(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 602 25 378 T2** 2009.03.26

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 271 882 B1**
(21) Deutsches Aktenzeichen: **602 25 378.0**
(96) Europäisches Aktenzeichen: **02 010 767.8**
(96) Europäischer Anmeldetag: **14.05.2002**
(97) Erstveröffentlichung durch das EPA: **02.01.2003**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **05.03.2008**
(47) Veröffentlichungstag im Patentblatt: **26.03.2009**

(51) Int Cl.[8]: ***H04L 29/06*** (2006.01)
G06F 1/00 (2006.01)

(30) Unionspriorität:
886146 **20.06.2001** **US**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE, TR

(73) Patentinhaber:
Microsoft Corp., Redmond, Wash., US

(74) Vertreter:
Grünecker, Kinkeldey, Stockmair & Schwanhäusser, 80802 München

(72) Erfinder:
Brezak, John E., Woodinville, WA 98072, US; Ward, Richard B., Redmond, WA 98053, US; Schmidt, Donald E., Redmond, WA 98052, US

(54) Bezeichnung: **Verfahren und Systeme zur Steuerung des Umfangs der Delegierung von Authentifizierungsdaten**

Beschreibung

Technisches Gebiet

[0001] Die Erfindung betrifft allgemein eine Computerzugriffssteuerung und insbesondere Verfahren und Systeme zur Steuerung des Umfanges einer Delegierung von Authentifizierungscredentials.

Hintergrund

[0002] Die Zugriffssteuerung ist für die Computersicherheit von überragender Bedeutung. Zum Schutz der Unversehrtheit von Computersystemen und der Vertraulichkeit von wichtigen Daten sind verschiedene Zugriffssteuerungsschemen implementiert worden, die verhindern, dass nichtautorisierte Anwender und böswillige Angreifer Zugriff auf Computerressourcen erlangen.

[0003] Zur Sicherstellung einer umfassenden Computersicherheit ist die Zugriffssteuerung oftmals in verschiedenen Ebenen implementiert. So wird beispielsweise auf der Ebene eines Computers üblicherweise verlangt, dass ein Anwender eine Logginprozedur durchläuft, in der der Computer bestimmt, ob der Anwender autorisiert ist, den Computer zu nutzen. Darüber hinaus wird auf der Ebene eines Computernetzwerkes üblicherweise verlangt, dass ein Anwender einen Anwenderauthentifizierungsprozess durchläuft, um den anwenderseitigen Zugriff auf verschiedene Netzwerkdienste zu steuern. Sogar nachdem ein Netzwerkzugriffssteuerungsserver den Anwender authentifiziert hat, muss der Anwender für einen spezifischen Server gegebenenfalls nochmals eine Erlaubnis anfordern, um einen Zugriff auf jenen Dienst zu erlangen. Es sind verschiedene Schemen auf Grundlage von verschiedenen Protokollen, so beispielsweise dem Kerberos-5-Protokoll, zur Steuerung der Netzwerkzugriffssteuerung mittels einer Anwenderauthentifizierung vorgeschlagen und implementiert worden.

[0004] Im Allgemeinen sind das anwenderseitige Einloggen in einem Computer und die Anwenderauthentifizierung für eine Netzwerkzugriffssteuerung zwei separate Prozeduren. Um die Anforderungen an einen Anwender im Umgang mit den verschiedenen Zugriffssteuerungsschemen zu minimieren, werden das anwenderseitige Einloggen und die Anwenderauthentifizierung für den Netzwerkzugriff jedoch bisweilen auch zusammen vorgenommen. Für den Fall, dass die Anwenderauthentifizierung beispielsweise unter dem Kerberos-Protokoll implementiert ist, kann, wenn sich der Anwender im Computer einloggt, der Computer ebenfalls einen Kerberos-Authentifizierungsprozess initiieren. Bei dem Authentifizierungsprozess tritt der Computer mit einer Kerberos-Schlüsselverteilungszentrale (key distribution center KDC) in Kontakt, um erstmalig ein TGT (ticket-granting ticket TGT, Ticket gewährendes Ticket) für den Anwender zu erwerben. Der Computer kann anschließend das TGT verwenden, um von der KDC ein Sitzungsticket (session ticket) für sich selbst zu erwerben.

[0005] Mit der fortschreitenden Entwicklung von Netzwerken entstand auch die Tendenz, mehrere Ebenen von Server-/Dienstcomputern bereitzustellen, die mit Clientcomputeranforderungen umgehen. Ein einfaches Beispiel stellt ein Clientcomputer dar, der über das Internet eine Anforderung auf einer WWW-Webseite tätigt. Es kann sich hierbei um einen Front-End-Webserver, der die Formatierung und die zugehörigen Regularien der Anforderung regelt, wie auch um einen Back-End-Server, der eine Datenbank für die Webseite verwaltet, handeln. Für zusätzliche Sicherheit kann die Webseite derart konfiguriert werden, dass ein Authentifizierungsprotokoll Credentials (Vertrauenswürdigkeitsnachweise), so beispielsweise das TGT des Anwenders, und/oder möglicherweise andere Informationen von dem Front-End-Server an den Back-End-Server weiterleitet (oder delegiert). Diese Praxis hat sich auf vielen Webseiten und/oder in anderen mehrere Ebenen aufweisenden Netzwerken verbreitet.

[0006] Damit kann ein beliebiger Server/Computer, der im Besitz eines TGT des Anwenders und eines zugehörigen Authentifizierers ist, Tickets im Auftrag des Anwenders/Client von der KDC anfordern. Diese Fähigkeit wird derzeit dafür eingesetzt, eine weitergeleitete Ticketdelegierung bereitstellen. Nachteiligerweise ist diese Delegierung an einen Server jedoch während der Lebensdauer des TGT prinzipiell unbeschränkt. Infolgedessen besteht Bedarf an verbesserten Verfahren und Systemen, die eine Delegierung von Authentifizierungscredentials in komplexen Netzwerkkonfigurationen in einer stärker beschränkten Weise unterstützen.

[0007] Zudem sind aus dem Beitrag „SESAME V2 Public Key und Authorization Extensions to Kerberos" von P. V. McMahon vom 16. Februar 1995 ein öffentlicher Schlüssel und Autorisierungserweiterungen für Kerberos bekannt. Insbesondere wird die Integration einer asymmetrischen Schlüsselverteilung und einer Autorisierungsunterstützung für erweitertes Kerberos beschrieben. Darüber hinaus wird als primäre Erweiterung die Unterstützung einer asymmetrischen zwischen Bereichen erfolgenden (inter-realm) Schlüsselverteilung beschrieben, um eine skalierbare sichere Zusammenarbeit (interworking) zwischen voneinander entfernten Bereichen praktikabel zu machen. Darüber hinaus wird ein Schema zum sicheren Propagieren von Grundprivilegien (principle privileges), darunter Rollen und Gruppen, von Clients an Server definiert, um die Zugriffssteuerungsverwaltungsoverheads in Endsystemen zu verringern, jedoch Befugnissteuerungssicherungen (policy control

safeguards) für eine Begrenzung dahingehend bereitzustellen, auf welche Anwendungen zugegriffen werden kann und welche überhaupt als Delegierte wirken.

[0008] Darüber hinaus ist aus dem Beitrag „On the Formal Verification of Delegation in SESAME" von M. M. Ayadi et al. vom 16. Juni 1997 die Verifizierung einer Delegierung in dem SESAME-Protokoll, einer kompatiblen Erweiterungsversion von Kerberos, bekannt. Darüber hinaus wird beschrieben, dass es das Protokoll einer Aufsicht in dem System ermöglicht, ihre Rechte an eine andere Aufsicht oder eine Gruppe von Aufsichten zu delegieren.

[0009] Darüber hinaus ist aus der Druckschrift EP-A-1 249 983, die im Zusammenhang mit Artikel 54(3) und (4) EPÜ relevant ist, eine Technik zum selektiven Steuern des Zugriffes auf die Authentifizierung mit Teilen hiervon beschrieben. Die Technik basiert auf einem Schema, bei dem die Authentifizierungsinformationen des Weiteren speziell codierte Abschnitte enthalten, die nur von ausgewählten serverbasierten Diensten/Prozessen decodiert werden können.

[0010] Zudem ist aus der Druckschrift EP-A-1 168 763, die im Zusammenhang mit Artikel 54(3) und (4) EPÜ relevant ist, eine Technik zum Authentifizieren einer Anwenderidentität zur Autorisierung eines Zugriffes auf anwendergeschützte Computerinformationen bekannt. Es wird beschrieben, dass eine anfängliche Authentifizierung zwischen einem Client und einem Server erfolgt und einem Server Delegierungsrechte entsprechend der anfänglichen Authentifizierung gewährt werden. Die dedizierten Rechte versetzen den Server in die Lage, eine Anforderung von dem Server an einen oder mehrere Endserver im Auftrag des Client zu authentifizieren.

[0011] Die Aufgabe der vorliegenden Erfindung besteht darin, verbesserte Verfahren und Systeme zur Bereitstellung einer beschränkten Delegierung von Authentifizierungscredentials bereitzustellen.

[0012] Die Aufgabe wird durch den Gegenstand der unabhängigen Ansprüche gelöst.

[0013] Bevorzugte Ausführungsbeispiele sind in den abhängigen Ansprüchen niedergelegt.

[0014] Dem vorstehend erwähnten Bedarf und darüber hinaus wird beispielsweise durch ein Verfahren entsprochen, das umfasst: ein Identifizieren eines Zieldienstes, auf den ein Zugriff im Auftrag eines Client gewünscht wird, und ein Veranlassen, dass ein Server ein neues Dienstcredential zur Verwendung durch den Server von einer vertrauenswürdigen dritten Seite anfordert. Um dies zu bewerkstelligen, stellt der Server der vertrauenswürdigen dritten Seite eine Credentialauthentifizierung, Informationen über den Zieldienst und ein Dienstcredential bereit, das vorher von dem Client oder von dem Server im Auftrag des Client erhalten worden ist. Hierbei wird das neue Dienstcredential in der Identität des Client und nicht derjenigen des Server gewährt, kann jedoch von dem Server verwendet werden, um einen Zugriff auf den Zieldienst zu erlangen.

Kurzbeschreibung der Zeichnung

[0015] Ein vollständigeres Verständnis der verschiedenen Verfahren und Systeme der vorliegenden Erfindung kann unter Bezugnahme auf die nachfolgende Detailbeschreibung in Zusammenschau mit der begleitenden Zeichnung erhalten werden, die sich wie folgt zusammensetzt.

[0016] Fig. 1 ist ein Blockdiagramm, das allgemein ein exemplarisches Computersystem darstellt, bei dem die vorliegende Erfindung implementiert werden kann.

[0017] Fig. 2 ist ein Blockdiagramm zur Darstellung eines S4U2proxy-Prozesses (service-for-user-to-proxy S4U2proxy), der innerhalb der Client-Server-Umgebung ausgeführt wird, entsprechend bestimmten exemplarischen Implementierungen der vorliegenden Erfindung.

[0018] Fig. 3A ist ein Blockdiagramm zur Darstellung eines S4U2self-Prozesses (service-for-user-to-self S4U2self), der innerhalb einer Client-Server-Umgebung ausgeführt wird, entsprechend bestimmten exemplarischen Implementierungen der vorliegenden Erfindung.

[0019] Fig. 3B ist ein Blockdiagramm zur Darstellung eines S4U2self-Prozesses (service-for-user-to-self S4U2self), der innerhalb einer Client-Server-Umgebung ausgeführt wird, entsprechend bestimmten weiteren exemplarischen Implementierungen der vorliegenden Erfindung.

[0020] Fig. 4 ist ein illustratives Diagramm zur Darstellung von ausgewählten Abschnitten eines Nachrichtenformates, das zur Verwendung bei bestimmten Implementierungen der vorliegenden Erfindung geeignet ist.

Detailbeschreibung

[0021] In der Zeichnung bezeichnen gleiche Bezugszeichen gleiche Elemente. Die Erfindung ist hierbei als in einer geeigneten Berechnungsumgebung implementiert dargestellt. Obwohl nicht erforderlich, wird die Erfindung im allgemeinen Kontext von computerseitig ausführbaren Anweisungen beschrieben, so beispielsweise von Programmmodulen, die von einem Personalcomputer ausgeführt

werden. Zu den Programmmodulen zählen im Allgemeinen Routinen, Programme, Objekte, Komponenten, Datenstrukturen und dergleichen mehr, die bestimmte Ausgaben ausführen oder bestimmte abstrakte Datentypen implementieren. Darüber hinaus erschließt sich einem Fachmann auf dem einschlägigen Gebiet, dass die Erfindung auch bei anderen Computersystemkonfigurationen Anwendung finden kann, darunter bei Handvorrichtungen, Multiprozessorsystemen, mikroprozessorbasierten oder programmierbaren Geräten der Unterhaltungselektronik, Netzwerk-PCs, Minicomputern, Mainframecomputern und dergleichen mehr. Die Erfindung kann auch in verteilten Berechnungsumgebungen zum Einsatz kommen, wo Aufgaben von entfernt angeordneten Verarbeitungsvorrichtungen ausgeführt werden, die über ein Kommunikationsnetzwerk verbunden sind. In einer verteilten Berechnungsumgebung können Programmmodule sowohl in am Ort befindlichen wie auch in entfernt angeordneten Speicherablagevorrichtungen befindlich sein.

[0022] Fig. 1 zeigt ein Beispiel einer geeigneten Berechnungsumgebung **120**, in der die nachfolgend beschriebenen Verfahren und Systeme implementiert sein können.

[0023] Die exemplarische Berechnungsumgebung **120** ist lediglich ein Beispiel für eine geeignete Berechnungsumgebung und soll keinerlei Beschränkung mit Blick auf den Verwendungsumfang oder die Funktionalität der verbesserten Verfahren und Systeme gemäß vorliegender Beschreibung beinhalten. Ebenso wenig soll die Berechnungsumgebung **120** dahingehend verstanden werden, dass eine Abhängigkeit oder Notwendigkeit in Bezug auf eine beliebige Komponente oder Kombinationen hieraus dergestalt besteht, wie dies in der Berechnungsumgebung **120** dargestellt ist.

[0024] Die verbesserten Verfahren und Systeme gemäß vorliegender Beschreibung funktionieren bei zahlreichen anderen Allzweck- oder Sonderzweckberechnungssystemumgebungen oder Konfigurationen. Beispiele für bekannte Berechnungssysteme, Umgebungen und/oder Konfigurationen, die geeignet sein können, umfassen unter anderem Personalcomputer, Servercomputer, thin clients, thick clients, Hand- oder Laptopvorrichtungen, Multiprozessorsysteme, mikroprozessorbasierte Systeme, Settopboxen, programmierbare Geräte der Unterhaltungselektronik, Netzwerk-PCs, Minicomputer, Mainframecomputer, verteilte Berechnungsumgebungen, die beliebige der vorgenannten Systeme oder Vorrichtungen beinhalten, und dergleichen mehr.

[0025] Wie in Fig. 1 gezeigt ist, umfasst die Berechnungsumgebung **120** eine Allzweckcomputervorrichtung in Form eines Computers **130**. Die Komponenten des Computers **130** können einen oder mehrere Prozessoren oder Verarbeitungseinheiten **132**, einen Systemspeicher **134** und einen Bus **136** beinhalten, der die verschiedenen Systemkomponenten koppelt, darunter einen Systemspeicher **134** mit einem Prozessor **132**.

[0026] Der Bus **136** verkörpert einen oder mehrere Typen von Busstrukturen, darunter einen Speicherbus oder einen Speichercontroller, einen Peripheriebus, einen beschleunigten Grafikport und einen Prozessor oder lokalen Bus, bei dem eine beliebige aus einer Vielzahl von Busarchitekturen zum Einsatz kommt. Zu diesen Architekturen zählen beispielsweise, jedoch nicht ausschließlich, der ISA-Bus (industry standard architecture ISA, Industriestandardarchitektur), der MCA-Bus (micro channel architecture MCA, Mikrokanalarchitektur), der EISA-Bus (enhanced industry standard architecture EISA, weiterentwickelte Industriestandardarchitektur), der VESA-Lokalbus (video electronics standard association VESA) und der PCI-Bus (peripheral component interconnects PCI), der auch als Mezzanin-Bus bekannt ist.

[0027] Der Computer **130** umfasst üblicherweise eine Vielzahl von computerlesbaren Medien. Derartige Medien können beliebige verfügbare Medien sein, auf die der Computer **130** zugreifen kann, wobei hierzu sowohl flüchtige wie auch nichtflüchtige Medien und sowohl herausnehmbare wie auch nichtherausnehmbare Medien zählen.

[0028] Wie in Fig. 1 gezeigt ist, umfasst der Systemspeicher **134** computerlesbare Medien in Form eines flüchtigen Speichers, so beispielsweise eines RAM (Speicher mit wahlfreiem Zugriff) **140**, und/oder eines nichtflüchtigen Speichers, so beispielsweise eines ROM (Nurlesespeicher) **138**. Ein grundlegendes Eingabe-/Ausgabe-System (basic input/output system BIOS) **142**, das die grundlegenden Routinen enthält, die den Transfer von Informationen zwischen Elementen innerhalb des Computers **130** beispielsweise während des Hochfahrens unterstützen, ist in dem ROM **138** gespeichert. Der RAM **140** enthält üblicherweise Daten und/oder Programmmodule, auf die unmittelbar durch den Prozessor **132** zugegriffen werden kann oder die von diesem momentan verarbeitet werden.

[0029] Der Computer **130** kann des Weiteren andere herausnehmbare/nichtherausnehmbare und flüchtige/nichtflüchtige Computerspeichermedien enthalten. So zeigt Fig. 1 beispielsweise ein Festplattenlaufwerk **144** zum Lesen von oder Schreiben auf nichtherausnehmbare, nichtflüchtige magnetische Medien (nicht gezeigt und üblicherweise „Festplattenlaufwerk" genannt), ein Laufwerk **146** für magnetische Platten zum Lesen von und Schreiben auf eine herausnehmbare, nichtflüchtige magnetische Platte **148** (beispielsweise eine „Floppydisk") und ein Laufwerk **150** für optische Platten zum Lesen von oder

Schreiben auf eine herausnehmbare, nichtflüchtige optische Platte **152**, so beispielsweise eine CD-ROM, eine CD-R, eine CD-RW, eine DVD-ROM, eine DVD-RAM oder andere optische Medien. Das Festplattenlaufwerk **144**, das Laufwerk **146** für magnetische Platten und das Laufwerk **150** für optische Platten sind jeweils mit dem Bus **136** über eine oder mehrere Schnittstellen **154** verbunden.

[0030] Die Laufwerke und die zugehörigen computerlesbaren Medien ermöglichen eine nichtflüchtige Speicherung von computerseitig lesbaren Anweisungen, Datenstrukturen, Programmmodulen und anderen Daten für den Computer **130**. Obwohl bei der exemplarischen hier beschriebenen Umgebung eine Festplatte, eine herausnehmbare magnetische Platte **148** und eine herausnehmbare optische Platte **152** zum Einsatz kommen, erschließt sich einem Fachmann auf dem einschlägigen Gebiet unmittelbar, dass andere Arten von computerseitig lesbaren Medien zum Einsatz kommen können, die Daten speichern können, auf die ein Computer zugreifen kann, so beispielsweise magnetische Kassetten, Flash-Memory-Karten, digitale Videodisks, RAMs, ROMs und dergleichen, die ebenfalls in der exemplarischen Betriebsumgebung zum Einsatz kommen können.

[0031] Eine Mehrzahl von Programmmodulen kann auf der Festplatte, der magnetischen Platte **148**, der optischen Platte **152**, in dem ROM **138** oder dem RAM **140** gespeichert sein, darunter beispielsweise ein Betriebssystem **158**, ein oder mehrere Anwendungsprogramme **160**, andere Programmmodule **162** und Programmdaten **164**.

[0032] Die verbesserten Verfahren und Systeme gemäß vorliegender Beschreibung können innerhalb des Betriebssystems **158**, eines oder mehrerer Anwendungsprogramme **160**, anderer Programmmodule **162** und/oder Programmdaten **164** implementiert werden.

[0033] Ein Anwender kann Befehle und Informationen in einen Computer **130** über Eingabevorrichtungen eingeben, so beispielsweise eine Tastatur **166** und eine Zeigevorrichtung **168** (so beispielsweise eine „Maus"). Andere Eingabevorrichtungen (nicht gezeigt) sind unter anderem ein Mikrofon, ein Joystick, ein Gamepad, eine Satellitenschüssel, ein serieller Port, ein Scanner, eine Kamera und dergleichen mehr. Diese und weitere Eingabevorrichtungen sind mit der Verarbeitungseinheit **132** über eine Anwendereingabeschnittstelle **170** verbunden, die mit dem Bus **136** gekoppelt ist; sie können jedoch auch über eine andere Schnittstelle und andere Busstrukturen gekoppelt sein, so beispielsweise einen Parallelport, einen Gameport oder einen universellen seriellen Bus (USB).

[0034] Ein Monitor **172** oder eine andere Art von Anzeigevorrichtung ist ebenfalls mit dem Bus **136** über eine Schnittstelle, so beispielsweise einen Videoadapter **174**, verbunden. Zusätzlich zu dem Monitor **172** umfassen Personalcomputer üblicherweise weitere Peripherieausgabevorrichtungen (nicht gezeigt), so beispielsweise Lautsprecher und Drucker, die über eine Peripherieausgabeschnittstelle **175** angeschlossen werden können.

[0035] Der Computer **130** kann in einer vernetzten Umgebung unter Verwendung logischer Verbindungen mit einem oder mehreren entfernt angeordneten Computern, so beispielsweise einem entfernt angeordneten Computer **182**, arbeiten. Der entfernt angeordnete Computer **182** kann viele oder alle Elemente und Merkmale enthalten, die hier in Zusammenhang mit dem Computer **130** beschrieben werden.

[0036] Die in Fig. 1 gezeigten logischen Verbindungen sind ein Netzwerk im Ortsbereich (local area network LAN) **177** und ein allgemeines Netzwerk im Weitbereich (wide area network WAN) **179**. Derartige Netzwerkumgebungen sind in Büros, unternehmensweiten Computernetzwerken, Intranets und dem Internet allgegenwärtig.

[0037] Bei Verwendung in einer LAN-Netzwerkumgebung ist der Computer **130** mit einem LAN **177** über eine Netzwerkschnittstelle oder einen Adapter **186** verbunden. Bei Verwendung in einer WAN-Netzwerkumgebung beinhaltet der Computer üblicherweise ein Modem **178** oder ein anderes Mittel zum Abwickeln von Kommunikationsvorgängen über das WAN **179**. Das WAN **178**, das intern oder extern sein kann, kann mit einem Systembus **136** über die Anwendereingabeschnittstelle **170** oder einen anderen geeigneten Mechanismus verbunden sein.

[0038] Fig. 1 zeigt eine spezifische Implementierung eines WAN über das Internet. Hierbei verwendet der Computer **130** ein Modem **178** zum Abwickeln von Kommunikationsvorgängen mit wenigstens einem entfernt angeordneten Computer **182** über das Internet **180**.

[0039] In einer vernetzten Umgebung können Programmmodule, die im Zusammenhang mit dem Computer **130** beschrieben worden sind, oder Teile hiervon in einer entfernt angeordneten Speicherablagevorrichtung gespeichert werden. Wie in Fig. 1 gezeigt ist, können die entfernt angeordneten Anwendungsprogramme **189** in einer Speichervorrichtung des entfernt angeordneten Computers **182** befindlich sein. Es ist einsichtig, dass die gezeigten und beschriebenen Netzwerkverbindungen exemplarisch sind und andere Mittel zum Abwickeln einer Kommunikationsverbindung zwischen den Computern verwendet werden können.

[0040] Die Beschreibung konzentriert sich nachste-

hend auf bestimmte Aspekte im Zusammenhang mit der vorliegenden Erfindung zum Steuern des Umfanges einer Delegierung von Authentifizierungscredentials in einer Client-Server-Netzwerkumgebung. Obwohl die nachfolgende Beschreibung auf exemplarische Kerberos-basierte Systeme und Verbesserungen hieran abstellt, sind die verschiedenen Verfahren und Systeme der vorliegenden Erfindung selbstredend auch bei anderen Authentifizierungssystemen und Techniken anwendbar. So können beispielsweise zertifikatbasierte Authentifizierungssysteme und Techniken ebenfalls bestimmte Aspekte der vorliegenden Erfindung umsetzen.

[0041] Wie vorstehend erläutert worden ist, versetzt der Besitz eines TGT (ticket granting ticket TGT, Ticket gewährendes Ticket) eines Client und des zugehörigen Authentifizierers den Halter in die Lage, Tickets im Auftrag des Client von der vertrauenswürdigen dritten Seite anzufordern, so beispielsweise einer Schlüsselverteilungszentrale (key distribution center KDC). Eine derartige unbeschränkte Delegierung wird derzeit in bestimmten Implementierungen von Kerberos, die über weitergeleitete Ticketdelegierungsschemen verfügen, unterstützt.

[0042] Eingedenk dessen werden Verfahren und Systeme bereitgestellt, die den Delegierungsprozess beschränken oder auf andere Weise besser steuern. Die Verfahren und Systeme können mit verschiedenen Authentifizierungsprotokollen verwendet werden. Der Delegierungsprozess wird bei bestimmten exemplarischen Implementierungen von einer S4U2proxy-Technik (service-for-user-to-proxy) gesteuert. Die S4U2proxy-Technik ist vorzugsweise als Protokoll implementiert, das sich eines Servers oder eines Dienstes bedient, so beispielsweise eines Front-End-Servers/Dienstes, um Diensttickets im Auftrag eines Client zur Verwendung mit anderen Servern/Diensten anzufordern. Wie nachstehend detaillierter beschrieben wird, ermöglicht das S4U2proxy-Protokoll vorteilhafterweise eine beschränkte steuerbare Delegierung, bei der nicht erforderlich ist, dass der Client ein TGT an den Front-End-Server weiterleitet.

[0043] Eine weitere hier vorgestellte Technik ist die S4U2self-Technik (service-for-user-to-self). Die S4U2self-Technik oder das zugehörige Protokoll versetzen einen Server in die Lage, ein Dienstticket für sich selbst anzufordern, und zwar mit der Identität des Client, die in dem resultierenden Dienstticket bereitgestellt wird. Dies versetzt beispielsweise einen Client, der von anderen Authentifizierungsprotokollen authentifiziert worden ist, in die Lage, im Wesentlichen über ein Dienstticket zu verfügen, das mit dem S4U2proxy-Protokoll zur Bereitstellung einer beschränkten Delegierung verwendet werden kann. Es gibt zwei exemplarische Formen für die S4U2self-Technik, nämlich die „nachweisfreie" („no evidence") Form und die „nachweisbehaftete" („evidence") Form. Bei der nachweisfreien Form ist der Server dahingehend vertrauenswürdig, dass er den Client authentifiziert, und zwar beispielsweise unter Verwendung eines anderen Sicherheits-/Authentifizierungsmechanismus, der beispielsweise servereigen ist. Bei der nachweisbehafteten Form vollzieht die KDC (oder eine vertrauenswürdige dritte Seite) die Authentifizierung auf Basis von Informationen (Nachweis, evidence), die über den Client bereitgestellt und erhalten werden, wenn der Client bei dem Server authentifiziert ist.

[0044] Bei den hier vorgeschlagenen Verfahren und Systemen kann ein Client auf Server/Dienste innerhalb einer Kerberos-Umgebung unabhängig davon zugreifen, ob der Client von Kerberos oder einem anderen Authentifizierungsprotokoll authentifiziert ist. Infolgedessen können Back-End- und/oder andere Server/Dienste in einer im Wesentlichen nur auf Kerberos basierenden Umgebung betrieben werden.

[0045] Bezug wird nachstehend auf das Blockdiagramm von Fig. 2 genommen, das ein S4U2proxy-Protokoll bzw. einen zugehörigen Prozess innerhalb der Client-Server-Umgebung **200** entsprechend bestimmten exemplarischen Implementierungen der vorliegenden Erfindung bereitstellt.

[0046] Wie gezeigt ist, ist ein Client **202** funktionell mit einer vertrauenswürdigen dritten Seite **204** gekoppelt, worin funktionell ein Authentifizierungsdienst **206** konfiguriert ist, so beispielsweise eine KDC, eine Zertifikaterteilungs- bzw. Gewährungsbehörde, ein Domänen-Controller und dergleichen mehr. Der Authentifizierungsdienst **206** ist derart konfiguriert, dass er auf Informationen zugreift, die in einer Datenbank **208** vorgehalten werden. Der Client **202** und die vertrauenswürdige dritte Seite **204** sind des Weiteren funktionell mit einem Server, nämlich einem Server A **210** gekoppelt. Man beachte, dass bei der vorliegenden Erfindung die Begriffe „Server" und „Dienst" synonym verwendet werden und dieselbe oder eine ähnliche Funktionalität bezeichnen.

[0047] Bei diesem Beispiel ist der Server A **210** ein Front-End-Server für eine Mehrzahl von anderen Servern. Wie dargestellt ist, ist der Server A210 funktionell mit dem Server B **212** und dem Server C **214** gekoppelt. Wie dargestellt ist, kann der Server B **202** ein replizierter Dienst sein. Zudem ist der Server C **214** funktionell mit einem Server D **216** gekoppelt.

[0048] In Reaktion auf ein anwenderseitiges Einloggen auf einem Client **202** wird eine AS_REQ-Nachricht **220** (authentication request AS_REQ, Authentifizierungsanforderung) an den Authentifizierungsdienst **206** gesendet, der mit einer AS_REP-Nachricht (authentication reply AS_REP, Authentifizierungsantwort) **222** antwortet. Innerhalb der

AS_REP-Nachricht **222** befindet sich ein TGT, das mit dem Anwender/Client verknüpft ist. Derselben oder einer ähnlichen Prozedur (nicht dargestellt) wird auch zum Authentifizieren des Servers A **210** gefolgt.

[0049] Wünscht der Client **202** einen Zugriff auf den Server A **210**, so sendet der Client eine TGS_REQ-Nachricht (ticket granting service request TGS_REQ, Ticketgewährungsdienstanforderung) **224** an den Authentifizierungsdienst **206**, der eine TGS_REP-Nachricht (ticket granting service reply TGS_REP, Ticketgewährungsdienstantwort) **226** zurücksendet. Die TGS_REP-Nachricht **226** beinhaltet ein Dienstticket, das mit dem Client **202** und dem Server A **210** verknüpft ist. Anschließend leitet der Client **202**, um eine Kommunikationssitzung zu initiieren, das Dienstticket an den Server A **210** in einer AP_REQ-Nachricht (application protocol request AP_REQ, Anwendungsprotokollanforderung) **228** weiter. Derartige Prozesse/Prozeduren sind bekannt, weshalb sie hier nicht im Detail erläutert werden.

[0050] Bislang war es notwendig, dass der Client für den Server A **210** das TGT des Client zur Unterstützung einer Delegierung bereitstellt, um den Server A **210** in die Lage zu versetzen, zusätzliche Dienstticketes im Auftrag des Client **202** anzufordern. Dies ist nun nicht mehr notwendig. Anstatt dessen arbeiten, wenn der Server A **210** einen Zugriff auf einen weiteren Server im Auftrag eines Client **202**, beispielsweise auf den Server C **214**, anfordert, der Server A **210** und der Authentifizierungsdienst **206** entsprechend einem S4U2proxy-Protokoll.

[0051] Entsprechend bestimmten exemplarischen Implementierungen des S4U2proxy-Protokolls sendet beispielsweise der Server A **210** eine TGS_REQ-Nachricht **230** an den Authentifizierungsdienst **206**. Die TGS_REQ-Nachricht **230** enthält das TGT für den Server A **210** und das von dem Client **202** empfangene Dienstticket und identifiziert den gewünschten oder angepeilten Server/Dienst, auf den der Client **102** einen Zugriff wünscht, so beispielsweise der Server C **214**. Bei Kerberos ist beispielsweise ein erweiterbares Datenfeld definiert, das üblicherweise als Feld für zusätzliche Tickets („additional tickets" field) bezeichnet wird. Dieses Feld für zusätzliche Tickets kann bei dem S4U2proxy-Protokoll verwendet werden, um das von dem Client **202** empfangene Dienstticket zu tragen, wobei ein KDC-Optionen-Feld ein Flag bzw. einen Merker oder einen anderen Indikator enthalten kann, der die empfangende KDC anweist, in dem Feld für zusätzliche Tickets nach einem Ticket zu sehen, das dann zur Bereitstellung einer Clientidentität verwendet wird. Einem Fachmann auf dem Gebiet erschließt sich, dass diese oder andere Felder und/oder Datenstrukturen zum Tragen der notwendigen Informationen zu dem Authentifizierungsdienst **206** verwendet werden können.

[0052] Bei der Verarbeitung der TGS_REQ-Nachricht **230** bestimmt der Authentifizierungsdienst **206**, ob der Client **202** über eine autorisierte Delegierung verfügt, und zwar beispielsweise auf Grundlage des Wertes eines „weiterleitbaren" („forwardable") Flags, das von dem Client **202** bereitgestellt wird. Daher wird eine Delegierung pro Client durch das Vorhandensein des weiterleitbaren Flags in dem Dienstticket des Client gefördert. Wünscht der Client **202** keine Teilnahme an der Delegierung, so wird das Ticket nicht durch das Flag als weiterleitbar markiert. Der Authentifizierungsdienst **206** wertet dieses Flag als clientseitig initiierte Einschränkung (client initiated restriction).

[0053] Bei anderen Implementierungen kann der Authentifizierungsdienst **206** auf zusätzliche Informationen in einer Datenbank **208** zugreifen, die ausgewählte Dienste definiert, hinsichtlich derer der Server A **210** die Erlaubnis hat, sie in Bezug auf den Client **202** zu delegieren (oder eben nicht zu delegieren).

[0054] Bestimmt der Authentifizierungsdienst **206**, dass der Server A **210** die Erlaubnis hat, den angepeilten Server/Dienst zu delegieren, so wird eine TGS_REP-Nachricht **232** an den Server A **210** gesendet. Die TGS_REP-Nachricht **232** enthält ein Dienstticket für den angepeilten Server/Dienst. Das Dienstticket wirkt derart, als hätte es der Client **202** direkt von dem Authentifizierungsdienst **206** beispielsweise unter Verwendung des TGT des Client angefordert. Dies ist jedoch nicht erfolgt. Anstatt dessen hat der Authentifizierungsdienst **206** auf ähnliche/notwendige Clientinformationen in der Datenbank **208** zugegriffen, nachdem sichergestellt worden ist, dass der authentifizierte Client in die Anforderung auf Basis des Diensttickets, das der authentifizierte Server A **210** von dem Client **202** empfangen hat und das die TGS_REQ-Nachricht **230** enthielt, im Wesentlichen einbezogen ist. Da jedoch die Clientinformationen in dem Ticket des Client getragen werden, muss der Server nur die Daten aus dem Ticket kopieren. Damit kann die Datenbank **208** verwendet werden, wobei jedoch das Kopieren der Daten in dem Ticket tendenziell effizienter ist.

[0055] Bei bestimmten Implementierungen identifiziert beispielsweise die TGS_REP-Nachricht **232** den angepeilten Server/Dienst und den Client **202** und enthält darüber hinaus implementierungsspezifische Identitäts-/Anwender-/Clientkontendaten, beispielsweise in Form eines PAC (privilege attribute certificate PAC, Privilegattributzertifikat), einer Sicherheitskennung (security identifier), einer UNIX-Kennung (UNIX identifier), einer Passportkennung (passport identifier), eines Zertifikates und dergleichen mehr. Ein PAC kann beispielsweise durch den Authentifizierungsdienst **206** erzeugt oder einfach aus dem Dienstticket des Client kopiert werden, das in der TGS-REQ-Nachricht **230** enthalten war.

[0056] Das PAC oder andere Anwender-/Clientkontendaten können ebenfalls derart konfiguriert sein, dass sie Informationen im Zusammenhang mit dem Umfang der Delegierung enthalten. Man betrachte hierzu Fig. 4, die ein illustratives Diagramm zur Darstellung von ausgewählten Teilen einer Kerberos-Nachricht **400** mit einem Header **402** und einem PAC **404** ist. Hierbei beinhaltet das PAC **404** Delegierungsinformationen **406**. Wie dargestellt ist, beinhalten die Delegierungsinformationen **406** zusammengesetzte Identitätsinformationen **408** und Zugriffseinschränkungsinformationen **410**.

[0057] Zusammengesetzte Identitätsinformationen **408** können beispielsweise aufgezeichnete Informationen über den Delegierungsprozess enthalten, so beispielsweise einen Hinweis dahingehend, dass der Server A **210** das Dienstticket im Auftrag eines Anwenders/Client **202** angefordert hat. Hierbei kann eine Mehrzahl von derartigen aufgezeichneten Informationen bereitgestellt werden, die zum Zusammenreihen (string together) oder anderweitigen Identifizieren des Verfahrensverlaufes (history) bei mehreren Delegierungsprozessen verwendet werden können. Derartige Informationen können zu Auditierungszwecken und/oder zu Zugriffssteuerungszwecken von Nutzen sein.

[0058] Zugriffseinschränkungsinformationen **410** können beispielsweise im Zusammenhang mit einem Zugriffssteuerungsmechanismus verwendet werden, bei dem ein Zugriff auf bestimmte Server/Dienste selektiv erlaubt wird, vorausgesetzt, der Client **202** hat entweder direkt oder indirekt durch den Server A **210** einen Zugriff auf den Server/Dienst gewünscht, jedoch nicht, wenn der Server/Dienst von dem Server B **212** indirekt gewünscht wird. Dieses Merkmal bietet eine zusätzliche Steuerung der Delegierung von Authentifizierungscredentials.

[0059] Bei den vorstehenden Beispielen wurde der Client **202** durch den Authentifizierungsdienst **206** authentifiziert. Hierbei ist jedoch zu beachten, dass andere Clients gegebenenfalls nicht auf diese Weise authentifiziert werden. Ein Beispiel für eine derartige Situation ist in Fig. 3A dargestellt. Hierbei ist ein Client **302** authentifiziert worden, wobei ein anderer Authentifizierungsprotokollmechanismus **303** verwendet worden ist. So kann beispielsweise ein Authentifizierungsprotokollmechanismus **303** einen Passport, eine SSL (secure sockets layer SSL), NTLM, einen Digest (Zusammenfassung) oder andere ähnliche authentifizierende Protokolle/Prozeduren enthalten. Hierbei wird bei diesem Beispiel davon ausgegangen, dass der Client **302** einen Zugriff auf einen angepeilten Dienst wählt, der gerade von dem Server C **214** bereitgestellt wird. Dieser Wahl kann unter Verwendung des vorbeschriebenen S4U2proxy-Protokolls entsprochen werden, jedoch erst nachdem der Server A **210** ein S4U2self-Protokoll bzw. eine zugehörige Prozedur beendet/verfolgt hat.

[0060] Eine Grundvoraussetzung für das S4U2self-Protokoll besteht darin, dass der Server, so beispielsweise der Server A **210**, in der Lage ist, ein Dienstticket für sich selbst für einen beliebigen Anwender/Client anzufordern, der auf den Server zugreift und den der Server selbst authentifiziert hat. Das hier beschriebene exemplarische S4U2self-Protokoll gemäß vorliegender Beschreibung ist derart konfiguriert, dass Clients, die über einen authentifizierenden Nachweis (evidence) verfügen, sowie Clients, die über keinen derartigen authentifizierenden Nachweis (evidence) verfügen, unterstützt werden.

[0061] Bei Nichtvorhandensein eines Authentifizierungsnachweises, der von dem Authentifizierungsdienst **206** bewertet werden kann, muss der Server A **210** auf den „vertrauenswürdigen" Client **302** zugreifen. Verfügt der Client **302** beispielsweise über ein Authentifizierungszertifikat oder einen ähnlichen Mechanismus **304**, den der Server A **210** validieren kann, so kann der Client **302** als „vertrauenswürdig" eingestuft werden. Hierbei wird der Client **302** im Wesentlichen von dem Server A **210** authentifiziert. Anschließend sendet der Server A **210** eine TGS_REQ-Nachricht **306** an den Authentifizierungsdienst **206** zur Anforderung eines Diensttickets für sich selbst für den Client **302**. In Reaktion hierauf erzeugt der Authentifizierungsdienst **206** eine TGS_REP-Nachricht **308**, die das angeforderte Dienstticket beinhaltet. Das empfangene Dienstticket wird anschließend in einem nachfolgenden S4U2proxy-Protokoll bzw. einer zugehörigen Prozedur zur Anforderung eines Diensttickets für den Server C **214** für den Client **302** verwendet. Bei bestimmten Kerberos-Implementierungen bedingt dies, dass ein weiterleitbares Flag in der TGS_REP-Nachricht **308** gesetzt ist, um eine Weiterleitung des Dienstticketes zu ermöglichen. Die vertrauenswürdige dritte Seite kann ebenfalls ein PAC für den Client **302** sein, der dann in dem resultierenden Dienstticket enthalten sein kann.

[0062] Existiert der Nachweis der Authentifizierung für einen Client **302'**, so kann der Server A **210** einen derartigen Nachweis in eine TGS_REQ-Nachricht **312** als zusätzliche Vorauthentifizierungsdaten aufnehmen. Dies ist illustrativ in der Umgebung **300'** von Fig. 3B dargestellt. Hierbei werden Nachweisinformationen **310** von dem Client **302'** für den Server A **210** bereitgestellt. Die Nachweisinformationen **310** können beispielsweise einen Challenge/Response-Dialog oder dergleichen oder andere Information enthalten, die von der weiteren „vertrauenswürdigen" Entität erzeugt werden. Beim Empfang der Nachweisinformationen **310** und der nachfolgenden Validierung gewährt der Authentifizierungsdienst **206** dem Server A **210** selbst das angeforderte Dienstti-

cket. Man beachte, dass es bei bestimmten Implementierungen mit der Verwendung des Nachweises für den Server möglich wird, ein eingeschränktes TGT für den Client zu erwerben.

[0063] Bei bestimmten Kerberos-Implementierungen kann das weiterleitbare Flag in der TGS_REP-Nachricht **314** gesetzt werden, um ein Weiterleiten des Diensttickets zu ermöglichen. Wurde ein PAC in der TGS_REQ-Nachricht **312** bereitgestellt, so kann es in dem Dienstticket verwendet werden, wohingegen andernfalls ein PAC durch den Authentifizierungsdienst **206** (hier eine KDC) auf Grundlage der Nachweisinformationen **310** erzeugt werden kann. Hierbei ist bei S4U2self die Identität des Client in den Vorauthentifizierungsdaten enthalten. Diese Identität kann beim Aufbau des PAC für jenen Client verwendet und dem ausgegebenen Dienstticket an den Server (für den Client) zugegeben werden.

[0064] Obwohl bestimmte bevorzugte Ausführungsbeispiele der verschiedenen Verfahren und Systeme der vorliegenden Erfindung in der begleitenden Zeichnung und in der vorhergehenden Detailbeschreibung dargelegt worden sind, ist einsichtig, dass die Erfindung nicht auf die exemplarischen offenbarten Ausführungsbeispiele beschränkt ist, sondern dass vielerlei Abwandlungen, Änderungen und Ersetzungen hieran vorgenommen werden können, ohne vom Schutzumfang der Erfindung gemäß Definition in den nachfolgenden Ansprüchen abzuweichen.

Patentansprüche

1. Verfahren zum Einschränken des Umfangs von Delegierung durch einen Client zu einem Server, das umfasst:
Identifizieren eines Ziel-Dienstes (**212**–**216**), auf den Zugriff im Auftrag eines Client (**202**) gewünscht wird;
Veranlassen, dass ein Server (**210**), der funktionell mit dem Client gekoppelt ist, von einer vertrauenswürdigen dritten Seite (**204**) Zugriff auf den Ziel-Dienst im Auftrag des Client anfordert, wobei der Server der vertrauenswürdigen dritten Seite ein Credential (**230**), das den Server authentifiziert, Informationen über den Ziel-Dienst und ein Dienst-Credential bereitstellt, das zuvor dem Server durch den Client bereitgestellt wurde; und
Veranlassen, dass die vertrauenswürdige dritte Seite dem Server ein neues Dienst-Credential (**232**) bereitstellt, das im Namen des Client anstelle des Servers erteilt wird, so dass das neue Dienst-Credential den Server autorisiert, im Auftrag des Client auf den Ziel-Dienst zuzugreifen, während Authentifizierungs-Credentials eines Client dem Server vorenthalten werden, wobei das neue Dienst-Credential, das im Namen des Client erteilt wird, auf einen Umfang beschränkt ist, der durch das zuvor durch den Client dem Server bereitgestellte Dienst-Credential spezifiziert wird.

2. Verfahren nach Anspruch 1, wobei die vertrauenswürdige dritte Seite (**204**) wenigstens einen Dienst (**206**) enthält, der aus einer Gruppe von Diensten ausgewählt wird, die einen Dienst einer Schlüsselverteilungszentrale (Key Distribution Center – KDC), einen Dienst einer Zertifikat-Erteilungsbehörde und einen Dienst eines Domänen-Controllers umfasst.

3. Verfahren nach Anspruch 2, wobei das neue Dienst-Credential (**232**) zur Nutzung durch den Server (**210**) und den Ziel-Dienst (**212**–**216**) konfiguriert ist, auf den Zugriff gewünscht wird.

4. Verfahren nach Anspruch 2, wobei das Credential (**230**), das den Server (**210**) authentifiziert, ein Ticket ist, das ein Ticket-Granting-Ticket enthält, das mit dem Server verknüpft ist.

5. Verfahren nach Anspruch 1, das des Weiteren umfasst:
Veranlassen, dass die vertrauenswürdige dritte Seite (**204**) verifiziert, dass der Client (**202**) über autorisierte Delegierung verfügt.

6. Verfahren nach Anspruch 5, wobei:
die vertrauenswürdige dritte Seite (**204**) eine Schlüsselverteilungszentrale (KDC) enthält; und
Veranlassen, dass die vertrauenswürdige dritte Seite verifiziert, dass der Client (**202**) über autorisierte Delegierung verfügt, Verifizieren des Status einer Einschränkung einschließt, die dem Ticket auferlegt ist, das von dem Client (**202**) stammt.

7. Verfahren nach Anspruch 1, das des Weiteren umfasst:
Veranlassen, dass die vertrauenswürdige dritte Seite auf Basis von Informationen, die aus einer Gruppe ausgewählt werden, die eine Identität des Client und einer mit dem Client verknüpfte Gruppenzugehörigkeit umfasst, selektiv bestimmt, ob es dem Client (**202**) gestattet ist, an Delegierung teilzunehmen.

8. Verfahren nach Anspruch 1, wobei der Server (**210**) ein Front-End-Server in Bezug auf einen Back-End-Server (**212**–**216**) ist, der mit dem Front-End-Server gekoppelt ist, und der Back-End-Server so konfiguriert ist, dass er den Ziel-Dienst bereitstellt, auf den Zugriff gewünscht wird.

9. Verfahren nach Anspruch 1, wobei:
die vertrauenswürdige dritte Seite (**204**) eine Schlüsselverteilungszentrale (KDC) enthält; und
der Server (**210**) das neue Dienst-Credential (**232**) in einer Nachricht (**230**) zum Anfordern eines Ticket-Erteilungsdienstes anfordert, die ein Dienst-Ticket enthält, das dem Server durch den Client (**202**) bereitge-

stellt wird.

10. Verfahren nach Anspruch 1, wobei das durch den Client (**202**) bereitgestellte Dienst-Credential implementierungsspezifische Identitätsinformationen enthält.

11. Verfahren nach Anspruch 10, wobei die implementierungsspezifischen Identitätsinformationen Informationen enthalten, die aus einer Gruppe ausgewählt werden, die Privilege-Attribute-Certificate-Informationen, Sicherheitskennungs-Informationen, Unix-Kennungsinformationen, Passportkennungs-Informationen und Zertifikat-Informationen umfasst.

12. Verfahren nach Anspruch 11, wobei die Privilege-Attribute-Certificate-Informationen zusammengesetzte Identitätsinformationen enthalten.

13. Verfahren nach Anspruch 11, wobei die Privilege-Attribute-Certificate-Informationen Zugriffssteuerungs-Einschränkungen zur Verwendung als Delegierungs-Beschränkungen enthalten.

14. Verfahren nach Anspruch 1, das des Weiteren umfasst:
separates Authentifizieren des Servers (**210**) und des Client (**202**);
Bereitstellen eines Server-Ticket-Granting-Ticket für den Server; und
Bereitstellen eines Client-Ticket-Granting-Ticket für den Client und eines Dienst-Ticket zur Verwendung mit dem Server.

15. Verfahren nach Anspruch 14, das des Weiteren umfasst:
Veranlassen, dass der Server (**210**) das neue Dienst-Credential (**232**) im Auftrag des Client (**202**) anfordert, indem er das Server-Ticket-Granting-Ticket, Informationen, die den neuen Dienst identifizieren und das Dienst-Ticket zu einer vertrauenswürdigen dritten Seite (**204**) weiterleitet.

16. Computerlesbares Medium, auf dem durch Computer ausführbare Befehle gespeichert sind, die bei Ausführung auf einem Computer zum Durchführen der folgenden Schritte konfiguriert sind:
in einem Server (**210**) Bestimmen eines Ziel-Dienstes **212**–**216**), auf den Zugriff im Auftrag eines Client (**202**) gewünscht wird, der mit dem Server gekoppelt ist; und
Anfordern eines neuen Dienst-Credential (**232**) von einer vertrauenswürdigen dritten Seite (**204**) durch Bereitstellen eines Credential (**230**), das den Server authentifiziert, von Informationen über den Ziel-Dienst und eines Service-Credential, das mit dem Client und dem anfordernden Server verknüpft ist, für die vertrauenswürdige dritte Seite; wobei
die vertrauenswürdige dritte Seite veranlasst wird, dem Server ein neues Dienst-Credential (**232**) bereitzustellen, das im Namen des Client anstelle des Servers erteilt wird, so dass das neue Dienst-Credential den Server autorisiert, im Auftrag des Client auf den Ziel-Dienst zuzugreifen, während Authentifizierungs-Credentials eines Client dem Server vorenthalten werden, wobei das neue Dienst-Credential, das im Namen des Client erteilt wird, auf einen Umfang beschränkt ist, der durch das zuvor durch den Client dem Server bereitgestellte Dienst-Credential spezifiziert wird.

17. Computerlesbares Medium nach Anspruch 16, wobei die vertrauenswürdige dritte Seite (**204**) wenigstens einen Dienst (**206**) enthält, der aus einer Gruppe von Diensten ausgewählt wird, die einen Dienst einer Schlüsselverteilungszentrale (KDC), einen Dienst einer Zertifikat-Erteilungsbehörde und einen Dienst eines Domänen-Controllers umfasst.

18. Computerlesbares Medium nach Anspruch 17, wobei das neue Dienst-Credential (**232**) zur Nutzung durch den Server (**210**) und den Ziel-Dienst (**212**–**216**) konfiguriert ist.

19. Computerlesbares Medium nach Anspruch 17, wobei das Credential (**230**), das den Server (**210**) authentifiziert, ein Ticket-Granting-Ticket enthält, das mit dem Server verknüpft ist.

20. Computerlesbares Medium nach Anspruch 16, das des Weiteren umfasst:
Veranlassen, dass die vertrauenswürdige dritte Seite (**204**) verifiziert, dass der Client (**202**) über autorisierte Delegierung verfügt.

21. Computerlesbares Medium nach Anspruch 20, wobei:
die vertrauenswürdige dritte Seite (**204**) eine Schlüsselverteilungszentrale (KDC) enthält; und
Veranlassen, dass die vertrauenswürdige dritte Seite verifiziert, dass der Client (**202**) über autorisierte Delegierung verfügt, Verifizieren des Status eines weiterleitbaren Flag-Wertes einschließt, der durch den Client (**202**) gesetzt wird.

22. Computerlesbares Medium nach Anspruch 16, wobei der Server (**210**) ein Front-End-Server in Bezug auf einen Back-End-Server (**212**–**216**) ist, der mit dem Front-End-Server gekoppelt ist, und der Back-End-Server so konfiguriert ist, dass er den Ziel-Dienst bereitstellt.

23. Computerlesbares Medium nach Anspruch 16, wobei:
die vertrauenswürdige dritte Seite (**204**) eine Schlüsselverteilungszentrale (KDC) enthält; und
der anfordernde Server (**210**) das neue Dienst-Credential (**232**) in einer Nachricht (**230**) zum Anfordern eines Ticket-Erteilungsdienstes anfordert, die ein Dienst-Ticket enthält, das dem Server durch den Cli-

ent (**202**) bereitgestellt wird.

24. Credential-Gewährungssystem (**204**), das so konfiguriert ist, dass es eine Anforderung eines neuen Dienst-Credential von einem Server (**210**) empfängt und in Reaktion darauf das neue Dienst-Credential erzeugt, wenn Delegierung zulässig ist, wobei das neue Dienst-Credential im Namen eines Client (**202**), der mit dem Server gekoppelt ist, anstelle des Servers erteilt wird, so dass das neue Dienst-Credential den Server autorisiert, auf einen Ziel-Dienst (**212**–**216**) im Auftrag des Client zuzugreifen, während Authentifizierungs-Credentials eines Client dem Server vorenthalten werden, wobei das neue Dienst-Credential, das im Namen des Client erteilt wird, auf einen Umfang beschränkt ist, der durch ein zuvor durch den Client dem Server bereitgestelltes Dienst-Credential spezifiziert wird, und die Anforderung enthält:
ein Credential (**230**), das den anfordernden Server authentifiziert,
Identifizierungsinformationen über den Ziel-Dienst, auf den Zugriff im Auftrag des Client gewünscht wird, und
ein Dienst-Credential, das dem Client zuvor zur Verwendung mit dem Server erteilt wurde.

25. System nach Anspruch 24, wobei das Credential-Erteilungssystem durch eine vertrauenswürdige dritte Seite (**204**) bereitgestellt wird und wenigstens einen Dienst (**206**) enthält, der aus einer Gruppe von Diensten ausgewählt wird, die einen Dienst einer Schlüsselverteilungszentrale, einen Dienst einer Zertifikat-Erteilungsbehörde und einen Dienst eines Domänen-Controllers umfasst.

26. System nach Anspruch 25, wobei das neue Dienst-Credential (**232**) zur Verwendung durch den Server (**210**) und den Ziel-Dienst (**212**–**216**) konfiguriert ist.

27. System nach Anspruch 25, wobei das Credential (**230**), das den Server (**210**) authentifiziert, ein Ticket-Granting-Ticket enthält, das mit dem Server verknüpft ist und das zuvor durch den Credential-Erteilungsmechanismus erteilt wurde.

28. Server-System (**210**), das so konfiguriert ist, dass es eine Anforderung eines neuen Dienst-Credential (**232**) von einer vertrauenswürdigen dritten Seite (**204**) empfängt, wobei das neue Dienst-Credential mit einem Client (**202**) und einem Ziel-Dienst (**212**–**216**) verknüpft ist, die Anforderung die vertrauenswürdige dritte Seite veranlasst, dem Server-System das neue Dienst-Credential bereitzustellen, das im Namen des Client anstelle des Server-Systems erteilt wird, so dass das neue Dienst-Credential das Server-System autorisiert, im Auftrag des Client auf den Ziel-Dienst zuzugreifen, während Authentifizierungs-Credentials eines Client dem Server-System vorenthalten werden, wobei das neue Dienst-Credential, das im Namen des Client erteilt wird, auf einen Umfang beschränkt ist, der durch das zuvor durch den Client dem Server-System bereitgestellte Dienst-Credential spezifiziert wird, und die Anforderung umfasst:
ein Credential (**230**), das das Server-System (**210**) authentifiziert,
Informationen über den Ziel-Dienst, und
ein Dienst-Credential, das mit dem Client und dem Server-System verknüpft ist.

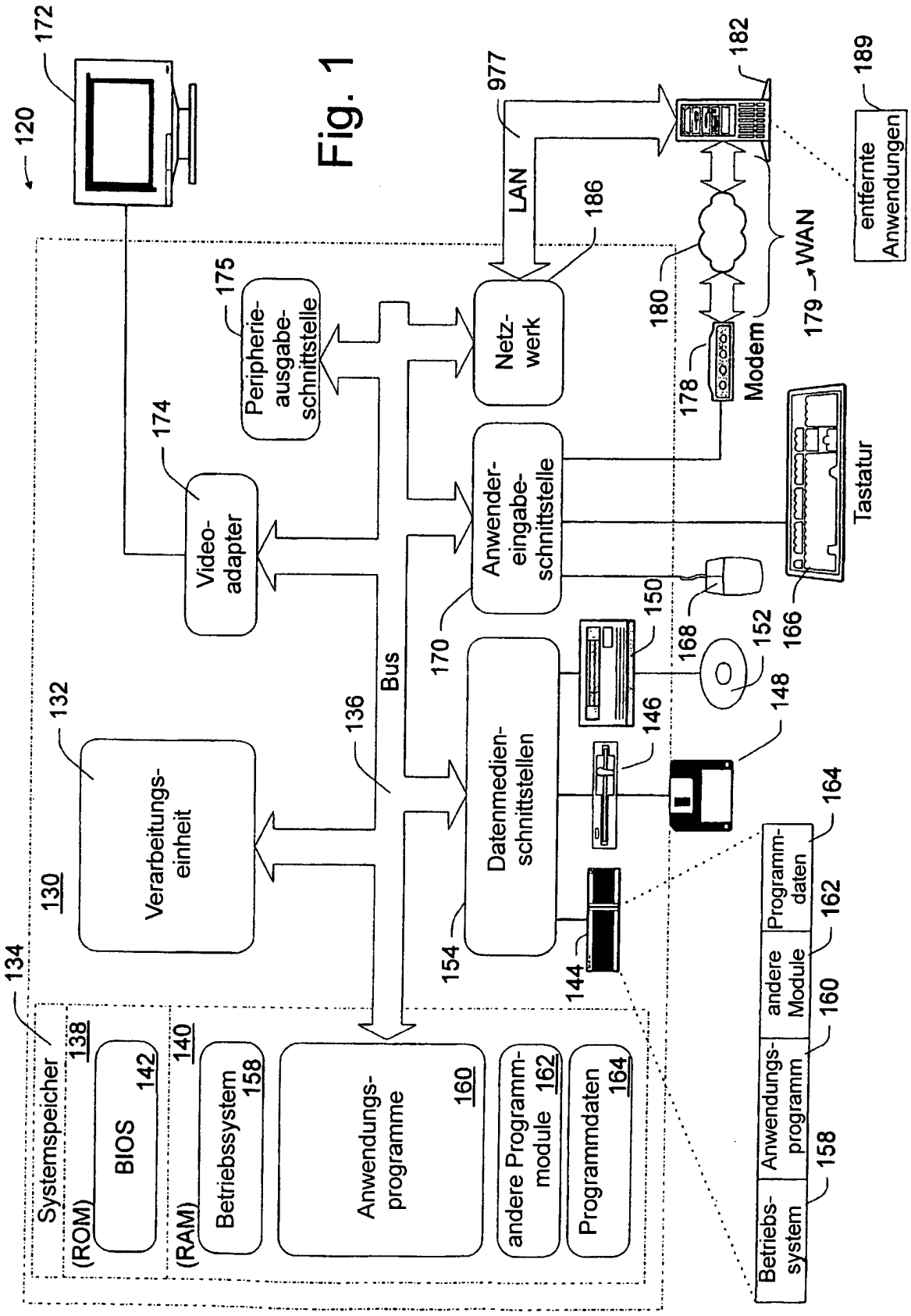
29. System nach Anspruch 28, wobei das Credential (**230**), das das Server-System (**210**) authentifiziert, ein Ticket-Granting-Ticket enthält, das mit dem Server-System verknüpft ist.

30. System nach Anspruch 28, wobei das Server-System (**210**) ein Front-End-Server in Bezug auf den Dienst (**212**–**216**) ist.

31. System nach Anspruch 28, wobei das Server-System (**210**) des Weiteren so konfiguriert ist, dass es das neue Dienst-Credential (**232**) in einer Nachricht zum Anfordern eines Ticket-Erteilungsdienstes anfordert, die das mit dem Client (**202**) und dem Server-System verknüpfte Dienst-Ticket enthält.

Es folgen 5 Blatt Zeichnungen

Anhängende Zeichnungen



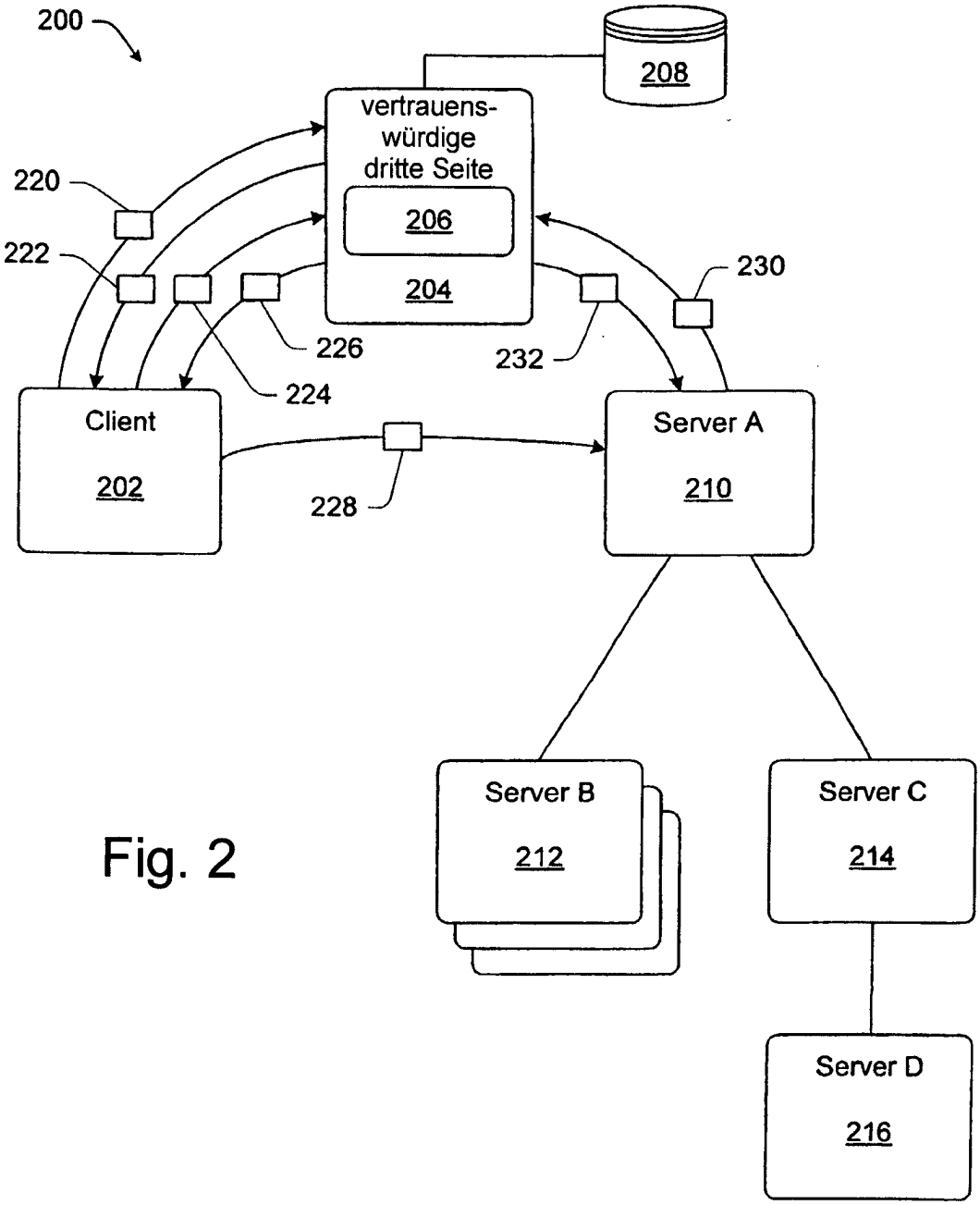

200
208
vertrauens-
würdige
dritte Seite
206
204
220
222
226
224
232
230
228
Client
202
Server A
210
Server B
212
Server C
214
Server D
216

Fig. 2

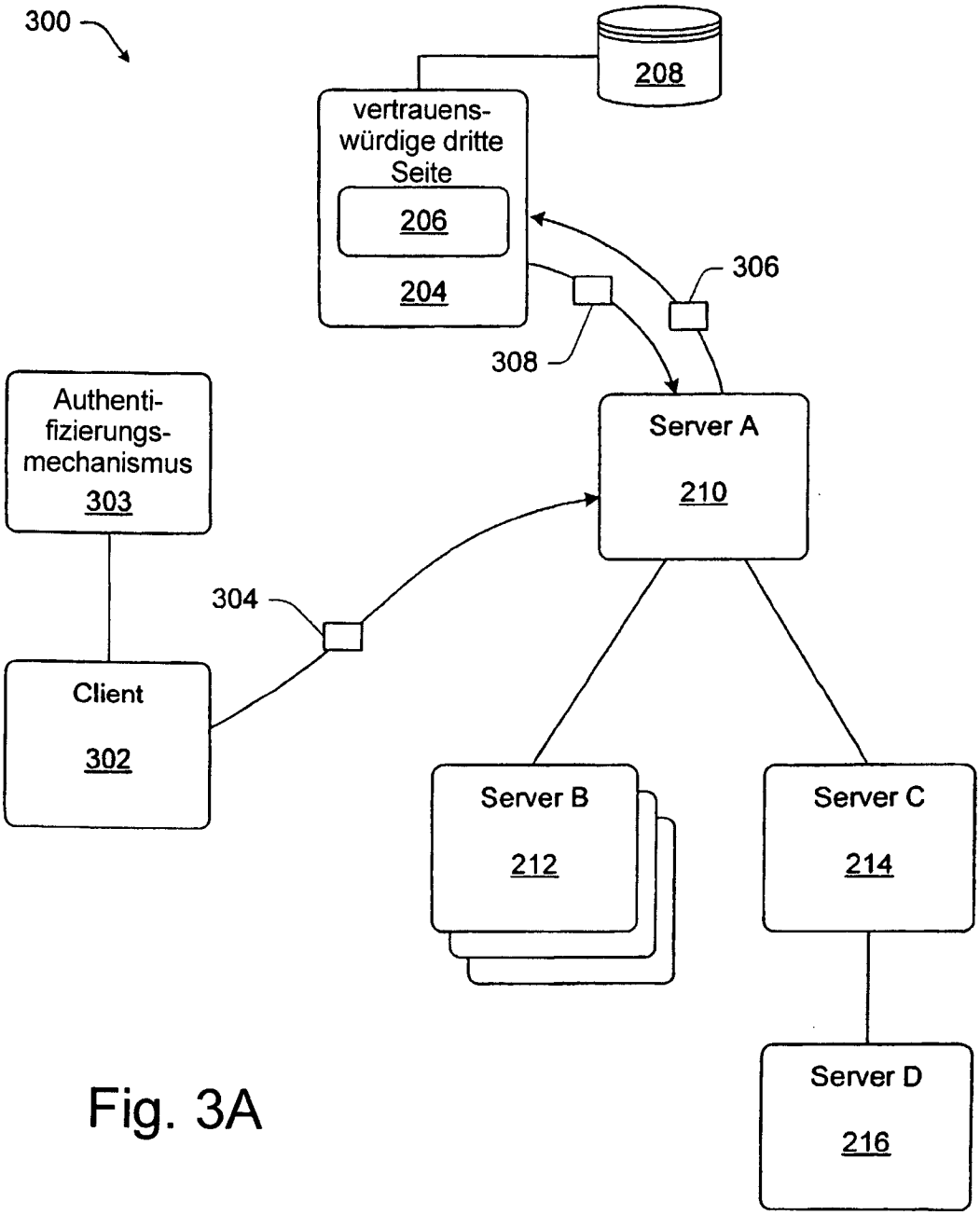

300
208
vertrauens-
würdige dritte
Seite
206
204
306
308
Authenti-
fizierungs-
mechanismus
303
Server A
210
304
Client
302
Server B
212
Server C
214
Server D
216

Fig. 3A

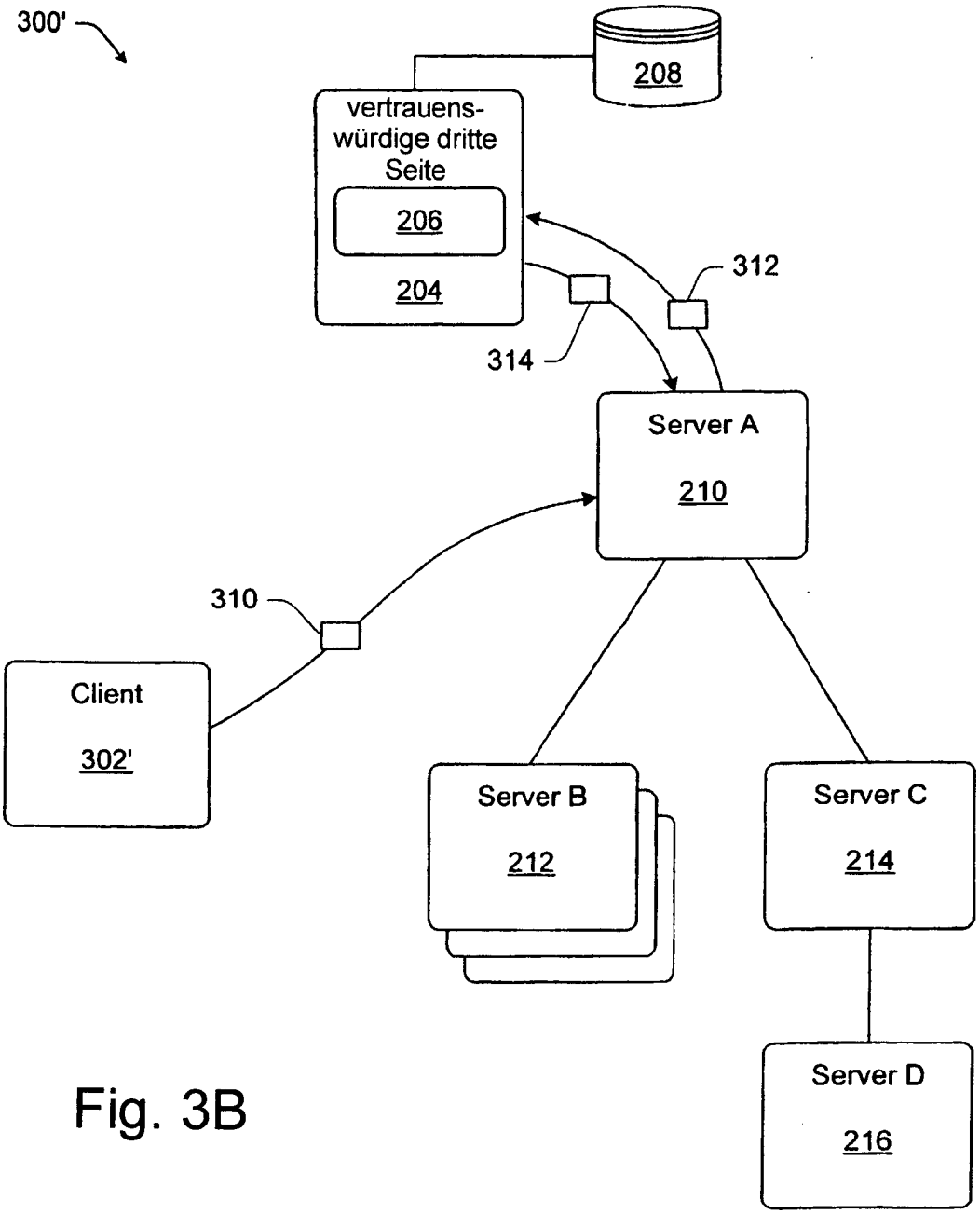

300'
208
vertrauens-
würdige dritte
Seite
206
204
312
314
Server A
210
310
Client
302'
Server B
212
Server C
214
Server D
216

Fig. 3B

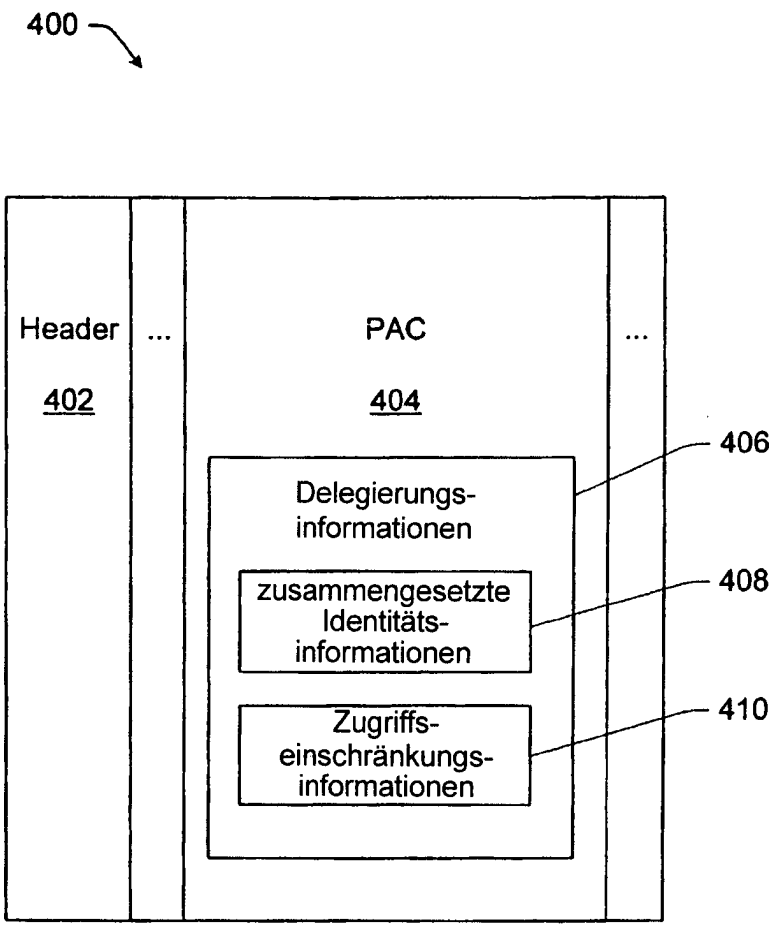

400
Header
402
...
PAC
404
...
Delegierungs-
informationen
406
zusammengesetzte
Identitäts-
informationen
408
Zugriffs-
einschränkungs-
informationen
410

Fig. 4