopieren} Gruppe2 → {Löschen, Umbenennen, Aktualisieren; Lesen verweigern} (IP=192.5.1.2 UND Zeit > 5 UND Tag= Montag): SCHNITTMENGE □ {Schreiben, Löschen}.

[0060] Für jedes Objekt werden durch das Zugangskontrollmodul **130** LAAs festgelegt. Die Einträge logischer Ausdrücke und die Basis-ZKL-Einträge sind mit dem Objekt verknüpft. Die LAAs entsprechen der Person. Mit den LAAs der Person werden die mit dem Objekt verknüpften ZKL-Einträge logischer Ausdrücke ausgewertet.

[0061] Hinsichtlich der Satzoperatorentypen gilt ferner folgende Definition für den Schnittmengen-Operator: Satz A SCHNITTMENGE Satz B = Satz C, wobei Satz C nur Elemente beinhaltet, die SOWOHL in A als auch in B enthalten sind. Es folgt ein Beispiel für einen Schnittmengen-Operator: {A,B,C,D} SCHNITTMENGE {B,C,E,F} = {B,C}. Die Schnittmengen-Operation führt zu einer Verringerung von Rechten für die Person, es sei denn, die beiden Sätze, aus denen die Schnittmenge gebildet wird, sind identisch.

[0062] Es folgt eine Definition für den Vereinigungs-Operator: Satz A VEREINIGUNG Satz B = Satz C, wobei Satz C Elemente aus A oder B enthält. Es folgt ein Beispiel für einen Vereinigungs-Operator: {A,B,C, D} VEREINIGUNG {B,C,E,F} = {A,B,C,D,E,F}. Die Vereinigungs-Operation führt zu einer Vergrößerung von Rechten für die Person, es sei denn, die beiden vereinigten Sätze sind identisch.

[0063] Die Ersetzungs-Operation ersetzt Basis-Berechtigungen durch die Berechtigungen des logischen Ausdrucks für die Ersetzungs-Berechtigungen, und es muss keine Übereinstimmung zwischen den Basis-Berechtigungen und den Ersetzungs-Berechtigungen geben.

[0064] In einer Umsetzung von beispielhaften Ausführungsformen wird bei der Verknüpfung der Basis-Berechtigungen der Basis-ZKL-Einträge mit den Berechtigungen der Vereinigungs-ZKL-Gesamteinträge, der Schnittmengen-ZKL-Gesamteinträge und der Ersetzungs-ZKL-Gesamteinträge zuerst die Ersetzungs-Operation durchgeführt, als zweites die Vereinigungs-Operation und als drittes die Schnittmengen-Operation.

[0065] Im Hinblick auf **Fig. 1** können beispielhafte Ausführungsformen möglicherweise gemäß dem in **Fig. 1** abgebildeten Blockdiagramm **100** umgesetzt sein, sind aber nicht auf dieses beschränkt. Zudem können die Server **20** für zahlreiche Server stehen. Bei den Kommunikationseinheiten **15** und den Personen **5** kann es sich um zahlreiche Kommunikationseinheiten und Personen handeln, die Gesamtgebilde (entities) repräsentieren. Die Arbeitsplatzrechner **10** und das Netzwerk **30** können für zahlreiche Arbeitsplatzrechner und Netzwerke stehen. Ebenso kann das Objekt **120** für zahlreiche Ressourcen stehen. Daher ist das in **Fig. 1** abgebildete Blockdiagramm **100** weder zahlenmäßig auf die darin dargestellten Elemente noch auf die exakte Konfiguration und funktionsmäßigen Verbindungen von Elementen beschränkt. Weiterhin ist für den Fachmann ersichtlich, dass zu den im System **100** von **Fig. 1** beschriebenen Elementen auch Elemente hinzugefügt, weggenommen oder ausgetauscht werden können. Ebenso können die Server **20**, die Kommunikationseinheiten **15** und die Arbeitsplatzrechner **10** in prozessorgestützten Computersystemen wie in **Fig. 6** erläutert eingesetzt und so programmiert sein, dass sie gemäß der beispielhaften Ausführungsformen arbeiten und funktionieren.

[0066] **Fig. 6** zeigt ein Beispiel eines Computers **600** mit Fähigkeiten, die Teil beispielhafter Ausführungsformen sein können. Vielfältige hierin erläuterte Verfahren, Prozeduren, Module, Ablaufpläne und Tech-

nologien können ebenfalls die Merkmale des Computers **600** verkörpern oder verwenden. Eine oder mehrere Fähigkeiten des Computers **600** können in jedem hierin erläuterten Element wie beispielsweise der Kommunikationseinheit **15**, dem Arbeitsplatzrechner **10** und den Servern **20** realisiert werden.

[0067] Generell kann der Computer **600** bezüglich der Hardware-Architektur einen oder mehrere Prozessoren **610**, computerlesbaren Speicher **620** und eine oder mehrere Eingabe- und/oder Ausgabe(E/A) -Einheiten **670** beinhalten, die zum Austausch von Daten über eine lokale Schnittstelle (nicht abgebildet) verbunden sind. Bei der lokalen Schnittstelle kann es sich beispielsweise um einen oder mehrere Busse oder andere kabelgebundene oder drahtlose Verbindungen handeln, wie sie in der Technik bekannt sind. Sie ist jedoch nicht darauf beschränkt. Die lokale Schnittstelle kann zusätzliche Elemente wie Steuereinheiten (controller), Zwischenspeicher (cache), Treiber, Verstärker (repeater) und Empfänger aufweisen, um einen Datenaustausch zu ermöglichen. Weiterhin kann die lokale Schnittstelle Adressen-, Steuerungs- und/oder Datenverbindungen einschließen, um einen geeigneten Austausch von Daten zwischen den zuvor genannten Komponenten zu ermöglichen.

[0068] Der Prozessor **610** ist eine Hardware-Einheit zur Ausführung von Software, die im Speicher **620** gespeichert sein kann. Der Prozessor **610** kann praktisch jeder anwendungsspezifische oder kommerziell verfügbare Prozessor, eine Zentraleinheit (central processing unit, CPU), ein Datensignalprozessor (data signal processor DSP) oder ein Hilfsprozessor unter mehreren dem Computer **600** zugehörigen Prozessoren sein, und der Prozessor **610** kann ein Mikroprozessor auf Halbleiterbasis (in Form eines Mikrochips) oder ein Makroprozessor sein.

[0069] Als computerlesbare Speicher **620** können eines oder eine Kombination der folgenden Speicherelemente infrage kommen: flüchtige Speicherelemente wie z.B. wahlfreier Speicher (random access memory RAM) wie dynamischer wahlfreier Speicher (dynamic random access memory DRAM), statischer wahlfreier Speicher (static random access memory SRAM), usw.) sowie nichtflüchtige Speicherelemente (z.B. ROM, löschbarer programmierbarer schreibgeschützter Speicher (erasable programmable read only memory EPROM), elektronisch löschbare programmierbare schreibgeschützte Speicher (electronically erasable programmable read only memory EEPROM), programmierbare schreibgeschützte Speicher (programmable read only memory PROM), Bänder, schreibgeschützte Compact-Disk-Speicher (compact disc read only memory CD-ROM), Festplatten, Disketten, Kassetten, Bandkassetten oder Ähnliches usw.).

[0070] Darüber hinaus können dem Speicher **620** elektronische, magnetische, optische und/oder andere Arten von Speichermedien zugeordnet werden. Es ist zu beachten, dass der Speicher **620** eine verteilte Architektur aufweisen kann, bei der vielfältige Komponenten entfernt voneinander angeordnet, auf die der Prozessor **610** jedoch zugreifen kann.

[0071] Die Software im computerlesbaren Speicher **620** kann ein oder mehrere separate Programme aufweisen, von denen jedes eine geordnete Liste ausführbarer Anweisungen zur Ausführung logischer Funktionen beinhalten kann. Die Software im Speicher **620** enthält ein Betriebssystem (BS) **650**, einen Kompilierer **640**, Quellcode **630** und eine oder mehrere Anwendungen **660** der beispielhaften Ausführungsformen in jeweils geeigneter Art. Wie dargelegt umfasst die Anwendung **660** zahlreiche funktionelle Komponenten zur Umsetzung der Merkmale, Prozesse, Verfahren, Funktionen und Operationen der beispielhaften Ausführungsformen. Die Anwendung **660** des Computers **600** kann für zahlreiche Anwendungen, Agenten, Softwarekomponenten, Module, Schnittstellen usw., wie sie hierein erläutert sind, stehen. Die Anwendung **660** ist jedoch nicht als Einschränkung aufzufassen.

[0072] Das Betriebssystem **650** kann die Ausführung anderer Computerprogramme steuern und stellt eine Zeitplanung, Steuerung der Eingabe/Ausgabe, Datei- und Datenverwaltung, Speicherverwaltung und die Steuerung der Datenübertragung und verwandte Dienste bereit.

[0073] Die Anwendung(en) **660** kann (können) eine dienstorientierte Architektur verwenden, die eine Sammlung miteinander kommunizierender Dienste sein kann. Die dienstorientierte Architektur erlaubt ferner zwei oder mehreren Diensten die Koordination und/oder Durchführung von Aktivitäten (zum Beispiel füreinander). Jede Interaktion zwischen Diensten kann eigenständig und lose gekoppelt erfolgen, so dass jede Interaktion unabhängig von jeder anderen Interaktion ist.

[0074] Ferner kann die Anwendung **660** ein Quellprogramm, ausführbares Programm (Objektcode), Skript oder jede andere Einheit sein, die einen Satz durchzuführender Anweisungen umfasst. Im Falle eines Quellprogramms wird das Programm üblicherweise über einen Kompilierer (wie der Kompilierer **640**), Assemblierer, Interpretierer oder Ähnliches übersetzt, der sich gegebenenfalls im Speicher **620** befindet und in Verbindung mit dem BS **650** ordnungsgemäß arbeitet. Weiterhin kann die Anwendung **660** in (a) einer objektorientierten Programmiersprache mit Klassen von Daten und Verfahren oder (b) einer Programmiersprache mit Routinen, Unterroutinen und/oder Funktionen geschrieben sein.

[0075] Zu den E/A-Einheiten **670** können Eingabeeinheiten (oder Peripheriegeräte) wie zum Beispiel, jedoch nicht darauf beschränkt, eine Maus, eine Tastatur, eine Abtasteinrichtung, ein Mikrofon, eine Kamera usw. gehören. Weiterhin können zu den E/A-Einheiten **670** Ausgabeeinheiten (oder Peripheriegeräte) wie beispielsweise, jedoch nicht darauf beschränkt, ein Drucker, eine Anzeige usw. gehören. Schließlich können die E/A-Einheiten **670** zudem Einheiten einschließen, die sowohl Eingaben als auch Ausgaben abwickeln wie beispielsweise, jedoch nicht darauf beschränkt, eine Netzwerkkarte (NIC) oder einen Modulator/Demodulator (zum Zugriff auf ferne Einheiten, anderen Dateien, Einheiten, Systeme oder ein Netzwerk), ein Funkfrequenz- (HF) oder andere Sendeempfänger (transceiver), eine Telefonschnittstelle, eine Brücke, ein Router usw. Die E/A-Einheiten **670** schließen auch Komponenten zur Datenübertragung über vielfältige Netzwerke wie das Internet oder ein Intranet ein. Die E/A-Einheiten **670** können unter Verwendung von Bluetooth-Verbindungen und Kabel (über z.B. Ports für den Universal Serial Bus (USB), serielle Anschlüsse, parallele Anschlüsse, Firewire, HDMI (High-Definition Multimedia Interface) usw.) mit dem Prozessor **610** verbunden sein und/oder mit ihm Daten austauschen.

[0076] Wenn der Computer **600** in Betrieb ist, ist der Prozessor **610** so eingerichtet, dass er im Speicher **620** gespeicherte Software ausführen, Daten zum und vom Speicher übertragen und allgemein Vorgänge des Computers **600** entsprechend der Software steuern kann. Die Anwendung **660** und das BS **650** werden im Ganzen oder in Teilen durch den Prozessor **610** ausgelesen, möglicherweise im Prozessor **610** gepuffert und dann ausgeführt.

[0077] Wenn die Anwendung **660** als Software ausgeführt ist, sollte beachtet werden, dass die Anwendung **660** auf praktisch jedem computerlesbaren Datenträger zur Verwendung durch oder in Verbindung mit jedem computerbezogenen System oder Verfahren gespeichert werden kann. Im Kontext dieses Dokuments kann ein computerlesbarer Datenträger eine elektronische, magnetische, optische oder andere physische Einheit oder ein Mittel sein, das ein Computerprogramm zur Verwendung durch oder in Verbindung mit einem computerbezogenen System oder Vefahren beinhalten oder speichern kann.

[0078] Die Anwendung **660** kann in jedem computerlesbaren Datenträger **620** zur Verwendung durch oder in Verbindung mit einem System, einer Vorrichtung, einem Server oder einer Einheit zur Ausführung von Anweisungen wie einem computergestützten System, einem einen Prozessor beinhaltenden System oder einem anderem System, das die Anweisungen vom System, der Vorrichtung oder der Einheit zur Ausführung von Anweisungen holen und die Anweisungen ausführen kann, ausgeführt sein. Im Kontext dieses Dokuments kann ein „computerlesbarer Datenträger“ jedes Mittel sein, das das Programm zur Verwendung durch oder in Verbindung mit einem System, einer Vorrichtung oder einer Einheit zur Ausführung von Anweisungen speichern, lesen, schreiben, übertragen oder transportieren kann. Der computerlesbare Datenträger kann beispielsweise, jedoch nicht darauf beschränkt, ein(e) elektronische(s), magnetische(s), optische(s) oder Halbleitersystem, - vorrichtung oder -einheit sein.

[0079] Eine (nicht vollständige) Liste spezifischerer Beispiele des computerlesbaren Datenträgers **620** enthält die folgenden: eine elektrische Verbindung (elektronisch) mit einer oder mehreren Leitungen, eine transportable Computerdiskette (magnetisch oder optisch), ein wahlfreier Speicher (random access memory RAM) (elektronisch), ein schreibgeschützter Speicher (read-only memory ROM) (elektronisch), ein löschbarer programmierbarer schreibgeschützter Speicher (erasable programmable read-only memory EPROM, EEPROM, oder Flash-Speicher) (elektronisch), ein Lichtwellenleiter (optisch) und ein transportabler Compact-Disk-Speicher (CDROM, CD R/W) (optisch). Es ist zu beachten, dass es sich bei dem computerlesbaren Datenträger auch um Papier oder ein anderes geeignetes handeln kann, auf welches das Programm gedruckt oder eingeprägt ist, da das Programm gegebenenfalls über beispielsweise optisches Abtasten (scannen) des Papiers oder anderen geeigneten Mediums, auf welches das Programm gedruckt oder eingeprägt ist, elektronisch erfasst, dann kompiliert, interpretiert oder anderweitig in geeigneter Weise verarbeitet und dann in einem Computerspeicher gespeichert werden kann.

[0080] In beispielhaften Ausführungsformen, bei denen die Anwendung **660** als Hardware ausgeführt ist, kann die Anwendung **660** mit einer oder einer Kombination der folgenden Technologien ausgeführt sein, die in der Technik bestens bekannt sind: eine oder mehrere diskrete Logikschaltung(en) mit logischen Gattern zur Umsetzung logischer Funktionen auf Datensignale, eine anwendungsspezifische integrierte Schaltung (application specific integrated circuit ASIC) mit geeigneten Gattern kombinatorischer Logik, ein oder mehrere programmierbare Gatter-Array(s) (programmable gate array(s) PGA), ein vor Ort programmierbares Gatter-Array (field programmable gate array FPGA) usw.

[0081] Es versteht sich, dass der Computer **600** ohne einschränkende Wirkung Beispiele von Software- und Hardwarekomponenten beinhalten kann, die in vielfältigen hierein erläuterten Einheiten, Servern und Systemen enthalten sein können, und es versteht sich, dass zusätzliche Software- und Hardwarekomponenten in vielfältigen in den beispielhaften Aus-

führungsformen erläuterten Einheiten und Systemen enthalten sein können.

Patentansprüche

1. Verfahren zur Modifikation von Basisberechtigungen von Zugangskontrolllisten durch Auswerten logischer Ausdrücke auf einem Server, wobei das Verfahren Folgendes umfasst:
Ermitteln von Basisberechtigungen für eine Person (subject) durch einen Server, indem ein Name der Person mit Zugangskontrolllisteneinträgen für ein Objekt verglichen werden;
Ermitteln der logische Ausdrücke umfassenden Zugangskontrolllisteneinträge für das Objekt durch einen Server;
Auswerten der Einträge logischer Ausdrücke der Zugangskontrolllisteneinträge für das Objekt mit logischen Ausdrucksattributen der Person durch einen Server, wobei die logischen Ausdruckseinträge so ausgewertet werden, dass festgestellt wird, welche Einträge logischer Ausdrücke für die logischen Ausdrucksattribute der Person wahr sind;
für logische Ausdrucksattribute, die wahr sind, Verknüpfen von Satzoperatoren der Einträge logischer Ausdrücke durch den Server dergestalt, dass eine einzige Vereinigungs-Zugangskontrollliste, eine einzige Schnittmengen-Zugangskontrollliste und eine einzige Ersetzungs-Zugangskontrollliste vorhanden ist;
wobei die Vereinigungs-Zugangskontrollliste eine Verknüpfung von Einträgen logischer Ausdrücke ist, die einen Vereinigungs-Operator verwenden;
wobei die Schnittmengen-Zugangskontrollliste eine Verknüpfung von Einträgen logischer Ausdrücke ist, die einen Schnittmengen-Operator verwenden, und
wobei die Ersetzungs-Zugangskontrollliste eine Verknüpfung von Einträgen logischer Ausdrücke ist, die einen Ersetzungs-Operator verwenden;
als Reaktion auf das Vorhandensein der Ersetzungs-Zugangskontrollliste Durchführen einer Ersetzungs-Operation durch den Server, um die Basisberechtigungen durch die Ersetzungs-Zugangskontrollliste im Verlauf eines inkrementellen Prozesses zu ersetzen, wobei ein Ergebnis der Ersetzungs-Operation eine erste Ausgabe ist, und wobei als Reaktion auf das Vorhandensein keiner Ersetzungs-Zugangskontrollliste die Basisberechtigungen die erste Ausgabe sind;
als Reaktion auf das Vorhandensein der Vereinigungs-Zugangskontrollliste Durchführen einer Vereinigungs-Operation an der ersten Ausgabe und der Vereinigungs-Zugangskontrollliste durch den Server im Verlauf eines inkrementellen Prozesses, wobei ein Ergebnis der Vereinigungs-Operation eine zweite Ausgabe ist, und wobei als Reaktion auf das Vorhandensein keiner Vereinigungs-Zugangskontrollliste die erste Ausgabe die zweite Ausgabe ist;
als Reaktion auf das Vorhandensein der Schnittmengen-Zugangskontrollliste Durchführen einer Schnittmengen-Operation an der zweiten Ausgabe und der Schnittmengen-Zugangskontrollliste durch den Server im Verlauf eines inkrementellen Prozesses, wobei ein Ergebnis der Schnittmengen-Operation eine dritte Ausgabe ist, und wobei als Reaktion auf das Vorhandensein keiner Schnittmengen-Zugangskontrollliste die zweite Ausgabe die dritte Ausgabe ist; und
Bereitstellen der dritten Ausgabe als Berechtigungen für die Person durch den Server,
wobei die Ersetzungs-Operation zuerst durchgeführt wird, die Vereinigungs-Operation als Zweites durchgeführt wird und die Schnittmengen-Operation als Drittes durchgeführt wird, um den inkrementellen Prozess zu definieren.

2. Verfahren nach Anspruch 1, wobei logische Ausdrucksattribute vom Subjekt erhalten werden.

3. Verfahren nach Anspruch 1, wobei logische Ausdrucksattribute Folgendes umfassen: Name einer Person, Name einer Gruppe, IP-Adressen, Zugangsdaten, Identitätsnachweis-Mechanismus, Zugangszeit, Zugangsdatum und Zugangstag.

4. Verfahren nach Anspruch 1, wobei die Vereinigungs-Zugangskontrollliste eine Verknüpfung von Berechtigungen für das Objekt ist.

5. Verfahren nach Anspruch 1, wobei die Schnittmengen-Zugangskontrollliste eine Verknüpfung von Berechtigungen für das Objekt ist.

6. Verfahren nach Anspruch 1, wobei die Ersetzungs-Zugangskontrollliste eine Verknüpfung von Berechtigungen für das Objekt ist.

7. Server, der umfasst:
einen Speicher zur Speicherung eines Programms; und
einen Prozessor, der funktionsmäßig mit dem Speicher verbunden ist, wobei der Prozessor auf durch Computer ausführbare Anweisungen reagieren kann, die in dem Programm enthalten sind, und eingerichtet ist, um die Schritte eines beliebigen der Ansprüche 1 bis 6 durchzuführen.

8. Speicher, wobei der Speicher ein Computerprogramm aufweisender computerlesbarer Datenträger ist, wobei das Computerprogramm Anweisungen enthält, um einen Computer zu veranlassen, die Schritte eines beliebigen der Ansprüche 1 bis 6 durchzuführen.

Es folgen 6 Seiten Zeichnungen

Anhängende Zeichnungen

FIG. 1

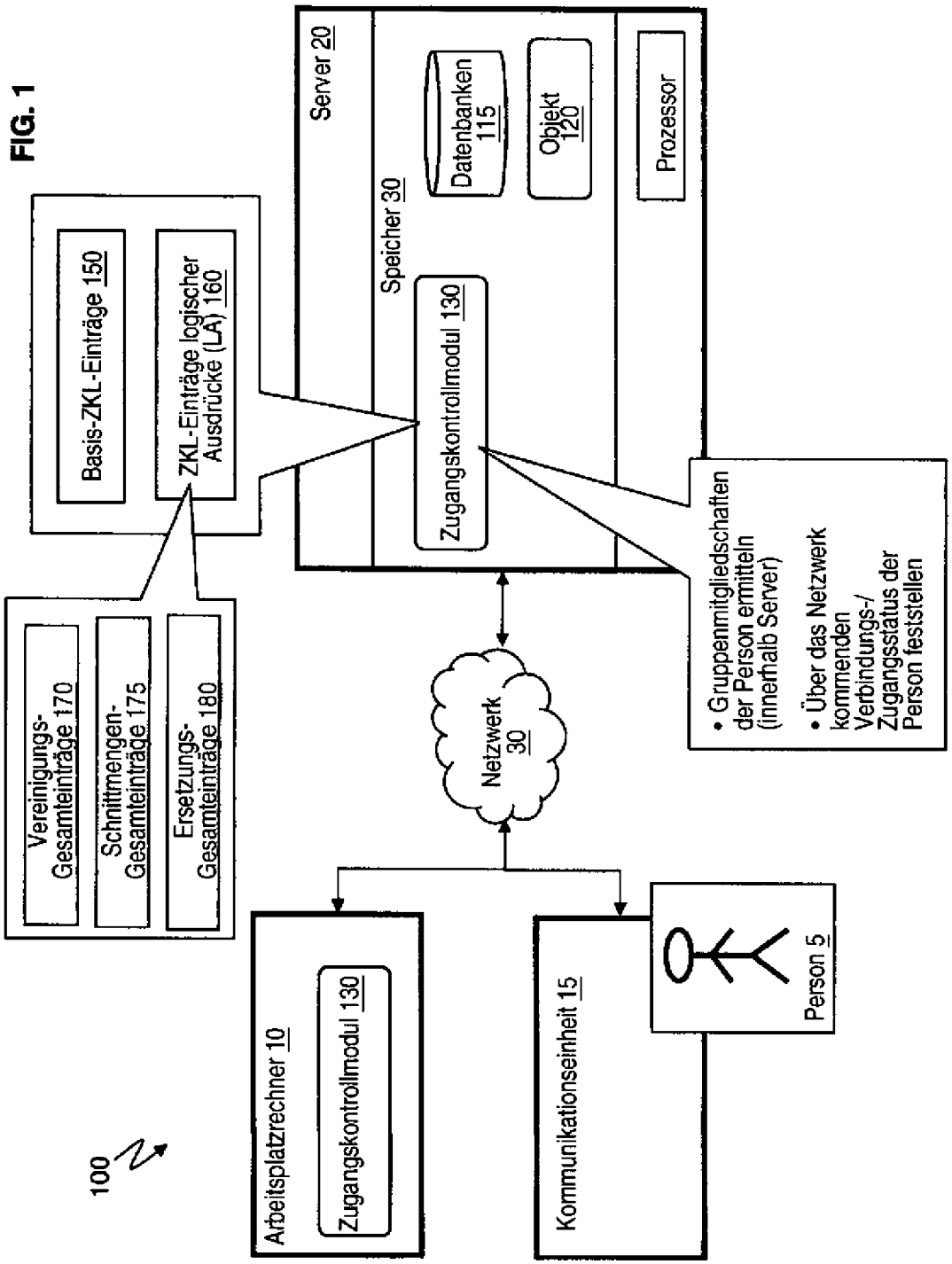


FIG. 2

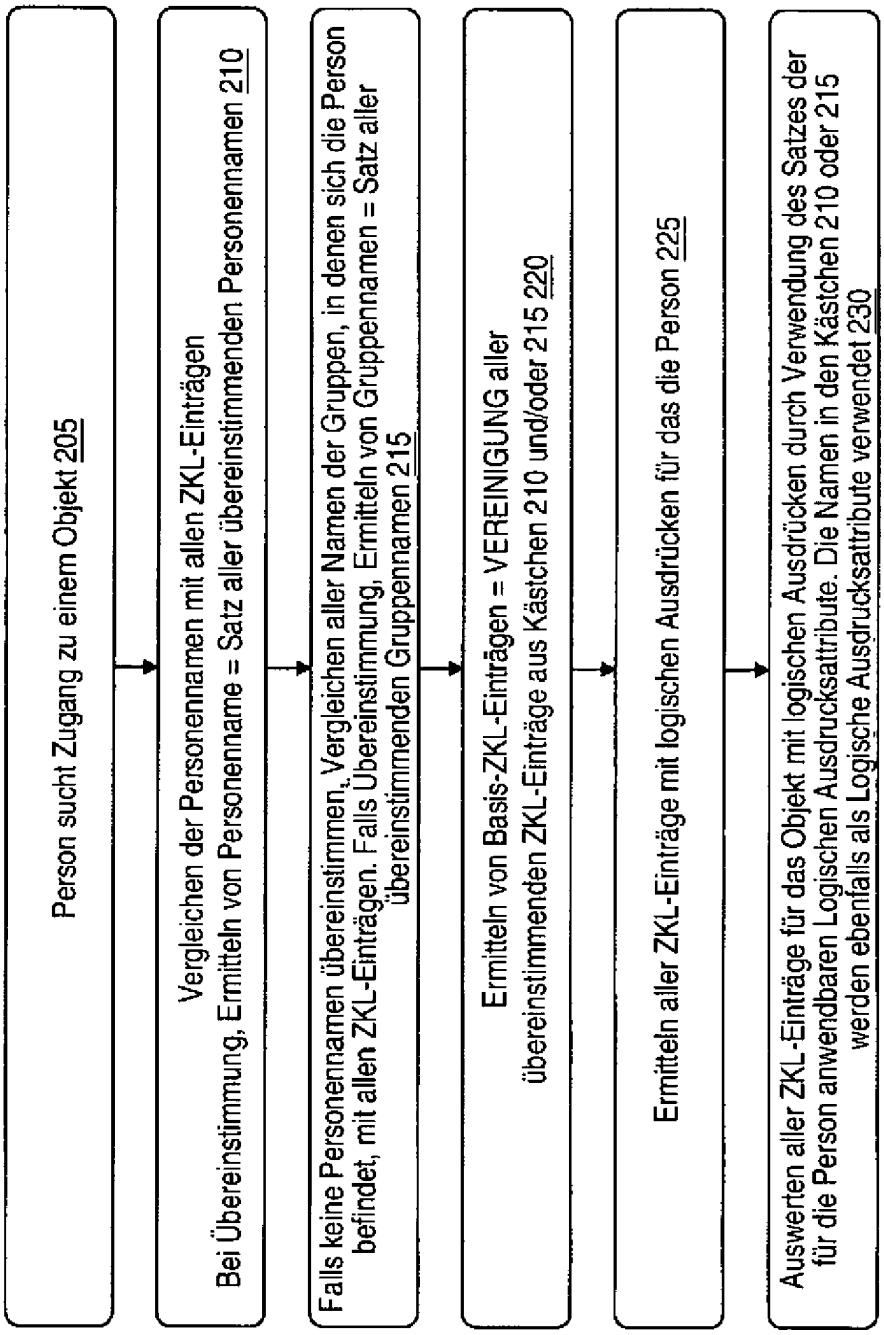

200
Person sucht Zugang zu einem Objekt 205
Vergleichen der Personennamen mit allen ZKL-Einträgen
Bei Übereinstimmung, Ermitteln von Personenname = Satz aller übereinstimmenden Personennamen 210
Falls keine Personennamen übereinstimmen, Vergleichen aller Namen der Gruppen, in denen sich die Person befindet, mit allen ZKL-Einträgen. Falls Übereinstimmung, Ermitteln von Gruppennamen = Satz aller übereinstimmenden Gruppennamen 215
Ermitteln von Basis-ZKL-Einträgen = VEREINIGUNG aller übereinstimmenden ZKL-Einträge aus Kästchen 210 und/oder 215 220
Ermitteln aller ZKL-Einträge mit logischen Ausdrücken für das die Person 225
Auswerten aller ZKL-Einträge für das Objekt mit logischen Ausdrücken durch Verwendung des Satzes der für die Person anwendbaren Logischen Ausdrucksattribute. Die Namen in den Kästchen 210 oder 215 werden ebenfalls als Logische Ausdrucksattribute verwendet 230

FIG. 3

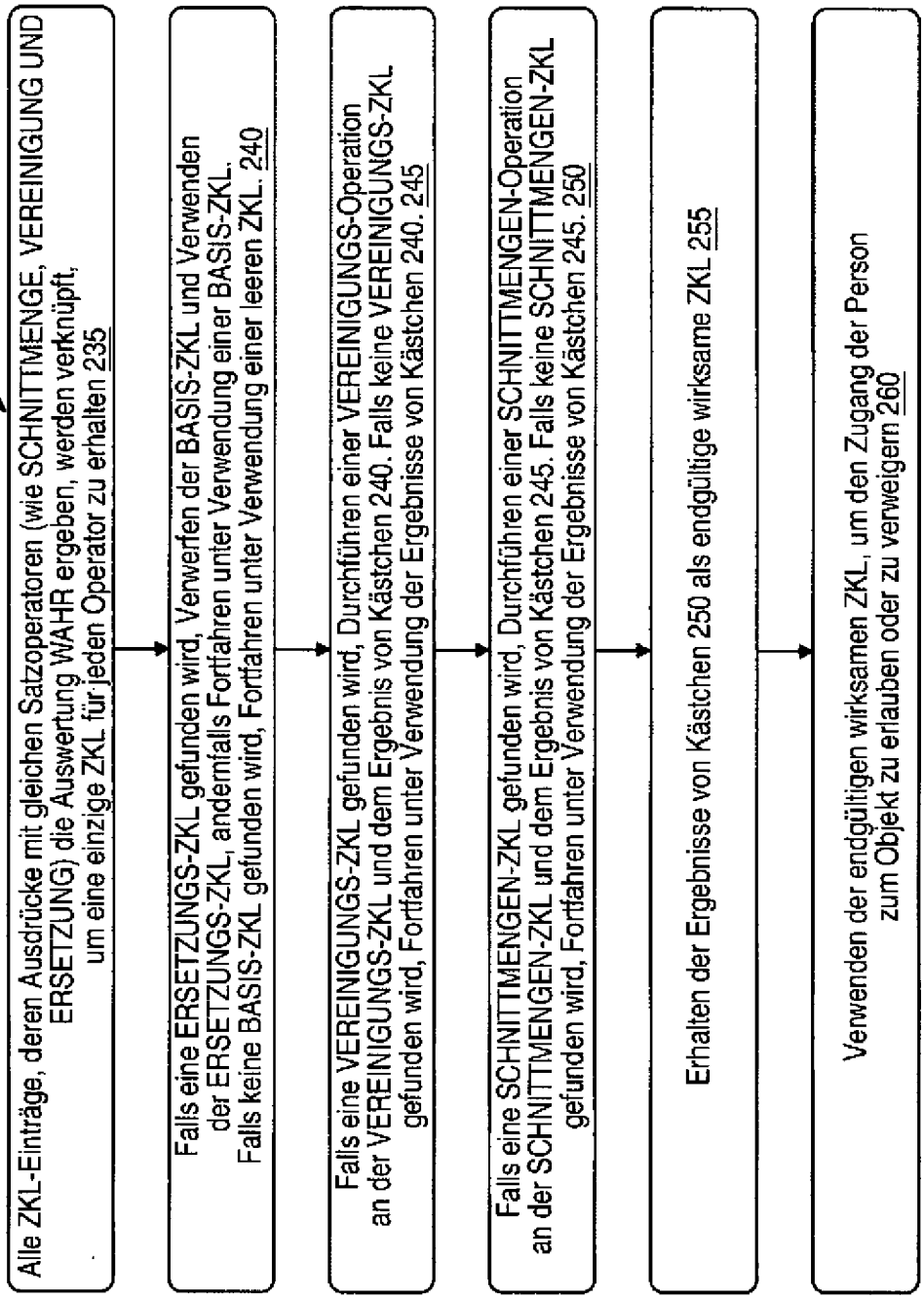

200
Alle ZKL-Einträge, deren Ausdrücke mit gleichen Satzoperatoren (wie SCHNITTMENGE, VEREINIGUNG UND ERSETZUNG) die Auswertung WAHR ergeben, werden verknüpft, um eine einzige ZKL für jeden Operator zu erhalten 235
Falls eine ERSETZUNGS-ZKL gefunden wird, Verwerfen der BASIS-ZKL und Verwenden der ERSETZUNGS-ZKL, andernfalls Fortfahren unter Verwendung einer BASIS-ZKL. Falls keine BASIS-ZKL gefunden wird, Fortfahren unter Verwendung einer leeren ZKL. 240
Falls eine VEREINIGUNGS-ZKL gefunden wird, Durchführen einer VEREINIGUNGS-Operation an der VEREINIGUNGS-ZKL und dem Ergebnis von Kästchen 240. Falls keine VEREINIGUNGS-ZKL gefunden wird, Fortfahren unter Verwendung der Ergebnisse von Kästchen 240. 245
Falls eine SCHNITTMENGEN-ZKL gefunden wird, Durchführen einer SCHNITTMENGEN-Operation an der SCHNITTMENGEN-ZKL und dem Ergebnis von Kästchen 245. Falls keine SCHNITTMENGEN-ZKL gefunden wird, Fortfahren unter Verwendung der Ergebnisse von Kästchen 245. 250
Erhalten der Ergebnisse von Kästchen 250 als endgültige wirksame ZKL 255
Verwenden der endgültigen wirksamen ZKL, um den Zugang der Person zum Objekt zu erlauben oder zu verweigern 260

FIG. 4

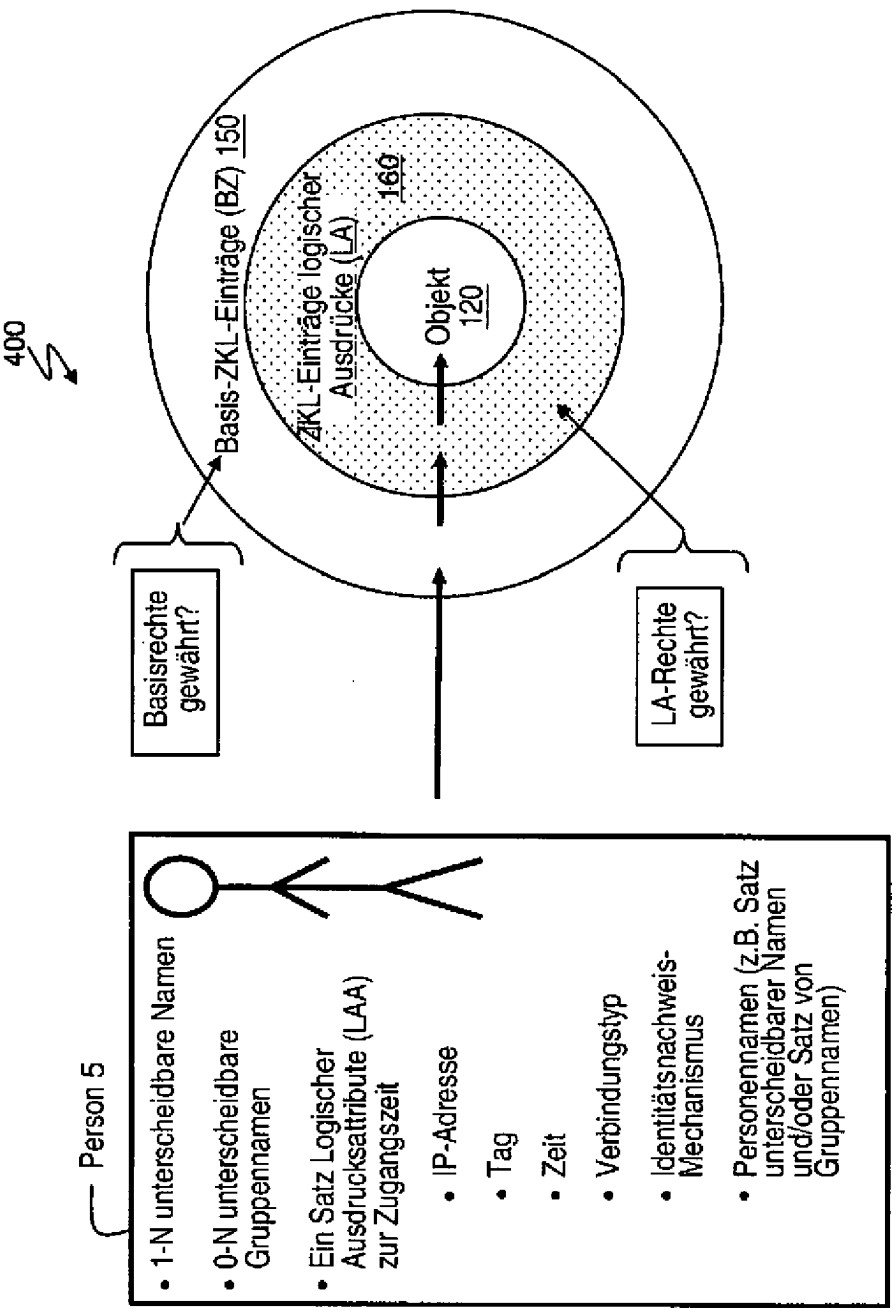

400
Basis-ZKL-Einträge (BZ) 150
ZKL-Einträge logischer Ausdrücke (LA) 160
Objekt 120
Basisrechte gewährt?
LA-Rechte gewährt?
Person 5
• 1-N unterscheidbare Namen
• 0-N unterscheidbare Gruppennamen
• Ein Satz Logischer Ausdrucksattribute (LAA) zur Zugangszeit
• IP-Adresse
• Tag
• Zeit
• Verbindungstyp
• Identitätsnachweis-Mechanismus
• Personennamen (z.B. Satz unterscheidbarer Namen und/oder Satz von Gruppennamen)

FIG. 5

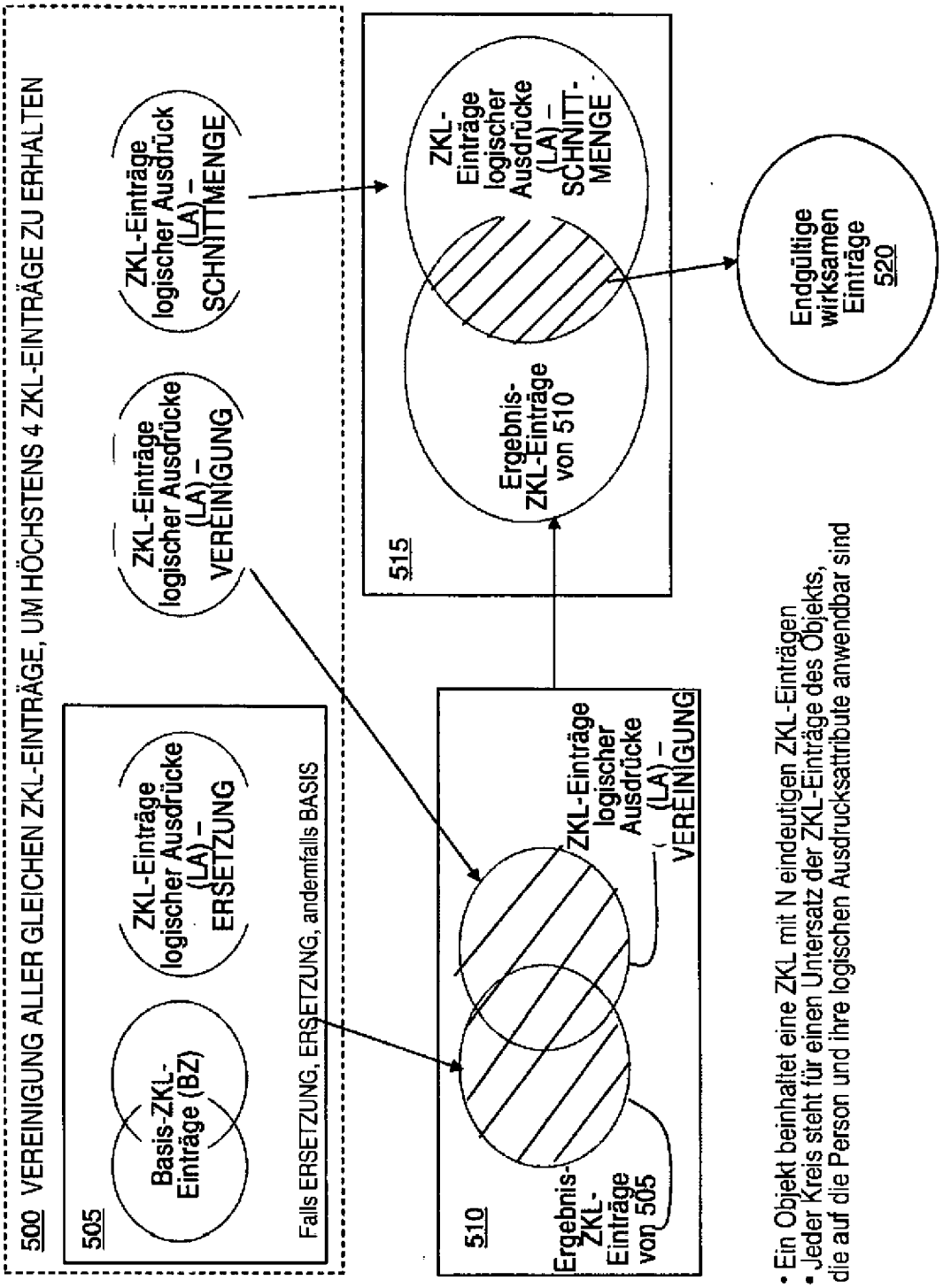
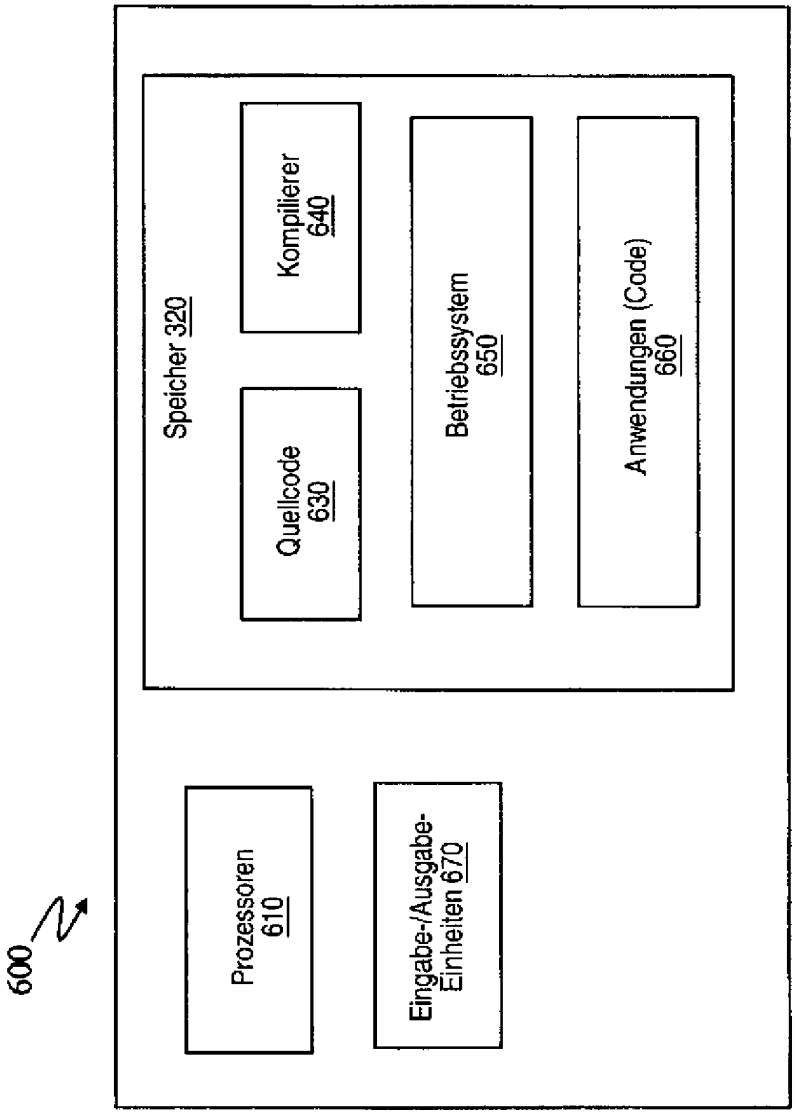

500 VEREINIGUNG ALLER GLEICHEN ZKL-EINTRÄGE, UM HÖCHSTENS 4 ZKL-EINTRÄGE ZU ERHALTEN
505
Basis-ZKL-Einträge (BZ)
ZKL-Einträge logischer Ausdrücke (LA) – ERSETZUNG
Falls ERSETZUNG, ERSETZUNG, andernfalls BASIS
ZKL-Einträge logischer Ausdrück (LA) – SCHNITTMENGE
ZKL-Einträge logischer Ausdrücke (LA) – VEREINIGUNG
510
Ergebnis-ZKL-Einträge von 505
ZKL-Einträge logischer Ausdrücke (LA) – VEREINIGUNG
515
Ergebnis-ZKL-Einträge von 510
ZKL-Einträge logischer Ausdrücke (LA) – SCHNITT-MENGE
Endgültige wirksamen Einträge 520
• Ein Objekt beinhaltet eine ZKL mit N eindeutigen ZKL-Einträgen
• Jeder Kreis steht für einen Untersatz der ZKL-Einträge des Objekts, die auf die Person und ihre logischen Ausdrucksattribute anwendbar sind

FIG. 6


600
Prozessoren 610
Eingabe-/Ausgabe-Einheiten 670
Speicher 320
Quellcode 630
Kompilierer 640
Betriebssystem 650
Anwendungen (Code) 660