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

(10) **DE 602 24 161 T2** 2008.12.04

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 322 091 B1**
(21) Deutsches Aktenzeichen: **602 24 161.8**
(96) Europäisches Aktenzeichen: **02 258 074.0**
(96) Europäischer Anmeldetag: **22.11.2002**
(97) Erstveröffentlichung durch das EPA: **25.06.2003**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **19.12.2007**
(47) Veröffentlichungstag im Patentblatt: **04.12.2008**

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

(30) Unionspriorität:
2001385869 19.12.2001 JP

(84) Benannte Vertragsstaaten:
DE, FI, FR, GB, SE

(73) Patentinhaber:
Canon K.K., Tokyo, JP

(72) Erfinder:
Arai, Shunji, Tokyo, JP

(74) Vertreter:
TBK-Patent, 80336 München

(54) Bezeichnung: **Kommunikationssystem, Servervorrichtung, Client-Einrichtung und Verfahren zur Steuerung derselben**

Beschreibung

[0001] Die Erfindung betrifft eine Servervorrichtung, die einen Zugangspunkt in einem Kommunikationssystem über einen Verschlüsselungsschlüssel informiert, der verwendet wird, wenn ein Client-Endgerät (d. h. ein Kommunikationsgerät) eine Kommunikation über den Zugangspunkt einleitet. Sie betrifft auch ein Verfahren zur Steuerung derselben, sowie ein Computer-lesbares Speichermedium, das Anweisungen zur Durchführung eines derartigen Verfahrens speichert.

[0002] Herkömmlich wurde ein Client-Endgerät in einem drahtlosen LAN-System mit einem Netzwerk über eine drahtlose Kommunikation mit einem Zugangspunkt in dem Netzwerk verbunden.

[0003] Es gibt auch ein drahtloses LAN-System, bei dem ein Client-Endgerät eine Authentisierung einer Verbindung zu einem Netzwerk über einen Zugangspunkt von einem Authentisierungsserver in einem Netzwerk empfängt.

[0004] Wenn in einem solchen System das Client-Endgerät eine Authentisierung von dem Authentisierungsserver empfängt, erzeugen das Client-Endgerät und der Authentisierungsserver einen Verschlüsselungsschlüssel eines "Wired Equivalent Privacy"-(WEP)Verschlüsselungssystems und informiert der Authentisierungsserver den Zugangspunkt über den erzeugten Verschlüsselungsschlüssel. Dann übermittelt das Client-Endgerät verschlüsselte Daten mit dem Zugangspunkt, indem der Verschlüsselungsschlüssel des WEP-Verschlüsselungssystems verwendet wird, um eine sichere bzw. geschützte drahtlose Kommunikation durchzuführen.

[0005] Im Übrigen ist ein übertragungs- bzw. kommunikationsfähiger Bereich des Zugangspunkts auf einen Bereich beschränkt, der durch elektrische Wellen erreicht wird. Andererseits kann das Client-Endgerät frei bewegt werden. Dementsprechend kann das Client-Endgerät von einem kommunikationsfähigen Bereich eines Zugangspunkts 1 in einen kommunikationsfähigen Bereich eines Zugangspunkts 2 bewegt werden. In diesem Fall muss das Client-Endgerät eine Authentisierung einer Verbindung zu dem Netzwerk von dem Authentisierungsserver erneut über eine drahtlose Kommunikation mit dem Zugangspunkt 2 empfangen, müssen das Client-Endgerät und der Authentisierungsserver einen neuen WEP-Schlüssel erzeugen, und muss der Authentisierungsserver den Zugangspunkt 2 über den neuen WEP-Schlüssel informieren.

[0006] Das heißt, dass eine Neuauthentisierung von dem Authentisierungsserver, eine Erzeugung eines neuen WEP-Schlüssels, eine Informierung über einen WEP-Schlüssel und dergleichen den Prozess verlängert haben, bis eine Kommunikation möglich wurde, wenn das Client-Endgerät den Zugangspunkt gewechselt hat. Folglich hat der Prozess Zeit gebraucht.

[0007] Zusätzlich wurde in einem System vieler Client-Endgeräte, da eine Authentisierung und Erzeugung eines WEP-Schlüssels einen Prozess verlängert haben, eine Last auf einem Authentisierungsserver unvermeidlich groß.

[0008] Außerdem wurde, da der Prozess Zeit gebraucht hat, wenn der Zugangspunkt gewechselt wurde, die Brauch- bzw. Nutzbarkeit reduziert.

[0009] Eine Servervorrichtung mit einer Authentisierungseinrichtung zum Authentisieren eines Kommunikationsgeräts, das mit einem ersten Zugangspunkt verbunden ist, und einer Informationseinrichtung zum Informieren des Zugangspunkts über einen Verschlüsselungsschlüssel, wenn eine gültige Authentisierung erfolgt, ist aus der WO-0124560-A und der WO-0296151-A bekannt.

[0010] Mit Blick auf eine Überwindung der hierin vorstehend erörterten Probleme ist in der internationalen Patentanmeldung WO-0221768-A2 eine Servervorrichtung offenbart, die aufweist:
eine Authentisierungseinrichtung zum Authentisieren eines Kommunikationsgeräts, das über einen ersten Zugangspunkt mit einem Netzwerk verbunden ist;
eine Informationseinrichtung zum Informieren des ersten Zugangspunkts, mit dem das Kommunikationsgerät verbunden ist, über einen Verschlüsselungsschlüssel gemäß dem Ergebnis der Authentisierung durch die Authentisierungseinrichtung;
eine Bestimmungseinrichtung zum Bestimmen, ob das Kommunikationsgerät authentisiert wurde oder nicht, auf Grundlage von von einem Zugangspunkt mitgeteilten Identifikationsinformationen des Kommunikationsgeräts; und
eine Steuereinrichtung zum i) Auffordern der Informationseinrichtung zum Informieren eines zweiten Zugangspunkts, an den die Identifikationsinformationen gemeldet werden, über den an den ersten Zugangspunkt mitgeteilten Verschlüsselungsschlüssel, wenn die Bestimmungseinrichtung bestimmt, dass das Kommunikationsgerät durch die Authentisierungseinrichtung mittels des ersten Zugangspunkts authentisiert wurde, und ii) Auffordern der Authentisierungseinrichtung zum Authentisieren des Kommunikationsgeräts, wenn die Bestimmungseinrichtung bestimmt, dass das Kommunikationsgerät nicht durch die Authentisierungseinrichtung authentisiert wurde.

[0011] Um diese Vorrichtung weiter zu verbessern, stellt die Erfindung eine Servervorrichtung gemäß Anspruch 1 bereit.

[0012] Die Erfindung stellt auch ein Steuerverfahren

für die Servervorrichtung gemäß Anspruch 4, sowie ein Computerlesbares Speichermedium gemäß Anspruch 5 bereit. Vorteilhafte Ausführungsbeispiele davon sind in entsprechenden abhängigen Ansprüchen offenbart.

[0013] Weitere Merkmale der Erfindung werden beim Studium der detaillierten Beschreibung und der Zeichnungen ersichtlich.

[0014] In den begleitenden Zeichnungen gilt:

[0015] Fig. 1 ist eine Konfigurationsdarstellung eines Systems gemäß einem Ausführungsbeispiel der Erfindung;

[0016] Fig. 2 ist ein Blockschaltbild eines Zugangspunkts gemäß dem Ausführungsbeispiel der Erfindung;

[0017] Fig. 3 ist ein Blockschaltbild eines Client-Endgeräts gemäß dem Ausführungsbeispiel der Erfindung;

[0018] Fig. 4 ist eine Ablaufdarstellung, die einen Systembetrieb gemäß dem Ausführungsbeispiel der Erfindung zeigt; und

[0019] Fig. 5 ist eine Ablaufdarstellung des Systembetriebs gemäß dem Ausführungsbeispiel der Erfindung.

AUSFÜHRLICHE BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSBEISPIELE

[0020] Als Nächstes wird eine Beschreibung eines Ausführungsbeispiels der Erfindung vorgenommen.

[0021] Fig. 1 ist eine Konfigurationsdarstellung eines Systems gemäß dem Ausführungsbeispiel der Erfindung.

[0022] Ein Bezugszeichen **101** bezeichnet ein Netzwerk, mit dem ein Zugangspunkt A103 und ein Zugangspunkt B104 verbunden sind. Die beiden Zugangspunkte sind gemäß Fig. 1 gezeigt, aber die Anzahl von installierten Punkten ist nicht auf zwei beschränkt. Jeder der Zugangspunkte A103 und B104 kann eine drahtlose Kommunikation mit einem Client-Endgerät **105** durchführen, das in übertragungs- bzw. kommunikationsfähigen Bereichen **106**, **107** gegenwärtig ist. Gemäß dem Ausführungsbeispiel wird als drahtloses Kommunikationssystem ein drahtloses lokales Netz (LAN) basierend auf einem Standard wie etwa IEEE 802.11, IEEE 802.11b oder IEEE 802.11a verwendet.

[0023] Das Bezugszeichen **105** stellt das Client-Endgerät dar, das über eine drahtlose Kommunikation mit dem Zugangspunkt A103 oder B104 mit dem Netzwerk **101** verbunden ist. Obwohl nicht gemäß Fig. 1 gezeigt, kann eine Vielzahl von Client-Endgeräten **105** gegenwärtig sein.

[0024] Ein Bezugszeichen **102** bezeichnet einen Authentisierungsserver, der das mit dem Netzwerk **101** verbundene Client-Endgerät **105** authentisiert und einen Verschlüsselungsschlüssel erzeugt, der in einem "Wired Equivalency Privacy"-(WEP)Verschlüsselungssystem verwendet wird.

[0025] Fig. 2 ist ein Blockschaltbild des Zugangspunkts A103.

[0026] Ein Fall des Zugangspunkts B104 ist ähnlich.

[0027] Ein Bezugszeichen **201** bezeichnet eine Drahtloseinheit, die drahtlose Daten übermittelt. Die Drahtloseinheit **201** besteht aus einer Sendeeinheit **210**, einer Empfangseinheit **211** und einer Antenne **212**.

[0028] Ein Bezugszeichen **202** bezeichnet eine Signalverarbeitungseinheit, die ein von der Empfangseinheit **211** empfangenes Signal erfasst, um dieses in ein digitales Signal zu konvertieren, und das Signal moduliert, um ein von einer Datenverarbeitungseinheit **203** gesendetes digitales Signal drahtlos zu übertragen. Zusätzlich hat die Signalverarbeitungseinheit **202** eine Funktion zum Hinzufügen eines Kopffelds oder dergleichen, um von der Datenverarbeitungseinheit **203** gesendete Daten für eine drahtlose Übertragung zu verwenden, und zum Entfernen eines Kopffelds oder dergleichen aus empfangenen Daten, um diese an die Datenverarbeitungseinheit **203** zu senden.

[0029] Das Bezugszeichen **203** stellt die Datenverarbeitungseinheit dar, die aus einer Sendedaten-Verarbeitungseinheit **205** zum Verschlüsseln von Daten von einer Netzwerkschnittstelle **208** mittels eines WEP-Verschlüsselungssystems und einer Empfangsdaten-Verarbeitungseinheit **206** zum Decodieren von verschlüsselten Daten besteht.

[0030] Ein Bezugszeichen **204** bezeichnet eine Steuereinheit, die eine Bestimmung der Gegenwart eines neuen Client-Endgeräts **105**, eine Steuerung des gesamten Zugangspunkts A103 und dergleichen ausführt.

[0031] Ein Bezugszeichen **207** bezeichnet eine Speichereinheit, die einen Verschlüsselungsschlüssel für eine WEP-Verschlüsselung und Informationen bezüglich einer ID oder dergleichen des Client-Endgeräts **105** speichert.

[0032] Das Bezugszeichen **208** stellt die Netzwerkschnittstelle dar, die eine Schnittstelle zwischen dem Zugangspunkt A103 und dem Netzwerk **101** ist.

[0033] Fig. 3 ist ein Blockschaltbild des Client-Endgeräts **105**.

[0034] Das Client-Endgerät **105** des Ausführungsbeispiels besteht aus einer Drahtlos-Kommunikationskarte.

[0035] Funktionen, die ähnlich zu denjenigen des gemäß Fig. 2 gezeigten Zugangspunkts A103 sind, sind mit ähnlichen Bezugszeichen bezeichnet.

[0036] Ein Bezugszeichen **301** bezeichnet eine Datenkommunikationsschnittstelle, die mit einem Informationsprozessor wie etwa einem Personal-Computer verbunden ist, um eine Datenkommunikation durchzuführen.

[0037] Ein Bezugszeichen **302** bezeichnet eine Speichereinheit, die einen Verschlüsselungsschlüssel für eine WEP-Verschlüsselung und Informationen bezüglich einer ID oder dergleichen des Client-Endgeräts **105** speichert, die für eine drahtlose Kommunikation mit dem Zugangspunkt A103 oder dem Zugangspunkt B104 notwendig sind. Gemäß dem Ausführungsbeispiel wird als ID des Client-Endgeräts **105** eine Medienzugriffssteuerung-(MAC)Adresse verwendet.

[0038] Als Nächstes wird eine Beschreibung eines Betriebs des gesamten Systems des Ausführungsbeispiels unter Bezugnahme auf die Zeichnungen vorgenommen.

[0039] Zunächst wird ein Prozess einer ersten Verbindung des Client-Endgeräts **105** mit dem Netzwerk **101** über den Zugangspunkt A103 erläutert, indem auf eine Ablaufdarstellung gemäß Fig. 4 Bezug genommen wird.

[0040] Das Client-Endgerät **105** führt eine offene Authentisierung in dem drahtlosen LAN aus, um mit dem Zugangspunkt A103 verbunden zu werden (S401).

[0041] Der Zugangspunkt A103 erhält eine ID des Client-Endgeräts **105** (S402).

[0042] Der Zugangspunkt A103 informiert den Authentisierungsserver **102** über die ID des Client-Endgeräts **105** (S403).

[0043] Der Authentisierungsserver **102** bestimmt, ob eine Authentisierung für die Verbindung des Client-Endgeräts **105** mit dem Netzwerk **101** abgeschlossen wurde oder nicht, basierend auf der von dem Zugangspunkt A103 mitgeteilten ID (S404). Das Client-Endgerät **105** stellt die Verbindung zum ersten Mal her, und die Authentisierung wurde nicht abgeschlossen. Daher wird bestimmt, dass die Authentisierung nicht abgeschlossen wurde.

[0044] Der Authentisierungsserver **102** fordert das Client-Endgerät **105** auf, einen Benutzernamen und ein Passwort einzugeben (S405).

[0045] Das Client-Endgerät **105** gibt den Benutzernamen und das Passwort ein (S406).

[0046] Um die Geheimhaltung des Benutzernamens und des Passworts zu steigern, die in Schritt S406 eingegeben wurden, führt das Client-Endgerät **105** eine nicht umkehrbare Zahlenwertverarbeitung aus, die Einweg-Hash genannt wird, und informiert es den Authentisierungsserver **102** über seine Einweg-Hash-Daten (S407).

[0047] Der Authentisierungsserver **102** ordnet die in Schritt S407 mitgeteilten Einweg-Hash-Daten einer Datengruppe bezüglich eines Benutzers zur Genehmigung einer Verbindung mit dem Netzwerk **101** zu, die in einer Datenbank in dem Authentisierungsserver **102** gespeichert ist. Ergibt ein Ergebnis der Zuordnung übereinstimmende Daten, wird dem Client-Endgerät **105** die Verbindung mit dem Netzwerk **101** genehmigt, und wird die ID des Client-Endgeräts **105** gespeichert (S408).

[0048] Das Client-Endgerät **105** und der Authentisierungsserver **102** erzeugen einen Verschlüsselungsschlüssel, der WEP-Sitzungsschlüssel genannt wird (S409). Der WEP-Sitzungsschlüssel ist ein Verschlüsselungsschlüssel, der in dem WEP-Verschlüsselungssystem verwendet wird und nur zur Verschlüsselung von Verkehr des Client-Endgeräts **105** gültig ist.

[0049] Der Authentisierungsserver **102** speichert den erzeugten WEP-Sitzungsschlüssel in Zusammenhang mit der ID des Client-Endgeräts **105** und meldet diesen an den Zugangspunkt A103 (S410).

[0050] Der Zugangspunkt A103 verschlüsselt einen Rundsendungsschlüssel mit dem WEP-Sitzungsschlüssel (S411) und sendet den verschlüsselten Rundsendungsschlüssel an das Client-Endgerät **105** (S412). Der Rundsendungsschlüssel ist ein Verschlüsselungsschlüssel, der verwendet wird, wenn Daten verschlüsselt werden, die von dem Zugangspunkt A103 an eine Vielzahl von Client-Endgeräten **105** rundgesendet werden.

[0051] Das Client-Endgerät **105** decodiert den verschlüsselten Rundsendungsschlüssel durch Verwendung des in Schritt S409 erzeugten WEP-Sitzungsschlüssels, um einen Rundsendungsschlüssel zu erhalten (S413).

[0052] Der Zugangspunkt A103 und das Client-Endgerät **105** beginnen WEP-Verschlüsselungsvorgänge (S414, S415).

[0053] Dann übermittelt der Zugangspunkt A103 bei einer Kommunikation mit einem Client-Endgerät **105** (Punkt-zu-Punkt-Kommunikation) mit dem WEP-Sitzungsschlüssel verschlüsselte Daten, um eine sichere bzw. geschützte drahtlose Kommunikation durchzuführen (S416). Bei einer Rundsendungskommunikation mit einer Vielzahl von Client-Endgeräten **105** (Punkt-zu-Mehrpunkt-Kommunikation) übermittelt der Zugangspunkt A103 mit dem Rundsendungsschlüssel verschlüsselte Daten, um eine sichere bzw. geschützte drahtlose Kommunikation durchzuführen (S416).

[0054] Fig. 5 zeigt eine Ablaufdarstellung eines Betriebs, wenn das Client-Endgerät **105**, für das eine Authentisierung seiner Verbindung mit dem Netzwerk **101** über den Zugangspunkt A103 abgeschlossen wurde, von dem kommunikationsfähigen Bereich **106** des Zugangspunkts A103 in den kommunikationsfähigen Bereich **107** des Zugangspunkts B104 bewegt wird, um über den Zugangspunkt B104 mit dem Netzwerk **101** verbunden zu werden.

[0055] Das Client-Endgerät **105** wird aus dem kommunikationsfähigen Bereich **106** des Zugangspunkts A103 heraus bewegt, so dass es mit dem Zugangspunkt A103 nicht kommunikationsfähig ist (S501). Dann wird das Client-Endgerät **105** in den kommunikationsfähigen Bereich **107** des Zugangspunkts B104 bewegt, so dass es mit dem Zugangspunkt B104 kommunikationsfähig ist.

[0056] Das Client-Endgerät **105** führt eine offene Authentisierung aus, um mit dem Zugangspunkt B104 verbunden zu werden (S502).

[0057] Der Zugangspunkt B104 erhält eine ID des Client-Endgeräts **105** (S503).

[0058] Der Zugangspunkt B104 informiert den Authentisierungsserver **102** über die ID des Client-Endgeräts **105** (S504).

[0059] Der Authentisierungsserver **102** bestimmt, ob eine Authentisierung für die Verbindung des Client-Endgeräts **105** mit dem Netzwerk **101** abgeschlossen wurde oder nicht, basierend auf der in Schritt S504 mitgeteilten ID und der gespeicherten ID des Client-Endgeräts **105**, für das die Authentisierung abgeschlossen wurde (S505). Hier wurde für das Client-Endgerät **105** die Authentisierung seiner Verbindung mit dem Netzwerk **101** über den Zugangspunkt A103 in Schritt S408 abgeschlossen (Fig. 4) und wurde die ID des Client-Endgeräts gespeichert. Daher wird bestimmt, dass die Authentisierung abgeschlossen wurde.

[0060] Der Authentisierungsserver **102** weist den Zugangspunkt A103 an, den in der Speichereinheit **207** gespeicherten WEP-Sitzungsschlüssel zu löschen, der für eine drahtlose Kommunikation mit dem Client-Endgerät **105** zu verwenden ist (S506).

[0061] Der Authentisierungsserver **102** informiert den Zugangspunkt B104 über den WEP-Sitzungsschlüssel, der in Schritt S410 (Fig. 4) in Zusammenhang mit der ID des Client-Endgeräts **105** gespeichert wird (S507).

[0062] Der Zugangspunkt B104 verschlüsselt einen Rundsendungsschlüssel mit dem in Schritt S507 mitgeteilten WEP-Sitzungsschlüssel (S508) und sendet den verschlüsselten Rundsendungsschlüssel an das Client-Endgerät **105** (S509).

[0063] Das Client-Endgerät **105** decodiert den verschlüsselten Rundsendungsschlüssel mittels des in Schritt S409 (Fig. 4) erzeugten WEP-Sitzungsschlüssels, um einen Rundsendungsschlüssel zu erhalten (S510).

[0064] Der Zugangspunkt B104 und das Client-Endgerät **105** beginnen WEP-Verschlüsselungsvorgänge (S511, S512).

[0065] Dann übermittelt der Zugangspunkt B104 bei einer Kommunikation mit einem Client-Endgerät **105** (Punkt-zu-Punkt-Kommunikation) Daten, die mit dem gleichen WEP-Sitzungsschlüssel wie demjenigen verschlüsselt sind, der für die Kommunikation zwischen dem Client-Endgerät **105** und dem Zugangspunkt A103 verwendet wird, um eine sichere bzw. geschützte drahtlose Kommunikation durchzuführen (S513). Bei einer Rundsendungskommunikation mit einer Vielzahl von Client-Endgeräten **105** (Punkt-zu-Mehrpunkt-Kommunikation) übermittelt der Zugangspunkt B104 Daten, die mit dem Rundsendungsschlüssel verschlüsselt sind, um eine sichere bzw. geschützte drahtlose Kommunikation durchzuführen (S513).

[0066] Bei dem Ausführungsbeispiel wird der in dem Authentisierungsserver **102** gespeicherte WEP-Sitzungsschlüssel in Schritt S507 an den Zugangspunkt B104 mitgeteilt. Der in dem Zugangspunkt A103 gespeicherte WEP-Sitzungsschlüssel kann jedoch über den Authentisierungsserver **102** an den Zugangspunkt B104 mitgeteilt werden.

[0067] Bei der vorangehenden Erläuterung war das Client-Endgerät **105** die Drahtlos-Kommunikationskarte. Eine Funktion, die ähnlich zu der Drahtlos-Kommunikationskarte ist, kann jedoch in einem Personal-Computer oder einem Persönlichen Digitalen Assistenten (PDA) eingebunden sein.

[0068] Es ist unnötig zu erwähnen, dass die Erfindung implementiert werden kann, indem ein Computer-lesbares Speichermedium, in dem Softwareprogrammteile zum Realisieren der Funktionen des Cli-

ent-Endgeräts, der Zugangspunkte und des Authentisierungsservers gespeichert sind, an einem System oder einer Vorrichtung vorgesehen wird und das System oder ein Computer (wahlweise CPU oder MPU) der Vorrichtung veranlasst wird, die in dem Speichermedium gespeicherten Programmcodes zu lesen und auszuführen.

[0069] In einem solchen Fall realisieren die von dem Speichermedium gelesenen Programmcodes selbst die Funktionen des Ausführungsbeispiels und stellt das Speichermedium, in dem die Programmcodes gespeichert sind, die Erfindung dar.

[0070] Als das Speichermedium zur Lieferung der Programmcodes kann ein ROM, eine Diskette, eine Festplatte, eine optische Platte, eine magnetooptische Platte, eine CD-ROM, eine CD-R, ein Magnetband, eine nichtflüchtige Speicherkarte oder dergleichen verwendet werden.

[0071] Es ist unnötig zu erwähnen, dass bei der Erfindung nicht nur der Fall einer Realisierung der Funktionen des Ausführungsbeispiels mittels Ausführung der durch den Computer gelesenen Programmcodes, sondern auch ein Fall umfasst ist, bei dem basierend auf Anweisungen der Programmcodes ein Teil von dem oder der gesamte eigentliche Prozess mittels eines OS oder dergleichen ausgeführt wird, das auf dem Computer arbeitet, um die Funktionen des Ausführungsbeispiels zu realisieren.

[0072] Außerdem ist es unnötig zu erwähnen, dass bei der Erfindung ein Fall umfasst ist, bei dem die von dem Speichermedium gelesenen Programmcodes in eine CPU oder dergleichen geschrieben werden, die auf einer in den Computer eingeführten Funktionserweiterungsbaugruppe oder einer mit dem Computer verbundenen Funktionserweiterungseinheit bereitgestellt ist, und dann basierend auf Anweisungen der Programmcodes die CPU oder dergleichen, die auf der Funktionserweiterungsbaugruppe oder der Funktionserweiterungseinheit bereitgestellt ist, einen Teil von dem oder den gesamten eigentlichen Prozess ausführt, um die Funktionen des Ausführungsbeispiels zu realisieren.

Patentansprüche

1. Servervorrichtung (**102**) mit:
einer Authentisierungseinrichtung zum Authentisieren (S404, S408) eines Kommunikationsgeräts (**105**), das über einen ersten Zugangspunkt (**103**) mit einem Netzwerk (**101**) verbunden ist;
einer Informationseinrichtung zum Informieren (S410) des ersten Zugangspunkts, mit dem das Kommunikationsgerät verbunden ist, über einen Verschlüsselungsschlüssel gemäß dem Ergebnis der Authentisierung durch die Authentisierungseinrichtung;
einer Bestimmungseinrichtung zum Bestimmen (S404 und S505), ob das Kommunikationsgerät (**105**) authentisiert wurde oder nicht, auf Grundlage von von einem Zugangspunkt (**104**) mitgeteilten Identifikationsinformationen des Kommunikationsgeräts; und
einer Steuereinrichtung zum i) Auffordern der Informationseinrichtung zum Informieren (S507) eines zweiten Zugangspunkts (**124**), an den die Identifikationsinformationen gemeldet werden, über den an den ersten Zugangspunkt (**103**) mitgeteilten (S410) Verschlüsselungsschlüssel, wenn die Bestimmungseinrichtung bestimmt, dass das Kommunikationsgerät (**106**) durch die Authentisierungseinrichtung mittels des ersten Zugangspunkts authentisiert wurde, und ii) Auffordern der Authentisierungseinrichtung zum Authentisieren des Kommunikationsgeräts (**105**), wenn die Bestimmungseinrichtung bestimmt, dass das Kommunikationsgerät (**106**) nicht durch die Authentisierungseinrichtung authentisiert wurde,
dadurch gekennzeichnet, dass sie ferner aufweist:
eine Anweisungseinrichtung zum Anweisen (S506) des ersten Zugangspunkts (**103**) zum Löschen des Verschlüsselungsschlüssels, wenn das Kommunikationsgerät über den zweiten Zugangspunkt (**104**) mit dem Netzwerk (**101**) verbunden ist.

2. Servervorrichtung gemäß Anspruch 1, ferner mit:
einer Erzeugungseinrichtung zum Erzeugen (S409) des Verschlüsselungsschlüssels, der für eine Kommunikation zwischen dem Kommunikationsgerät (**105**) und dem ersten Zugangspunkt (**103**) verwendet wird, gemäß der Authentisierung (S408) durch die Authentisierungseinrichtung; und wobei
die Servervorrichtung (**102**) eingerichtet ist zum Speichern des durch die Erzeugungseinrichtung erzeugten Verschlüsselungsschlüssels zur späteren Verwendung beim Informieren (S410) des zweiten Zugangspunkts (**104**) durch die Informationseinrichtung.

3. Servervorrichtung gemäß Anspruch 1, ferner mit:
einer Erzeugungseinrichtung zum Erzeugen (S409) des Verschlüsselungsschlüssels, der für eine Kommunikation zwischen dem Kommunikationsgerät und dem ersten Zugangspunkt (**103**) verwendet wird, gemäß der Authentisierung (S408) durch die Authentisierungseinrichtung; und wobei
die Servervorrichtung (**102**) eingerichtet ist zum Erhalten des Verschlüsselungsschlüssels, der durch die Informationseinrichtung an den ersten Zugangspunkt (**103**) mitgeteilt wird (S410), von dem ersten Zugangspunkt (**103**).

4. Steuerverfahren für eine Servervorrichtung (**102**), mit:
einem Authentisierungsschritt (S408) eines Authentisierens eines Kommunikationsgeräts (**105**), das über

einen ersten Zugangspunkt (**103**) mit einem Netzwerk (**101**) verbunden ist;
einem Informationsschritt (S410) eines Informierens des ersten Zugangspunkts (**103**), mit dem das Kommunikationsgerät (**105**) verbunden ist, über einen Verschlüsselungsschlüssel gemäß dem Ergebnis der Authentisierung in dem Authentisierungsschritt;
einem Bestimmungsschritt (S404 und S505) eines Bestimmens, ob das Kommunikationsgerät (**105**) authentisiert wurde oder nicht, auf Grundlage von von einem Zugangspunkt (**104**) mitgeteilten Identifikationsinformationen des Kommunikationsgeräts (**105**); und
in Abhängigkeit von der in dem Bestimmungsschritt (S404 und S505) vorgenommenen Bestimmung:
i) einem Informationsschritt (S507) eines Informierens eines zweiten Zugangspunkts (**124**), an den die Identifikationsinformationen gemeldet werden, über den an den ersten Zugangspunkt (**103**) mitgeteilten (S410) Verschlüsselungsschlüssel, wenn bestimmt wird, dass das Kommunikationsgerät (**106**) mittels des ersten Zugangspunkts authentisiert wurde, und
ii) einem Authentisierungsschritt eines Authentisierens des Kommunikationsgeräts (**105**), wenn bestimmt wird, dass das Kommunikationsgerät (**106**) nicht authentisiert wurde,
gekennzeichnet durch den Schritt:
Anweisen (S506) des ersten Zugangspunkts (**103**) zum Löschen des Verschlüsselungsschlüssels, wenn das Kommunikationsgerät über den zweiten Zugangspunkt (**104**) mit dem Netzwerk (**101**) verbunden ist.

5. Computer-lesbares Speichermedium mit Computerausführbaren Anweisungen, die die gemäß Anspruch 4 definierten Verfahrensschritte durchführen, wenn sie auf einem Computer ausgeführt werden.

Es folgen 5 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

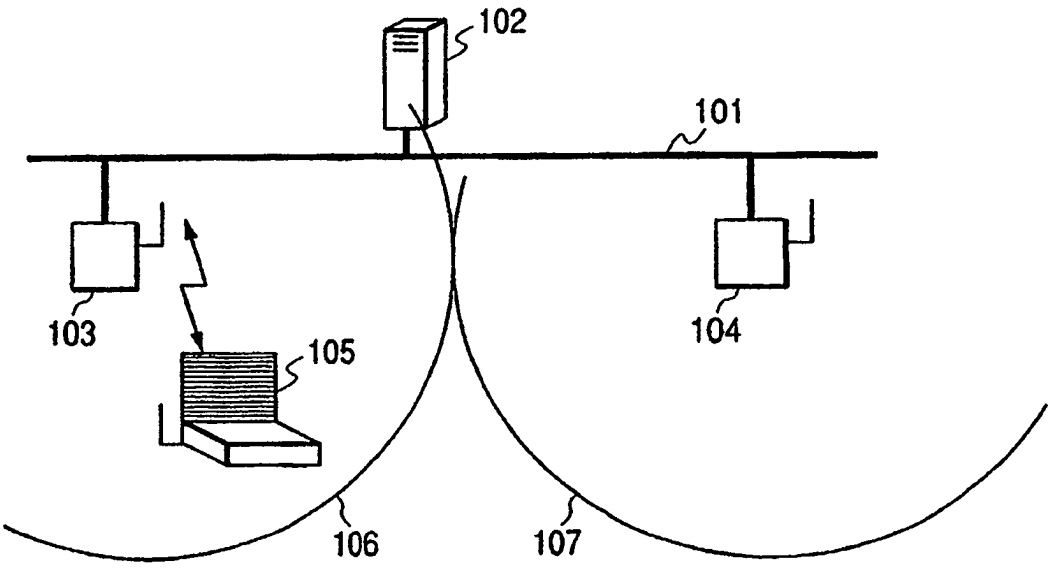


FIG. 2

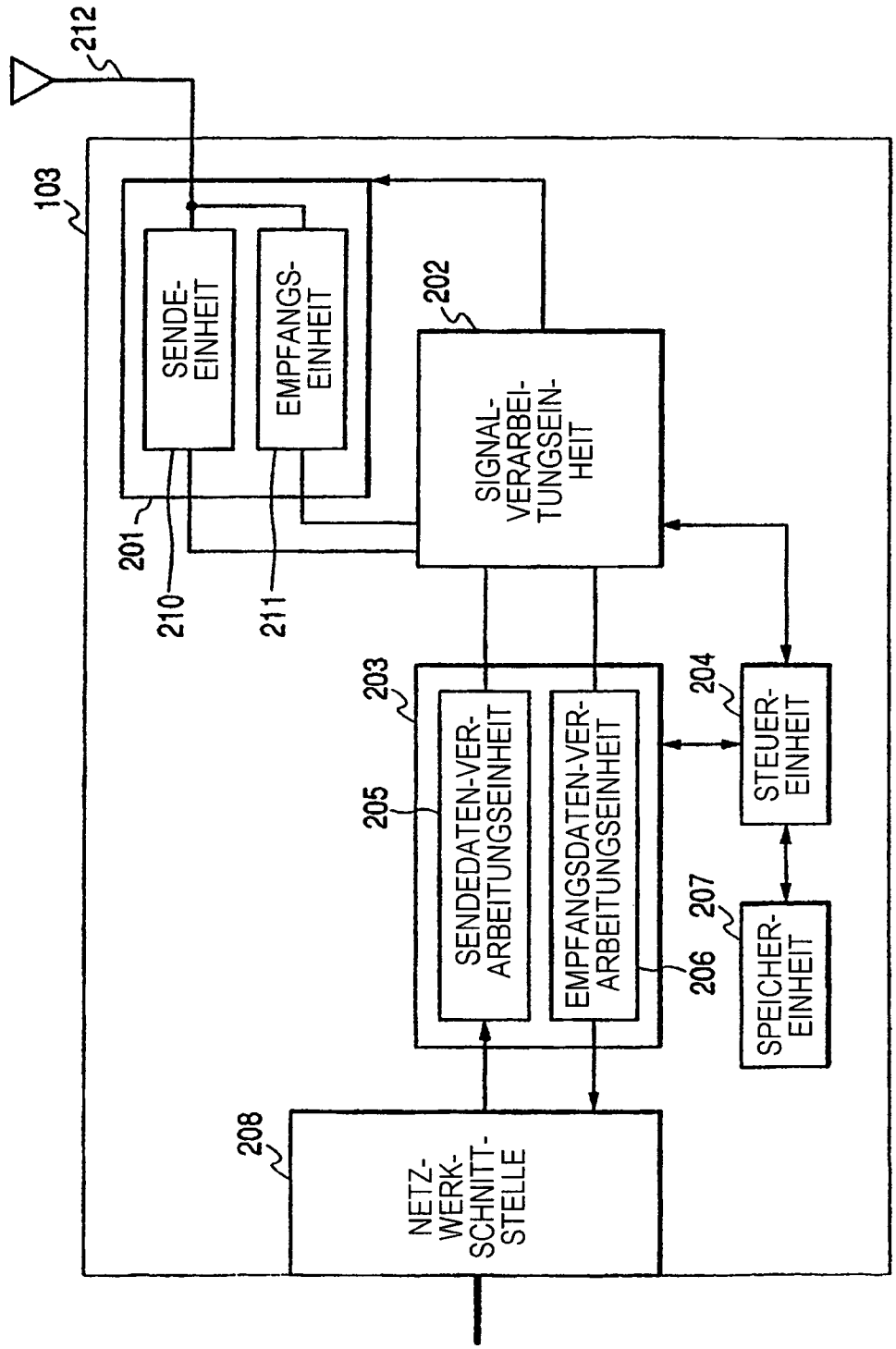

212
103
SENDE-EINHEIT
EMPFANGS-EINHEIT
202
SIGNAL-VERARBEI-TUNGSEIN-HEIT
201
210
211
203
204
205
SENDEDATEN-VER-ARBEITUNGSEINHEIT
EMPFANGSDATEN-VER-ARBEITUNGSEINHEIT
STEUER-EINHEIT
207
206
SPEICHER-EINHEIT
208
NETZ-WERK-SCHNITT-STELLE

FIG. 3

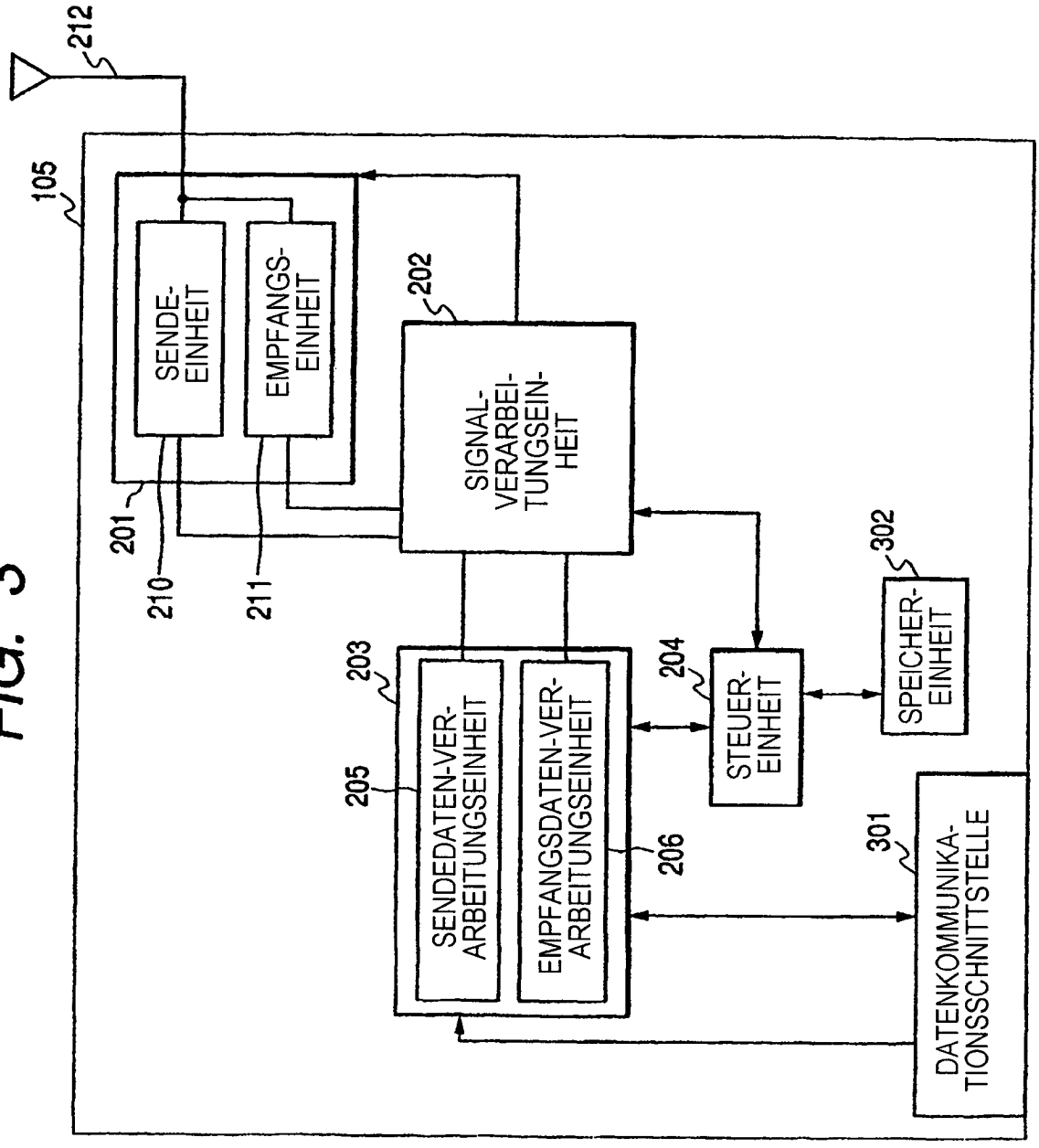

212
105
SENDE-EINHEIT
EMPFANGS-EINHEIT
202
SIGNAL-VERARBEI-TUNGSEIN-HEIT
201
210
211
302
SPEICHER-EINHEIT
203
204
STEUER-EINHEIT
205
SENDEDATEN-VER-ARBEITUNGSEINHEIT
EMPFANGSDATEN-VER-ARBEITUNGSEINHEIT
206
301
DATENKOMMUNIKA-TIONSSCHNITTSTELLE

FIG. 4

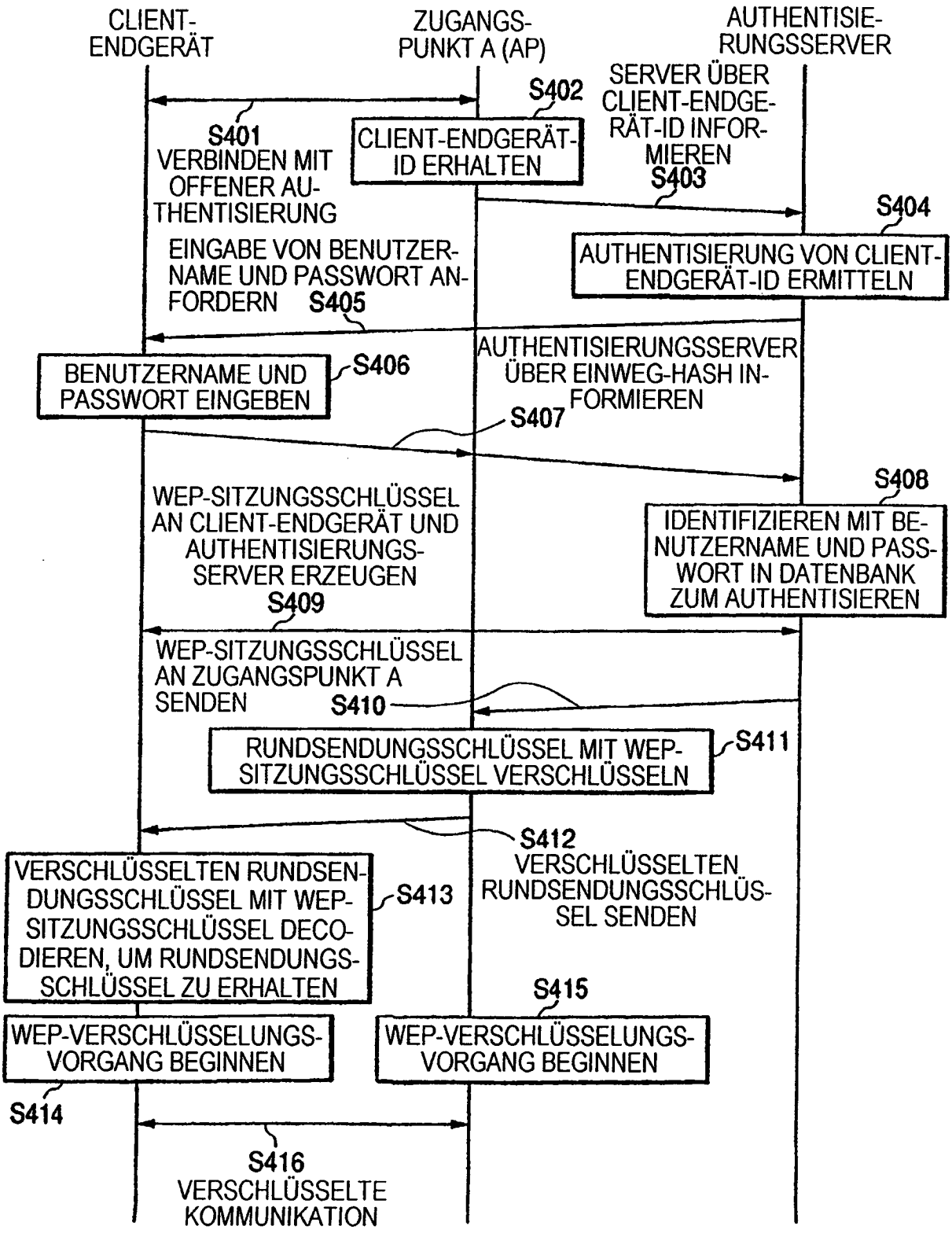
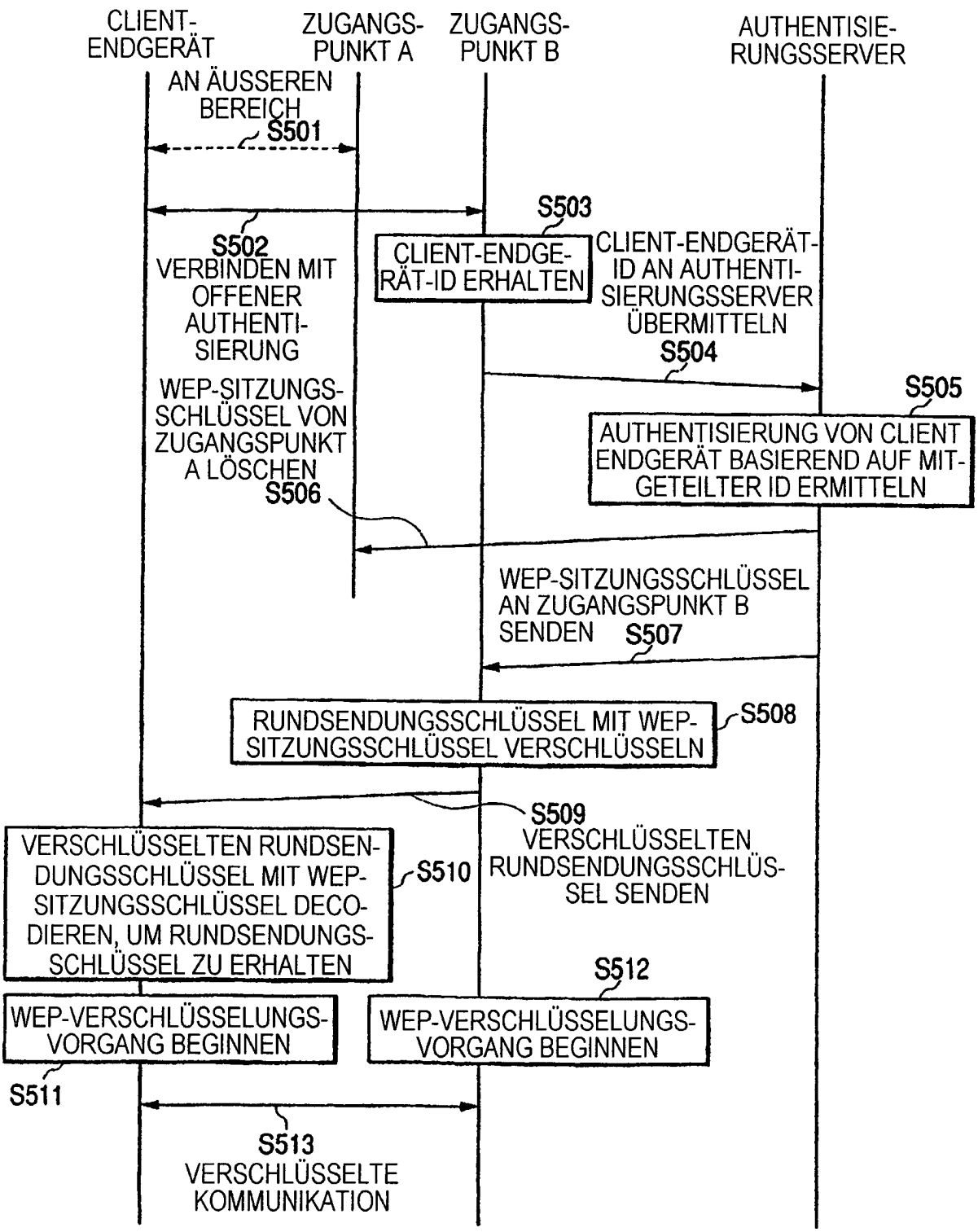

CLIENT-ENDGERÄT
ZUGANGS-PUNKT A (AP)
AUTHENTISIE-RUNGSSERVER
S401
VERBINDEN MIT OFFENER AU-THENTISIERUNG
S402
CLIENT-ENDGERÄT-ID ERHALTEN
SERVER ÜBER CLIENT-ENDGE-RÄT-ID INFOR-MIEREN
S403
S404
AUTHENTISIERUNG VON CLIENT-ENDGERÄT-ID ERMITTELN
EINGABE VON BENUTZER-NAME UND PASSWORT AN-FORDERN
S405
BENUTZERNAME UND PASSWORT EINGEBEN
S406
AUTHENTISIERUNGSSERVER ÜBER EINWEG-HASH IN-FORMIEREN
S407
S408
IDENTIFIZIEREN MIT BE-NUTZERNAME UND PASS-WORT IN DATENBANK ZUM AUTHENTISIEREN
WEP-SITZUNGSSCHLÜSSEL AN CLIENT-ENDGERÄT UND AUTHENTISIERUNGS-SERVER ERZEUGEN
S409
WEP-SITZUNGSSCHLÜSSEL AN ZUGANGSPUNKT A SENDEN
S410
RUNDSENDUNGSSCHLÜSSEL MIT WEP-SITZUNGSSCHLÜSSEL VERSCHLÜSSELN
S411
S412
VERSCHLÜSSELTEN RUNDSENDUNGSSCHLÜS-SEL SENDEN
VERSCHLÜSSELTEN RUNDSEN-DUNGSSCHLÜSSEL MIT WEP-SITZUNGSSCHLÜSSEL DECO-DIEREN, UM RUNDSENDUNGS-SCHLÜSSEL ZU ERHALTEN
S413
S415
WEP-VERSCHLÜSSELUNGS-VORGANG BEGINNEN
WEP-VERSCHLÜSSELUNGS-VORGANG BEGINNEN
S414
S416
VERSCHLÜSSELTE KOMMUNIKATION

FIG. 5


CLIENT-ENDGERÄT
ZUGANGS-PUNKT A
ZUGANGS-PUNKT B
AUTHENTISIE-RUNGSSERVER
AN ÄUSSEREN BEREICH
S501
S502
VERBINDEN MIT OFFENER AUTHENTI-SIERUNG
S503
CLIENT-ENDGE-RÄT-ID ERHALTEN
CLIENT-ENDGERÄT-ID AN AUTHENTI-SIERUNGSSERVER ÜBERMITTELN
S504
WEP-SITZUNGS-SCHLÜSSEL VON ZUGANGSPUNKT A LÖSCHEN
S505
AUTHENTISIERUNG VON CLIENT ENDGERÄT BASIEREND AUF MIT-GETEILTER ID ERMITTELN
S506
WEP-SITZUNGSSCHLÜSSEL AN ZUGANGSPUNKT B SENDEN
S507
RUNDSENDUNGSSCHLÜSSEL MIT WEP-SITZUNGSSCHLÜSSEL VERSCHLÜSSELN
S508
S509
VERSCHLÜSSELTEN RUNDSENDUNGSSCHLÜSSEL SENDEN
VERSCHLÜSSELTEN RUNDSEN-DUNGSSCHLÜSSEL MIT WEP-SITZUNGSSCHLÜSSEL DECO-DIEREN, UM RUNDSENDUNGS-SCHLÜSSEL ZU ERHALTEN
S510
S512
WEP-VERSCHLÜSSELUNGS-VORGANG BEGINNEN
WEP-VERSCHLÜSSELUNGS-VORGANG BEGINNEN
S511
S513
VERSCHLÜSSELTE KOMMUNIKATION