(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2004 045 147 A1** 2006.03.23

(12) **Offenlegungsschrift**

(21) Aktenzeichen: **10 2004 045 147.8**
(22) Anmeldetag: **17.09.2004**
(43) Offenlegungstag: **23.03.2006**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)
H04L 29/06 (2006.01)

(71) Anmelder:
Fujitsu Ltd., Kawasaki, Kanagawa, JP;
Fraunhofer-Gesellschaft Institute for Secure Telecooperation (FhG SIT), 64295 Darmstadt, DE

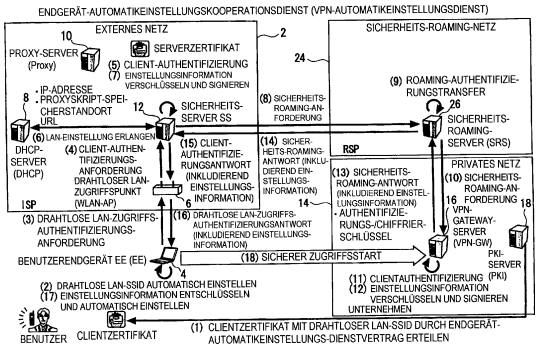
(74) Vertreter:
HOFFMANN & EITLE, 81925 München

(72) Erfinder:
Taniguchi, Hiroyuki, Kawasaki, Kanagawa, JP;
Sato, Izuru, Kawasaki, Kanagawa, JP; Ohnishi, Takeshi, Yokohama, Kanagawa, JP; Schneider, Markus, 64295 Darmstadt, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Einstellungsinformations-Verteilungsvorrichtung, Verfahren, Programm und Medium, Authentifizierungseinstellungs-Transfervorrichtung, Verfahren, Programm und Medium und Einstellungsinformations-Empfangsprogramm**

(57) Zusammenfassung: Eine Einstellungsinformations-Verteilungsvorrichtung, die zu einem ersten Netz gehört, umfasst: eine Authentifizierungseinheit, die eine Authentifizierungsanforderung von einem Benutzerendgerät empfängt und authentifiziert, das eine Zugriffsauthentifizierung anfordert, durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen dem Benutzerendgerät und dem ersten Netz; eine Übertragungseinheit, die eine Authentifizierungskooperationsanforderung, die Einstellungsdaten anfordert, die zu dem Benutzerendgerät einzustellen sind, zu einem anderen Netz überträgt durch Verwenden der Netzzugriffsauthentifizierungsprozedur und einer Authentifizierungskooperationsprozedur zwischen einer Vielzahl von Netzen; und eine Verteilungseinheit, die eine erste Antwortnachricht, der Einstellungsdaten hinzugefügt sind, zu dem Benutzerendgerät verteilt durch Erzeugen der ersten Antwortnachricht entsprechend der Authentifizierungsanforderung durch Hinzufügen der Einstellungsdaten, inkludiert in einer zweiten Antwortnachricht entsprechend der Authentifizierungskooperationsanforderung.



Beschreibung

HINTERGRUND DER ERFINDUNG

[0001] Die Erfindung bezieht sich auf eine Einstellungsinformations-Verteilungsvorrichtung, Verfahren, Programm und Medium, eine Authentifizierungseinstellungs-Transfervorrichtung, Verfahren, Programm und Medium und ein Einstellungsinformations-Empfangsprogramm.

Stand der Technik

[0002] In den letzten Jahren werden mit einer Erhöhung in verschiedenen Netzen, die durch ein IMT-2000-System und ein drahtloses LAN dargestellt werden, und der Verbreitung von Informationsbenutzerendgeräten, wie etwa einem Personalcomputer (hierin nachstehend als "PC" bezeichnet) mit einer Funkkommunikationsfunktion oder einem persönlichen digitalen Assistenten (hierin nachstehend als "PDA" bezeichnet), Umgebungen, wo verschiedene Dienste durch eine Verbindung mit einem Netz zu jeder Zeit und überall verwendet werden können, verbessert.

[0003] Die Netze und Dienste werden durch eine Vielzahl von Anbieterdomänen und Systemen betrieben, und ein Benutzer schließt mit jedem Anbieter einen Vertrag und verwendet verschiedene Dienste. Es ist üblich, entfernt auf ein privates Netz, wie etwa ein Firmennetz, von dem Netz mit einem öffentlichen drahtlosen LAN durch Verwenden derartiger Umgebungen zuzugreifen.

[0004] Eine Erhöhung von Verbrechen unter Verwendung der Netze, wie etwa Manipulation (spoofing) oder Lauschen, wird gleichzeitig mit der Erweiterung der Benutzer, die einen Dienst über ein Netz verwenden, wahrgenommen, mit dem Ergebnis, dass die Benutzer selbst gefordert sind, die Sicherheitsmaßnahmen durchzuführen. Als die Sicherheitsmaßnahmen ist es allgemein üblich, dass eine Erfassungsanwendung (Programm oder Programmprodukt) wie eine Virus-/Wurm-Maßnahme in einem Benutzerendgerät installiert ist, das mit dem Netz verbunden ist. Es ist auch üblich, dass ein Firewall als eine Eindringungsmaßnahme, eine Verschlüsselungsanwendung als eine Abhörmaßnahme und eine Authentifizierungsfunktion in dem Benutzerendgerät installiert sind. Außerdem verschlüsselt die Netzseite wiederum Funksignale in Anbetracht der Sicherheit zwischen Benutzern in einem öffentlichen drahtlosen LAN etc.

[0005] In den Sicherheitsmaßnahmen ist es jedoch, da der Benutzer selbst die Einrichtung (setup) von verschiedenen Werkzeugen, Aktualisierung einer Virusdefinition oder dergleichen durchführen muss, wahrscheinlich, dass ein Betriebsfehler auftritt. Insbesondere ist es in den mobilen Umgebungen auch notwendig, dass der Chiffrierschlüssel eines drahtlosen LAN geändert wird oder IP-Adressen eines DNS, eines Gateway, eines Proxy und dergleichen durch das Endgerät selbst geändert werden, und bei der Änderung ist es auch wahrscheinlich, dass ein Betriebsfehler auftritt. In der gegenwärtigen Situation beeinträchtigt das Sicherheitsproblem die mobilen Umgebungen nachteilig nicht nur dadurch, dass die Sicherheit des Benutzers selbst nicht aufrechterhalten werden kann, sondern sich auch ein Schaden, der von dem Virus oder dem Wurm hervorgerufen wird, zu der Netzseite ausbreitet, die einen Dienst anbietet. In der Zukunft sind die Technologie und die Betriebstechnik zum Aufrechterhalten hoher Sicherheit mit der Steigerung des Komforts des Benutzers in den mobilen Umgebungen erforderlich, die ihre Entwicklung weithin fortsetzen.

(1) In dem drahtlosen LAN, das als eines der Zugriffsnetze entwickelt wurde, gibt es als eine Technik, in der die Chiffrierschlüsseleinrichtung automatisiert ist und die Zugriffssteuerung des Benutzers durchgeführt wird, ein System, welches IEEE 802.1x (port-basierte Netzzugriffssteuerung), welches ein Standard einer Maßnahme ist. Dies ist eine Zugriffssteuerungstechnik, die in einem drahtlosen LAN-Zugriffspunkt oder einem Switch implementiert wird, durch die das Netz den Benutzer authentifiziert, der auf das Netz zugegriffen hat, durch den Benutzerauthentifikator einer ID oder eines elektronischen Zertifikates, und nur dem autorisierten Benutzer wird erlaubt, den drahtlosen LAN-Dienst zu verwenden. Außerdem kann Hochsicherheitsbetrieb durch Verteilen und Aktualisieren des Chiffrierschlüssels (WEP) eines drahtlosen LAN gleichzeitig durchgeführt werden. Da jedoch ein Verschlüsselungsalgorithmus eines WEP verwundbar ist, und ein Werkzeug, das den Verschlüsselungsalgorithmus entschlüsselt, leicht erhalten werden kann, ist es sehr gefährlich, WEP zu verwenden. Obwohl die Sicherheitsfunktion, die IEEE 802.1x enthält, als IEEE 802.11i standardisiert ist, und nun ein robuster Verschlüsselungsalgorithmus angewendet wird, braucht es Zeit, den Verschlüsselungsalgorithmus zu verteilen.

(2) Um das drahtlose LAN zu verwenden, wird außerdem von dem Benutzer selbst gefordert, die Zugriffs-ID (SSID) zum Unterscheiden eines drahtlosen LAN-Netzes einzurichten, welches sich in Organisationseinheiten, wie etwa Anbietern, unterscheidet. Ähnlich unterscheiden sich wiederum Benutzeridentifikatoren für jede Organisation. Da von dem Benutzer verschiedene Arten einer Einrichtung gefordert werden, gibt es, während der Komfort abgesenkt wird, eine Tendenz für einen Benutzer, einfach den gleichen Benutzeridentifikator und das gleiche Passwort einzurichten. Deshalb existieren potenziell viele Einrichtungen des Benutzerendgerätes, was für Sicherheit nicht wünschenswert ist. Außerdem kann die

SSID durch den Besitzer eines drahtlosen LAN-Zugriffspunktes frei eingerichtet werden, und es ist möglich, eine Manipulation einfach durchzuführen, mit dem Ergebnis, dass es sehr gefährlich ist, SSID zu verwenden.

Um die Niedrigkeit des Komforts dessen zu beseitigen, dass der Benutzer selbst SSID zu einem Benutzerendgerät für jeden Anbieter einstellt, gibt es einen Dienst, in dem alle Zugriffs-IDs (SSIDs) der angeschlossenen öffentlichen drahtlosen LAN-Dienste vereinigt sind, und es wird eine Einstellungsliste zu einem mobilen Benutzerendgerät im voraus verteilt. In iPass und GRIC, die einen Roaming-Dienst weltweit ausführen, wird die Einstellungsliste in einem Verbindungswerkzeug gehalten, und während einer Verbindung mit dem Netz kann die Einsetllungsliste automatisch aktualisiert werden. Einem Speichermedium des mobilen Benutzerendgerätes, welches die Information des Benutzerendgerätes speichert, werden jedoch viele Lasten auferlegt, während sich die Zahl von angeschlossenen Diensten erhöht. Da die Lasten wiederum auf einem Server platziert sind, der zentralisiertes Management der Einstellungslisten für automatische Aktualisierung durchführt, sind beträchtliche Managementkosten erforderlich.

(3) Um den Dienst durch eine Verbindung mit einem Netz zu verwenden, ist es außerdem notwendig, die IP-Adresse, DNS-Serveradresse, Gateway-Adresse etc. des Benutzerendgerätes zu erlangen. Als eine Technik, die die Einrichtung automatisiert und die Einrichtung dynamisch verteilt, gibt es DHCP (dynamisches Host-Konfigurationsprotokoll, dynamic host configuration protocol), spezifiziert durch RFC2131, welches ein Standard einer Maßnahme ist. Es gibt jedoch keine Sicherheitsmaßnahmen in DHCP, und ein böswilliger Benutzer, der mit den gleichen Teilnetz verbunden ist, kann als der DHCP-Server manipulieren und eine falsche Einrichtung zu dem Benutzer verteilen.

Damit ein Web-Browser auf einen Web-Server, einen Mail-Server, einen FTP-Server etc. in dem Internet oder Intranet zugreifen kann, kann der Web-Browser über einen Proxy-Server gehen müssen. Ein Proxy-Server wird verwendet, um eine Anforderung für einen Zugriff auf den Web-Server und seine Reaktion darauf zwischenzuspeichern (cache), die Anforderung von einer großen Zahl von Clients effizient zu übertragen und den Zugriff auf das Internet zu steuern. Da ein Proxy-Server mit verschiedenen Strukturen gemäß einer Einrichtung eines Netzes, einem Verfahren zur Lastverteilung oder dergleichen verwendet wird, ist es nicht einfach, das Netz vollständig gemäß der Situation für jede Organisation einzurichten. Es gibt WPAD (Web-Proxy-Autoerkennungsprotokoll, web proxy autodiscovery protocol) als eine Technik, die die Einrichtung automatisiert und die Einrichtung dynamisch verteilt. Da es jedoch keine Sicherheitsmaßnahmen in WPAD gibt und Zugriff durch DHCP oder DNS in der automatischen Einrichtung inkludiert ist, kann eine falsche Einrichtung zu dem Benutzer durch die Manipulation vom DHCP-Server verteilt werden.

Falls der Mail-Server oder Web-Server, auf den der Benutzer zugreift, Sicherheit von SSL angenommen hat, wird die Möglichkeit einer falschen Weitergabe oder Abhörung durch ein drahtloses LAN gering, was die sichere Verwendung eines Dienstes erlaubt. Es müssen jedoch sowohl alle Server als auch Clients diese Maßnahmen befolgen, und es ist Zeit für eine perfekte Ausbreitung wegen den erforderlichen Kosten erforderlich.

(4) Gewöhnlich sind der Mail-Server oder der Web-Server, auf die durch den Benutzer zugegriffen wird, in Netzen eines Unternehmens oder eines Anbieters verteilt, mit dem der Benutzer einen Vertrag schließt. In dem Fall, wo das gesamte Netz oder ein Bereich, wo sich der Mail-Server oder der Web-Server befinden, sicher ist, gibt es ein System, das (i) ein virtuelles privates Netz verwendet, spezifiziert durch RFC2764 (ein Rahmenwerk für IP-basierte virtuelle private Netze), was ein Standard einer Maßnahme ist als eine Technik, die sicher auf einen sicheren Bereich des Netzes von einem Netz zugreift, das sich von dem Netz unterscheidet, und (ii) IPsec, spezifiziert durch RFC2401 (Sicherheitsarchitektur für das Internetprotokoll) als eine Technik, die die Verschlüsselung und Authentifizierung zum Garantieren der Vertraulichkeit und Sicherheit eines IP-Paketes ausführt, oder (iii) IKE, spezifiziert durch RFC2409 (der Internet-Schlüsselaustausch) als eine Schlüsselaustauschtechnologie für Verschlüsselung. Die Anwendung, die diese Techniken zusammen kombiniert, wird auf einen Gateway-Server, der in den Eingang zu einem sicheren Bereich des Netzes gebracht wird, und das Benutzerendgerät gebracht, um dadurch die Zugriffssteuerung durch Benutzerauthentifizierung und den sicheren Zugriff auf den sicheren Bereich des Netzes von dem Netz durch Verschlüsselung von Kommunikationsinformation zu realisieren. Da jedoch der Benutzer selbst gefordert ist, die IP-Adressen des Gateway-Servers und des zugehörigen Proxy-Servers einzurichten, kann hoher Komfort nicht erreicht werden.

(5) Vor Herstellen der sicheren Kommunikation durch IPsec wird ein Chiffrierschlüsselaustausch durch IKE durchgeführt. Obwohl der Gateway-Server des Netzes den Benutzer authentifiziert, der den Schlüsselaustausch anfordert, unterscheidet sich, da sich verwaltende Behörden/Organe voneinander unterscheiden, der Benutzeridentifikator, der für die Benutzerauthentifizierung zur Zeit eines Zugriffs auf ein öffentliches Netz verwendet wird, von dem Benutzeridentifika-

tor, der für die Benutzerauthentifizierung zur Zeit einer Verbindung mit einem privaten oder Unternehmensnetz verwendet wird. Deshalb muss ein Benutzer mindestens zwei oder mehr Benutzeridentifikatoren managen, und der Komfort wird gering. Außerdem richten alle Benutzer mit geringem Sicherheitsbewusstsein den gleichen Benutzeridentifikator und das gleiche Passwort ein und reduzieren die Sicherheit des Netzes.

Wenn in diesem Beispiel die Benutzerauthentifizierung durch Verwenden von PKI (öffentliche Schlüsselinfrastruktur, public key infrastructure), die eine robuste Benutzerauthentifizierungstechnologie ist, durchgeführt wird, kann ein Schaden, der sich aus dem Verlust eines Passworts ableitet, eliminiert werden. Obwohl der gleiche Benutzerauthentifikator für die Zugriffsauthentifizierung eines externen Netzes und die Zugriffsauthentifizierung zu einem Netz verwendet wird, da die gleiche Authentifizierungsbearbeitung wiederholt wird, braucht es jedoch Zeit, die sichere Kommunikation herzustellen, und der Komfort wird gering.

(6) Andererseits wird in dem iPass, der den Roaming-Dienst ausführt, auf ein bestimmtes angeschlossenes Netz durch Verwenden eines Benutzerauthentifikators (z.B. ID/Passwort des Netzes) zwischen den Netzen, die das Netz enthalten, für das ein Vertrag abgeschlossen wurde, zugegriffen, der Benutzerauthentifikator wandert, der Authentifizierungsserver des Netzes, der den Benutzerauthentifikator managt, führt die Authentifizierung und Autorisierung durch, und es ist möglich, ferner die gemeinsame Authentifizierungs- und Autorisierungsverarbeitung und Chiffrierschlüsselverteilung auszuführen, die mit dem Gateway-Server des Netzes gemeinsam bearbeitet wird. Es wird jedoch ein spezifisches Protokoll für Gateway-Server für eine Zusammenarbeit zwischen dem Authentifizierungsserver des Netzes und dem Gateway-Server verwendet. Außerdem ist die Zusammenarbeit auf die Domäne und das System des gleichen Anbieters beschränkt. Es gibt keine Flexibilität, die eine automatische Einrichtung mit Bezug auf die Dienste, die durch verschiedene Anbieter und Systeme durchgeführt werden, sicher durchführen kann.

[0006] **Fig.** 22 ist ein Diagramm zum Erläutern eines Verfahrens, das einen Fernzugriff auf ein Netz eines Unternehmens durchführt, das sich in der Managementeinheit von dem Netz, wie etwa dem öffentlichen drahtlosen LAN, von dem Netz des öffentlichen drahtlosen LAN unterscheidet, in Übereinstimmung mit einem Stand der Technik.

[0007] Das Netz **102**, das in **Fig.** 22 gezeigt wird, ist ein Netz **102**, das durch ein öffentliches drahtloses LAN dargestellt wird, und es wird ein Netzverbindungsdienst durch den Anbieter angeboten. Das Netz **102** ist mit dem Internet oder dergleichen verbunden. Außerdem ist das öffentliche drahtlose LAN ein Verbindungsnetz einer Domänenbegrenzung, was durch ein drahtloses LAN oder dergleichen aufgebaut wird, und was z.B. das Netz **102** ist, aufgebaut durch das drahtlose LAN oder dergleichen in dem Bürogebäude eines Kaufhauses oder eines Unternehmens. Obwohl das öffentliche drahtlose LAN unter dem Dienst eines mobilen Kommunikationsanbieters ist, schließt ein Kaufhaus oder ein Unternehmen einen Vertrag mit dem mobilen Kommunikationsanbieter, und das öffentliche drahtlose LAN ist in dem Bürogebäude des Kaufhauses oder Unternehmens begrenzt.

[0008] Bis jetzt managen, wie in **Fig.** 22 gezeigt, Kommunikationsanbieter, wie etwa ein Internetdienstanbieter (ISP), den öffentlichen drahtlosen LAN-Dienst und bieten den Netzverbindungsdienst zu dem Internet oder dergleichen an. Es wird ein DHCP-Server **104**, der die IP-Adressen von verschiedenen Servern verteilt, beim ISP installiert. Außerdem wird ein Gateway, wie ein IPsec-Gateway-Server **108** zum Zugriff auf ein Netz von dem Internet etc. in dem Netz eines Unternehmens oder dergleichen installiert, welches das private Netz **106** ist. Außerdem wird ein Roaming-Authentifizierungsserver **112** zum Roaming einer Vielzahl von ISP und Durchführen von Netzzugriffsauthentifizierung zu dem öffentlichen drahtlosen LAN-Dienst durch eine ID/Passwort, die z.B. durch ein Unternehmen gemanagt wird, in dem Roaming-Netzanbieter (RSP) installiert, welches das Roaming-Netz **110** ist, wie etwa iPass. Hierin nachstehend wird eine Beschreibung einer Sequenz, die in **Fig.** 23 gezeigt wird, gegeben, in der das Benutzerendgerät **114** eine Zugriffsverbindung zu dem Netz eines Unternehmens oder dergleichen durch das Internet von dem öffentlichen drahtlosen LAN mit Bezug auf **Fig.** 22 sicher durchführt.

<Verbindung von Netzverknüpfung (Schicht 2, Datenverknüpfung: Verwundbarkeit vom Verschlüsselungsalgorithmus>

[0009] Zuerst richtet ein Benutzer SSID ein, was der Identifikator des öffentlichen drahtlosen LAN-Dienstes ist, der im voraus in dem Benutzerendgerät **114** ((2) von **Fig.** 22) registriert wurde, SSID, das in einem Signalfeuer (beacon) enthalten ist, das von einem drahtlosen LAN-Zugriffspunkt gesendet wird, wird erfasst und ausgewählt, und eine Netzzugriffsauthentifizierung wird gestartet ((3) von **Fig.** 22. Der drahtlose LAN-Zugriffspunkt **116** fängt die Kommunikation von dem Benutzerendgerät **114** zeitweilig ab, empfängt die Authentifizierungsinformation von dem Benutzerendgerät **114** und validiert eine Dienstverwendung des Benutzerendgerätes **114** zu dem ISP-Authentifizierungsserver **118** innerhalb von ISP ((4) und (5) von **Fig.** 22). Falls das Benutzerendgerät **114** zu dieser Zeit ein wandernder (roaming) Benutzer ist,

wird eine Roaming-Authentifizierungsanforderung zu einem Unternehmensnetz über RSP erteilt, und Authentifizierung wird durch den Unternehmensauthentifizierungsserver **120** eines Unternehmens durchgeführt ((6) bis (9) von **Fig.** 22). Falls ein Authentifizierungsergebnis gut ist, gibt der drahtlose LAN-Zugriffspunkt **116** eine Netzverknüpfung zu dem Benutzer frei, der abgefangen wurde ((10) bis (13) von **Fig.** 22). Obwohl die Daten, die in der Verknüpfung des drahtlosen LAN fließen, durch WEP verschlüsselt sind, ist, da der Verschlüsselungsalgorithmus verwundbar ist, Abhören möglich und die Authentifizierung ist als Sicherheit nicht sicher.

<Verbindung vom IP-Netz: Manipulation>

[0010] Wenn das Benutzerendgerät **114** vollständig die Netzverknüpfung verbunden hat, erteilt das Benutzerendgerät **114** als Nächstes eine Anforderung zum Erlangen einer LAN-Einstellung, enthaltend IP-Adressen des Benutzerendgerätes **114**, einen DNS-Server, ein Gateway, das eine Verbindung mit dem Internet durchführt, und dergleichen, zu dem DHCP-Server **104**, und empfängt eine LAN-Einstellung ((14) von **Fig.** 22). Vom Benutzer wird nicht gefordert, die IP-Adresse des DHCP-Servers **104** selbst usw. im voraus zu bestimmen. Wenn eine Vorrichtung, die als der DHCP-Server **104** manipuliert, innerhalb des gleichen öffentlichen drahtlosen LAN existiert, werden Abhören, Dienststörung etc. durch betrügerische Weitergabe erzielt, und Sicherheit kann nicht sichergestellt werden.

<Komfort des Benutzers>

[0011] Um die sichere Kommunikation durch IPsec zu der IP-Adresse des Gateway-Servers eines Netzes, die im voraus zu dem Benutzerendgerät **114** eingestellt ist, zu beginnen, wird ferner eine IKE-Prozedur gestartet, die ein Schlüsselaustausch ist. Benutzerauthentifizierung für einen Schlüsselaustausch kann in der IKE-Prozedur durchgeführt werden. Obwohl der IKE selbst ein sicheres Protokoll ist, gibt es eine Reihe von Prozeduren zum sicheren Starten eines Dienstes vom Netzzugriff, und der Komfort des Benutzers bis zum tatsächlichen sicheren Starten eines Dienstes wird gestört. Außerdem ist es in dem Dienst, der durch den iPass oder dergleichen angeboten wird, für einen Authentifizierungsserver und einen Gateway-Server möglich, gleichzeitig mit Authentifizierung eines Netzzugriffs zusammenzuarbeiten und Schlüsselverteilung durchzuführen. Es wird jedoch nicht angenommen, dass die zusammenhängende Authentifizierung und eine automatische Einrichtung eines Dienstes durch zwei oder mehr Anbieter vor einem Starten sicherer Kommunikation mit dem Netz durchgeführt werden. Wenn z.B. ein anderes unabhängiges Netz **102** den Heimatagentenserver eines mobilen IP-Dienstes und den SIP-Server für einen VoIP-Dienst hat, wird nicht angenommen, dass alle Authentifizierungen veranlasst werden zusammenzuarbeiten. Angesichts dieser Sache ist die Flexibilität des Standes der Technik gering.

[0012] Ferner ist das Folgende eine Technik zum automatischen Einrichten eines bekannten Endgerätes, aber eine derartige Technik löst die Probleme nicht.

[0013] Patentliteraturstelle 1 bezieht sich auf ein Adresseinstellungsverfahren und eine Vorrichtung. Diese Patentliteraturstelle legt ein IP-Adressen-Automatikeinstellungssystem zu dem Endgerät für eine beliebige MAC-Adresse offen.

[Patentliteraturstelle 1] JP 11-234342 A

[0014] In dem wie oben erwähnten konventionellen System ist, da die Dienststartprozedur der Netze, die sich in der Managementeinheit der Anbieter unterscheidet, nicht miteinander zusammenarbeiten können, der Komfort für den Benutzer, der einen Dienst sicher und frühzeitig verwenden möchte, weit davon entfernt hoch zu sein. Um die Einrichtung von verschiedenen Diensten zu einem Benutzerendgerät sicher zu verteilen, ist eine Maßnahme zum Herstellen einer sicheren Route zwischen dem Benutzerendgerät und den jeweiligen Anbietern erforderlich. Die Prozedur wird auch in diesem Fall kompliziert, und deshalb wird ein Komfort des Benutzers gestört.

Aufgabenstellung

ZUSAMMENFASSUNG DER ERFINDUNG

[0015] Die Erfindung wurde unternommen, um die Probleme zu lösen, und hat deshalb ein Ziel, eine Vorrichtung, ein Verfahren, ein Programm und ein Medium für Einstellungsinformationsverteilung, eine Vorrichtung, ein Verfahren, ein Programm und ein Medium für Authentifizierungseinstellungstransfer und ein Einstellungsinformations-Empfangsprogramm vorzusehen, die verschiedene Dienstanforderungen und die Verteilung einer Einrichtung gemeinsam bearbeiten, die unabhängig in einer Vielzahl von Domänen durchgeführt werden, und den Komfort des Benutzers verbessern und die Richtigkeit von Verteilungsinformation in jeder Domäne garantieren.

[0016] Gemäß einem Aspekt der Erfindung wird eine Einstellungsinformations-Verteilungsvorrichtung, die zu einem ersten Netz gehört, vorgesehen, gekennzeichnet durch Inkludieren: einer Authentifizierungseinheit, die eine Authentifizierungsanforderung von einem Benutzerendgerät empfängt und authentifiziert, das eine Zugriffsauthentifizierung anfordert durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen dem Benutzerendgerät und dem ersten Netz; einer Übertragungseinheit, die eine Authentifizierungskooperationsanforderung, die an-

fordert, dass Einstellungsdaten zu dem Benutzerendgerät einzustellen sind, zu einem anderen Netz durch Verwenden der Netzzugriffsauthentifizierungsprozedur und einer Authentifizierungskooperationsprozedur zwischen einer Vielzahl von Netzen überträgt; und einer Verteilungseinheit, die eine erste Antwortnachricht, der Einstellungsdaten hinzugefügt sind, zu dem Benutzerendgerät verteilt durch Erzeugen der ersten Antwortnachricht entsprechend der Authentifizierungsanforderung durch Hinzufügen der Einstellungsdaten, die in einer zweiten Antwortnachricht inkludiert sind, entsprechend der Authentifizierungskooperationsanforderung.

[0017] Gemäß der Einstellungsinformations-Verteilungsvorrichtung der Erfindung können die Einstellungsdaten der Benutzerendgeräte, die jeweils durch eine Vielzahl von Netzen (eine Vielzahl von Domänen) generiert wurden, schließlich gemeinsam in einer Nachricht eines Authentifizierungsprotokolls zwischen den Benutzerendgeräten und den Netzen inkludiert sein. Als ein Ergebnis können die Einstellungsdaten des Benutzerendgerätes zu der Vielzahl von Netzen zu dem Benutzerendgerät während einer Authentifizierungsbearbeitung sicher verteilt werden, bevor sich der Benutzer mit dem Netz verbindet. Das heißt die Einstellungsinformations-Verteilungsvorrichtung der Erfindung kann eine Verteilung der verschiedenen Dienstanforderungen und die Verteilung der Einrichtung, die in der Vielzahl von Domänen unabhängig durchgeführt werden, gemeinsam bearbeiten.

[0018] Da die Authentifizierungskooperationsprozedur zwischen der Vielzahl von Netzen verwendet wird, ist des weiteren die Verschlüsselung, die durch den öffentlichen Schlüssel eines Clients durchgeführt wird, oder die Signatur, die durch jeden Server durchgeführt wird, in der Nachricht inkludiert, die gegenseitig zwischen den Netzen gesendet wird, wobei dadurch Abhören und die Änderung unmöglich gemacht werden. Jede Netzdomäne verwendet die Nachrichtenerweiterung, die die Einstellungsdaten speichern kann, so, um die Einstellungsdaten, die zu einem Benutzerendgerät eingerichtet werden sollten, sicher zu verteilen.

[0019] Gemäß einem anderen Aspekt der Erfindung wird eine Authentifizierungstransfervorrichtung vorgesehen, gekennzeichnet durch Inkludieren: einer Empfangseinheit, die ein elektronisches Zertifikat eines Clients, das für Zugriffsauthentifizierung verwendet wird, von einem ersten Netz empfängt, das eine Authentifizierung bei Empfang einer Authentifizierungsanforderung von einem Benutzerendgerät durchführt, das die Zugriffsauthentifizierung anfordert, durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen dem Benutzerendgerät und dem ersten Netz; und einer Bestimmungseinheit, die eine Authentifizierungskooperationsvorrichtung bestimmt, die mit Bezug auf das elektronisches Zertifikat des Client, das durch die Empfangseinheit empfangen wird, zu kooperieren hat.

[0020] Gemäß der Authentifizierungseinstellungs-Transfervorrichtung der Erfindung, kann, da auf Kooperationsdaten, wie etwa eine IP-Adresse des Servers (Authentifizierungskooperationsvorrichtung), die durch Server gemanagt wird, wie etwa einen Erteilungsserver, der ein elektronisches Zertifikat eines Clients erteilt und der Authentifizierungskooperation ausführen sollte, verwiesen wird, eine Authentifizierungskooperationsvorrichtung in der Netzzugriffsauthentifizierungsprozedur effizient bestimmt werden. Außerdem werden die Kooperationsdaten, wie etwa die IP-Adresse, in der Datenbank des Authentifizierungsservers, der kooperiert, gemanagt, während die IP-Adresse, URL oder dergleichen direkt in dem elektronischen Zertifikat des Clients beschrieben wird, oder ein Flag, das dem Server erlaubt, spezifiziert zu werden, indirekt in dem elektronischen Zertifikat des Clients beschrieben wird.

[0021] Gemäß noch einem anderen Aspekt der Erfindung wird ein Einstellungsinformations-Empfangsprogramm vorgesehen zum Veranlassen eines Computers, zu funktionieren als: eine Authentifizierungsanforderungseinheit, die eine Zugriffsauthentifizierung zu einem ersten Netz anfordert, durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen einem Benutzerendgerät und dem ersten Netz; eine Empfangseinheit, die Einstellungsdaten empfängt, die zu dem Benutzerendgerät mit Bezug auf ein anderes Netz eingestellt sind, die von einem anderen Netz erlangt werden, durch Verwenden der Netzzugriffsauthentifizierungsprozedur und einer Authentifizierungskooperationsprozedur zwischen einer Vielzahl von Netzen, die miteinander kooperieren; und eine Einstellungseinheit, die die Einstellungsdaten, die von der Empfangseinheit empfangen werden, auf der Basis von Daten sequenziell einstellt, die eine Kooperationsrangfolge von anderen Netzen anzeigen, inkludiert in dem elektronischen Zertifikat des Clients.

[0022] Gemäß dem Einstellungsinformations-Empfangsprogramm der Erfindung wird in dem Fall, wo es eine Vielzahl von Netzen gibt, die in einer Authentifizierung miteinander zu kooperieren haben, eine Einrichtung auf der Basis von Netzinformation, die miteinander zu kooperieren hat, die durch ein elektronisches Zertifikat (Daten, die eine Rangfolge der Netze anzeigen, die zu kooperieren haben), sequenziell durchgeführt. Als ein Ergebnis wird der Komfort des Benutzers verbessert und die Richtigkeit von Verteilungsinformation kann in jeder Domäne garantiert werden.

[0023] Da wie oben beschrieben die Gültigkeit von jeder Authentifizierungskooperationsnachricht durch

Verifizieren der Signatur, die durch jedes der Netze durchgeführt wird, verifiziert werden kann, ist die Benutzereinstellungsinformation, die für eine Dienstanforderung relevant ist, von jedem der Kooperationsserver sicher verfügbar. Außerdem kann jeder der Kooperationsserver so eingestellt werden, um eine Einrichtung für einen eigenen Server, der das Benutzerendgerät mit einem Dienst versieht, in der Authentifizierungskooperationsprozedur zwischen der Vielzahl von Netzen durchzuführen.

BESCHREIBUNG DER ZEICHNUNGEN

[0024] Fig. 1 ist ein erläuterndes Diagramm, das einen automatischen Einstellungsdienst eines Benutzerendgerätes gemäß der Erfindung zeigt.

[0025] **Fig.** 2 ist ein erläuterndes Diagramm, das ein Sequenzbeispiel des automatischen Einstellungsdienstes eines Benutzerendgerätes gemäß der Erfindung zeigt.

[0026] Fig. 3 ist ein erläuterndes Diagramm, das einen Funktionsblock und ein System gemäß der Erfindung zeigt.

[0027] Fig. 4 ist ein erläuterndes Diagramm, das die Details eines TLS-Protokolls (Client-Hallo) zeigt.

[0028] **Fig.** 5 ist ein erläuterndes Diagramm, das die Details des TLS-Protokolls (Server fertig) zeigt.

[0029] **Fig.** 6 ist ein erläuterndes Diagramm, das das detaillierte Beispiel (ISP → RSP) eines SAML-Protokolls (Anforderung) zeigt.

[0030] **Fig.** 7 ist ein erläuterndes Diagramm, das das detaillierte Beispiel (RSP → Unternehmensnetz) des SAML-Protokolls (Anforderung) zeigt.

[0031] **Fig.** 8 ist ein erläuterndes Diagramm, das das detaillierte Beispiel (Unternehmensnetz → RSP) des SAML-Protokolls (Antwort) zeigt.

[0032] **Fig.** 9 ist ein erläuterndes Diagramm, das das detaillierte Beispiel (RSP → ISP) des SAML-Protokolls (Antwort) zeigt.

[0033] **Fig.** 10 ist ein erläuterndes Diagramm, das das detaillierte Beispiel eines elektronischen Zertifikates zeigt.

[0034] Fig. 11 ist ein Flussdiagramm, das ein Beispiel eines gesamten Verarbeitungsflusses eines Sicherheitsservers SS (SS1) zeigt.

[0035] Fig. 12 ist ein Flussdiagramm, das ein Beispiel des gesamten Verarbeitungsflusses des Sicherheitsservers SS (SS2) zeigt.

[0036] Fig. 13 ist ein Flussdiagramm, das ein Beispiel des gesamten Verarbeitungsflusses des Sicherheitsservers SS (SS3) zeigt.

[0037] Fig. 14 ist ein Flussdiagramm, das ein Beispiel des gesamten Verarbeitungsflusses eines Sicherheits-Roaming-Servers SRS (SRS1) zeigt.

[0038] Fig. 15 ist ein Flussdiagramm, das ein Beispiel des gesamten Verarbeitungsflusses des Sicherheits-Roaming-Servers SRS (SRS2) zeigt.

[0039] Fig. 16 ist ein Flussdiagramm, das ein Beispiel eines gesamten Verarbeitungsflusses eines VPN-Gateway-Servers VPN zeigt.

[0040] Fig. 17 ist ein Flussdiagramm, das ein Beispiel eines gesamten Verarbeitungsflusses eines Benutzerendgerätes EE (EE0) zeigt.

[0041] Fig. 18 ist ein Flussdiagramm, das ein Beispiel des gesamten Verarbeitungsflusses des Benutzerendgerätes EE (EE1) zeigt.

[0042] Fig. 19 ist ein Flussdiagramm, das ein Beispiel des gesamten Verarbeitungsflusses des Benutzerendgerätes EE (EE2) zeigt.

[0043] Fig. 20 ist ein erläuterndes Diagramm, das ein Beispiel einer VPN-Schlüsselgenerierungssequenz unter Verwendung einer Authentifizierungskooperation zeigt.

[0044] Fig. 21 ist eine Tabelle, die eine IP-Adresse des VPN-Gateway-Servers eines Unternehmens in einer Dienstdatenbank zeigt.

[0045] Fig. 22 ist ein erläuterndes Diagramm zum Erläutern eines automatischen Einstellungsdienstes eines Benutzerendgerätes im Stand der Technik.

[0046] **Fig.** 23 ist ein erläuterndes Diagramm, das ein Beispiel einer Sequenz des automatischen Einstellungsdienstes eines Benutzerendgerätes im Stand der Technik zeigt.

Ausführungsbeispiel

DETAILLIERTE BESCHREIBUNG DER ERFINDUNG

[0047] Hierin nachstehend wird der bester Modus zum Ausführen der Erfindung mit Bezug auf die Zeichnungen beschrieben.

<Überblick über Systemfunktion>

[0048] Fig. 1 und 2 sind Diagramme, die jedes ein Beispiel eines Fernzugriffsdienstes und ein Beispiel einer Dienstsequenz davon gemäß der Erfindung

zeigen. Fig. 3 ist ein Funktionsblockdiagramm gemäß der Erfindung.

[0049] Hierin nachstehend wird der Überblick über die Systemfunktion gemäß der Erfindung mit Bezug auf Fig. 3 beschrieben.

<1. Externes Netz 2>

[0050] Ein externes Netz **2** ist ein Internetdienstanbieter (ISP), der alle Benutzerendgeräte **4** mit IP-Netzdiensten versieht, und einen drahtlosen LAN-Zugriffspunkt **6** (WLAN-AP) usw. anbietet. Außerdem weist das externe Netz **2** jedem der Benutzerendgeräte **4** eine IP-Adresse zu, um einen Internet-Zugriffsdienst vorzusehen. Allgemein hat ein DHCP-Server **8** eine Funktion, die IP-Adresse dynamisch zuzuweisen, und eine Funktion, einen Speicher-Ziel-URL eines automatischen Einstellungsskriptes, wie etwa eines Proxy-Servers **10**, zu verteilen. Zusätzlich zu den Funktionselementen inkludiert das externe Netz **2** gemäß der Ausführungsform einen Sicherheitsserver **12** (SS), der eine Authentifizierungsfunktion zum Durchführen einer Authentifizierungs- und Autorisierungsbearbeitung des Benutzerendgerätes **4**, die in dem Fall notwendig sind, wo der Benutzer den Dienst verwendet, und eine automatische Einstellungsfunktion des Benutzerendgerätes **4** hat.

<2. Privates Netz 14>

[0051] Ein privates Netz **14** ist auf ein Organisationsnetz eines Unternehmens, einer Universität oder eines Regierungsbüros gerichtet, welches eine begrenzte Zahl von Benutzern mit einem IP-Netzdienst versieht, und hat allgemein einen VPN-Gateway-Server (VPN-GW) **16** zum Trennen des Netzes von einem öffentlichen Netz wie dem Internet. Um das Benutzerendgerät **4** zu begrenzen, welches das private Netz **14** verwenden kann, hat das private Netz **14** außerdem einen Server mit einer Authentifizierungsfunktion. In der Ausführungsform wird PKI, was eine öffentliche Schlüsselinfrastruktur ist, für Authentifizierung verwendet, und Authentifizierung wird durch Verwenden eines elektronischen Zertifikates durchgeführt, das dem Benutzer erteilt wird. Ein PKI-Server **18** (PKI), der später zu beschreiben ist, wird in dem privaten Netz **14** als ein Managementserver von PKI installiert, und ein VPN-Gateway-Server **22** (VPN-GW), der später beschrieben wird, wird als ein Gateway für das Benutzerendgerät **4** installiert, das mit dem privaten Netz **14** von außerhalb durch Verwenden eines VPN-Protokolls **20** verbindet. Der VPN-Gateway-Server **22** hat eine Funktion zum Authentifizieren des Benutzers mit dem elektronischen Zertifikat oder dergleichen. Fig. 3 zeigt ein System, in dem der VPN-Gateway-Server **22** mit einem Sicherheits-Roaming-Netz verbunden ist, das nachstehend beschrieben wird, sodass ein mobiler Benutzer indirekt auf das private Netz **14** zugreifen kann. Hierin nachstehend wird für eine Beschreibung einer Ausführungsform der Erfindung ein Unternehmensnetz als ein repräsentatives Beispiel des privaten Netzes **14** beschrieben.

<3. Sicherheits-Roaming-Netz 24>

[0052] Ein Sicherheits-Roaming-Netz **24** ist ein Roaming-Dienstanbieter (RSP), der Sicherheit inkludierend Authentifizierung und Autorisierung der vielen externen Netze **2** oder der privaten Netze **14** kooperiert. RSP sieht einen Dienst zum Ausführen der Verifizierungsfunktion des elektronischen Zertifikates in der Authentifizierung durch Proxy vor, um die Vertrauensbeziehung zwischen zwei oder mehr Netzen **102** zu garantieren, in denen zu wandern ist. Das externe Netz **2** kann als RSP dienen und ein Modus eines vorgesehenen Dienstes ist nicht begrenzt. In der Ausführungsform ist das Sicherheits-Roaming-Netz **24** ein Netz **102**, welches den Sicherheits-Roaming-Server **26** (SRS), der später beschrieben wird, als einen Server hat, der das Roaming von Sicherheit managt.

<4. Benutzerendgerät 4>

[0053] Das Benutzerendgerät **4** besteht aus vier Steuereinheiten, die nachstehend beschrieben werden.

[0054] Zuerst (**1**) wird eine Authentifizierungsprotokoll-Steuereinheit EE28 von einer Netzzugriffsanwendung aufgerufen, die in dem Fall verwendet wird, wo der Benutzer einen Dienst verwendet, und führt die Benutzerauthentifizierungsprozedur durch das elektronische Zertifikat durch. Als Nächstes (**2**) wird eine Automatikeinstellungs-Protokollsteuereinheit EE30 von der Authentifizierungsprotokoll-Steuereinheit EE28 aufgerufen und führt die Einrichtung in verschiedenen Steuereinheiten auf der Basis der automatischen Einstellungsinformation (Einstellungsdaten) durch, die in einer Antwortnachricht gespeichert ist. Dann (3) richtet eine LAN-Steuereinheit EE32 verschiedene IP-Adressen des Benutzerendgerätes **4**, eines Gateway-Servers, eines DNS-Servers und eines Proxy-Servers **10** ein. Des weiteren (4) führt eine Sicherheitssteuereinheit EE34 eine sichere Kommunikation mit dem VPN-Gateway-Server **22** auf der Basis eines Chiffrierschlüssels oder eines Authentifizierungsschlüssels mit einem üblichen IP-sec-Client aus.

<5. Sicherheitsserver 12>

[0055] Der Sicherheitsserver **12** besteht aus vier Steuereinheiten, die nachstehend beschrieben werden. Zuerst (1) hat eine Authentifizierungsprotokoll-Steuereinheit SS36 eine Benutzerauthentifizierungsfunktion durch das elektronische Zertifikat, eine

Verifizierungsfunktion, um das elektronische Zertifikat zu validieren, und eine Autorisierungsfunktion eines Dienstes. Als Nächstes (2) wird eine Automatikeinstellungs-Protokollsteuereinheit SS38 von der Authentifizierungsprotokoll-Steuereinheit SS36 aufgerufen, und fügt die Einstellungsinformation (Einstellungsdaten), die durch die Einstellungssteuereinheit gesammelt werden, zum Durchführen der verschiedenen automatischen Einrichtung und das kooperierende Netz **102** zu der Autorisierungsantwortnachricht, die erweitert wurde, für eine Verteilung zu dem Benutzer hinzu. Der erweiterte Teil der Autorisierungsantwortnachricht ist ein ursprünglicher erweiterter Teil gemäß der Erfindung, wie in **Fig.** 5 gezeigt wird. Dann (3) managt eine LAN-Einstellungssteuereinheit SS40 den drahtlosen LAN-Zugriffspunkt **6** in dem externen Netz **2**, und den DHCP-Server **8**, und sammelt geeignete LAN-Einstellung gemäß der Situation (z.B. die IP-Adresse des Benutzerendgerätes **4**, die IP-Adresse des Gateway und DNS, einen Speicherziel-URL einer Automatikeinstellungs-Skriptdatei des Proxy-Servers **10** etc.) durch Verwenden eines DHCP-Protokolls etc. Des Weiteren (**4**) gibt eine Authentifizierungskooperations-Protokollsteuereinheit SS42 das Netz **102**, welches Authentifizierungskooperation der Benutzerauthentifizierung ausführen sollte, und Autorisierungsinformation über ein eigenes Netz, und die generierte Einstellung bekannt, und empfängt ein Einzelanmeldungs-Authentifizierungsergebnis und Einstellungsinformation (Einstellungsdaten) von jedem von Authentifizierungskooperationsnetzen.

<6. DHCP-Server 8>

[0056] Der DHCP-Server **8** hat LAN-Einstellungsfunktionen (die Zuweisung einer Benutzerendgerät-IP-Adresse, die Verteilung der IP-Adressen des DNS-Servers und des Gateway-Servers, die Bekanntgabe eines Speicherziel-URL des automatischen Einstellungsskriptes des Proxy-Servers **10**), die für das Benutzerendgerät **4** notwendig sind, um auf das Netz **102** zuzugreifen. In der Ausführungsform ist der DHCP-Server **8** ein normaler DHCP-Server **8**, der mit RFC2131 übereinstimmt, was ein Standard einer Maßnahme ist, und unterstützt zusätzlich eine WPAD-Funktion (eine Option, die auf einen Speicherziel-URL des automatischen Einstellungsskriptes von Proxy-Server **10** zugreift), die normalerweise durch den DHCP-Server **8** von Microsoft Corporation unterstützt wird. Das DHCP-Protokoll **44** wird zwischen dem Sicherheitsserver **12** und dem DHCP-Server **8** verwendet.

<7. Sicherheits-Roaming-Server 26>

[0057] Der Sicherheits-Roaming-Server **26** besteht aus zwei Steuereinheiten und einer Datenbank, die nachstehend beschrieben werden. Zuerst (**1**) bestimmt eine Dienstdatenbank **46** (Server-DB) die IP-Adresse des Servers (Authentifizierungskooperationsvorrichtung), der Authentifizierungskooperation durchführen sollte, durch Verwenden der Information in einem elektronischen Zertifikat des Clients als einen Suchschlüssel. Fig. 3 stellt den Sicherheitsserver **12**, den Sicherheits-Roaming-Server **26** und den VPN-Gateway-Server **22** als die Authentifizierungskooperationsvorrichtung beispielhaft dar. (2) Eine Authentifizierungskooperations-Protokollsteuereinheit SRS48 (i) empfängt eine Einzelanmeldungs-Authentifizierungsanforderung und Antwort inkludierend die Benutzerauthentifizierung und Autorisierungsergebnis und die Einstellungsinformation, die von der Authentifizierungskooperations-Protokollsteuereinheit SS42 des Sicherheitsservers **12** oder der Authentifizierungskooperations-Protokollsteuereinheit VPN **50** des VPN-Gateway-Servers **22** übertragen wurden, (ii) bestimmt einen Server, der der Authentifizierungskooperation unterzogen werden sollte, auf der Basis der Server-Adressinformation innerhalb des elektronischen Zertifikates des Clients oder der Dienstdatenbank **46** (Dienst-DB), und (iii) leitet die Benutzerauthentifizierung und das Autorisierungsergebnis und die Einstellungsinformation zu dem Server weiter, der bestimmt wurde, der Authentifizierungskooperation unterzogen zu werden. Dann (3) hat eine Authentifizierungsprotokoll-Steuereinheit SRS52 eine Benutzerauthentifizierungsfunktion basierend auf dem elektronischen Zertifikat, eine Verifizierungsfunktion, um das elektronische Zertifikat zu validieren, und eine Autorisierungsfunktion des Dienstes.

<8. VPN-Gateway-Server 22>

[0058] Ein VPN-Gateway-Server **22** besteht aus zwei Steuereinheiten, die nachstehend beschrieben werden. Zuerst (1) empfängt eine Authentifizierungskooperations-Protokollsteuereinheit VPN **50** die Einzelanmeldungs-Authentifizierungsanforderung inkludierend das Authentifizierungs- und Autorisierungsergebnis und die Einstellungsinformation von jedem der Authentifizierungskooperationsnetze, wie etwa den Sicherheits-Roaming-Server **26**, und überträgt eine Einzelanmeldungs-Authentifizierungsantwort inkludierend das Authentifizierungsergebnis und die Einstellungsinformation in dem VPN-Gateway-Server **22** zu dem Sicherheits-Roaming-Server **26**. Als Nächstes (2) wird eine VPN-Steuereinheit **54** von der Authentifizierungsprotokoll-Steuereinheit VPN aufgerufen, führt Benutzerauthentifizierung durch, generiert und verteilt den VPN-Schlüssel, der die Authentifizierung und Verschlüsselung für das Paket des Benutzers durchführt, und führt Zugriffssteuerung und Verschlüsselungskommunikation mit dem VPN-Schlüssel wie in dem üblichen VPN-Gateway-Server **22** durch. In der Ausführungsform ist der VPN-Gateway-Server **22** der VPN-Gateway-Server **16**, der mit IPsec übereinstimmt, spezifiziert durch RFC2401 (Sicherheitsarchitektur für das Internetpro-

tokoll), was ein Standard einer Maßnahme ist.

<9. PKI-Server 18>

[0059] Ein PKI-Server **18** besteht aus einer Managementfunktion, die das PKI elektronische Zertifikat erteilt und außer Kraft setzt, und einer PKI-Datenbank **56** (PKI-DB), die das PKI elektronische Zertifikat sichert. Die Form des elektronischen Zertifikates ist erweitert, um Information zu speichern, die das Netz **102** anzeigt, welches in dem Fall von Authentifizierung des Benutzerendgerätes **4** kooperieren sollte, in der Form, spezifiziert durch RFC3280 von IETF. In der Ausführungsform speichert die Form eines elektronischen Zertifikates ein Identifikationsflag, das die IP-Adresse des VPN-Gateway-Servers **22** anzeigt, und die Dienstautorisierungsinformation, die Zugriffsfreigabebedingungen (Zeit, Wochentag etc.) anzeigt.

<10. Einzelanmeldungs-Protokoll 58>

[0060] Ein Einzelanmeldungs-Protokoll **58** ist ein Authentifizierungs- und Autorisierungskooperationsprotokoll, das zwischen dem Sicherheitsserver **12**, dem Sicherheits-Roaming-Server **26** und dem VPN-Gateway-Server **22** verwendet wird. Das Einzelanmeldungs-Protokoll **58** wird verwendet, um das Authentifizierungs- und Autorisierungsergebnis und die Sicherheitseinrichtung zu übertragen, wenn das Benutzerendgerät **4** des mobilen Benutzers den öffentlichen drahtlosen LAN-Dienst verwendet. In der Ausführungsform der Erfindung wird die Verwendung von SAML angenommen, was das typische Einzelanmeldungs-Protokoll **58** ist. Es wird ein Informationselement in der SAML-Antwortnachricht beschrieben, definiert durch das SAML-Protokoll bei Übertragung der Sicherheitseinstellungsinformation, die in der Ausführungsform der Erfindung benötigt wird. Das beschriebene Informationselement ist Information, die eine VPN-Einrichtung betrifft.

<11. TLS-Protokoll 60>

[0061] Ein TLS-Protokoll **60** ist ein Authentifizierungsprotokoll, das zwischen dem Benutzerendgerät **4**, dem drahtlosen LAN-Zugriffspunkt **6** und dem Sicherheitsserver **12** verwendet wird. Wenn das Benutzerendgerät **4** den öffentlichen drahtlosen LAN-Dienst verwendet, überträgt das TLS-Protokoll **60** zu dem Benutzerendgerät **4** (i) das Serverzertifikat für das Benutzerendgerät **4**, das den Sicherheitsserver **12** oder den drahtlosen LAN-Zugriffspunkt **6** authentifiziert, und (ii) die automatische Einstellungsinformation (Einstellungsdaten). In der Ausführungsform werden (i) ein EAP-TLS-Protokoll, ein EAP-TTLS-Protokoll und ein PEAP-Protokoll, die zwischen dem Benutzerendgerät **4** und dem drahtlosen LAN-Zugriffspunkt **6** durch IEEE 802.1x unterstützt werden, angenommen, und (ii) wird ein RADIUS-Protokoll (Authentifizierungsprotokoll **62**), das das EAP zwischen dem drahtlosen LAN-Zugriffspunkt **6** und dem Sicherheitsserver **12** inkludiert, angenommen. Die Übertragung der automatischen Einstellungsinformation, die in der Ausführungsform der Erfindung erforderlich ist, wird durch Verwenden der TLS-Erweiterung, die durch RFC3546 von IETF, die eine Standardisierungsorganisation ist, spezifiziert ist, und Trennen und Beschreiben des Informationselementes für eine neue automatische Einrichtung in der Erweiterungsnachricht für jedes von Netzen, die kooperieren, realisiert. Das beschriebene Informationselement ist die Information (Einstellungsdaten) bezogen auf eine LAN-Einstellung der IP-Adresse etc., und die Sicherheitseinrichtung, wie etwa ein Chiffrierschlüssel, der durch IPsec angewendet wird.

<Fernzugriffsdienstmodell>

[0062] Fig. 1 zeigt ein Fernzugriffsdienstmodell gemäß der Ausführungsform. Dies ist ein Dienstmodell, durch das ein mobiler Benutzer, der zu einem Unternehmen gehört, unter Verwendung einer öffentlichen Schlüsselinfrastruktur (PKI) sicher auf ein Unternehmensnetz von einer Vielzahl von externen öffentlichen drahtlosen LAN-Diensten zugreift. Damit ein ISP, der eine Vielzahl von öffentlichen drahtlosen LAN-Diensten managt, zum RSP, was ein Roaming-Anbieter für Authentifizierungs-Roaming ist, angeschlossen werden kann und eine gegenseitige Identität garantieren kann, erteilt als eine Voraussetzung der ISP gegenseitig das Kreuzzertifikat, das durch PKI verwendet wird. Damit das Unternehmen wiederum eine Vielzahl von öffentlichen drahtlosen LAN-Diensten über RSP verwenden kann, ist das Unternehmen zu RSP angeschlossen und erteilt gegenseitig das Kreuzzertifikat. Das Unternehmen muss zu dem ISP nicht im voraus angeschlossen sein. Das Modell einer derartigen PKI wird allgemein "Brückenmodell" genannt. Die Dienstsequenz gemäß der Erfindung wird in **Fig.** 2 gezeigt.

[0063] Hierin nachstehend werden die Details der Ausführungsform mit Bezug auf Fig. 1 beschrieben.

[0064] Das Unternehmen hat eine Authentifizierungsbasis durch PKI. Der PKI-Server **18** hat das elektronische Zertifikat des Clients zum Garantieren einer Identität zu den Benutzern, die Angestellte sind, und verschiedenen Arten von Servern ((1) von Fig. 1) erteilt. Außerdem wird ein Unternehmensroutenzertifikat zum Verifizieren der Gültigkeit des elektronischen Zertifikates in dem Unternehmen in dem Benutzerendgerät **4** als eine Voraussetzung installiert. Das Unternehmen hat im voraus das elektronische Zertifikat für Fernzugriffsauthentifizierung zu dem Benutzer erteilt, der externe Aktivitäten durchführt, wie etwa ein Geschäft. Dienstautorisierungsinformation, wie etwa Fernzugriffsdienstinformation (ein Dienstserveridentifikator, Zugriffsfreigabedatum und Zeit),

und SSID des öffentlichen drahtlosen LAN-Dienstes, der gebunden wurde, sind in dem elektronischen Zertifikat ausgefüllt. Da das elektronische Zertifikat durch einen Aussteller unterzeichnet wurde, und die Änderung unmöglich ist, kann der mobile Benutzer im Gegensatz zu der Absicht des Unternehmens daran gehindert werden, einen Fernzugriffsdienst zu verwenden. Außerdem wird das elektronische Zertifikat direkt in dem Benutzerendgerät **4** des mobilen Benutzers gespeichert, oder wird in dem Benutzerendgerät **4** durch eine externe Vorrichtung, wie etwa eine IC-Karte gespeichert.

[0065] In diesem Fall wird SSID des öffentlichen drahtlosen LAN-Dienstes innerhalb des elektronischen Zertifikates durch die Automatikeinstellungs-Protokollsteuereinheit EE30 extrahiert und wird automatisch zu der LAN-Steuereinheit EE32, die Zugriff zu dem drahtlosen LAN steuert, als eine Vorgabe eingestellt. Deshalb muss sich der Benutzer der vorherigen Einrichtung nicht bewusst sein.

<Verarbeitung von EE0>

[0066] Der Verarbeitungsfluss des Benutzerendgerätes **4** wird in Fig. 17 (EE0) gezeigt. SSID (drahtlose LAN-Einstellung) des Clientzertifikates wird erfasst (S60), und es wird beurteilt, ob die drahtlose LAN-Einstellung eines Betriebssystems (OS) des Benutzerendgerätes **4** SSID enthält, die von dem Clientzertifikat erfasst wurde (S61). Wenn die drahtlose LAN-Einstellung SSID enthält, wird die Einstellungsbearbeitung von SSID abgeschlossen. Wenn die drahtlose LAN-Einstellung SSID nicht enthält, wird SSID zu der drahtlosen LAN-Einstellung vom OS des Benutzerendgerätes **4** eingestellt (S62, (2) von Fig. 1).

<Verarbeitung von EE1>

[0067] Der Verarbeitungsfluss des Benutzerendgerätes **4** wird in Fig. 18 (EE1) gezeigt. Das Benutzerendgerät **4** erfasst SSID in dem Funkfeuer, welches der drahtlose LAN-Zugriffspunkt **6** sendet (S63). Es wird beurteilt, ob eine drahtlose LAN-Einstellung vom OS des Benutzerendgerätes **4** die erfasste SSID enthält (S64). Wenn die drahtlose LAN-Einstellung die erfasste SSID enthält, beginnt das Benutzerendgerät **4** eine Netzzugriffsauthentifizierungs- (EAP-Authentifizierung) Prozedur (S66, (3) bis (5) von Fig. 1). Diese Verarbeitung ist in Mehrzweck- OS's enthalten, wie etwa WindowsXP. Wenn sich die erfasste SSID von einer drahtlosen LAN-Einstellung des Benutzerendgerätes **4** unterscheidet, stellt das Benutzerendgerät **4** SSID eines Funkfeuers als eine drahtlose LAN-Einstellung vom OS eines Clientendgerätes ein (S65).

[0068] Wenn das Benutzerendgerät **4** TLS_start empfängt, wird als Nächstes der Automatikeinstellungs-Roaming-Dienst des Clientzertifikates erfasst (S67), "7" wird zu dem Erweiterungstyp des erweiterten Teils von TLS eingestellt (Client-Hallo) (S68, Fig. 4), und es wird eine TLS- (Client-Hallo) Nachricht zu dem externen Netz **2** übertragen (in der Ausführungsform der Sicherheitsserver **12** durch den drahtlosen LAN-Zugriffspunkt 6) (S69, (3) bis (5) in Fig. 1).

<Verarbeitung von SS1>

[0069] Der Verarbeitungsfluss des Sicherheitsservers **12** wird in Fig. 11 (SS1) gezeigt. Als Nächstes empfängt der Sicherheitsserver **12** eine TLS- (Client-Hallo) Nachricht von dem Benutzerendgerät **4** (S1, (5) von Fig. 1). Da das elektronische Zertifikat, das durch den Sicherheitsserver **12** empfangen wurde, nicht ein elektronisches Zertifikat ist, das durch den ISP erteilt wird, wird die Gültigkeit des elektronischen Zertifikates durch Verwenden des Zertifikatszertifizierungsprotokolls **64** (SCVP) und Abfragen der Authentifizierungs-Protokollsteuereinheit SRS52 von RSP über Gültigkeit (S2) verifiziert. Als Nächstes erfasst der Sicherheitsserver **12** eine Automatikeinstellungs-Roaming-Dienstanforderung (Erweiterungstyp = 7) von dem erweiterten Teil einer TLS- (Client-Hallo) Nachricht (S3), und beurteilt, ob es eine Endgerät-Automatikeinstellungs-Roaming-Funktion gibt oder nicht (S4). Wenn es eine Endgerät-Automatikeinstellungs-Roaming-Funktion (Erweiterungstyp = 7) gibt, werden die Serverzertifikat-Verifizierungsdaten in dem Bereich gespeichert, der in der Server-Hallo-Nachricht in dem TLS-Protokoll **60** erweitert ist, und die TLS(Server-Hallo) Nachricht wird zu dem Benutzerendgerät **4** durch Verwenden der Schutzfunktion von TLS (S6, S7) sicher zurück gesendet. Wenn die automatische Einrichtung der Seite von Netzwerk **102** nicht ausgeführt werden kann (wenn die Endgerät-Automatikeinrichtungs-Roaming-Funktion ausgeschaltet ist), wird die Verarbeitung auf der Basis einer Authentifizierungsprozedur NG durchgeführt (S5).

[0070] Die Netzzugriffsauthentifizierung wird auf der Basis von Standard IEEE 802.1x und der TLS-Authentifizierungsprozedur durchgeführt. Der drahtlose LAN-Zugriffspunkt **6** greift zeitweilig Zugriffe mit Ausnahme der Authentifizierungsanforderung von dem Benutzerendgerät **4** auf der Basis der TLS-Authentifizierungsprozedur ab. Die LAN-Steuereinheit EE32 des Benutzerendgerätes **4** fordert die Serverauthentifizierung von dem drahtlosen LAN-Zugriffspunkt **6** an, um den verbundenen drahtlosen LAN-Zugriffspunkt **6** zu validieren. Unter den gegenwärtigen Umständen ersetzt der drahtlose LAN-Zugriffspunkt **6** die Anforderung von einem Benutzer durch das RADIUS-Protokoll und transferiert das ersetzte RADIUS-Protokoll zu dem Sicherheitsserver **12** mit der Vertrauensbeziehung durch einen gemeinsam genutzten Schlüssel oder dergleichen im voraus. Die

Authentifizierungsprotokoll-Steuereinheit SS36 des Sicherheitsservers **12** überträgt das Serverzertifikat zu dem Benutzerendgerät **4** gemäß der Serverauthentifizierungsanforderung.

[0071] Um das Serverzertifikat zu verifizieren, ist es gewöhnlich notwendig, dass das selbst unterzeichnete Zertifikat (Root-Zertifikat) einer Erteilungsbehörde (CA, issue office), die das Serverzertifikat erteilt hat, in dem Benutzerendgerät **4** gespeichert wird. Da das Routenzertifikat einer typischen elektronischen Zertifikatserteilungsorganisation, wie etwa VerSign, auf das OS des Benutzerendgerätes **4** oder dergleichen im voraus eingestellt ist, kann Verifizierung durch das Benutzerendgerät **4** durchgeführt werden. In der Ausführungsform der Erfindung unterstützt die Authentifizierungsprotokoll-Steuereinheit SS36 des Sicherheitsservers **12**, gezeigt in Fig. 3, die TLS-Erweiterung, die durch RFC3546 von IETF, welches eine Standardisierungsorganisation ist, spezifiziert wird, verifiziert ein Serverzertifikat auf der Seite des externen Netzes **2**, inkludiert das Verifizierungsergebnis in der TLS-Erweiterung und überträgt die Nachricht zu dem Benutzerendgerät **4**. Das Verifizierungsergebnis wird durch die Authentifizierungsprotokoll-Steuereinheit EE28 bestätigt, nachdem die LAN-Steuereinheit EE32 der Seite des Benutzerendgerätes **4** die Nachricht empfangen hat, wobei dadurch die Serverauthentifizierung ermöglicht wird. Um die Clientauthentifizierung durchzuführen, der nach Authentifizierung und Autorisierung zum ISP anfragt, der den drahtlosen LAN-Dienst anbietet, überträgt danach die Authentifizierungsprotokoll-Steuereinheit EE28 des Benutzerendgerätes **4** das Clientzertifikat, das von dem Unternehmens-PKI-Server erteilt wurde, zum ISP ((4) von Fig. 1).

<Verarbeitung von SS2>

[0072] Der Verarbeitungsfluss des Sicherheitsservers **12** wird in Fig. 12 (SS2) gezeigt. Der Sicherheitsserver **12**, der das Clientzertifikat empfangen hat, authentifiziert den Benutzer durch Verifizieren des Clientzertifikates durch die Authentifizierungsprotokoll-Steuereinheit SS36, und genehmigt den Dienst (S8, (5) von Fig. 1). Da das elektronische Zertifikat, das von dem Benutzerendgerät **4** empfangen wird, nicht ein elektronisches Zertifikat ist, das durch einen ISP erteilt wird, wird seine Gültigkeit durch Abfragen des PKI-Servers **18** eines Unternehmens über die Gültigkeit durch die Authentifizierungsprotokoll-Steuereinheit SRS52 vom RSP mit der Brücken-CA-Funktion von PKI, spezifiziert nach RFC3280 von IETF, was eine Standardorganisation ist, durch Verwenden des Zertifikatsverifizierungsprotokolls **64** (SCVP) wie ein Serverzertifikat (S9) verifiziert. Die Authentifizierungsprotokoll-Steuereinheit SRS52 vom RSP arbeitet als ein Weitergabeserver oder ein Ersatzserver zum Verifizieren des Zertifikates. Wenn RSP die Verfallsinformation über das elektronische Zertifikat unterhält, das durch den PKI-Server **18** des Unternehmens gemanagt wird, wird die Verifizierung des Zertifikates von dem Sicherheitsserver **12** nur durch Befragen von RSP abgeschlossen. Nach der Verifizierung ist die Netzzugriffsauthentifizierung auf der Seite des ISP abgeschlossen.

[0073] Die Authentifizierungsprotokoll-Steuereinheit SS36 des Sicherheitsservers **12** gibt das Authentifizierungs- und Autorisierungsergebnis zu der Automatikeinstellungs-Protokollsteuereinheit SS38 aus (S10). Die Authentifizierungsprotokoll-Steuereinheit SS36 führt den LAN-Einstellungsmanagementteil SS von der Automatikeinstellungs-Protokollsteuereinheit SS38, um eine LAN-Einstellung zu erhalten, die IP-Adressen des Benutzerendgerätes **4**, DNS, des Gateways usw. von dem DHCP-Server **8** etc. enthält, bevor das Authentifizierungsergebnis zu dem Benutzer zurück gesendet wird (S11). Dann beurteilt die Automatikeinstellungs-Protokollsteuereinheit SS38, ob es die Automatikeinstellungs-Roaming-Dienstanforderung (Erweiterungstyp = 7) gibt, mit der Tatsache, dass das Benutzerendgerät **4** einen Sicherheits-Roaming-Dienst anfordert, wobei die Tatsache der TLS-Erweiterung hinzugefügt wird, oder nicht (S12). Die Automatikeinstellungs-Protokollsteuereinheit SS38 befragt die Authentifizierungskooperations-Protokollsteuereinheit SS42, um die Einstellungsinformation über das Netz **102**, welches kooperiert, oder über den Dienst zu sammeln, durch Verwenden des Authentifizierungskooperationsprotokolls. Wenn die Sicherheitsdienst-/Sicherheits-Roaming-Dienstanforderung nicht ausgeführt wurde (d.h. Erweiterungstyp ist nicht "6" oder "7"), wird die LAN-Einstellungsinformation in einem Bereich gespeichert, der innerhalb der Serverbeendigungsnachricht in dem TLS-Protokoll **60** erweitert ist, und dann zu dem Benutzer durch eine Verwendung einer Schutzfunktion von TLS sicher zurück gesendet (von S13 bis S15).

[0074] Die Authentifizierungskooperations-Protokollsteuereinheit SS42 des Sicherheitsservers **12** beurteilt das Netz **102**, welches kooperiert, oder den Dienst mit Bezug auf die Dienstautorisierungsinformation, die in dem elektronischen Zertifikat des Clients beschrieben ist. Um Einstellungsinformation über sie zu sammeln, wird die Sicherheits-Roaming-Dienstanforderung inkludierend das Authentifizierungs- und Autorisierungsergebnis des Benutzerendgerätes **4** und die LAN-Einstellung, die Einstellungsinformation über einen ISP ist, dem Authentifizierungskooperationsserver in Dienstautorisierungsinformation gegeben ((8) von Fig. 1). In diesem Beispiel wird eine Roaming-Dienstanforderung zu dem Sicherheits-Roaming-Server **26** vom RSP gegeben, der diese Roaming-Verarbeitungen gemeinsam gemäß der Automatikeinstellungs-Dienstanforderung (Erweiterungstyp = 7, Fig. 4), gezeigt in dem TLS-Er-

weiterungsteil, durchführt. Speziell wird unter Verwendung des SAML-Protokolls, welches eine Standard-Einzelanmeldungs-Nachricht ist, Roaming zu einer Autorisierungsentscheidungsabfrage in der SAML-Anforderungsnachricht beschrieben, um eine Dienstanforderung vorzusehen (S16, **Fig.** 6). (i) die Benutzerauthentifizierung und Autorisierungsinformation, alle TLS-Authentifizierungsnachrichten und (ii) die LAN-Einstellungsinformation werden einer Aussage hinzugefügt, die das Netzzugriffsauthentifizierungsergebnis in ISP anzeigt, und diese Stücke von Information werden übertragen (von S17 bis S19). Außerdem enthält die SAML-Nachricht das elektronische Zertifikat des Clients. Die SAML-Nachricht ist durch die elektronische Signatur vom ISP und Verschlüsselung geschützt.

<Verarbeitung von SRS1>

[0075] Der Verarbeitungsfluss des Sicherheits-Roaming-Servers **26** wird in Fig. 14 (SRS1) gezeigt. Der Sicherheits-Roaming-Server **26** vom RSP empfängt die SAML-Nachricht, die eine Sicherheits-Roaming-Dienstanforderung ist, in der Authentifizierungskooperations-Protokollsteuereinheit SRS48, und bestätigt die Gültigkeit der Nachricht durch elektronische Signatur (S30). In der Authentifizierungskooperations-Protokollsteuereinheit SRS48 wird eine Kooperation des spezifizierten Netzes **102** und eines Dienstes mit Bezug auf die Dienstautorisierungsinformation gestartet, die durch das elektronische Zertifikat des Clients beschrieben wird, das in der SAML-Nachricht enthalten ist (S31, (9) und (10) von Fig. 1). Speziell wird, wie in **Fig.** 7 gezeigt, eine Durchführung von VPN, um auf das Unternehmensnetz zuzugreifen, in dem elektronischen Zertifikat des Clients beschrieben. Die Authentifizierungskooperations-Protokollsteuereinheit SRS48 (i) extrahiert die IP-Adresse des VPN-Gateway-Servers **22** des gemanagten Unternehmens im voraus in der Dienstdatenbank **46** im RSP von dem VPN-Serverflag der Information in dem elektronischen Zertifikat, und (ii) überträgt die SAML-Nachricht inkludierend das Netzzugriffsauthentifizierungs- und Autorisierungsergebnis und die LAN-Einstellungsinformation in dem Benutzerendgerät **4** zu dem VPN-Gateway-Server **22**, und (iii) erteilt eine VPN-Verbindungs- (Schlüsselaustausch) Anforderung (S32 bis S34, (10) von Fig. 1). Fig. 21 ist eine Tabelle, die die IP-Adresse des VPN-Gateway-Servers **22** des Unternehmens in der Dienstdatenbank **46** zeigt. Die SAML-Nachricht wird durch die elektronische Signatur vom RSP und Verschlüsselung geschützt. Obwohl das Netz **102**, welches kooperiert, nur eines der VPN-Gateway-Server **22** des Unternehmens in der Ausführungsform ist, dient in dem Fall, wo eine Vielzahl von VPN-Gateway-Servern vorgesehen ist, der Sicherheits-Roaming-Server **26** als ein zentraler Server, und kooperiert einer nach dem anderen unter Verwendung eines Authentifizierungskooperationsprotokolls, wobei dadurch Kooperation mit einer Vielzahl von Servern erlaubt wird. In dieser Situation wird die Reihenfolge einer Kooperation wichtig und wird auch in dem elektronischen Zertifikat des Clients beschrieben, und die Richtungen, denen gefolgt werden kann. Wenn der Server ein Server (Authentifizierungskooperationsvorrichtung) mit der Authentifizierungskooperations-Protokollsteuereinheit ist, ist auch Kooperation in einer Weitergabeweise möglich.

<Verarbeitung von VPN>

[0076] Der Verarbeitungsfluss des VPN-Gateway-Servers **22** wird in VPN von Fig. 16 gezeigt. Der VPN-Gateway-Server **22** des Unternehmens empfängt die SAML-Nachricht, die die VPN-Verbindungsanforderung ist, gezeigt in **Fig.** 7, in der Authentifizierungskooperations-Protokollsteuereinheit VPN **50**, und bestätigt die Gültigkeit einer Nachricht durch eine elektronische Signatur (S50). In der Authentifizierungskooperations-Protokollsteuereinheit VPN **50** wird eine Benutzerauthentifizierung zuerst mit Bezug auf das Ergebnis (Aussage) von Netzzugriffsauthentifizierung und Autorisierung des Benutzers als Reaktion auf die VPN-Verbindungsanforderung, gezeigt durch die SAML-Nachricht, durchgeführt (S51, (11) von Fig. 1). Als Nächstes werden die Schlüsselgenerierung und eine Einrichtung für VPN-Kommunikation entsprechend dem Benutzerendgerät **4** zu der VPN-Steuereinheit **54** mit Bezug auf die LAN-Einstellungs- (IP-Adresse) Information in dem Benutzerendgerät **4**, enthalten in der Aussage, angefordert (S52). Die VPN-Steuereinheit **54** führt eine sichere Kommunikationseinrichtung von IPsec etc. durch, und überträgt die Einrichtung der Sicherheit (IP-Adresse des VPN-Servers, den Chiffrierschlüssel und die interne IP-Adresse des VPN-Clients etc.), die zu dem Benutzerendgerät **4** übertragen wird, was eine VPN-Client-Seite ist, zu der Authentifizierungskooperations-Protokollsteuereinheit VPN **50** (S53). Die Authentifizierungskooperations-Protokollsteuereinheit VPN **50** überträgt die SAML-Antwortnachricht, die die Sicherheitseinrichtung und das Ergebnis der Benutzerauthentifizierung und Autorisierung durch den VPN-Gateway-Server **22** in der SAML-Antwortnachricht inkludiert, zu dem Sicherheits-Roaming-Server **26** vom RSP (S54 bis S57, **Fig.** 8 und (13) von Fig. 1). In dieser Situation wird Sicherheit durch Verschlüsseln der Sicherheitseinrichtung innerhalb der Authentifizierungs- und Autorisierungsergebnis-(Aussage) Information mit einem öffentlichen Schlüssel des Benutzers geschützt (S55, (12) von Fig. 1). Außerdem wird die SAML-Nachricht durch die elektronische Signatur des Unternehmens und Verschlüsselung geschützt. Eine Verarbeitungspriorität der Information, die zu dem Benutzerendgerät **4** einzustellen ist, wird gemäß der Verarbeitungsprioritäts-Einstellungsrichtlinie bestimmt, die im voraus klassifiziert wurde. Der VPN-Einrichtung, die von dem VPN-Gateway-Server **22** erhalten wird, wird

eine Priorität "A" gegeben, sodass Einstellungsverarbeitung zuerst ausgeführt werden kann. Wenn es Einstellungsinformation über eine Vielzahl von Diensten gibt, wird die Einstellungsverarbeitungspriorität von jeder Information untersucht und es wird eine Verarbeitungsrangfolge zu der Information der gleichen Priorität auf der Basis einer vorbestimmten Verarbeitungsrangfolgen-Einstellungsrichtlinie bestimmt. Die Werte einer Verarbeitungspriorität und einer Verarbeitungsrangfolge werden in der SAML-Antwortnachricht beschrieben.

<Verarbeitung von SRS2>

[0077] Der Verarbeitungsfluss des Sicherheits-Roaming-Servers **26** wird in Fig. 15 (SRS2) gezeigt. Der Sicherheits-Roaming-Server **26** vom RSP empfängt die SAML-Antwortnachricht in der Authentifizierungskooperations-Protokollsteuereinheit SRS48, und bestätigt die Gültigkeit einer Nachricht durch elektronische Signatur (S35). In der Authentifizierungskooperations-Protokollsteuereinheit SRS48 wird als eine Antwort der Sicherheits-Roaming-Dienstanforderung vom ISP die Information in der SAML-Antwortnachricht erfolgreich sein und wird zu dem Sicherheitsserver **12** vom ISP übertragen (S36 bis S40, **Fig.** 9 und (14) von Fig. 1). Die SAML-Nachricht wird durch die elektronische Signatur, durchgeführt durch RSP, und die Verschlüsselung geschützt. Wenn der Server mit einer Vielzahl von Netzen **102** kooperiert und es eine Vielzahl von Einstellungsinformation gibt, wird das Ergebnis (Aussage) der Authentifizierung und Autorisierung inkludierend jede Einstellungsinformation in einer SAML-Nachricht eines nach dem anderen angeordnet, und es wird eine Antwort durchgeführt.

<Verarbeitung von SS3>

[0078] Der Verarbeitungsfluss des Sicherheitsservers **12** wird in Fig. 13 (SS3) gezeigt. Der Sicherheitsserver **12** des ISP empfängt die SAML-Antwortnachricht in der Authentifizierungskooperations-Protokollsteuereinheit SS42, und bestätigt die Gültigkeit der Nachricht durch eine elektronische Signatur (S20). In der Authentifizierungskooperations-Protokollsteuereinheit SS42 werden die Sicherheitseinrichtung und die LAN-Einstellung, die empfangen und verschlüsselt wurden, zu der Automatikeinstellungs-Protokollsteuereinheit SS38 gesendet, um diese Einrichtungen zu dem Benutzerendgerät **4** zu übertragen. Die Automatikeinstellungs-Protokollsteuereinheit SS38 extrahiert die Einstellungsinformation für jede Ressource innerhalb von SAML (Antwort) (S24). Dann speichert die Automatikeinstellungs-Protokollsteuereinheit SS38 die Einstellungsinformation sequenziell in dem erweiterten Bereich in der Serverbeendigungsnachricht in dem TLS-Protokoll **60** für jedes Netz **102** oder Dienst, und antwortet zu dem Benutzerendgerät **4** sicher durch die Authentifizierungsprotokollsteuereinheit SS36 durch Verwenden der Schutzfunktion von TLS als eine Antwort der Netzzugriffsauthentifizierung (S24 bis S26, (15) von Fig. 1). Wenn die Antwort des Sicherheitsdienstes NG in der SAML-Antwortnachricht enthalten ist, empfängt der Benutzer eine Antwort als eine Benutzerauthentifizierung NG auf der Basis der TLS-Prozedur (S22, S23). Außerdem wird in dem Fall von NG eine Anforderung, die die IP-Adresse des erlangten Benutzerendgerätes **4** öffnet, von der Automatikeinstellungs-Protokollsteuereinheit SS38 zu der LAN-Einstellungssteuereinheit SS40 gegeben. Die TLS-Nachricht wird in dem RADIUS-Protokoll gespeichert und zu dem drahtlosen LAN-Zugriffspunkt **6** übertragen, und die Kommunikation, die auf der Basis des Authentifizierungsergebnisses des Benutzers unterbrochen wurde, wird in dem drahtlosen LAN-Zugriffspunkt **6** geöffnet. Außerdem wird Information zu dem Benutzerendgerät **4** durch Verwenden einer Einheit übertragen, die durch IEEE 802.1x spezifiziert ist. Eine Verarbeitungspriorität der LAN-Einstellungsinformation, die zu dem Benutzerendgerät **4** durch den ISP einzustellen ist, wird gemäß der Verarbeitungsprioritäts-Einstellungsrichtlinie bestimmt, die im voraus klassifiziert wurde. In dieser Situation wird, wenn die Einstellungsverarbeitungspriorität von jeder Information untersucht wird und die Information der gleichen Priorität existiert, eine Verarbeitungsrangfolge auf der Basis der vorbestimmten Verarbeitungsrangfolgen-Einstellungsrichtlinie bestimmt. Außerdem folgt die Einstellungsinformation, die durch SAML empfangen wird, der Verarbeitungspriorität und Verarbeitungsrangfolge, die in der empfangenen SAML-Nachricht beschrieben werden. Die Werte von einer Verarbeitungspriorität und der Verarbeitungsrangfolge werden in der Prioritätseinrichtung von jedem TLS-Erweiterungsbereich beschrieben.

<Verarbeitung von EE2>

[0079] Der Verarbeitungsfluss des Benutzerendgerätes **4** wird in Fig. 19 (EE2) gezeigt. Das Benutzerendgerät **4** empfängt die TLS-Nachricht durch die Authentifizierungsprotokollsteuereinheit EE28, und führt eine Netzzugriffsauthentifizierungs- (EAP-Authentifizierung) Prozedur bis zum Abschluss durch (S71). Die Authentifizierungsprotokollsteuereinheit EE28 erfasst den Automatikeinstellungs-Roaming-Dienst (Erweiterungstyp = 7) von einem TLS- (Server fertig) Erweiterungsteil (S72). Als Nächstes überträgt die Authentifizierungsprotokollsteuereinheit EE28 die Information in einer Sicherheitseinrichtung, inkludiert in einer TLS-Erweiterung, und einer LAN-Einstellung zu der Automatikeinstellungs-Protokollsteuereinheit EE30. Die Automatikeinstellungs-Protokollsteuereinheit EE30 verarbeitet die Einstellungsinformation, die für jedes Netz angeboten wird, gemäß der Priorität, die durch das elektronische Zertifikat des Clients beschrieben wird (S73 bis

S75). In diesem Beispiel wird Priorität der Einstellungsverarbeitung von dem Unternehmensnetz gegeben, eine verschlüsselte Sicherheitseinrichtung wird mit einem privaten Schlüssel des Benutzers entschlüsselt und zu der Sicherheitssteuereinheit EE34 übertragen, um die sichere Kommunikationseinrichtung von IPsec automatisch durchzuführen etc. (S81). Als Nächstes wird die Einstellungsverarbeitung vom ISP durchgeführt, die LAN-Einstellung der IP-Adresse des Benutzerendgerätes **4** etc. wird zu der LAN-Steuereinheit übertragen, und die Kommunikationseinrichtung wird automatisch durchgeführt (S81).

[0080] Mit der Prozedur wird die Einrichtung zum sicheren Kommunizieren in dem Unternehmensnetz von dem Benutzerendgerät **4** abgeschlossen, und sichere Kommunikation kann unmittelbar nach der Authentifizierungsantwort vom Netzzugriff durchgeführt werden.

[0081] Die Beispiele zeigen das Verfahren zum Verteilen der Sicherheitseinrichtung zu dem Benutzerendgerät **4** von dem VPN-Gateway-Server **22** des Unternehmens. Eine Verteilung der VPN-Schlüsselinformation durch das Netz **102** hat jedoch ein Risiko eines Verlustes, und als seine Gegenmaßnahme ist eine hohe Verarbeitungslast in dem Server in der Verschlüsselungs-/Entschlüsselungsverarbeitung erforderlich.

<Generierung des VPN-Schlüssels unter Verwendung von unbestimmter Information>

[0082] Eine Schlüsselgenerierungssequenz wird in Fig. 19 gezeigt. An Stelle einer Verteilung eines VPN-Schlüssels wird unbestimmte Information, wie etwa Zufallszahleninformation und Zeit, die zur Zeit der Netzzugriffsauthentifizierung generiert wird, zu dem Unternehmensnetz in der Authentifizierungskooperationsprozedur übertragen, und es kann das Schlüsselgenerierungsverfahren verwendet werden, welches den gleichen VPN-Schlüssel generiert. Der gleiche VPN-Schlüssel kann durch den Server des Unternehmensnetzes bzw. das Benutzerendgerät **4** durch Kombinieren der unbestimmten Information, des voreingestellten Unternehmensnetzes und eines gemeinsam genutzten Schlüssels des Benutzers generiert werden (das Schlüsselgenerierungsverfahren). Speziell ist unbestimmte Information in der Client-Hallo-Nachricht und Server-Hallo-Nachricht von TLS unter den Nachrichten der TLS-Authentifizierungsprozedur inkludiert, die eine Netzzugriffsauthentifizierungsprozedur in ISP ist. Diese Nachrichten sind in der Nachricht inkludiert, die den VPN-Server des Unternehmens über das Authentifizierungs- und Autorisierungsergebnis in ISP durch das Authentifizierungskooperationsprotokoll benachrichtigt, um in dem Unternehmensnetz verteilt zu werden. Der Server des Unternehmensnetzes und das Benutzerendgerät können jeweils den gleichen VPN-Schlüssel durch eine Hash-Funktion, die unbestimmte Information und den gemeinsam genutzten Schlüssel, der in dem elektronischen Zertifikat verschlüsselt wurde, generieren.

[0083] Eine TLS-Nachricht (Client-Hallo, Server-Hallo), inkludierend die unbestimmte Information, ist auch die Information zum Verifizieren eines Authentifizierungs- und Autorisierungsergebnisses, und die TLS-Nachricht ist dominante Information, wenn ein Unternehmen das Authentifizierungsergebnis in ISP zu verifizieren wünscht. In diesem Beispiel kann, obwohl ein Teil einer TLS-Nachricht als die unbestimmte Information verteilt wird, wenn eine Verifizierung hohen Grades benötigt wird, die Nachricht von allen TLS-Authentifizierungssequenzen der Netzzugriffsauthentifizierung in ISP als die unbestimmte Information inkludiert sein.

[0084] Obwohl die IP-Adresse des VPN-Servers, der Chiffrierschlüssel und die interne IP-Adresse des VPN-Clients zu dem Benutzerendgerät **4** als eine Sicherheitseinrichtung verteilt werden, ist es in dem oben erwähnten VPN-Dienst möglich, den VPN-Dienst, der sicherer und in der Server- oder Benutzerendgerät-Verarbeitungslast kleiner ist, durch Inkludieren der VPN-Schlüsselgenerierungseinheit anzubieten.

[0085] In der Ausführungsform der Erfindung kann in dem Netzverbindungsdienst von dem öffentlichen drahtlosen LAN eine automatische Einrichtung eines Dienstes, der höher als die IP-Schicht ist, die durch die Vielzahl von Netzen **102** vorgesehen wird, zur Zeit vom Abschluss der Netzauthentifizierung einer Verknüpfungsschicht, die niedriger als die IP-Schicht ist, durchgeführt werden.

[0086] Gemäß der Erfindung ist es möglich, die jeweiligen Stücke von Einstellungsinformation gemeinsam zu dem Benutzerendgerät **4** in der geschützten Authentifizierungsprozedur zu verteilen, die durchgeführt wird, wenn das Benutzerendgerät **4** auf das Netz **102** zugreift, und die Einrichtung kann zwischen der Vielzahl von Netzen **102**, die Dienste vorsehen, die konventionell unabhängig angeboten wurden, effizient und sicher durchgeführt werden. Da das Management von jeder Einstellungsinformation in einer Verteilung durch jeden Server durchgeführt wird, wird ein System realisiert, das im Vergleich zu dem Fall, wo jede Einrichtung intensiv gemanagt wird, eine hohe Skalierbarkeit aufweist. Außerdem können die Gültigkeit, die durch elektronische Signatur etc. garantiert wird, und die Maßnahme gegen einen Informationsverlust durch Verschlüsselung in den Nachrichten zwischen dem Server von jedem Netz **102** und einem Server, und zwischen dem Server und einen Client durchgeführt werden. Deshalb kann in der Ausführungsform hohe Sicherheit angeboten wer-

den. Mit dem sicheren und effizienten System, das automatisch das Benutzerendgerät **4** einrichtet, können verschiedene Einstellungsdaten zuverlässig zu dem Benutzerendgerät **4** eingestellt werden, bevor der Benutzer Datenkommunikationen startet. Des weiteren wird nicht nur der Komfort des Benutzers gesteigert, sondern die Seite des Netzes **102** kann auch den Sicherheitsschaden verhindern, der dem Einstellungsfehler in dem Benutzerendgerät **4** zuzuschreiben ist.

[0087] Eine Vorrichtung, ein Verfahren, ein Programm und ein Medium für Einstellungsinformationsverteilung, eine Vorrichtung, ein Verfahren, ein Programm und ein Medium für Authentifizierungseinstellungstransfer, und ein Einstellungsinformations-Empfangsprogramm in Übereinstimmung mit der Erfindung kooperieren verschiedene Dienstanforderungen und die Verteilung einer Einrichtung, die unabhängig in einer Vielzahl von Domänen durchgeführt werden, und sie verbessern einen Komfort des Benutzers und garantieren die Korrektheit von Verteilungsinformation in jeder Domäne.

Patentansprüche

1. Einstellungsinformations-Verteilungsvorrichtung, die zu einem ersten Netz gehört, umfassend:
eine Authentifizierungseinheit, die eine Authentifizierungsanfrage von einem Benutzerendgerät empfängt und authentifiziert, das eine Zugriffsauthentifizierung anfordert durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen dem Benutzerendgerät und dem ersten Netz;
eine Übertragungseinheit, die eine Authentifizierungskooperationsanforderung, die Einstellungsdaten anfordert, die zu dem Benutzerendgerät einzustellen sind, zu einem anderen Netz überträgt durch Verwenden der Netzzugriffsauthentifizierungsprozedur und einer Authentifizierungskooperationsprozedur zwischen einer Vielzahl von Netzen; und
eine Verteilungseinheit, die eine erste Antwortnachricht, der Einstellungsdaten hinzugefügt sind, zu dem Benutzerendgerät überträgt durch Erzeugen der ersten Antwortnachricht entsprechend der Authentifizierungsanforderung durch Hinzufügen der Einstellungsdaten inkludiert in einer zweiten Antwortnachricht entsprechend der Authentifizierungskooperationsanforderung.

2. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 1, ferner umfassend eine Empfangseinheit, die die zweite Antwortnachricht zu der Authentifizierungskooperationsanforderung von einem anderen Netz empfängt.

3. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 1, wobei das erste Netz ein System hat, das zum Verwenden einer Authentifizierung mit einem öffentlichen Schlüssel fähig ist.

4. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 1, ferner umfassend eine Erteilungseinheit, die eine digitale Signatur durch Verwenden eines Serverzertifikates erteilt, das signiert ist, um das Benutzerendgerät zu schützen.

5. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 1, wobei die zweite Antwortnachricht ein Authentifizierungskooperationsprotokoll ist, inkludierend die Einstellungsdaten des Benutzerendgerätes, generiert durch ein anderes Netz.

6. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 1, wobei das elektronische Zertifikat Information inkludiert, die mit einer Vielzahl von Netzen in Beziehung steht, die miteinander zu kooperieren haben, wenn die Vielzahl von Netzen, die miteinander zu kooperieren haben, in der Authentifizierungskooperationsprozedur vorgesehen sind.

7. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 6, wobei die Information, die mit der Vielzahl von Netzen in Beziehung steht, die miteinander zu kooperieren haben, Daten inkludiert, die eine Rangfolge anzeigen, mit der die Vielzahl von Netzen für eine sequenzielle Auswahl der Vielzahl von Netzen zu kooperieren haben, die funktional zu kooperieren haben.

8. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 2, wobei ein SAML-Protokoll, spezifiziert durch OASIS, als das Authentifizierungskooperationsprotokoll verwendet wird, was durch eine Signatur des Netz es geschützt ist, und die Empfangseinheit die SAML-Nachricht empfängt, die als die zweite Antwortnachricht dient, in der die Einstellungsdaten des Benutzerendgerätes, generiert durch ein anderes Netz, in der Authentifizierungskooperationsprozedur eingebettet sind, die auf der Basis des SAML-Protokolls geschützt ist.

9. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 1, wobei die Einstellungsdaten alle Daten inkludieren, die durch ein IKE-Protokoll, spezifiziert durch RFC2409 von IETF, verteilt werden können.

10. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 1, wobei die Einstellungsdaten alle Daten eines TLS-Protokolls, spezifiziert durch RFC2246 von IETF, und eines TLS-Erweiterungsprotokolls, spezifiziert durch RFC3546, inkludieren.

11. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 1, ferner umfassend eine Bestimmungseinheit, die die Authentifizierungskooperationsvorrichtung bestimmt, die zu kooperieren hat mit Bezug auf das elektronische Zertifikat, das für die Zugriffsauthentifizierung des Benutzerendgerätes verwendet wird.

12. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 11, wobei die Authentifizierungskooperationsvorrichtung zu einem anderen Netz gehört.

13. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 1, wobei das andere Netz ein Unternehmensnetz ist, und die Authentifizierungskooperationsanforderung, die zu dem Unternehmensnetz übertragen wird, eine VPN-Verbindungsanforderung inkludiert.

14. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 13, ferner umfassend eine Empfangseinheit, die einen VPN-Schlüssel empfängt, der als Reaktion auf die VPN-Verbindungsanforderung in der Authentifizierungskooperationsprozedur generiert wurde, ohne Betreiben des Internet-Schlüsselaustauschs.

15. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 13, wobei die Übertragungseinheit unbestimmte Information zum Generieren des VPN-Schlüssels zu dem Unternehmensnetz in der Authentifizierungskooperationsprozedur überträgt.

16. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 15, wobei die unbestimmte Information Information ist, die zur Zeit von Netzzugriffsauthentifizierung generiert wird.

17. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 15, wobei die unbestimmte Information durch das Benutzerendgerät verwendet wird, um den VPN-Schlüssel zu generieren.

18. Einstellungsinformations-Verteilungsvorrichtung nach Anspruch 15, wobei ein TLS-Protokoll, spezifiziert durch RFC2246 von IETF, als die Netzzugriffsauthentifizierungsprozedur verwendet wird, und eine Zufallszahl und eine Zeiteinrichtung unbestimmte Information zum Generieren des VPN-Schlüssels sind.

19. Einstellungsinformations-Verteilungsverfahren, umfassend:
einen Authentifizierungsschritt zum Empfangen und Authentifizieren einer Authentifizierungsanforderung von einem Benutzerendgerät, das eine Zugriffsauthentifizierung anfordert, durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen dem Benutzerendgerät und einem ersten Netz;
einen Übertragungsschritt zum Übertragen einer Authentifizierungskooperationsanforderung, die Einstellungsdaten anfordert, die zu dem Benutzerendgerät einzustellen sind, zu einem anderen Netz durch Verwenden der Netzzugriffsauthentifizierungsprozedur und einer Authentifizierungskooperationsprozedur zwischen einer Vielzahl von Netzen; und
einen Verteilungsschritt zum Verteilen einer ersten Antwortnachricht, der Einstellungsdaten hinzugefügt sind, zu dem Benutzerendgerät durch Erzeugen der ersten Antwortnachricht entsprechend der Authentifizierungsanforderung durch Hinzufügen der Einstellungsdaten, inkludiert in einer zweiten Antwortnachricht entsprechend der Authentifizierungskooperationsanforderung.

20. Einstellungsinformations-Verteilungsverfahren nach Anspruch 19, ferner umfassend einen Empfangsschritt zum Empfangen der zweiten Antwortnachricht zu der Authentifizierungskooperationsanforderung von einem anderen Netz.

21. Einstellungsinformations-Verteilungsverfahren nach Anspruch 19, wobei das erste Netz ein System hat, das zum Verwenden einer Authentifizierung mit einem öffentlichen Schlüssel fähig ist.

22. Einstellungsinformations-Verteilungsverfahren nach Anspruch 19, ferner umfassend einen Erteilungsschritt zum Erteilen eines Serverzertifikates, das signiert ist, um das Benutzerendgerät zu schützen.

23. Einstellungsinformations-Verteilungsverfahren nach Anspruch 19, wobei die zweite Antwortnachricht ein Authentifizierungskooperationsprotokoll ist, inkludierend die Einstellungsdaten des Benutzerendgerätes, generiert durch ein anderes Netz.

24. Einstellungsinformations-Verteilungsverfahren nach Anspruch 19, wobei das elektronische Zertifikat Information inkludiert, die mit einer Vielzahl von Netzen in Beziehung steht, die miteinander zu kooperieren haben, wenn die Vielzahl von Netzen, die miteinander zu kooperieren haben, in der Authentifizierungskooperationsprozedur vorgesehen sind.

25. Einstellungsinformations-Verteilungsverfahren nach Anspruch 24, wobei die Information, die mit der Vielzahl von Netzen in Beziehung steht, die miteinander zu kooperieren haben, Daten inkludiert, die eine Rangfolge anzeigen, mit der die Vielzahl von Netzen zu kooperieren haben, zum sequenziellen Auswählen der Vielzahl von Netzen, die funktional zu kooperieren haben.

26. Einstellungsinformations-Verteilungsverfahren nach Anspruch 20, wobei ein SAML-Protokoll, spezifiziert durch OASIS, als das Authentifizierungskooperationsprotokoll verwendet wird, das durch eine Signatur des Netzes geschützt ist, und der Empfangsschritt Empfangen der SAML-Nachricht inkludiert, die als die zweite Antwortnachricht dient, in der die Einstellungsdaten des Benutzerendgerätes, generiert durch ein anderes Netz, in der Authentifizierungskooperationsprozedur eingebettet sind, die auf der Basis des SAML-Protokolls geschützt ist.

27. Einstellungsinformations-Verteilungsverfahren nach Anspruch 19, wobei die Einstellungsdaten alle Daten inkludieren, die durch ein IKE-Protokoll, spezifiziert durch RFC2409 von IETF, verteilt werden können.

28. Einstellungsinformations-Verteilungsverfahren nach Anspruch 19, wobei die Einstellungsdaten alle Daten eines TLS-Protokolls, spezifiziert durch RFC2246 von IETF, und eines TLS-Erweiterungsprotokolls, spezifiziert durch RFC3546, inkludieren.

29. Einstellungsinformations-Verteilungsverfahren nach Anspruch 19, ferner umfassend einen Bestimmungsschritt zum Bestimmen der Authentifizierungskooperationsvorrichtung, die zu kooperieren hat mit Bezug auf das elektronische Zertifikat, das für die Zugriffsauthentifizierung des Benutzerendgerätes verwendet wird.

30. Einstellungsinformations-Verteilungsverfahren nach Anspruch 29, wobei die Authentifizierungskooperationsvorrichtung zu einem anderen Netz gehört.

31. Einstellungsinformations-Verteilungsverfahren nach Anspruch 19, wobei das andere Netz ein Unternehmensnetz ist, und die Authentifizierungskooperationsanforderung, die zu dem Unternehmensnetz übertragen wird, eine VPN-Verbindungsanforderung inkludiert.

32. Einstellungsinformations-Verteilungsverfahren nach Anspruch 31, ferner umfassend einen Empfangsschritt zum Empfangen eines VPN-Schlüssels, der als Reaktion auf die VPN-Verbindungsanforderung in der Authentifizierungskooperationsprozedur generiert wurde, ohne Betreiben des Schlüsselaustauschprotokolls.

33. Einstellungsinformations-Verteilungsverfahren nach Anspruch 31, wobei der Übertragungsschritt Übertragen unbestimmter Information zum Generieren des VPN-Schlüssels zu dem Unternehmensnetz in der Authentifizierungskooperationsprozedur inkludiert.

34. Einstellungsinformations-Verteilungsverfahren nach Anspruch 33, wobei die unbestimmte Information Information ist, die zur Zeit von Netzzugriffsauthentifizierung generiert wird.

35. Einstellungsinformations-Verteilungsverfahren nach Anspruch 33, wobei die unbestimmte Information durch das Benutzerendgerät verwendet wird, um den VPN-Schlüssel zu generieren.

36. Einstellungsinformations-Verteilungsverfahren nach Anspruch 33, wobei ein TLS-Protokoll, spezifiziert durch RFC2246 von IETF, als die Netzzugriffsauthentifizierungsprozedur verwendet wird, und eine Zufallszahl und eine Zeiteinrichtung unbestimmte Information zum Generieren des VPN-Schlüssels sind.

37. Einstellungsinformations-Verteilungsprogramm zum Veranlassen eines Computers, zu funktionieren als:
eine Authentifizierungseinheit, die eine Authentifizierungsanforderung von einem Benutzerendgerät empfängt und authentifiziert, das eine Zugriffsauthentifizierung anfordert durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen dem Benutzerendgerät und dem ersten Netz;
eine Übertragungseinheit, die eine Authentifizierungskooperationsanforderung, die Einstellungsdaten anfordert, die zu dem Benutzerendgerät einzustellen sind, zu einem anderen Netz überträgt durch Verwenden der Netzzugriffsauthentifizierungsprozedur und einer Authentifizierungskooperationsprozedur zwischen einer Vielzahl von Netzen; und
eine Verteilungseinheit, die eine erste Antwortnachricht, der Einstellungsdaten hinzugefügt sind, zu dem Benutzerendgerät verteilt, durch Erzeugen der ersten Antwortnachricht entsprechend der Authentifizierungsanforderung durch Hinzufügen der Einstellungsdaten, inkludiert in der zweiten Antwortnachricht entsprechend der Authentifizierungskooperationsanforderung.

38. Einstellungsinformations-Verteilungsprogramm nach Anspruch 37, ferner umfassend eine Empfangseinheit, die die zweite Antwortnachricht zu der Authentifizierungskooperationsanforderung von einem anderen Netz empfängt.

39. Einstellungsinformations-Verteilungsprogramm nach Anspruch 37, wobei das ersten Netz ein System hat, das zum Verwenden einer Authentifizierung mit öffentlichem Schlüssel fähig ist.

40. Einstellungsinformations-Verteilungsprogramm nach Anspruch 37, ferner umfassend eine Erteilungseinheit, die eine digitale Signatur durch Verwenden eines Serverzertifikates erteilt, das signiert ist, um das Benutzerendgerät zu schützen.

41. Einstellungsinformations-Verteilungsprogramm nach Anspruch 37, wobei die zweite Antwortnachricht ein Authentifizierungskooperationsprotokoll ist, inkludierend die Einstellungsdaten des Benutzerendgerätes, generiert durch ein anderes Netz.

42. Einstellungsinformations-Verteilungsprogramm nach Anspruch 37, wobei das elektronische Zertifikat Information inkludiert, die zu einer Vielzahl von Netzen in Beziehung steht, die miteinander zu kooperieren haben, wenn die Vielzahl von Netzen, die miteinander zu kooperieren haben, in der Authentifizierungskooperationsprozedur vorgesehen sind.

43. Einstellungsinformations-Verteilungsprogramm nach Anspruch 42, wobei die Information, die mit der Vielzahl von Netzen in Beziehung steht, die miteinander zu kooperieren haben, Daten inkludiert, die eine Rangfolge anzeigen, mit der die Vielzahl von Netzen zu kooperieren haben, zum sequenziellen Auswählen der Vielzahl von Netzen, die funktional zu kooperieren haben.

44. Einstellungsinformations-Verteilungsprogramm nach Anspruch 38, wobei ein SAML-Protokoll, spezifiziert durch OASIS, als das Authentifizierungskooperationsprotokoll verwendet wird, was durch eine Signatur des Netzes geschützt ist, und die Empfangseinheit die SAML-Nachricht empfängt, die als die zweite Antwortnachricht dient, in der die Einstellungsdaten des Benutzerendgerätes, generiert durch ein anderes Netz, in der Authentifizierungskooperationsprozedur eingebettet sind, die auf der Basis des SAML-Protokolls geschützt ist.

45. Einstellungsinformations-Verteilungsprogramm nach Anspruch 37, wobei die Einstellungsdaten alle Daten inkludieren, die durch ein IKE-Protokoll, spezifiziert durch RFC2409 von IETF, verteilt werden können.

46. Einstellungsinformations-Verteilungsprogramm nach Anspruch 37, wobei die Einstellungsdaten alle Daten eines TLS-Protokolls, spezifiziert durch RFC2246 von IETF, und eines TLS-Erweiterungsprotokolls, spezifiziert durch RFC3546, inkludieren.

47. Einstellungsinformations-Verteilungsprogramm nach Anspruch 37, ferner umfassend eine Bestimmungseinheit, die die Authentifizierungskooperationsprozedur bestimmt, die zu kooperieren haben mit Bezug auf das elektronische Zertifikat, das für die Zugriffsauthentifizierung des Benutzerendgerätes verwendet wird.

48. Einstellungsinformations-Verteilungsprogramm nach Anspruch 47, wobei die Authentifizierungskooperationsvorrichtung zu einem anderen Netz gehört.

49. Einstellungsinformations-Verteilungsprogramm nach Anspruch 37, wobei das andere Netz ein Unternehmensnetz ist, und die Authentifizierungskooperationsanforderung, die zu dem Unternehmensnetz übertragen wird, eine VPN-Verbindungsanforderung inkludiert.

50. Einstellungsinformations-Verteilungsprogramm nach Anspruch 49, ferner umfassend eine Empfangseinheit, die einen VPN-Schlüssel empfängt, der als Reaktion auf die VPN-Verbindungsanforderung in der Authentifizierungskooperationsprozedur generiert wurde, ohne Betreiben des Schlüsselaustauschprotokolls.

51. Einstellungsinformations-Verteilungsprogramm nach Anspruch 49, wobei die Übertragungseinheit unbestimmte Information zum Generieren des VPN-Schlüssels zu dem Unternehmensnetz in der Authentifizierungskooperationsprozedur überträgt.

52. Einstellungsinformations-Verteilungsprogramm nach Anspruch 51, wobei die unbestimmte Information Information ist, die zur Zeit von Netzzugriffsauthentifizierung generiert wird.

53. Einstellungsinformations-Verteilungsprogramm nach Anspruch 51, wobei die unbestimmte Information durch das Benutzerendgerät verwendet wird, um den VPN-Schlüssel zu generieren.

54. Einstellungsinformations-Verteilungsprogramm nach Anspruch 51, wobei ein TLS-Protokoll, spezifiziert durch RFC2246 von IETF, als die Netzzugriffsauthentifizierungsprozedur verwendet wird, und eine Zufallszahl und eine Zeiteinrichtung unbestimmte Information zum Generieren des VPN-Schlüssels sind.

55. Speichermedium, das durch einen Computer lesbar ist, und ein Programm zum Veranlassen des Computers speichert, zu funktionieren als:
eine Authentifizierungseinheit, die eine Authentifizierungsanforderung von einem Benutzerendgerät empfängt und authentifiziert, das eine Zugriffsauthentifizierung anfordert durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen dem Benutzerendgerät und dem ersten Netz;
eine Übertragungseinheit, die eine Authentifizierungskooperationsanforderung, die Einstellungsdaten anfordert, die zu dem Benutzerendgerät einzustellen sind, zu einem anderen Netz überträgt durch Verwenden der Netzzugriffsauthentifizierungsprozedur und einer Authentifizierungskooperationsprozedur zwischen einer Vielzahl von Netzen; und
eine Verteilungseinheit, die eine erste Antwortnachricht, der Einstellungsdaten hinzugefügt sind, zu dem Benutzerendgerät verteilt durch Erzeugen der ersten Antwortnachricht entsprechend der Authentifizierungsanforderung durch Hinzufügen der Einstellungsdaten, inkludiert in einer zweiten Antwortnachricht entsprechend der Authentifizierungskooperationsanforderung.

56. Authentifizierungstransfervorrichtung, umfassend:
eine Empfangseinheit, die ein elektronisches Zertifikat eines Clients, das für Zugriffsauthentifizierung verwendet wird, von einem ersten Netzwerk empfängt, das eine Authentifizierung bei Empfang einer Authentifizierungsanforderung von einem Benutzerendgerät durchführt, das die Zugriffsauthentifizierung anfordert, durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen dem Benutzerendgerät und dem ersten Netz; und

eine Bestimmungseinheit, die eine Authentifizierungskooperationsvorrichtung bestimmt, die zu kooperieren hat, mit Bezug auf das elektronische Zertifikat eines Clients, das durch die Empfangseinheit empfangen wird.

57. Authentifizierungstransferverfahren, umfassend:
einen Empfangsschritt zum Empfangen eines elektronischen Zertifikates eines Clients, das für Zugriffsauthentifizierung verwendet wird, von einem ersten Netz, das eine Authentifizierung bei Empfang einer Authentifizierungsanforderung von einem Benutzerendgerät durchführt, das die Zugriffsauthentifizierung anfordert, durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen dem Benutzerendgerät und dem ersten Netz; und
einen Bestimmungsschritt zum Bestimmen einer Authentifizierungskooperationsvorrichtung, die zu kooperieren hat, mit Bezug auf das elektronische Zertifikat des Clients, das in dem Empfangsschritt empfangen wird.

58. Authentifizierungstransferprogramm zum Veranlassen eines Computers, zu funktionieren als:
eine Empfangseinheit, die ein elektronisches Zertifikat eines Clients, das für Zugriffsauthentifizierung verwendet wird, von einem ersten Netz empfängt, das eine Authentifizierung bei Empfang einer Authentifizierungsanforderung von einem Benutzerendgerät durchführt, das die Zugriffsauthentifizierung anfordert, durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen dem Benutzerendgerät und dem ersten Netz; und
eine Bestimmungseinheit, die eine Authentifizierungskooperationsvorrichtung bestimmt, die zu kooperieren hat, mit Bezug auf das elektronische Zertifikat des Clients, das durch die Empfangseinheit empfangen wird.

59. Speichermedium, das durch einen Computer lesbar ist, und ein Programm zum Veranlassen des Computers speichert, zu funktionieren als:
eine Empfangseinheit, die ein elektronisches Zertifikat eines Clients, das für Zugriffsauthentifizierung verwendet wird, von einem ersten Netz empfängt, das eine Authentifizierung bei Empfang einer Authentifizierungsanforderung von einem Benutzerendgerät durchführt, das die Zugriffsauthentifizierung anfordert, durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen dem Benutzerendgerät und dem ersten Netz; und
eine Bestimmungseinheit, die eine Authentifizierungskooperationsvorrichtung bestimmt, die zu kooperieren hat, mit Bezug auf das elektronische Zertifikat des Clients, das durch die Empfangseinheit empfangen wird.

60. Einstellungsinformations-Empfangsprogram m zum Veranlassen eines Computers, zu funktionieren als:
eine Authentifizierungsanforderungseinheit, die eine Zugriffsauthentifizierung zu einem ersten Netz anfordert, durch Verwenden einer Netzzugriffsauthentifizierungsprozedur zwischen einem Benutzerendgerät und dem ersten Netz;
eine Empfangseinheit, die Einstellungsdaten empfängt, die zu dem Benutzerendgerät eingestellt werden, mit Bezug auf ein anderes Netz, was von einem anderen Netz erlangt wird, durch Verwenden der Netzzugriffsauthentifizierungsprozedur und einer Authentifizierungskooperationsprozedur zwischen einer Vielzahl von Netzen, die miteinander kooperieren; und
eine Einstellungseinheit, die die Einstellungsdaten sequenziell einstellt, die von der Empfangseinheit empfangen werden, auf der Basis von Daten, die eine Kooperationsrangfolge von anderen Netzen anzeigen, inkludiert in dem elektronischen Zertifikat des Clients.

Es folgen 30 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

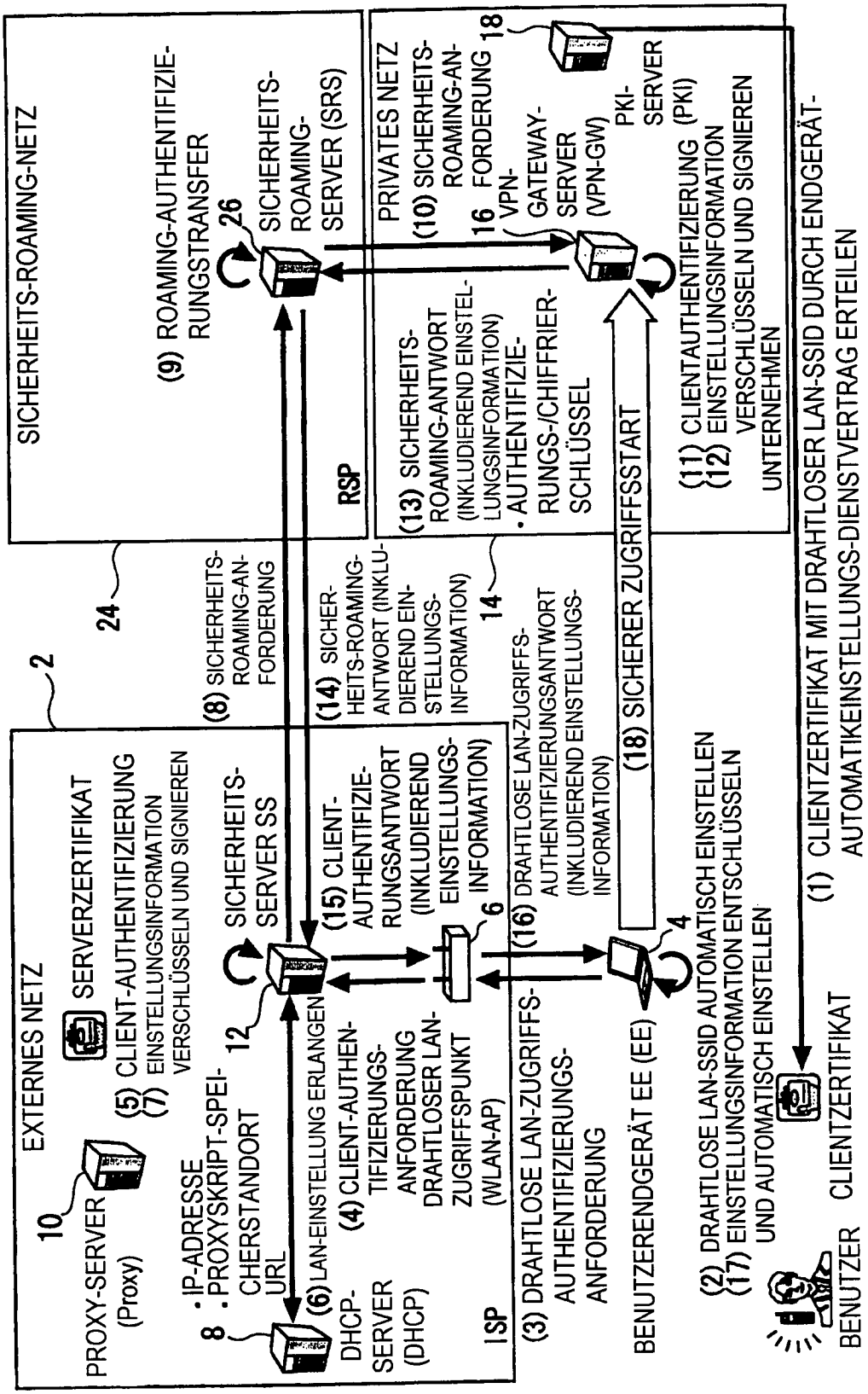


FIG. 2A

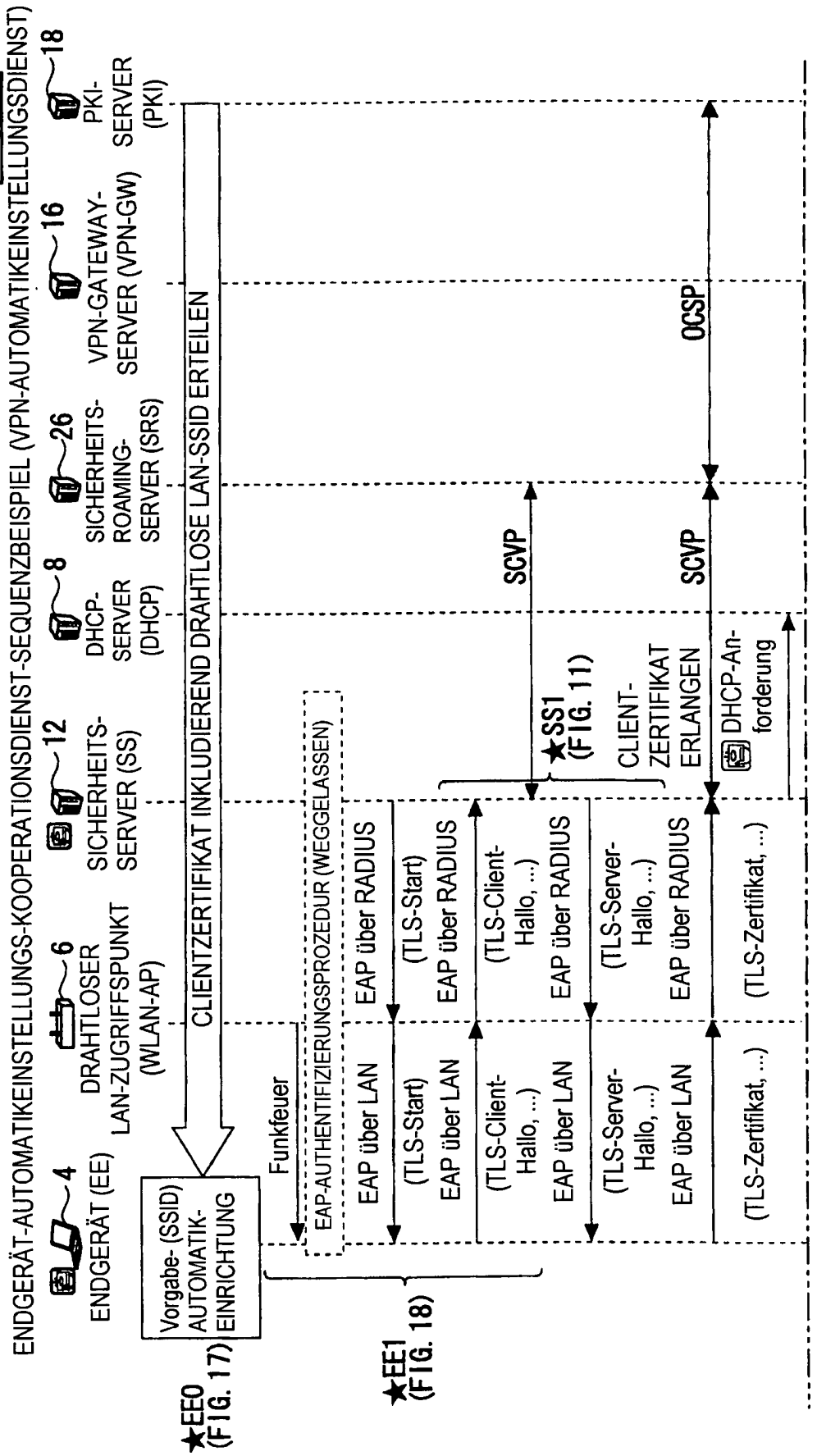

ENDGERÄT-AUTOMATIKEINSTELLUNGS-KOOPERATIONSDIENST-SEQUENZBEISPIEL (VPN-AUTOMATIKEINSTELLUNGSDIENST)
FIG2
FIG2A
FIG2B
4
ENDGERÄT (EE)
6
DRAHTLOSER LAN-ZUGRIFFSPUNKT (WLAN-AP)
12
SICHERHEITS-SERVER (SS)
8
DHCP-SERVER (DHCP)
26
SICHERHEITS-ROAMING-SERVER (SRS)
16
VPN-GATEWAY-SERVER (VPN-GW)
18
PKI-SERVER (PKI)
CLIENTZERTIFIKAT INKLUDIEREND DRAHTLOSE LAN-SSID ERTEILEN
Vorgabe- (SSID) AUTOMATIK-EINRICHTUNG
Funkfeuer
EAP-AUTHENTIFIZIERUNGSPROZEDUR (WEGGELASSEN)
EAP über LAN
EAP über RADIUS
(TLS-Start)
EAP über LAN
EAP über RADIUS
(TLS-Client-Hallo, ...)
EAP über LAN
EAP über RADIUS
(TLS-Server-Hallo, ...)
EAP über LAN
EAP über RADIUS
(TLS-Zertifikat, ...)
(TLS-Zertifikat, ...)
SCVP
SCVP
OCSP
★SS1 (FIG. 11)
CLIENT-ZERTIFIKAT ERLANGEN
DHCP-An-forderung
★EE0 (FIG. 17)
★EE1 (FIG. 18)

FIG. 2B

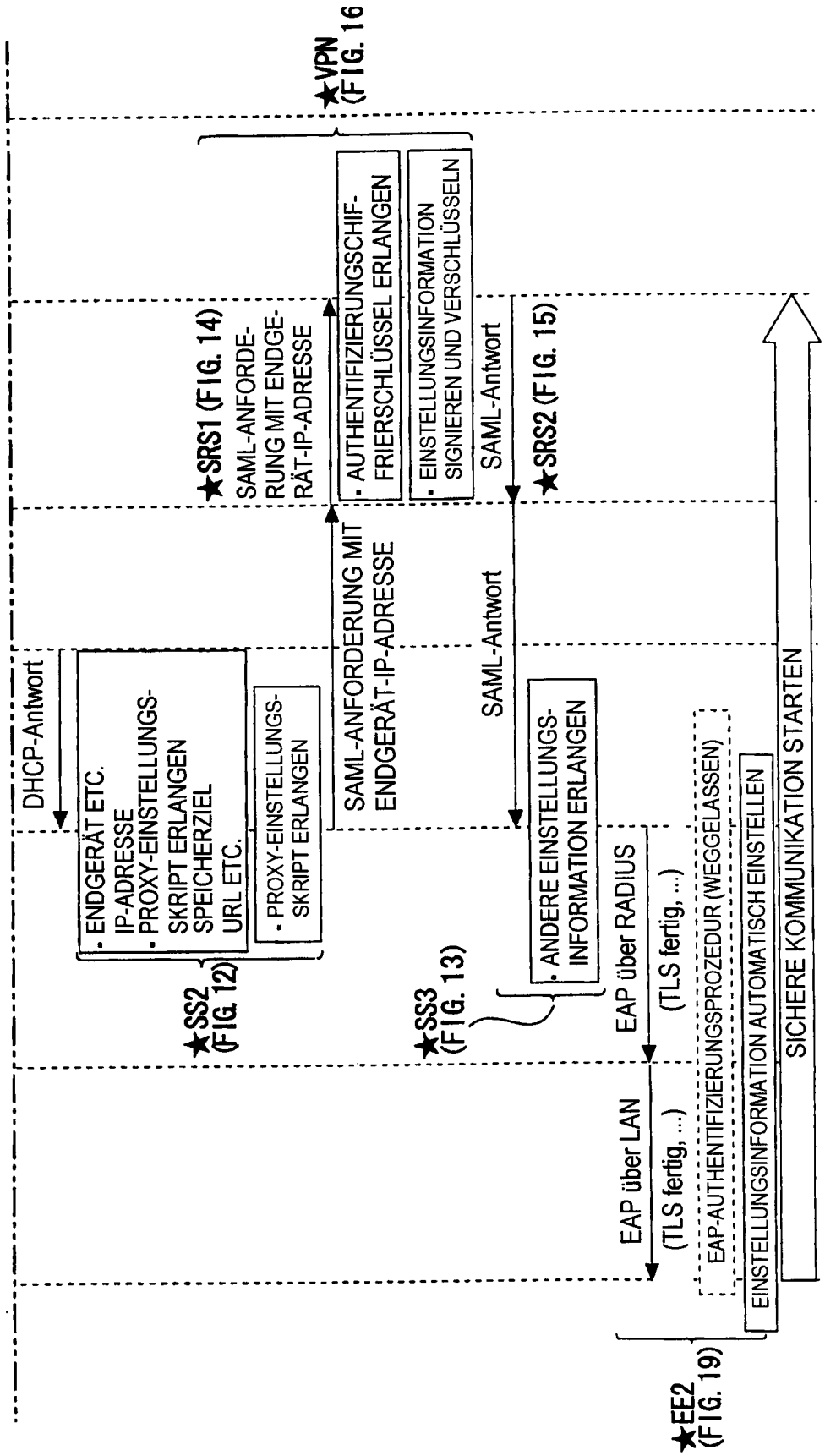

★VPN (FIG. 16)
★SRS1 (FIG. 14)
SAML-ANFORDERUNG MIT ENDGERÄT-IP-ADRESSE
• AUTHENTIFIZIERUNGSCHIFFRIERSCHLÜSSEL ERLANGEN
• EINSTELLUNGSINFORMATION SIGNIEREN UND VERSCHLÜSSELN
SAML-Antwort
★SRS2 (FIG. 15)
DHCP-Antwort
• ENDGERÄT ETC.
IP-ADRESSE
• PROXY-EINSTELLUNGSSKRIPT ERLANGEN
SPEICHERZIEL
URL ETC.
• PROXY-EINSTELLUNGSSKRIPT ERLANGEN
★SS2 (FIG. 12)
SAML-Antwort
• ANDERE EINSTELLUNGSINFORMATION ERLANGEN
★SS3 (FIG. 13)
EAP über RADIUS
(TLS fertig, ...)
EAP-AUTHENTIFIZIERUNGSPROZEDUR (WEGGELASSEN)
EAP über LAN
(TLS fertig, ...)
EINSTELLUNGSINFORMATION AUTOMATISCH EINSTELLEN
SICHERE KOMMUNIKATION STARTEN
★EE2 (FIG. 19)

FIG. 3

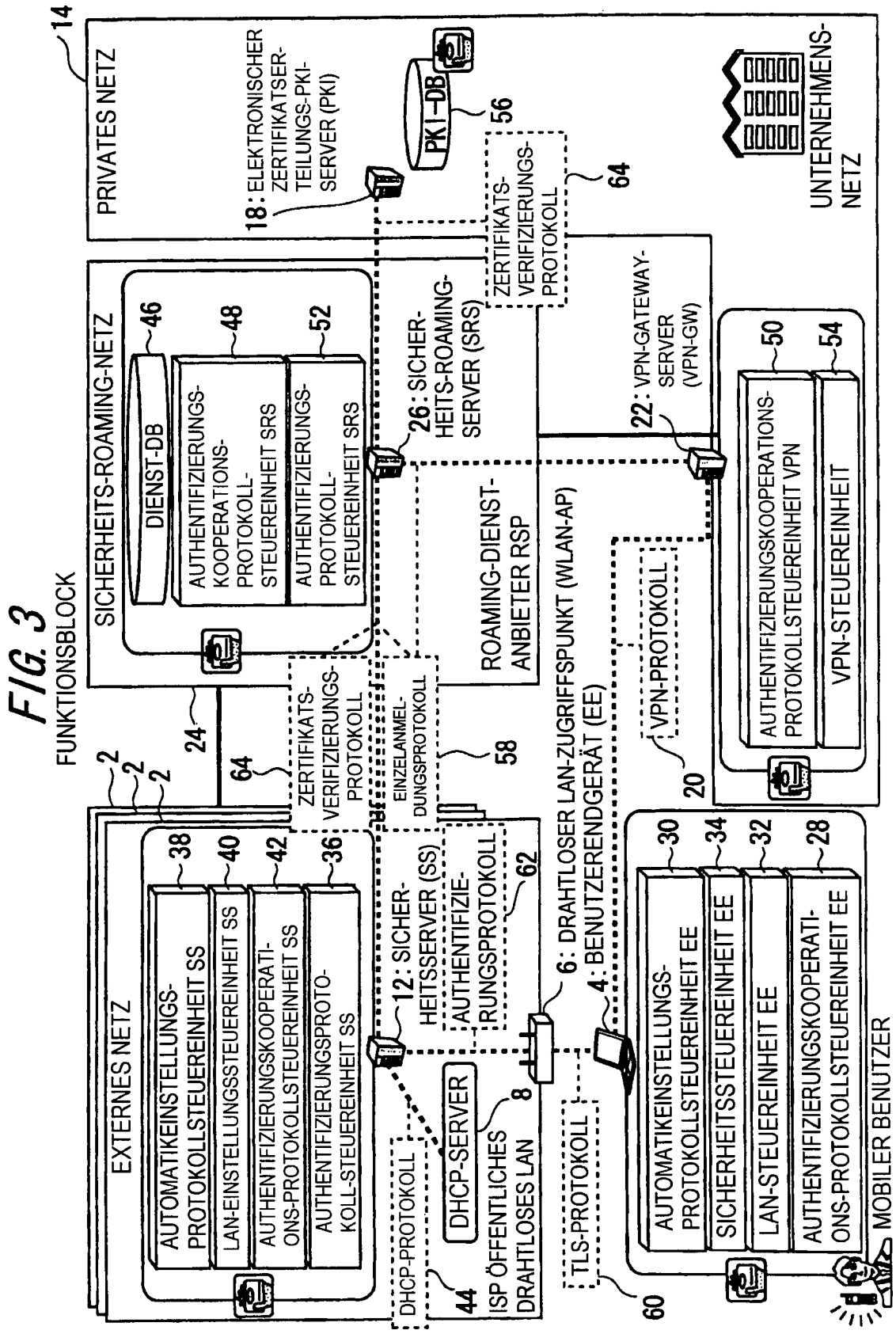

FUNKTIONSBLOCK
14
PRIVATES NETZ
18: ELEKTRONISCHER ZERTIFIKATSER-TEILUNGS-PKI-SERVER (PKI)
PKI-DB
56
UNTERNEHMENS-NETZ
SICHERHEITS-ROAMING-NETZ
DIENST-DB
46
AUTHENTIFIZIERUNGS-KOOPERATIONS-PROTOKOLL-STEUEREINHEIT SRS
48
AUTHENTIFIZIERUNGS-PROTOKOLL-STEUEREINHEIT SRS
52
26: SICHER-HEITS-ROAMING-SERVER (SRS)
ZERTIFIKATS-VERIFIZIERUNGS-PROTOKOLL
64
22: VPN-GATEWAY-SERVER (VPN-GW)
AUTHENTIFIZIERUNGSKOOPERATIONS-PROTOKOLLSTEUEREINHEIT VPN
50
VPN-STEUEREINHEIT
54
EXTERNES NETZ
AUTOMATIKEINSTELLUNGS-PROTOKOLLSTEUEREINHEIT SS
38
LAN-EINSTELLUNGSSTEUEREINHEIT SS
40
AUTHENTIFIZIERUNGSKOOPERATI-ONS-PROTOKOLLSTEUEREINHEIT SS
42
AUTHENTIFIZIERUNGSPROTO-KOLL-STEUEREINHEIT SS
36
2
2
2
24
64
ZERTIFIKATS-VERIFIZIERUNGS-PROTOKOLL
EINZELANMEL-DUNGSPROTOKOLL
58
ROAMING-DIENST-ANBIETER RSP
DHCP-PROTOKOLL
12: SICHER-HEITSSERVER (SS)
AUTHENTIFIZIE-RUNGSPROTOKOLL
62
VPN-PROTOKOLL
20
DHCP-SERVER
44
8
ISP ÖFFENTLICHES DRAHTLOSES LAN
6: DRAHTLOSER LAN-ZUGRIFFSPUNKT (WLAN-AP)
4: BENUTZERENDGERÄT (EE)
TLS-PROTOKOLL
60
AUTOMATIKEINSTELLUNGS-PROTOKOLLSTEUEREINHEIT EE
30
SICHERHEITSSTEUEREINHEIT EE
34
LAN-STEUEREINHEIT EE
32
AUTHENTIFIZIERUNGSKOOPERATI-ONS-PROTOKOLLSTEUEREINHEIT EE
28
MOBILER BENUTZER

FIG. 4

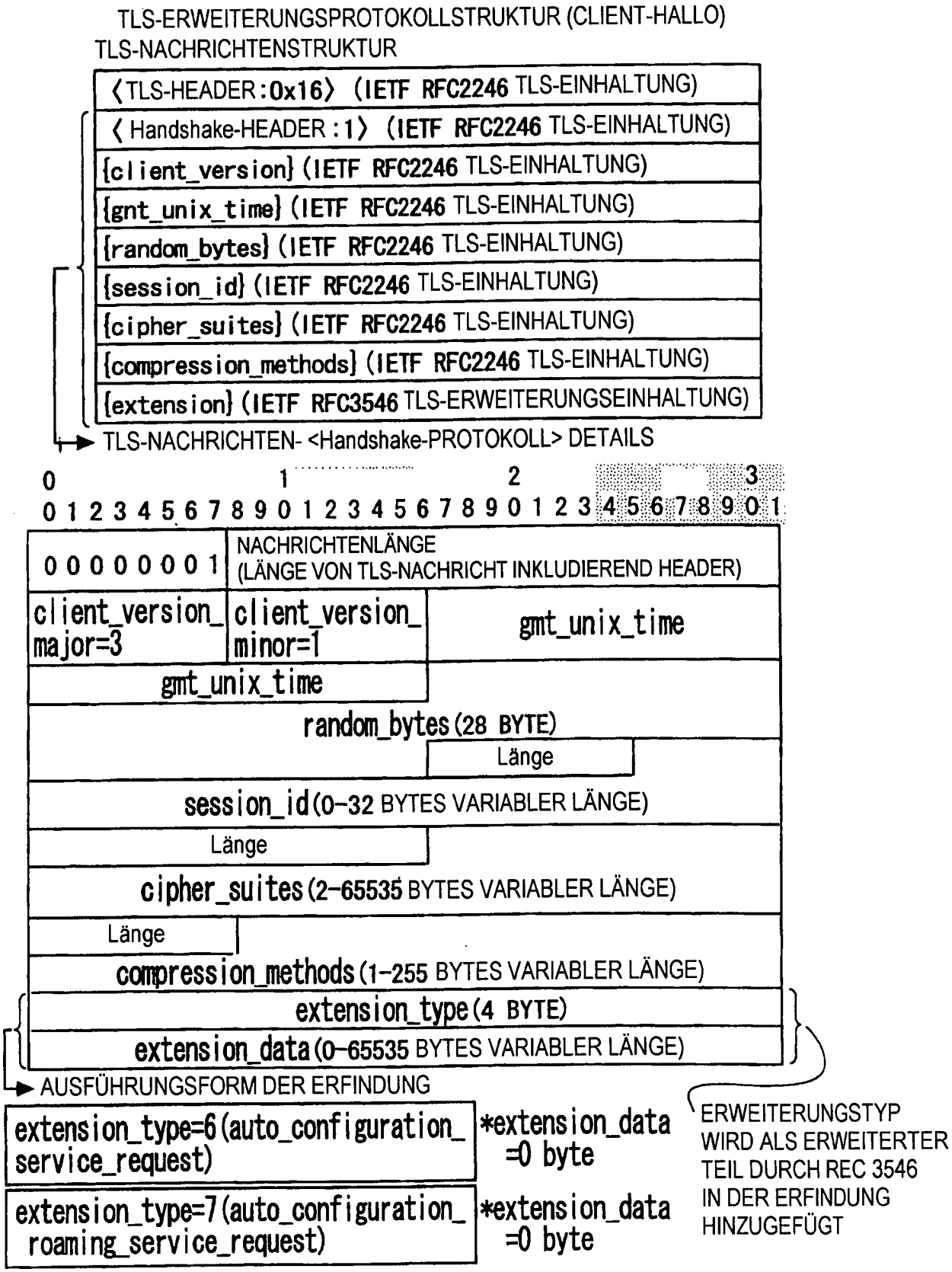

TLS-ERWEITERUNGSPROTOKOLLSTRUKTUR (CLIENT-HALLO)
TLS-NACHRICHTENSTRUKTUR
〈TLS-HEADER:0x16〉 (IETF RFC2246 TLS-EINHALTUNG)
〈 Handshake-HEADER : 1〉 (IETF RFC2246 TLS-EINHALTUNG)
{client_version} (IETF RFC2246 TLS-EINHALTUNG)
{gmt_unix_time} (IETF RFC2246 TLS-EINHALTUNG)
{random_bytes} (IETF RFC2246 TLS-EINHALTUNG)
{session_id} (IETF RFC2246 TLS-EINHALTUNG)
{cipher_suites} (IETF RFC2246 TLS-EINHALTUNG)
{compression_methods} (IETF RFC2246 TLS-EINHALTUNG)
{extension} (IETF RFC3546 TLS-ERWEITERUNGSEINHALTUNG)
TLS-NACHRICHTEN- <Handshake-PROTOKOLL> DETAILS
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
0 0 0 0 0 0 0 1
NACHRICHTENLÄNGE
(LÄNGE VON TLS-NACHRICHT INKLUDIEREND HEADER)
client_version_major=3
client_version_minor=1
gmt_unix_time
gmt_unix_time
random_bytes (28 BYTE)
Länge
session_id (0-32 BYTES VARIABLER LÄNGE)
Länge
cipher_suites (2-65535 BYTES VARIABLER LÄNGE)
Länge
compression_methods (1-255 BYTES VARIABLER LÄNGE)
extension_type (4 BYTE)
extension_data (0-65535 BYTES VARIABLER LÄNGE)
AUSFÜHRUNGSFORM DER ERFINDUNG
extension_type=6 (auto_configuration_service_request)
*extension_data =0 byte
extension_type=7 (auto_configuration_roaming_service_request)
*extension_data =0 byte
ERWEITERUNGSTYP WIRD ALS ERWEITERTER TEIL DURCH REC 3546 IN DER ERFINDUNG HINZUGEFÜGT

FIG. 5A

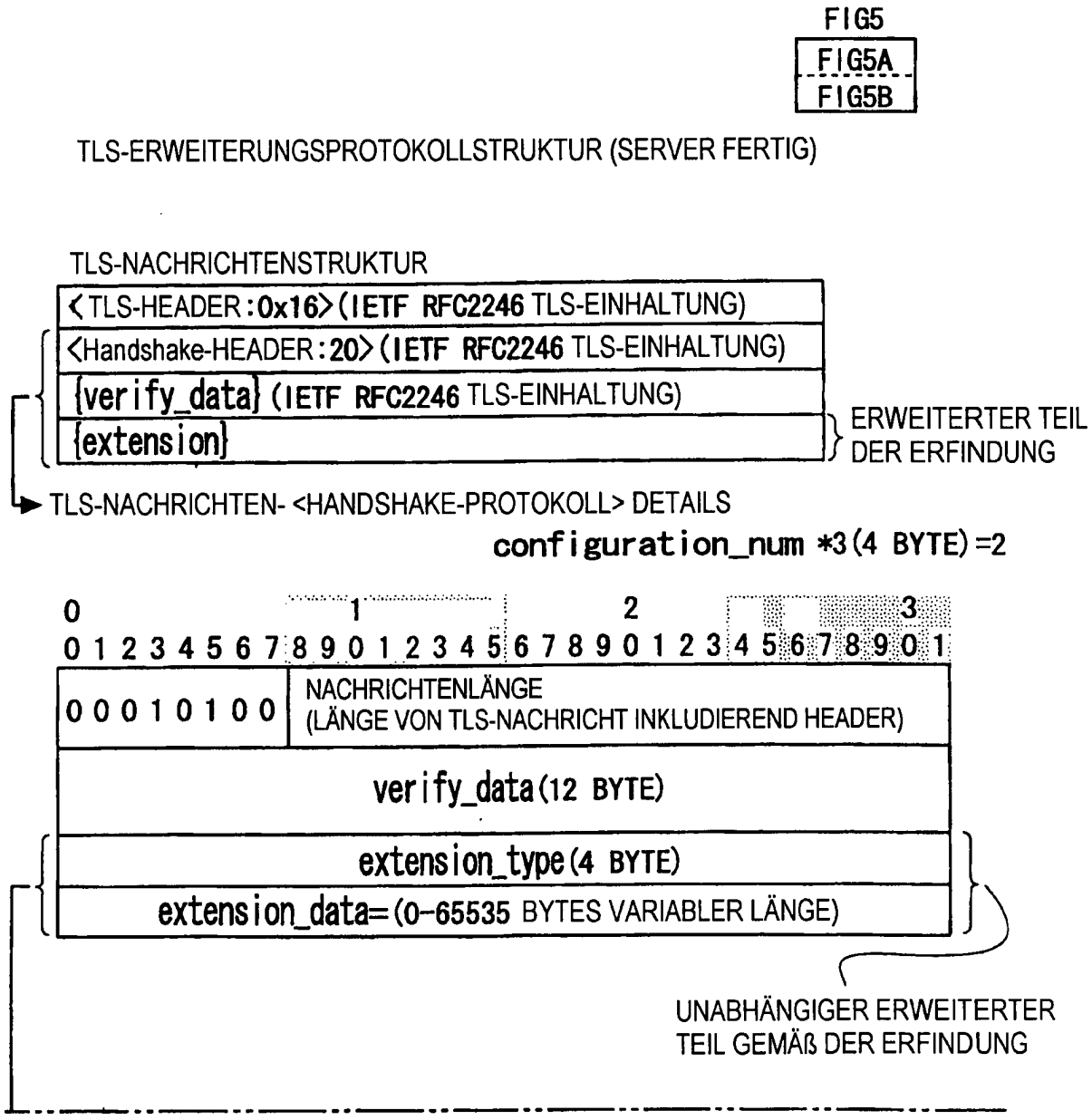


FIG5
FIG5A
FIG5B
TLS-ERWEITERUNGSPROTOKOLLSTRUKTUR (SERVER FERTIG)
TLS-NACHRICHTENSTRUKTUR
<TLS-HEADER:0x16>(IETF RFC2246 TLS-EINHALTUNG)
<Handshake-HEADER:20>(IETF RFC2246 TLS-EINHALTUNG)
{verify_data} (IETF RFC2246 TLS-EINHALTUNG)
{extension}
ERWEITERTER TEIL DER ERFINDUNG
TLS-NACHRICHTEN- <HANDSHAKE-PROTOKOLL> DETAILS
configuration_num *3(4 BYTE)=2
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
00010100
NACHRICHTENLÄNGE
(LÄNGE VON TLS-NACHRICHT INKLUDIEREND HEADER)
verify_data(12 BYTE)
extension_type(4 BYTE)
extension_data=(0-65535 BYTES VARIABLER LÄNGE)
UNABHÄNGIGER ERWEITERTER TEIL GEMÄß DER ERFINDUNG

FIG. 5B

AUSFÜHRUNGSFORM DER ERFINDUNG:

<table>
<tr><td colspan="3">extension_type*1=6(auto_configuration_service_request)</td></tr>
<tr><td colspan="3">extension_size*2(0-65535 BYTES VARIABLER LÄNGE)</td></tr>
<tr><td colspan="3">configuration_network_num *9(4 BYTE)=3</td></tr>
<tr><td>network_number *10=1(ISP)</td><td colspan="2">configuration_num *3(2 BYTE)=1</td></tr>
<tr><td>configuration_type *4=1(DHCP)</td><td>priority *5=Z</td><td>number *6=1</td></tr>
<tr><td colspan="3">configuration_size *7=(0-65535 BYTES VARIABLER LÄNGE)</td></tr>
<tr><td colspan="3">configuration_data *8={Endgerät-IP-Adresse, Teilnetzmaske, Gateway-IP-Adresse, Primär-DNS-IP-Adresse, Sekundär-DNS-IP-Adresse, Domänenname, Lebensdauer, ···}</td></tr>
<tr><td>network_number *10=2(UNTERNEHMEN)</td><td colspan="2">configuration_num *3(2 BYTE)=1</td></tr>
<tr><td>configuration_type=2(IKE)</td><td>priority=A</td><td>number=1</td></tr>
<tr><td colspan="3">configuration_size=(0-65535 BYTES VARIABLER LÄNGE)</td></tr>
<tr><td colspan="3">configuration_data={Sicherheitskonfiguration)</td></tr>
</table>

*1	extension_type	: ERWEITERUNGSTYP
*2	extension_size	: ERWEITERUNGSDATENGRÖßE
*3	configuration_num	: ZAHL VON STÜCKEN VON EINSTELLUNGSDATEN
*4	configuration_type	: ART VON EINSTELLUNGSDATEN
*5	priority	: EINSTELLUNGSPRIORITÄT (A: PRIORITÄT, B: NICHT-PRIORITÄT, C: EINRICHTUNG BEI HOCHFAHREN VON ANWENDUNG; Z: LETZTE EINRICHTUNG VON VERARBEITUNGSEINRICHTUNG)
*6	number	: RANGFOLGE (1-225: EINRICHTUNG IST IN DER REIHENFOLGE VON "1" DURCHGEFÜHRT)
*7	configuration_size	: EINSTELLUNGSDATENGRÖßE (BYTE)
*8	configuration_data	: EINSTELLUNGSDATEN SELBST
*9	configuration_network_num	: ZAHL VON EINSTELLUNGSNETZEN
*10	configuration_type	: ART VON EINSTELLUNGSNETZ

FIG. 6A

FIG6
FIG6A
FIG6B

SAML-ANFORDERUNGSNACHRICHTENBEISPIEL 1 (ISP→RSP)

```
〈samlp:Request
MajorVersion="1"MinorVersion="0"
IssueInstant="UTC Data/Time"
RequestID="128.14.234.20.12345678"
RespondWith0="AuthorizationDecisionStatement"〉
 〈samlp:AuthorizationDecisionQuery
   Resource="SRS"〉                                  } KOOPERATIONSANFORDERUNG ZU RSP ANZEIGEN
   〈saml:Action〉 roaming 〈/saml:Action〉           } ROAMING-VERBINDUNGSANFORDERUNG ANZEIGEN
   〈saml:Evidence〉
     〈saml:Assertion〉
       〈saml:AuthenticationStatement
         AuthenticationMethod="...URI..."
         AuthenticationInstant="2004-12-03T10:02:00Z"〉  } AUTHENTIFIZIERUNGSAUSSAGE ANZEIGEN
         〈saml:Subject〉
```

FIG. 6B

```
            〈saml:NameIdentifier
            SecurityDomain="OOOO.com"
            Name="tarouser"/〉
            〈saml:SubjestConfirmation〉
              〈saml:ConfirmationMethod〉
              Cipher Suite
              〈/saml:ConfirmationMethod〉
              〈saml:SubjectConfirmationData〉
              Signed TLS handshake messages(base64)
              tag
              Signature(base64)
              ISP-LAN
              ClientAddress="128.14.234.20"
              〈/saml:SubjectConfirmationData〉
            〈/saml:SubjectConfirmation〉
          〈/saml:Subject〉
        〈/saml:AuthenticationStatement〉
      〈/saml:Assertion〉
    〈/saml:Evidence〉
  〈/samlp:AuthorizationDecisionQuery〉
〈/samlp:Request〉
```

AUTHENTIFIZIERUNGSDATEN ANZEIGEN

LAN-EINSTELLUNGSINFORMATION VON ISP ANZEIGEN

FIG. 7A

FIG7
FIG7A
FIG7B

SAML-ANFORDERUNGSNACHRICHTENBEISPIEL 2 (UNTERNEHMEN → NETZ)

```
<samlp:Request
MajorVersion="1"MinorVersion="0"
IssueInstant="UTC Data/Time"
RequestID="128.14.234.20.12345678"
RespondWith0="AuthorizationDecisionStatement">
 <samlp:AuthorizationDecisionQuery
   Resource="Server1">
   <saml:Action> vpnconnect </saml:Action>
   <saml:Evidence>
     <saml:Assertion>
       <saml:AuthenticationStatement
         AuthenticationMethod="...URI..."
         AuthenticationInstant="2004-12-03T10:02:00Z">
         <saml:Subject>
```

KOOPERATIONSANFORDERUNG ZU UNTERNEHMEN ANZEIGEN

VPN-VERBINDUNGSANFORDERUNG ANZEIGEN

AUTHENTIFIZIERUNGSAUSSAGE ANZEIGEN

FIG. 7B

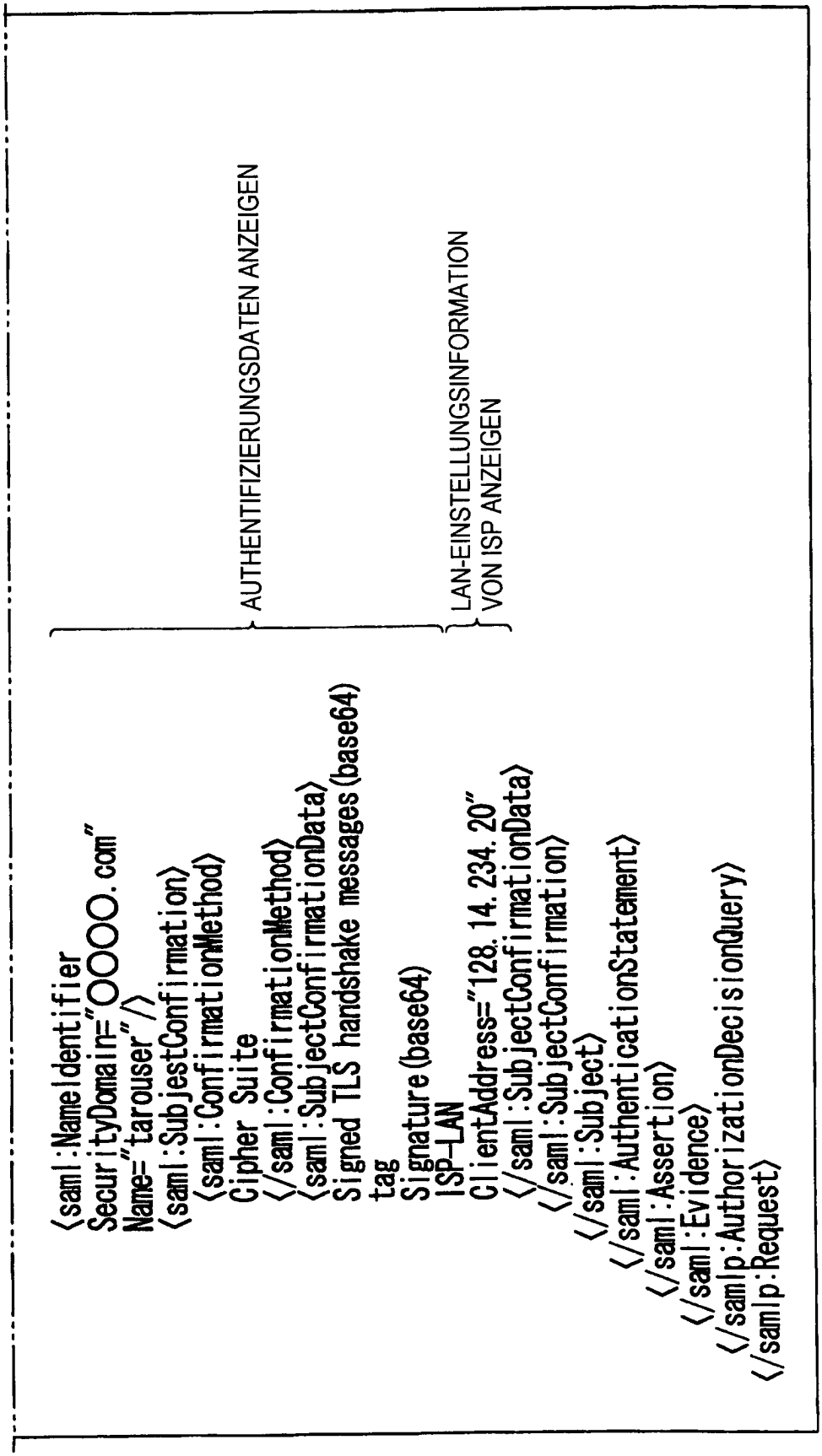

<saml:NameIdentifier
SecurityDomain="OOOO.com"
Name="tarouser" />
<saml:SubjectConfirmation>
<saml:ConfirmationMethod>
Cipher Suite
</saml:ConfirmationMethod>
<saml:SubjectConfirmationData>
Signed TLS handshake messages(base64)
tag
Signature(base64)
ISP-LAN
ClientAddress="128.14.234.20"
</saml:SubjectConfirmationData>
</saml:SubjectConfirmation>
</saml:Subject>
</saml:AuthenticationStatement>
</saml:Assertion>
</saml:Evidence>
</samlp:AuthorizationDecisionQuery>
</samlp:Request>
AUTHENTIFIZIERUNGSDATEN ANZEIGEN
LAN-EINSTELLUNGSINFORMATION
VON ISP ANZEIGEN

FIG. 8A

FIG8
FIG8A
FIG8B

SAML-ANTWORTNACHRICHTENBEISPIEL 1 (UNTERNEHMENSNETZ → RSP)

```
<samlp:Response
  MajorVersion="1"MinorVersion="0"
  IssueInstant="UTC Data/Time"
  ResponseID="128.14.234.20.90123456"
  InResponseTo="128.14.234.20.12345678"
  StatusCode="Success">
  <saml:Assertion
    MajorVersion="1"MinorVersion="0"
    AssertionID="128.9.167.32.12345678"
    Issuer="Server1"
    <saml:Conditions
      NotBefore="2004-12-03T10:00:00Z"
      NotAfter="2004-12.03T10:05:00Z"/>
    <saml:AuthorizationDecisionStatement
      Resource="Server1"                    } UNTERNEHMENSNETZ ANZEIGEN
      Decision="Permit">                    } AUTHENTIFIZIERUNGSERGEBNIS ANZEIGEN
      <saml:Subject>
        <saml:SubjestConfirmation>
```

FIG. 8B

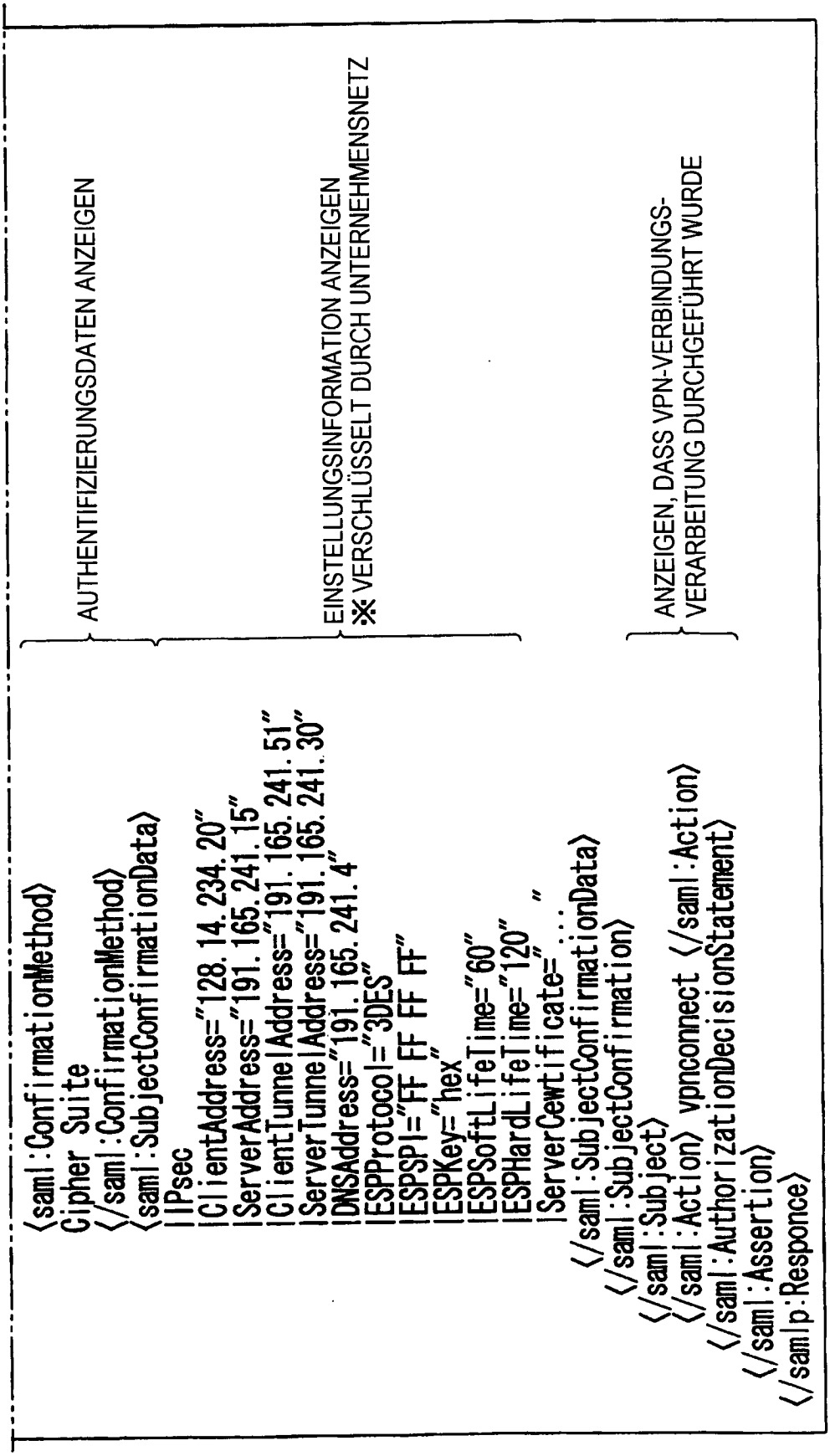

<saml:ConfirmationMethod>
Cipher Suite
</saml:ConfirmationMethod>
<saml:SubjectConfirmationData>
IPsec
ClientAddress="128.14.234.20"
ServerAddress="191.165.241.15"
ClientTunnelAddress="191.165.241.51"
ServerTunnelAddress="191.165.241.30"
DNSAddress="191.165.241.4"
ESPProtocol="3DES"
ESPSPI="FF FF FF FF"
ESPKey="hex"
ESPSoftLifeTime="60"
ESPHardLifeTime="120"
ServerCewtificate="....."
</saml:SubjectConfirmationData>
</saml:SubjectConfirmation>
</saml:Subject>
</saml:Action> vpnconnect </saml:Action>
</saml:AuthorizationDecisionStatement>
</saml:Assertion>
</samlp:Responce>
AUTHENTIFIZIERUNGSDATEN ANZEIGEN
EINSTELLUNGSINFORMATION ANZEIGEN
※ VERSCHLÜSSELT DURCH UNTERNEHMENSNETZ
ANZEIGEN, DASS VPN-VERBINDUNGS-
VERARBEITUNG DURCHGEFÜHRT WURDE

FIG. 9A

FIG9
FIG9A
FIG9B

SAML-ANTWORTNACHRICHTENBEISPIEL 2 (RSP → ISP)

```
<samlp:Response
  MajorVersion="1"MinorVersion="0"
  IssueInstant="UTC Data/Time"
  ResponseID="128.14.234.20.90123456"
  InResponseTo="128.14.234.20.12345678"
  StatusCode="Success">
  <saml:Assertion
    MajorVersion="1"MinorVersion="0"
    AssertionID="128.9.167.32.12345678"
    Issuer="SRS"
    <saml:Conditions
      NotBefore="2004-12-03T10:00:00Z"
      NotAfter="2004-12.03T10:05:00Z"/>
    <saml:AuthorizationDecisionStatement
      Resource="RSP"
      Decision="Permit">                          } RSP ANZEIGEN
      <saml:Subject>                              } AUTHENTIFIZIERUNGSERGEBNIS ANZEIGEN
        <saml:SubjestConfirmation>
          <saml:ConfirmationMethod>
          Cipher Suite                            }
          </saml:ConfirmationMethod>              } AUTHENTIFIZIERUNGSDATEN ANZEIGEN
          <saml:SubjectConfirmationData>          }
```

FIG. 9B

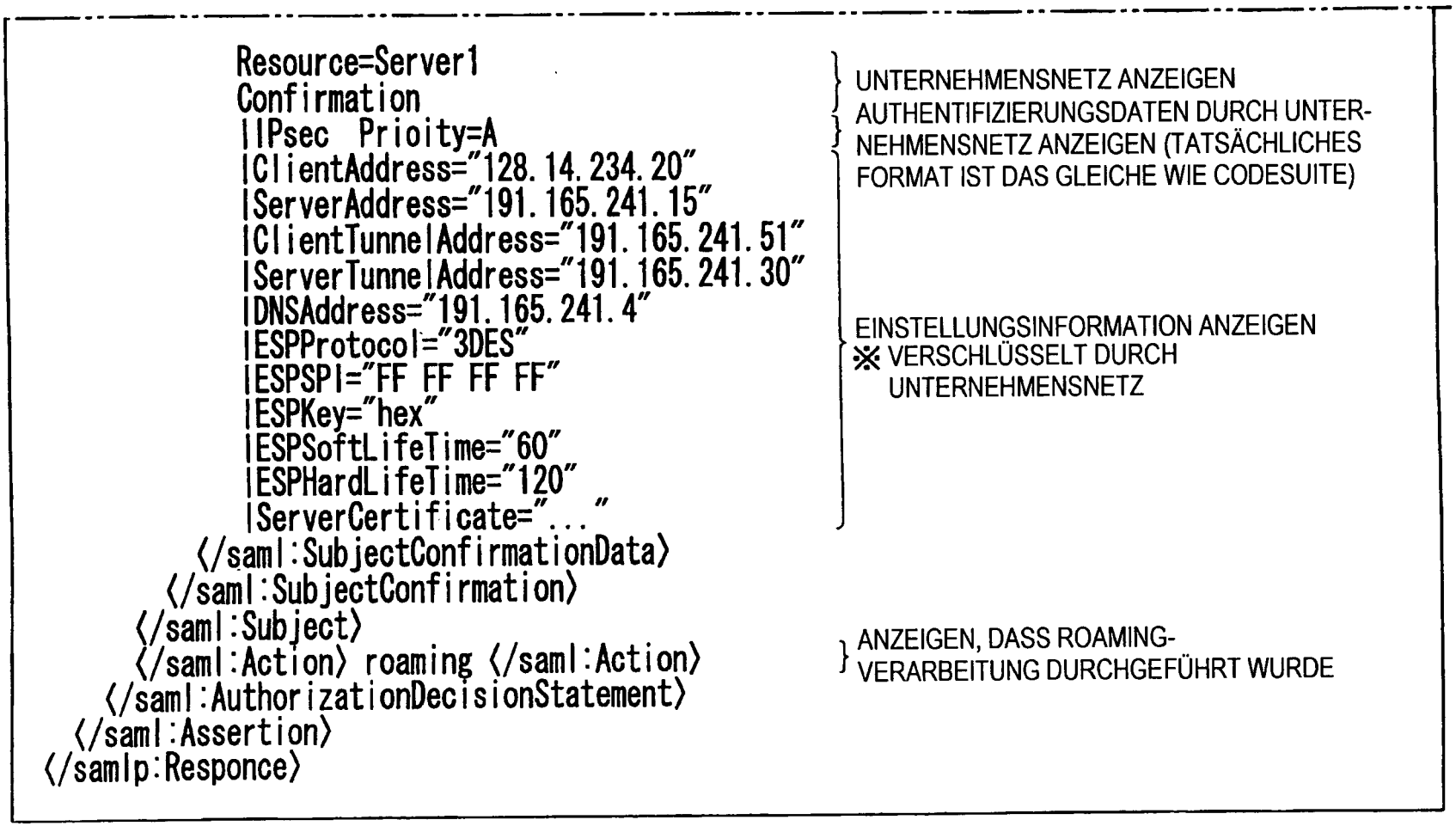

Resource=Server1
Confirmation
IIPsec Prioity=A
IClientAddress="128.14.234.20"
IServerAddress="191.165.241.15"
IClientTunnelAddress="191.165.241.51"
IServerTunnelAddress="191.165.241.30"
IDNSAddress="191.165.241.4"
IESPProtocol="3DES"
IESPSPI="FF FF FF FF"
IESPKey="hex"
IESPSoftLifeTime="60"
IESPHardLifeTime="120"
IServerCertificate="..."
〈/saml:SubjectConfirmationData〉
〈/saml:SubjectConfirmation〉
〈/saml:Subject〉
〈/saml:Action〉 roaming 〈/saml:Action〉
〈/saml:AuthorizationDecisionStatement〉
〈/saml:Assertion〉
〈/samlp:Responce〉
UNTERNEHMENSNETZ ANZEIGEN
AUTHENTIFIZIERUNGSDATEN DURCH UNTER-
NEHMENSNETZ ANZEIGEN (TATSÄCHLICHES
FORMAT IST DAS GLEICHE WIE CODESUITE)
EINSTELLUNGSINFORMATION ANZEIGEN
※ VERSCHLÜSSELT DURCH
UNTERNEHMENSNETZ
ANZEIGEN, DASS ROAMING-
VERARBEITUNG DURCHGEFÜHRT WURDE

FIG. 10A

FIG10
FIG10A
FIG10B

FORMAT VOM ELEKTRONISCHEN ZERTIFIKAT (ASN.1)

```
Certificate::=SEQUENCE {
        tbsCerticate            TBSCertificate,
        signatureAlgorithm      AlgorithmIdentifier,
        signatureValue          BIT STRING}

TBSCertificate::=SEQUENCE {
        Version                 EXPLICIT Version,
        serialNumber            CertificateSerialNumber,
        signature               AlgorithmIdentifier,
        issuer                  Name,
        validity                Valodity,
        subject                 Name,
        subjectPublicKeyInfo    SubjectPublicKeyInfo,
        extensions              EXPLICIT Extensions OPTIONAL}
        Version::=INTEGER {v1(0), v2(1), v3(2)}
        CertificateSerialNumber::=INTEGER
        Validity::=SEQUENCE {
                notBefore Time, notAfter Time}
                Time::=CHOICE {
                        utcTime UTCTime, generalTime GeneralizedTime}
        subjectPublicKeyInfo::=SEQUENCE {
                algorithm AlgorithmIdentifier, subjectPublicKey BIT STRING}
        Extensions::=SEQUENCE SIZE(1.MAX)OF Extension
```


DE 10 2004 045 147 A1 2006.03.23

FIG. 10B

```
Extension::=SEQUENCE {
                                        extnID    OBJECT IDENTIFIER,
                                        critical  BOOLEAN DEFAULT FALSE,
                                        roanconf  BOOLEAN DEFAULT TRUE,
                                        ssid      Name,
                                        extValue  RSextension}

RSExtension::=CHOICE {
                ipServices IpServices, vpnServices VpnServices}
ipServices::=SEQUENCE {
                permDestionations PermDestinations, day Days, daytime Daytime, pri Priority}
VpnServices::=SEQUENCE {
                permDestionations PermDestinations, day Days, daytime Daytime, pri Priority}
Days=::SET OF Day
Day::=ENUMERATED {
                Monday(0), Tuesday(1), wednesday(2), Thursday(3), Friday(4), Saturday(5), Sunday(6)}
Daytime=::SEQUENCE {
                notBeforeHour  Time, notAfterHour Time}
PermDistinations::=CHOICE {
                Server1(0), Server2(1), Server3(2), Server4(3)}
Priority::=CHOICE {
                S(0), A(1), B(2), C(3), Z(4)}
```

DIE FOLGENDE INFORMATIONEN DURCH VERWENDEN VON ERWEITERUNG VON X.509 VERSION 3 HINZUFÜGEN

- ROAMING-AUTOMATIK-EINSTELLUNGS-DIENSTBESTÄTIGUNG
- DRAHTLOSE LAN-SSID
- DIENSTBESTÄTIGUNGS-INFORMATION

DE 10 2004 045 147 A1 2006.03.23

FIG. 11

GESAMTER VERARBEITUNGSFLUSS (SS2) VOM SICHERHEITSSERVER (SS)

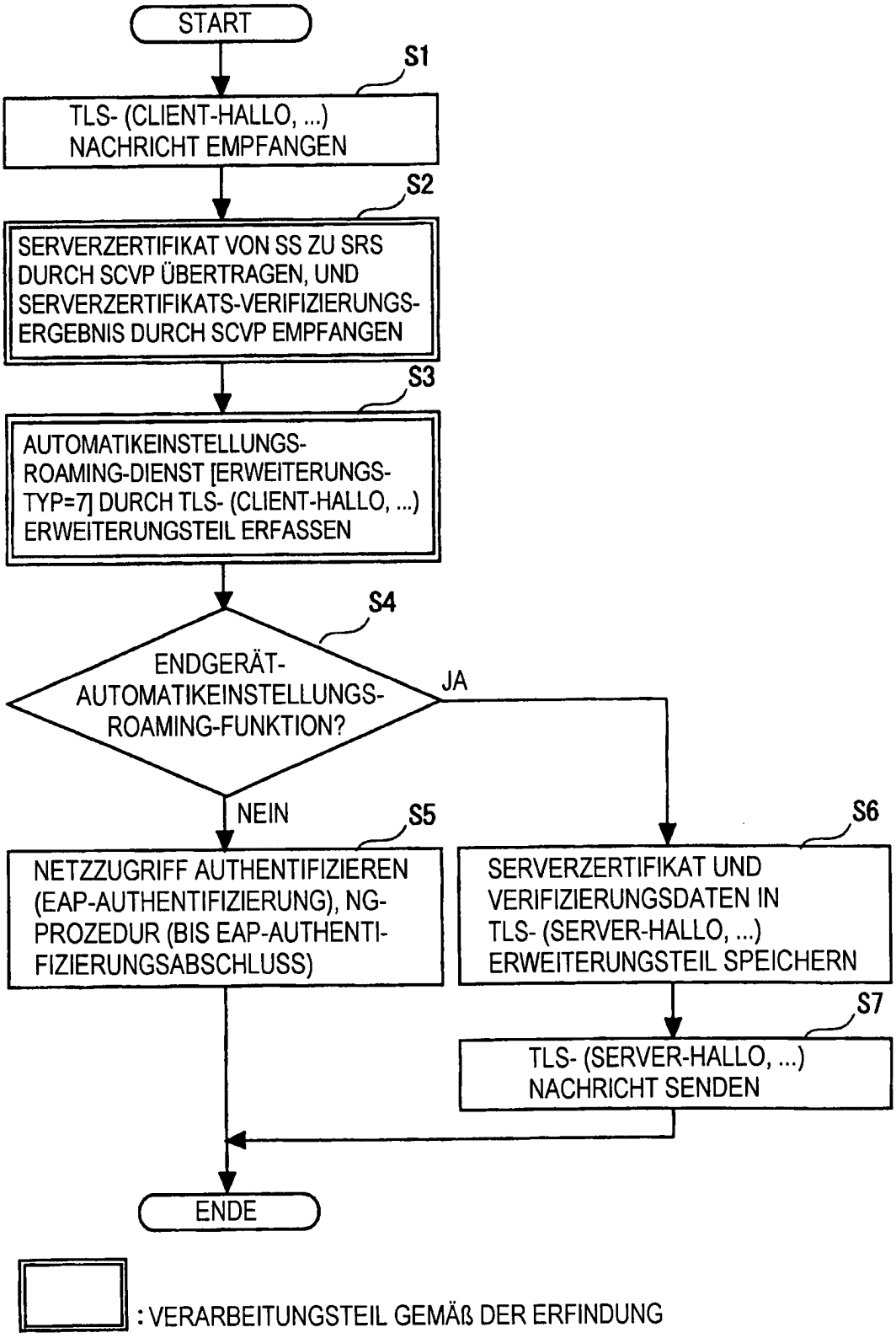


FIG. 12

GESAMTER VERARBEITUNGSFLUSS (SS2) VOM SICHERHEITSSERVER (SS)

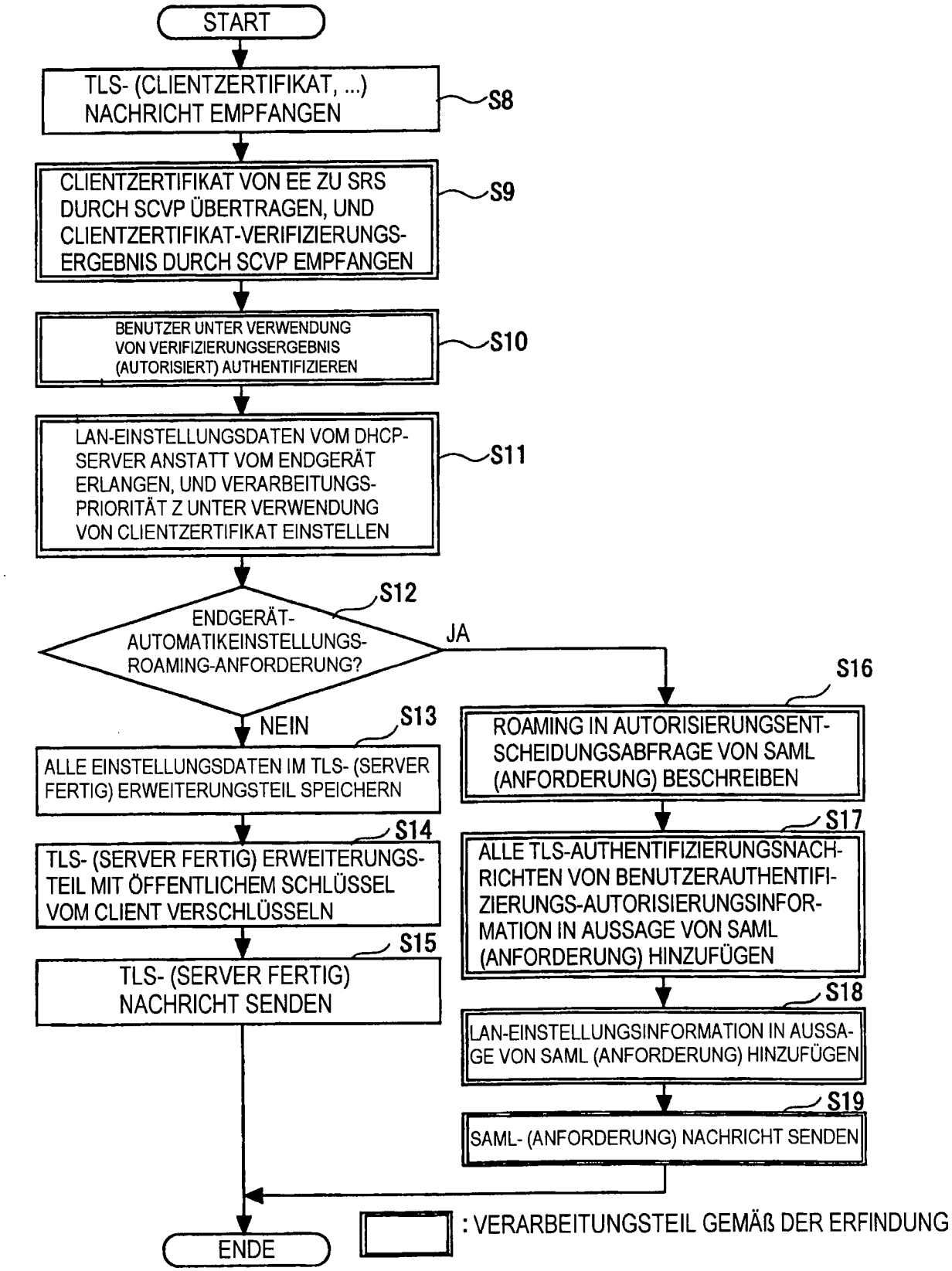
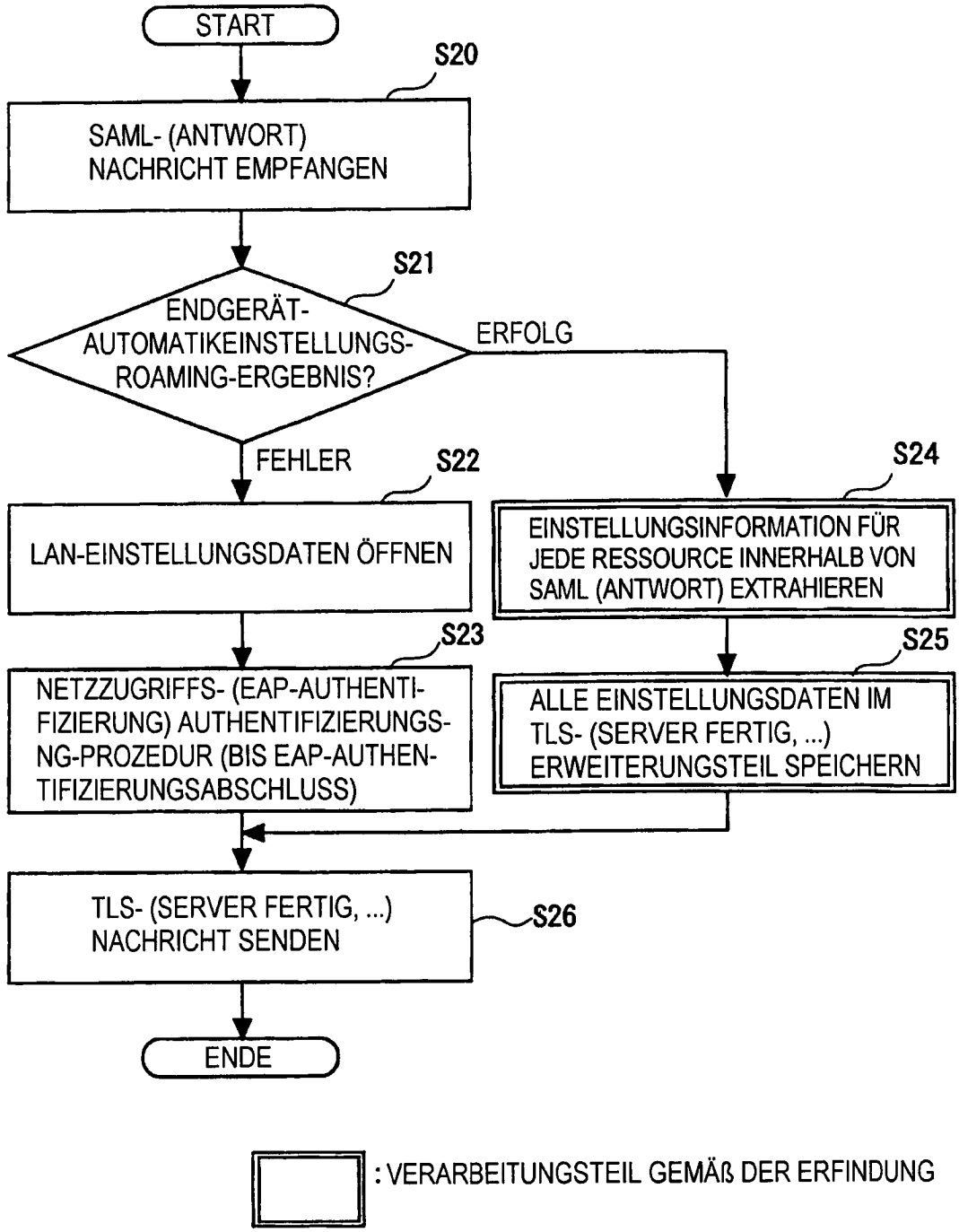


FIG. 13

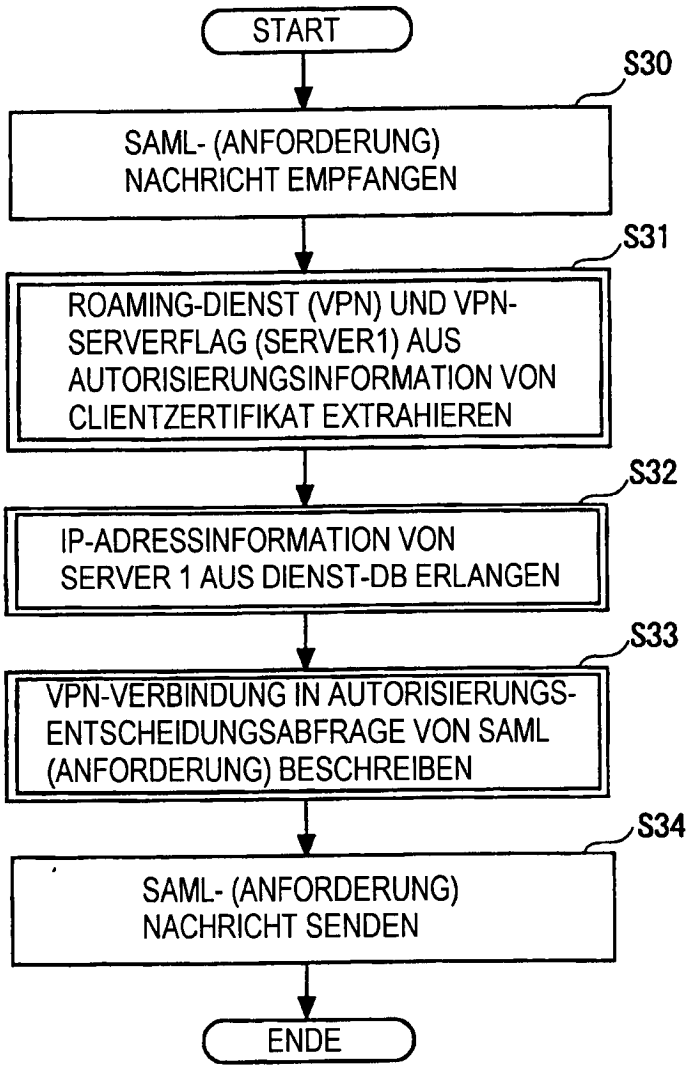
GESAMTER VERARBEITUNGSFLUSS (SS3) VOM SICHERHEITSSERVER (SS)



: VERARBEITUNGSTEIL GEMÄß DER ERFINDUNG

FIG. 14

GESAMTER VERARBEITUNGSFLUSS (SRS1) VOM SICHERHEITS-ROAMING-SERVER (SRS)



: VERARBEITUNGSTEIL GEMÄß DER ERFINDUNG

FIG. 15

GESAMTER VERARBEITUNGSFLUSS (SRS2) VOM SICHERHEITS-ROAMING-SERVER (SRS)

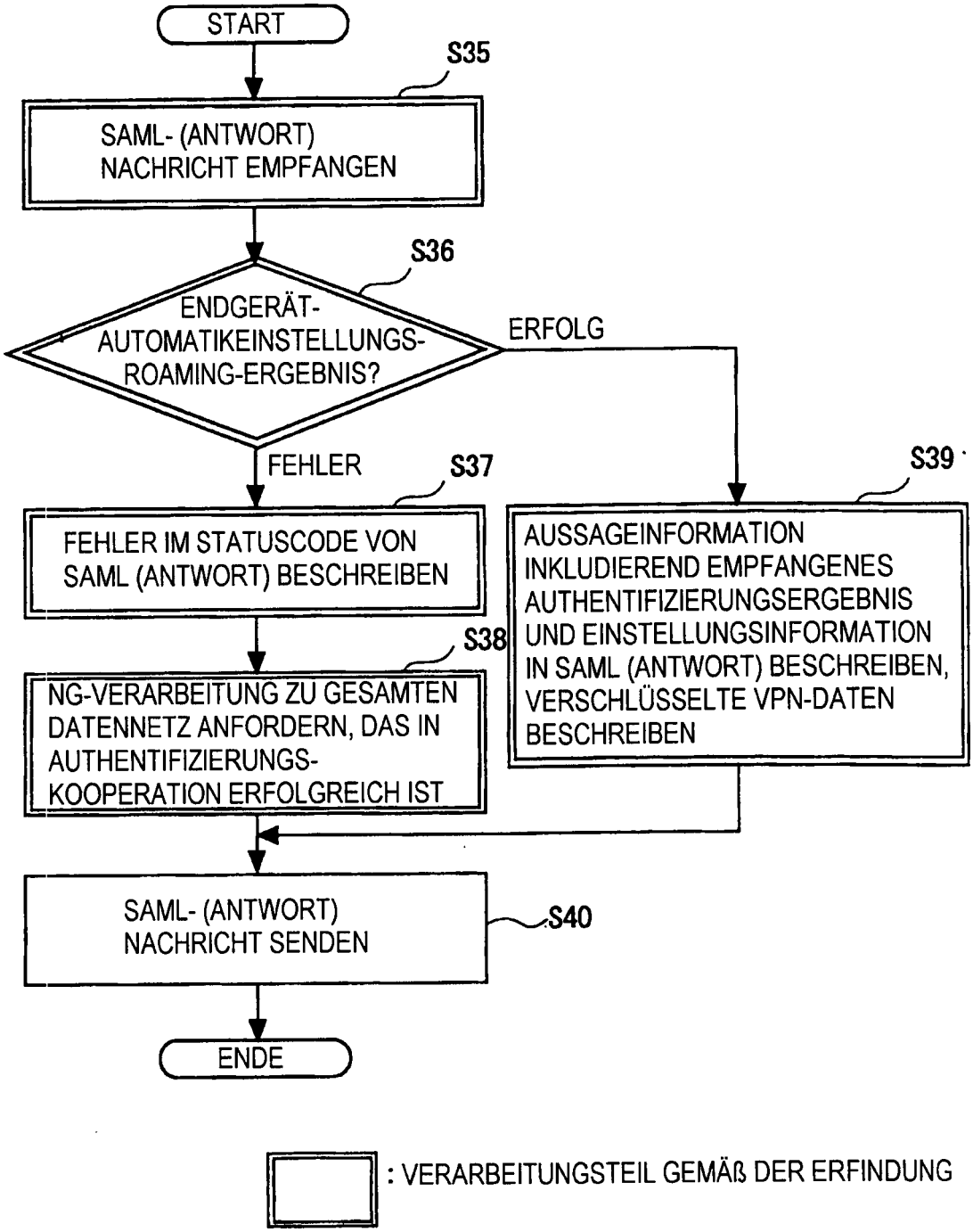
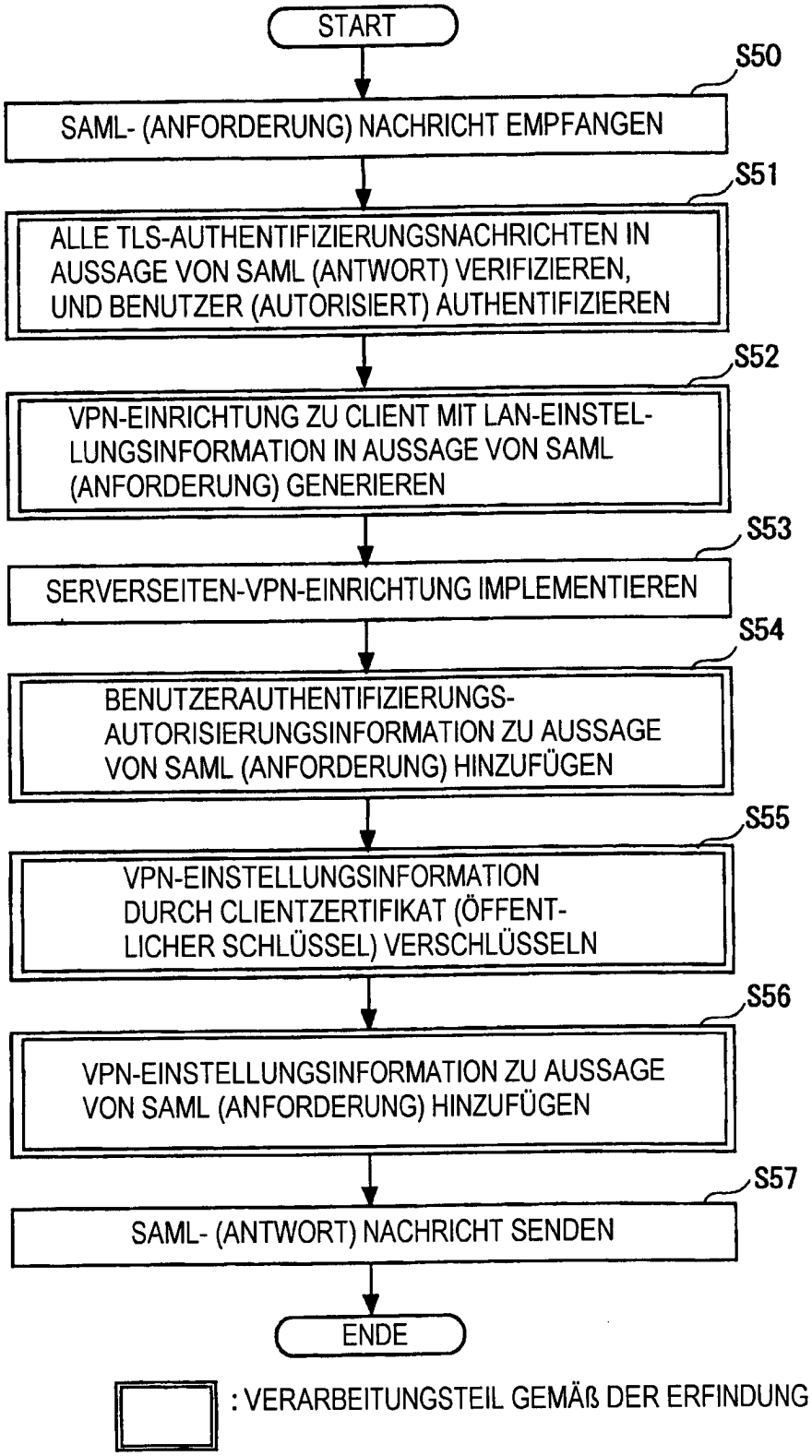


FIG. 16

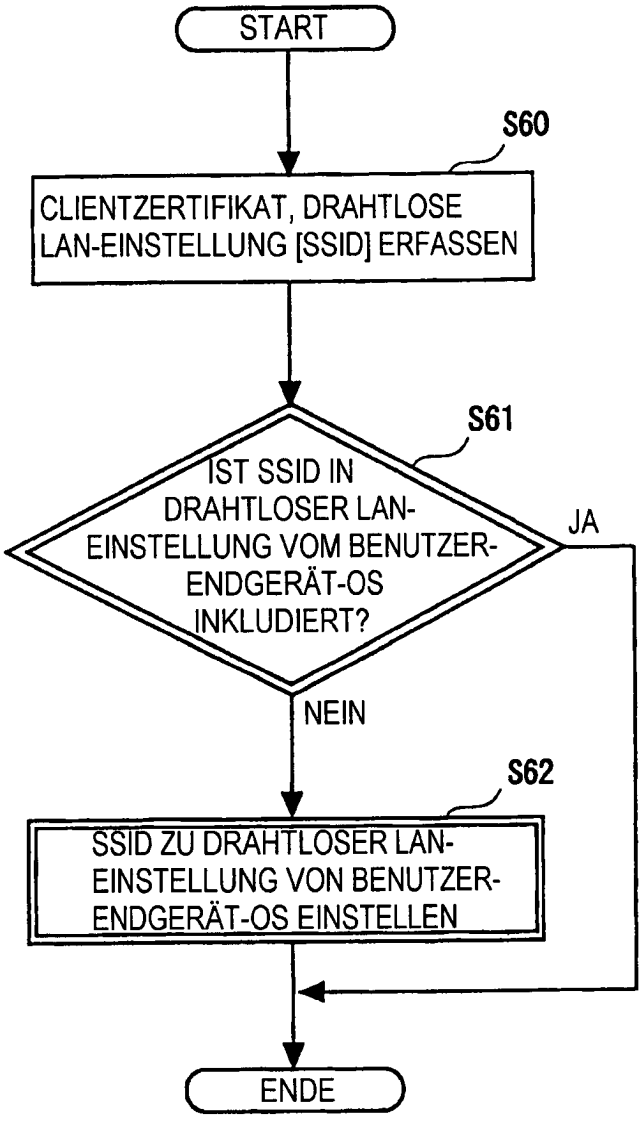
GESAMTER VERARBEITUNGSFLUSS (VPN) VOM VPN-GATEWAY-SERVER (VPN)



: VERARBEITUNGSTEIL GEMÄß DER ERFINDUNG

FIG. 17

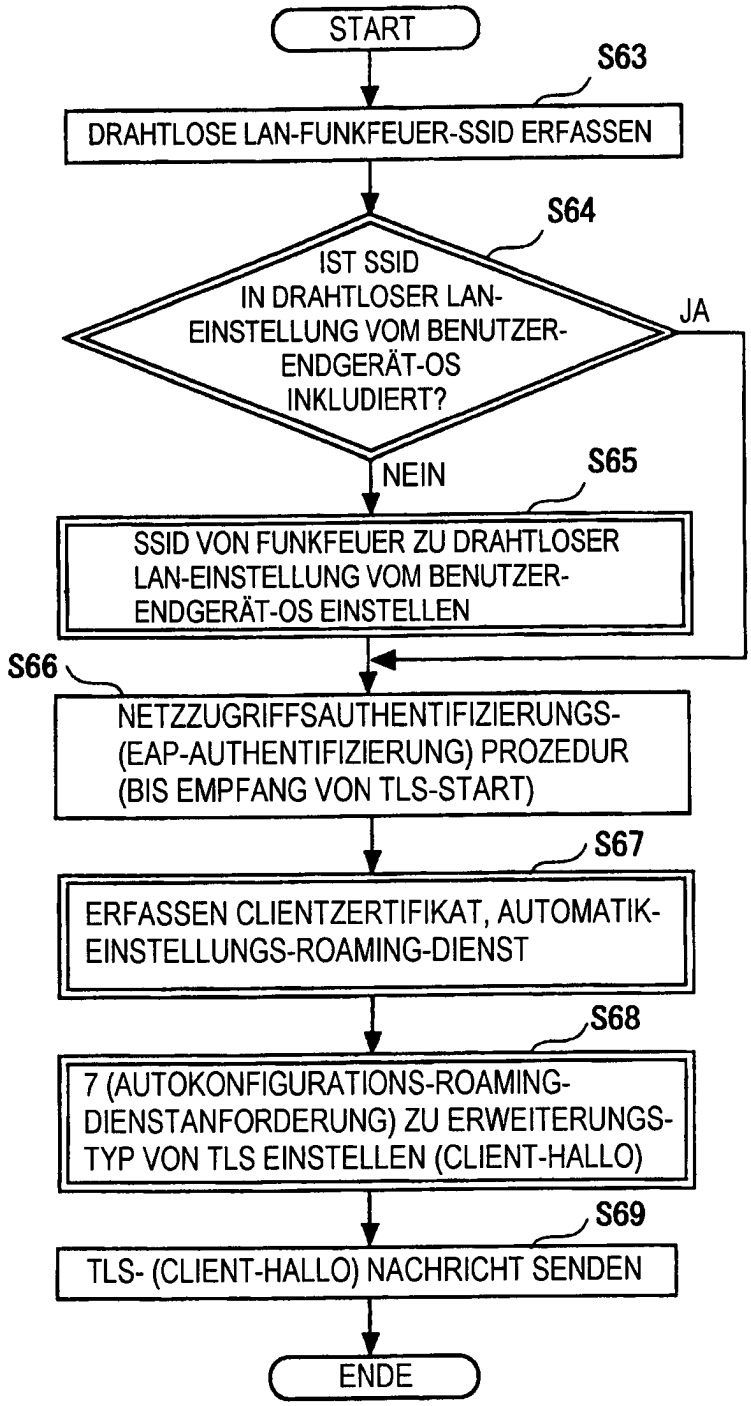
GESAMTER VERARBEITUNGSFLUSS (EE0) VOM ENDGERÄT (EE)



: VERARBEITUNGSTEIL GEMÄß DER ERFINDUNG

FIG. 18

GESAMTER VERARBEITUNGSFLUSS (EE1) VOM ENDGERÄT (EE)



: VERARBEITUNGSTEIL GEMÄß DER ERFINDUNG

FIG. 19

GESAMTER VERARBEITUNGSFLUSS (EE2) VOM ENDGERÄT (EE)

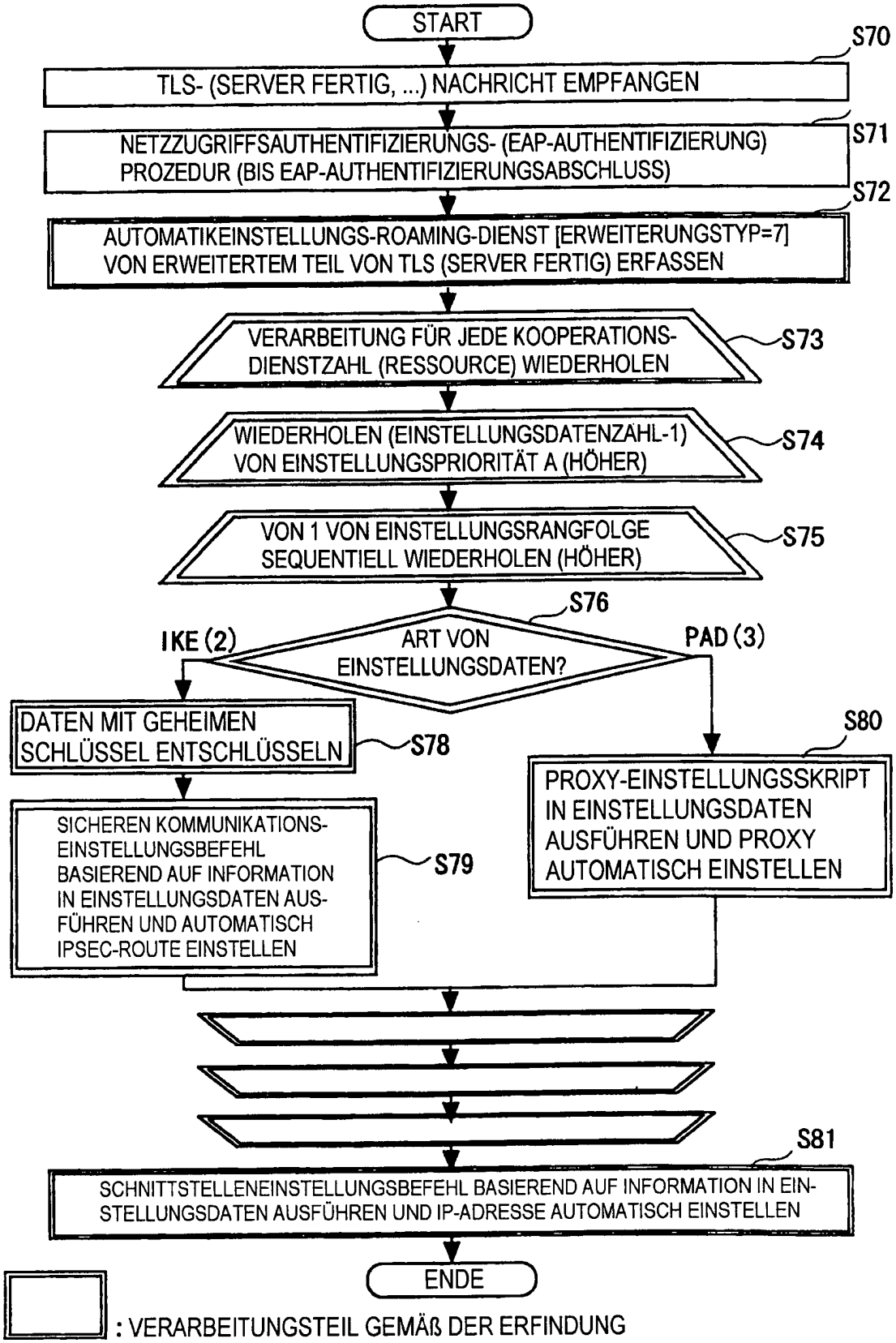
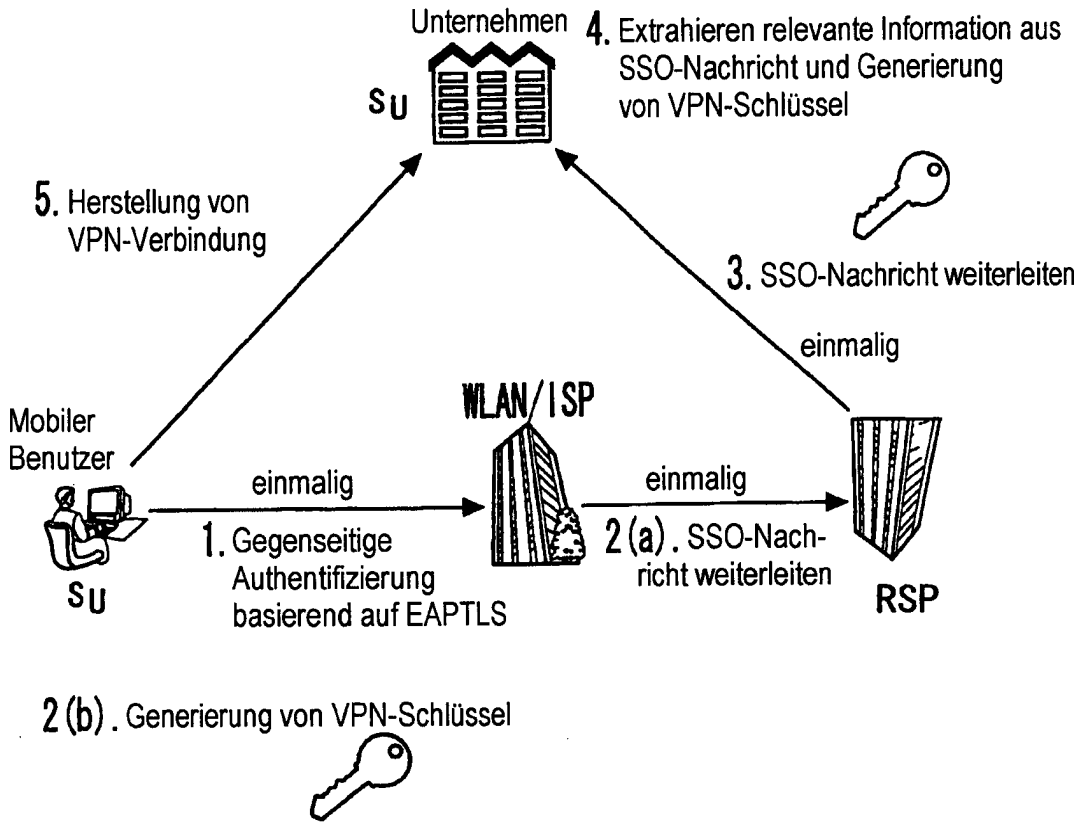


FIG. 20

VPN-SCHLÜSSELERSTELLUNGSSEQUENZ EINMALIG (BY NONCE)



INFORMATION, DIE IN AUTHENTIFIZIERUNGSNACHRICHTEN ENTHALTEN IST

: einmalig= $(id_U, time,$ Client_zufällig, Server_zufällig)

VPN-SCHLÜSSELERSTELLUNGSVERFAHREN: Schlüssel=Hash $(s_U,$ einmalig)

FIG. 21

VPN-FLAG	IP-ADRESSE VON VPN-GATEWAY-SERVER
1	10. 25. 192. 15
2	10. 25. 193. 11
3	10. 25. 194. 10
⋮	⋮

FIG. 22

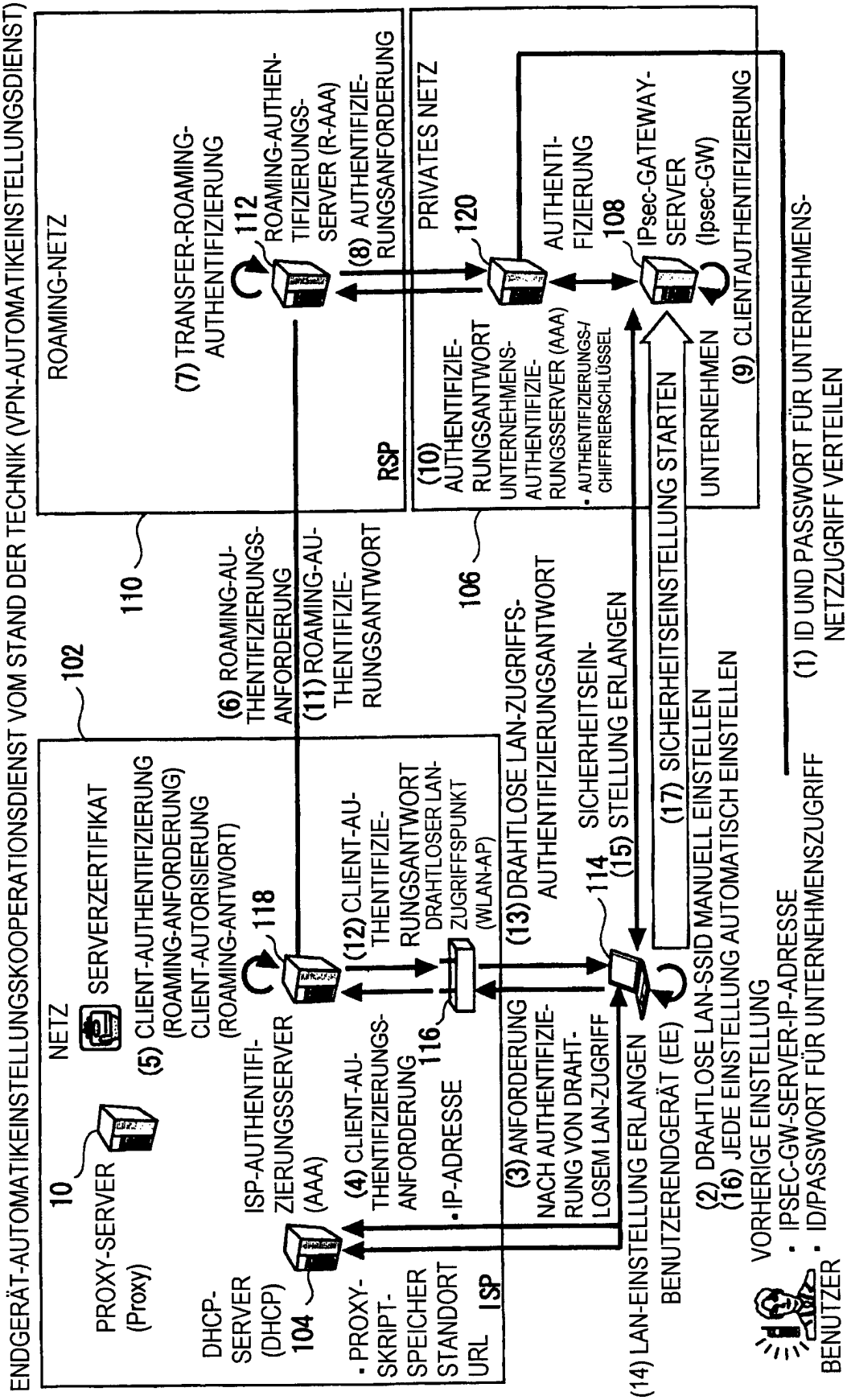

ENDGERÄT-AUTOMATIKEINSTELLUNGSKOOPERATIONSDIENST VOM STAND DER TECHNIK (VPN-AUTOMATIKEINSTELLUNGSDIENST)
ROAMING-NETZ
102
110
PRIVATES NETZ
RSP
106
PROXY-SERVER (Proxy)
10
NETZ
SERVERZERTIFIKAT
(5) CLIENT-AUTHENTIFIZIERUNG (ROAMING-ANFORDERUNG)
CLIENT-AUTORISIERUNG (ROAMING-ANTWORT)
DHCP-SERVER (DHCP)
104
ISP-AUTHENTIFIZIERUNGSSERVER (AAA)
118
• PROXY-SKRIPT-SPEICHER STANDORT URL
ISP
(4) CLIENT-AUTHENTIFIZIERUNGS-ANFORDERUNG
116
• IP-ADRESSE
(12) CLIENT-AUTHENTIFIZIERUNGSANTWORT
DRAHTLOSER LAN-ZUGRIFFSPUNKT (WLAN-AP)
(3) ANFORDERUNG NACH AUTHENTIFIZIERUNG VON DRAHTLOSEM LAN-ZUGRIFF
(6) ROAMING-AUTHENTIFIZIERUNGS-ANFORDERUNG
(11) ROAMING-AUTHENTIFIZIERUNGSANTWORT
(7) TRANSFER-ROAMING-AUTHENTIFIZIERUNG
112
ROAMING-AUTHENTIFIZIERUNGS-SERVER (R-AAA)
(8) AUTHENTIFIZIERUNGSANFORDERUNG
(10) AUTHENTIFIZIERUNGSANTWORT UNTERNEHMENS-AUTHENTIFIZIERUNGSSERVER (AAA)
• AUTHENTIFIZIERUNGS-/CHIFFRIERSCHLÜSSEL
120
(13) DRAHTLOSE LAN-ZUGRIFFS-AUTHENTIFIZIERUNGSANTWORT
114
(15) SICHERHEITSEINSTELLUNG ERLANGEN
(14) LAN-EINSTELLUNG ERLANGEN
BENUTZERENDGERÄT (EE)
AUTHENTIFIZIERUNG
108
IPsec-GATEWAY-SERVER (Ipsec-GW)
(17) SICHERHEITSEINSTELLUNG STARTEN
UNTERNEHMEN
(9) CLIENTAUTHENTIFIZIERUNG
(2) DRAHTLOSE LAN-SSID MANUELL EINSTELLEN
(16) JEDE EINSTELLUNG AUTOMATISCH EINSTELLEN
(1) ID UND PASSWORT FÜR UNTERNEHMENS-NETZZUGRIFF VERTEILEN
VORHERIGE EINSTELLUNG
• IPSEC-GW-SERVER-IP-ADRESSE
• ID/PASSWORT FÜR UNTERNEHMENSZUGRIFF
BENUTZER

FIG. 23A

FIG23 FIG23A-FIG23B

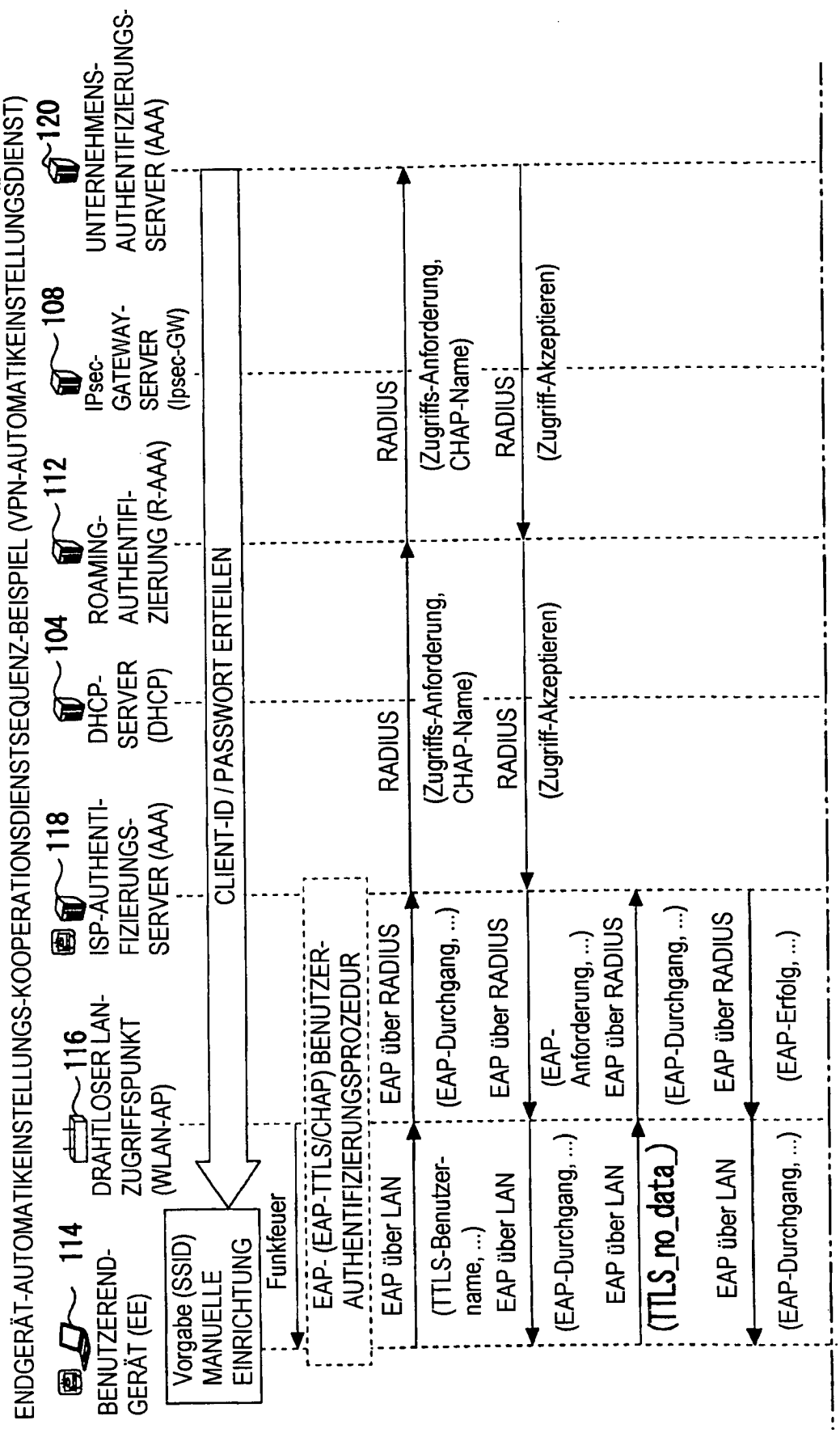
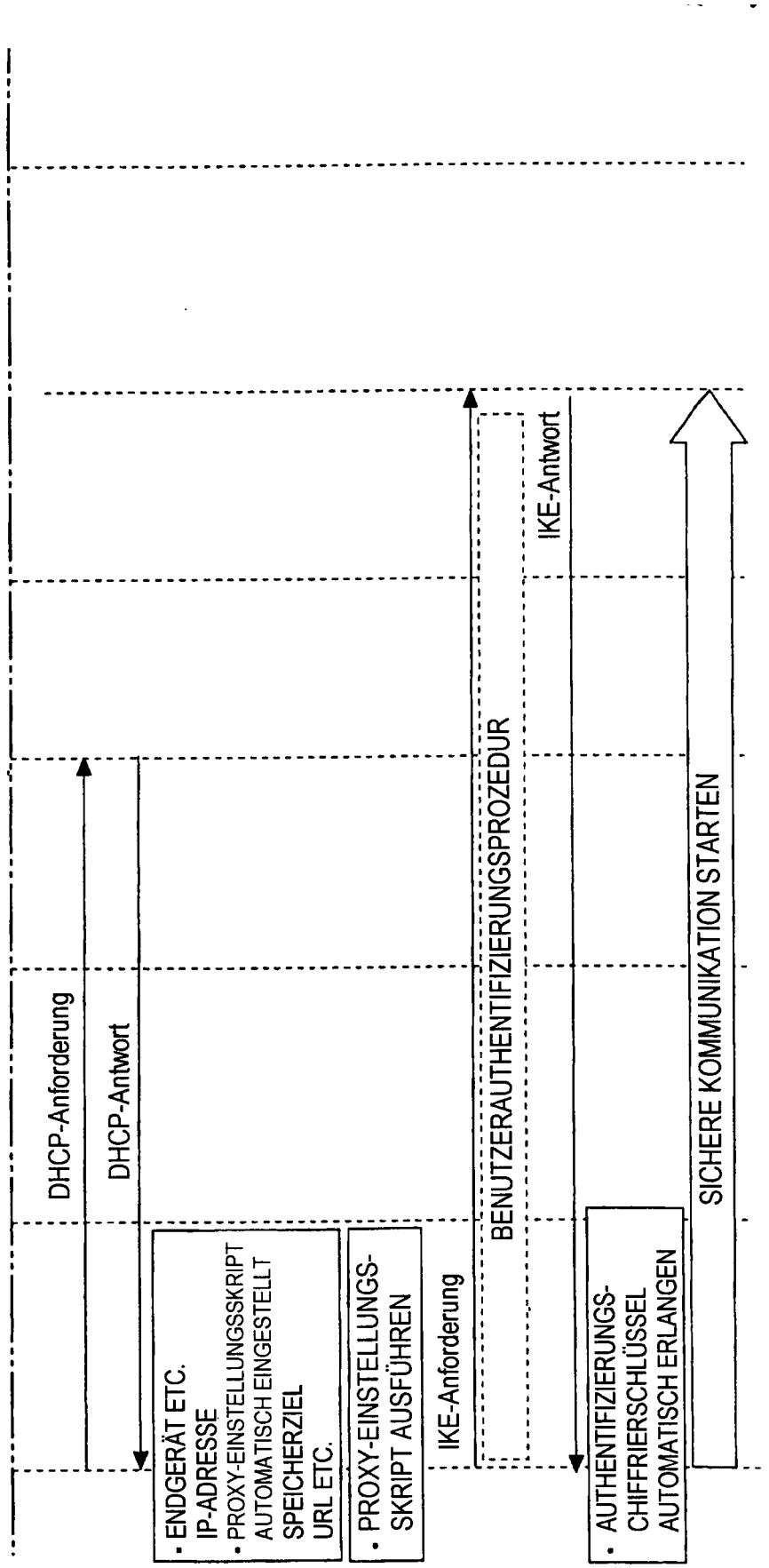


FIG. 23B


DHCP-Anforderung
DHCP-Antwort
• ENDGERÄT ETC.
IP-ADRESSE
• PROXY-EINSTELLUNGSSKRIPT
AUTOMATISCH EINGESTELLT
SPEICHERZIEL
URL ETC.
• PROXY-EINSTELLUNGS-
SKRIPT AUSFÜHREN
IKE-Anforderung
BENUTZERAUTHENTIFIZIERUNGSPROZEDUR
IKE-Antwort
• AUTHENTIFIZIERUNGS-
CHIFFRIERSCHLÜSSEL
AUTOMATISCH ERLANGEN
SICHERE KOMMUNIKATION STARTEN