



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 698 28 809 T2 2005.12.22**

(12)

Übersetzung der europäischen Patentschrift

(97) **EP 1 025 675 B1**

(51) Int Cl.⁷: **H04L 9/32**

(21) Deutsches Aktenzeichen: **698 28 809.2**

(86) PCT-Aktenzeichen: **PCT/FI98/00928**

(96) Europäisches Aktenzeichen: **98 955 634.5**

(87) PCT-Veröffentlichungs-Nr.: **WO 99/027678**

(86) PCT-Anmeldetag: **26.11.1998**

(87) Veröffentlichungstag

der PCT-Anmeldung: **03.06.1999**

(97) Erstveröffentlichung durch das EPA: **09.08.2000**

(97) Veröffentlichungstag

der Patenterteilung beim EPA: **26.01.2005**

(47) Veröffentlichungstag im Patentblatt: **22.12.2005**

(30) Unionspriorität:

974341 26.11.1997 FI

(84) Benannte Vertragsstaaten:

**AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT,
LI, LU, MC, NL, PT, SE**

(73) Patentinhaber:

Nokia Corp., Espoo, FI

(72) Erfinder:

LEIWO, Jussipekka, FIN-00420 Helsinki, FI

(74) Vertreter:

TBK-Patent, 80336 München

(54) Bezeichnung: **SICHERHEIT VON DATENVERBINDUNGEN**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

Gebiet der Erfindung

[0001] Die Erfindung betrifft die Sicherheit von Datenverbindungen bei mit Telefonnetzwerken verbundenen Datennetzwerken, insbesondere Mobiltelekommunikationsnetzwerken.

Hintergrund der Erfindung

[0002] Eine Anordnung zur Verbindung eines Mobilkommunikationsteilnehmers mit Datendiensten ist in [Fig. 1](#) gezeigt. Gemäß der Figur hat der Teilnehmer seinen PC (persönlichen Computer) mit seiner GSM-Mobilstation MS verbunden. Die MS hat eine Verbindung mit einer Basissende-/Empfangsstation BTS des GSM-Netzwerks aufgebaut. Die BTS leitet die durch die MS gesendeten Daten an die Basisstationssteuereinrichtung BSC weiter, die wiederum die Informationen an das Mobilvermittlungszentrum MSC weiterleitet. Das MSC ist mit dem privaten Datennetzwerk des die LAN-Zugangseinheit verwendenden Betreibers verbunden. In dem privaten Netzwerk stellt die intelligente Datenvermittlungseinrichtung IDA eine Intelligenz für Zwecke wie etwa Rechnungsstellung sowie Betrieb und Wartung von Datenverbindungen bereit. Das private Netzwerk ist mit anderen Netzwerken wie etwa ATM-Netzwerken (Asynchronous Transfer Mode – asynchrone Übertragungsbetriebsart), X.21-Netzwerken, FR-Netzwerken (Frame Relay – Datenrahmenweiterleitung) und dem Internet verbunden.

[0003] Eine Anordnung, wodurch der Teilnehmer die durch eine Dienstbereitstellungsvorrichtung (Server) in einem anderen privaten Netzwerk bereitgestellten Dienste verwendet, ist in [Fig. 2](#) gezeigt. Gemäß der Figur ist das zweite private Netzwerk mit dem Betreiber Netzwerk über ein schlichtendes Netzwerk oder eine Vielzahl von schlichtenden Netzwerken verbunden. Wenn das private Netzwerk beispielsweise ein privates Unternehmensnetzwerk ist, muss die Sicherheit der Datenverbindung von dem Teilnehmer zum Server durchgesetzt werden. Das GSM-System stellt eine Authentisierung sowie eine sichere Datenübertragung zwischen dem Mobilteilnehmer MS und dem Mobilvermittlungszentrum MSC bereit.

[0004] Bei GSM basiert der Authentisierungsvorgang auf einem Aufforderung-Antwort-Ablauf, wodurch das Netzwerk dem in der Mobilstation installierten Teilnehmeridentitätsmodul SIM eine zufällige Aufforderung sendet. Die Mobilstation reagiert mit einer Antwort gemäß auf der zufälligen Aufforderung basierten Berechnungen sowie einem lediglich dem Authentisierungszentrum des Netzwerks und der SIM bekannten geheimen Schlüssel. Die Antwort auf die zufällige Aufforderung und der Geheimschlüssel wird

ebenfalls in dem Authentisierungszentrum berechnet. Falls die durch die SIM und das Authentisierungszentrum berechneten Antworten identisch sind, wurde die Authentität des Mobilteilnehmers durch den Authentisierungsvorgang bestätigt.

[0005] Eine Datenübertragung zwischen der Basisstation und der Mobilstation wird mit einem auf der Basis der zufälligen Aufforderung und dem Geheimschlüssel berechneten geheimen Chiffrierschlüssel verschlüsselt. Dieses Verfahren der Verschlüsselung mit geheimen Schlüssel, das auch symmetrisches Verschlüsselungsverfahren genannt wird, ist nachstehend näher beschrieben.

[0006] Ein Verfahren zur Organisation und Verwendung von Geheimschlüsseln ist aus der Druckschrift GB-A-2287160 bekannt.

[0007] Obwohl angenommen werden kann, dass die GSM-Verbindungen sicher sind, ist die Verbindung zwischen dem Teilnehmer und dem Server unsicher, falls über das schlichtende Netzwerk keine Authentisierung und Verschlüsselung verwendet werden.

[0008] Eine Vielzahl von Verfahren zur Sicherung einer Verbindung zwischen zwei Netzwerkelementen ist aus dem Stand der Technik bekannt. Die [Fig. 3](#) und [Fig. 4](#) der beiliegenden Zeichnung zeigen Blockschaltbilder von zwei bekannten Verschlüsselungsalgorithmen, die zum Schutz einer Übertragung verwendet werden können: ein symmetrischer und ein asymmetrischer Algorithmus.

[0009] [Fig. 3](#) zeigt einen symmetrischen Verschlüsselungsvorgang auf der Grundlage eines zwischen den Teilnehmern gemeinsam genutzten Geheimschlüssels. Auf der Seite der Partei A wird die an die Partei B zu sendende Nachricht mit dem gemeinsam genutzten Geheimschlüssel verschlüsselt. Die Nachricht wird über eine Übertragungsrouten in verschlüsselter Form gesendet. Die empfangende Partei B entschlüsselt die verschlüsselte Nachricht mit demselben Geheimschlüssel K, um die Originalnachricht zu erhalten. Ein die Übertragung abhörender Eindringling muss den Geheimschlüssel erfahren, um in der Lage zu sein, die verschlüsselte Nachricht zu lesen und zu verstehen, die übertragen wurde. Eine andere Alternative ist, eine Schwachstelle im Algorithmus selbst zu finden. Daher ist die Verwendung von öffentlich analysierten Algorithmen wie etwa dem DES-Algorithmus (Data Encryption Standard – Datenverschlüsselungsstandard) vorzuziehen. Die Verschlüsselung und Entschlüsselung des symmetrischen Vorgangs kann durch die nachstehend angeführten Gleichungen ausgedrückt werden:

$$C = E_K(M), \text{ und}$$

$$M = D_K(C),$$

wobei C die verschlüsselte Nachricht bezeichnet, M die Nachricht in Klartext bezeichnet, E_K die Verschlüsselung mit dem Schlüssel K bezeichnet, und D_K die Entschlüsselung mit dem Schlüssel K bezeichnet.

[0010] [Fig. 4](#) zeigt einen Verschlüsselungsvorgang mit einem öffentlichen Schlüssel als asymmetrischen Ansatz. Dieser Algorithmus basiert auf zwei Schlüsseln: einem öffentlichen Schlüssel und einem privaten Schlüssel. Diese beiden Schlüssel stehen derart in Bezug zueinander, dass eine mit einem öffentlichen Schlüssel verschlüsselte Nachricht lediglich mit dem entsprechenden privaten Schlüssel entschlüsselt werden kann und umgekehrt. Der öffentliche Schlüssel kann leicht unter Verwendung des entsprechenden privaten Schlüssels berechnet werden. Es ist jedoch computertechnisch nicht machbar, einen privaten Schlüssel auf der Grundlage des entsprechenden öffentlichen Schlüssels zu berechnen. Gemäß [Fig. 4](#) wird eine Nachricht auf der Seite der Partei A mit dem öffentlichen Schlüssel des gewünschten Empfängers, d.h. Partei B, verschlüsselt. Die verschlüsselte Nachricht wird über eine Übertragungsleitung zu der Partei B hin übertragen, wo sie mit dem entsprechenden privaten Schlüssel der Partei B entschlüsselt wird, und die ursprüngliche Nachricht erhalten wird. Auch hier werden öffentlich analysierte Algorithmen wie etwa der RSA-Algorithmus (Rivest-Shamir-Adleman) bevorzugt.

[0011] Die Verschlüsselung und Entschlüsselung des asymmetrischen Algorithmus kann auch durch die nachstehend wiedergegebenen Gleichungen ausgedrückt werden:

$$C = E_B^+(M), \text{ und}$$

$$M = D_B^-(C),$$

wobei C die verschlüsselte Nachricht bezeichnet, M die Nachricht in Klartext bezeichnet, E_B^+ die Verschlüsselung mit dem öffentlichen Schlüssel des Empfängers K_B^+ bezeichnet, und D_B^- die Entschlüsselung mit dem privaten Schlüssel des Empfängers K_B^- bezeichnet. Aufgrund der Eigenschaften der Verschlüsselungsfunktion E ist es computertechnisch nicht machbar, eine unter Verwendung des öffentlichen Schlüssels des Empfängers verschlüsselte Nachricht zu entschlüsseln, falls der private Schlüssel nicht bekannt ist.

[0012] Da asymmetrische Schlüssel üblicher Weise viel länger als symmetrische Schlüssel sind, erfordern die asymmetrischen Algorithmen viel mehr Verarbeitungskapazität. Somit sind asymmetrische Algorithmen zur Verschlüsselung von großen Datenmengen ungeeignet, da der Vorgang bezüglich des öf-

fentlichen Schlüssels zu langsam für Netzwerke sein kann, die sehr hohe Übertragungsgeschwindigkeiten ermöglichen.

[0013] Eine hybride Kryptographie verwendet die beiden vorstehend beschriebenen Algorithmen zusammen. Es werden beispielsweise lediglich Einmalschlüssel unter Verwendung des Algorithmus bezüglich des öffentlichen Schlüssels ausgetauscht, und der Rest der Kommunikation wird unter Anwendung des symmetrischen Verfahrens verschlüsselt.

[0014] Bei einem Algorithmus bezüglich eines öffentlichen Schlüssels wirkt die Verschlüsselung einer Nachricht mit dem privaten Schlüssel des Nachrichtenabsenders als digitale Signatur, da jeder die Nachricht mit dem bekannten öffentlichen Schlüssel des Absenders entschlüsseln kann. Dieses Merkmal kann zur Bereitstellung einer Nachrichtenintegrität und -Authentisierung bei einer Verbindung verwendet werden. Die Verwendung von digitalen Signaturen ist in den [Fig. 5](#) und [Fig. 6](#) gezeigt.

[0015] Der Ablauf zur Erzeugung einer digitalen Signatur ist in [Fig. 5](#) gezeigt. Der Absender berechnet aus der Nachricht einen Nachrichtenextrakt unter Verwendung einer kryptographisch starken Einweg-Hash-Funktion. Der Nachrichtenextrakt ist irgendwie analog zu den in der Telekommunikation weit verbreiteten Fehlerprüfcodes. Im Gegensatz zu den Fehlerprüfcodes wird jedoch angenommen, dass es computertechnisch nicht machbar ist, eine Nachricht mit einer anderen zu ersetzen, so dass ein identischer Nachrichtenextrakt erzeugt wird.

[0016] Der Nachrichtenextrakt wird unter Verwendung des privaten Schlüssels des Absenders verschlüsselt, und der verschlüsselte Nachrichtenextrakt wird als digitale Signatur verwendet. Die digitale Signatur wird sodann an den Empfänger zusammen mit der Nachricht gesendet.

[0017] Der Ablauf zur Verifizierung einer digitalen Signatur für die empfangene Partei ist in [Fig. 6](#) gezeigt. Nach dem Empfang der Nachricht der digitalen Signatur berechnet der Empfänger den Nachrichtenextrakt der Nachricht unter Verwendung des Nachrichtenextraktalgorithmus. Falls in der Nachricht keine Abwandlungen auftraten, ist der resultierende Nachrichtenextrakt identisch zu dem durch den Absender berechneten Nachrichtenextrakt. Andererseits wäre es aufgrund der Eigenschaften des Algorithmus für einen Eindringling computertechnisch nicht machbar, die Nachricht mit einer anderen zu ersetzen, die einen identischen Nachrichtenextrakt erzeugen würde.

[0018] Die empfangene digitale Signatur ist der unter Verwendung des privaten Schlüssels des Absenders verschlüsselte Nachrichtenextrakt. Der Nach-

richtenextrakt kann somit durch Entschlüsseln der digitalen Signatur unter Verwendung des öffentlichen Schlüssels des Absenders erhalten werden, der dem Empfänger bekannt ist. Falls die Entschlüsselung unter Verwendung des privaten Schlüssels stattfand, der dem öffentlichen Schlüssel des vermuteten Absenders entspricht, wird der wiederhergestellte Nachrichtenextrakt zu dem durch den Absender berechneten Nachrichtenextrakt identisch sein. Dieser wiederum ist nur dann identisch zu dem durch den Empfänger berechneten Nachrichtenextrakt, wenn keine Änderungen in der Nachricht auftraten. Falls der Vergleich zeigt, dass der aus der empfangenen Nachricht berechnete Nachrichtenextrakt und der durch Entschlüsseln der digitalen Signatur berechnete Nachrichtenextrakt identisch sind, kann somit gefolgert werden, dass die Nachricht nicht abgewandelt wurde, und dass sie von dem behaupteten Absender gesendet wurde.

[0019] Bei der Methodik der Geheimschlüsselchiffrierung kann eine Nachrichtenauthentisierung unter Verwendung eines zu der digitalen Signatur ähnlichen Nachrichtenauthentizitätscodes MAC (Message Authentication Code) bereitgestellt werden. Der MAC kann beispielsweise mit einem Einweg-Hash-Algorithmus auf die nachstehend angegebene Weise berechnet werden:

$$\text{MAC} = H(K, M, K),$$

wobei K den Schlüssel bezeichnet, M die Nachricht bezeichnet, und H eine Hash-Funktion bezeichnet. Die Eingabe kann aus der Ausgabe geschlossen werden. Wenn ein MAC einer Nachricht angefügt wird, kann die Nachricht nicht korumpiert oder personifiziert werden. Die empfangende Partei berechnet den MAC unter Verwendung der empfangenen Nachricht und derselben Hash-Funktion bzw. desselben Schlüssels wie die übertragende Partei und vergleicht dann diesen berechneten MAC mit dem an die Nachricht angefügten MAC zur Verifizierung.

[0020] Bei der vorliegenden Anmeldung wird der Begriff „Authentizitätscode“ als gemeinsamer Name für alle eine Nachricht mit Authentizität und Integrität bereitstellende Codes verwendet, d.h. sowohl für digitale Signaturen als auch für Nachrichtenauthentizitätscodes.

[0021] Der Stand der Technik stellt eine Einrichtung zur Sicherung einer Datenverbindung vom Teilnehmer zum GSM-Netzwerk sowie von dem privaten Netzwerk des Betreibers zu einem anderen privaten Netzwerk wie etwa ein Unternehmensnetzwerk bereit, wie in [Fig. 7](#) dargestellt ist. Das Betreibernetzwerk kann jedoch durch eine Vielzahl von Benutzern verwendet werden, von denen nicht alle eine Berechtigung für die Dienste des Unternehmensnetzwerks aufweisen. Im Stand der Technik muss ihr Zugriff auf

das Unternehmensnetzwerk unter Verwendung eines Passwort-basierten Authentisierungsablaufs zwischen dem Teilnehmer und dem Unternehmensnetzwerk verweigert werden. Dies ist unbequem, weil das Passwort übertragen werden muss, wann immer die Verbindung aufgebaut wird.

[0022] Die Aufgabe der Erfindung ist die Lösung des vorstehend beschriebenen Problems. Diese Aufgabe wird unter Verwendung des in den unabhängigen Patentansprüchen definierten Verfahrens bzw. Gerätes erzielt.

Erfindungszusammenfassung

[0023] Die Grundidee der Erfindung ist die Weiterleitung der Authentisierung des Telefonsystems an die Teilstrecke zwischen den privaten Netzwerken. Erfindungsgemäß umfasst ein mit dem Telefonsystem verbundenes zuverlässiges Betreibernetzwerk einen Authentisierungsserver. Auch ein zweites privates Netzwerk, das vorliegend Unternehmensnetzwerk genannt wird, umfasst einen ähnlichen Authentisierungsserver.

[0024] Der Authentisierungsablauf wird initiiert, wenn der Teilnehmer einen durch einen Server in dem Unternehmensnetzwerk bereitgestellten Dienst anfragt. Während dieses Ablaufs signiert der Authentisierungsserver AS_O des Betreibernetzwerks eine authentifizierte Kennung des Teilnehmers in digitaler Weise unter Verwendung seines eigenen privaten Schlüssels und bildet eine Nachricht mit der Kennung und der Signatur. Ein Beispiel einer für den Zweck zur Identifizierung des Teilnehmers geeigneten Kennung ist die MSISDN-Nummer (Mobile Subscriber Integrated Services Digital Network – Digitalnetzwerk mit integrierten Diensten für Mobilteilnehmer) des Teilnehmers. Die Signatur bestätigt die Authentizität der Nachricht. Vorzugsweise wird die Nachricht zusätzlich unter Verwendung des öffentlichen Schlüssels des Authentisierungsservers AS_C des Unternehmensnetzwerks verschlüsselt. Die Verschlüsselung verhindert eine Identifizierung des einen diensteanfragenden Benutzers durch einen abhörenden Punkt. Die signierte und verschlüsselte Nachricht wird an den Authentisierungsserver des Unternehmensnetzwerks über das schlichtende Netzwerk gesendet.

[0025] Der Authentisierungsserver des Unternehmensnetzwerks empfängt die Nachricht und verifiziert die Signatur, um die Authentizität der Nachricht zu bestätigen. Falls eine Verschlüsselung verwendet wurde, wird die Nachricht unter Verwendung des privaten Schlüssels des AS_C entschlüsselt. Der Authentisierungsserver überprüft die Rechte des Teilnehmers an dem Datendienst, und falls der Teilnehmer zu dem Dienst berechtigt ist, erzeugt es den in der Verbindung zu verwendenden Einmalschlüssel. Eine Nachricht mit dem Einmalschlüssel wird an das

Betreibernetzwerk bevorzugt verschlüsselt unter Verwendung des öffentlichen Schlüssels von AS_O und vorzugsweise unter Verwendung des privaten Schlüssels von AS_C signiert an das Betreibernetzwerk übertragen. Zudem wird der Einmalschlüssel an den Server übermittelt.

[0026] AS_O empfängt den verschlüsselten und signierten Einmalschlüssel, entschlüsselt den Schlüssel unter Verwendung seines eigenen privaten Schlüssels und verifiziert die Authentizität des Schlüssels unter Verwendung des öffentlichen Schlüssels von AS_C. Falls der Authentisierungsablauf erfolgreich ist, wird der Einmalschlüssel an das die Verschlüsselung des Datenverkehrs handhabende Netzwerkelement übertragen, und der Datenverkehr beginnt.

Kurzbeschreibung der Zeichnung

[0027] Die Erfindung wird nachstehend unter Bezugnahme auf die beiliegende schematische Zeichnung näher beschrieben. Es zeigen:

[0028] [Fig. 1](#) ein Mobiltelekommunikationssystem, das mit Datennetzwerken verbunden ist;

[0029] [Fig. 2](#) zwei private Datennetzwerke, die über schlichtende Netzwerke verbunden sind;

[0030] [Fig. 3](#) einen symmetrischen Verschlüsselungsablauf;

[0031] [Fig. 4](#) einen Verschlüsselungsablauf auf der Grundlage eines öffentlichen Schlüssels;

[0032] [Fig. 5](#) die Erzeugung einer digitalen Signatur;

[0033] [Fig. 6](#) die Verifikation einer digitalen Signatur;

[0034] [Fig. 7](#) ein Authentisierungsverfahren;

[0035] [Fig. 8](#) zwei private Datennetzwerke, die über schlichtende Netzwerke verbunden sind;

[0036] [Fig. 9](#) einen Authentisierungsablauf;

[0037] [Fig. 10](#) einen Verschlüsselungsablauf;

[0038] [Fig. 11](#) eine weitergeleitete Authentisierung;

[0039] [Fig. 12](#) eine sichere Datenübertragung;

[0040] [Fig. 13](#) den Authentisierungsserver des Betreibernetzwerks; und

[0041] [Fig. 14](#) den Authentisierungsserver des Unternehmensnetzwerks.

Ausführliche Beschreibung der Erfindung

[0042] [Fig. 8](#) zeigt zwei Netzwerke, ein Betreiber-netzwerk und ein Unternehmensnetzwerk, die miteinander über ein schlichtendes Netzwerk verbunden sind. Das Betreibernetzwerk ist mit dem Benutzer über ein Telefonsystem wie etwa das GSM-System verbunden. Sowohl bei dem Betreibernetzwerk als auch bei dem Unternehmensnetzwerk wurden Authentisierungsserver hinzugefügt. Die Server werden AS_O (Authentisierungsserver im Betreibernetzwerk) und AS_C (Authentisierungsserver im Unternehmensnetzwerk) genannt. Zudem sind die Authentisierungsserver im Betreibernetzwerk mit Schlüssel-datenbanken verbunden. Die mit dem Authentisierungsserver AS_O des Betreibernetzwerks verbundene Schlüsseldatenbank enthält die nachstehend wiedergegebenen Informationen:

- öffentliche Schlüssel der Authentisierungsserver wie etwa des AS_C der Unternehmensnetzwerke, mit denen das Betreibernetzwerk verbunden werden kann, und
- sowohl den öffentlichen als auch den privaten Schlüssel von AS_O.

[0043] Die mit dem Authentisierungsserver AS_C verbundene Datenbank des Unternehmensnetzwerks enthält die nachstehend wiedergegebenen Informationen:

- den öffentlichen Schlüssel von AS_O, und
- sowohl den öffentlichen als auch den privaten Schlüssel von AS_C.

[0044] Dies garantiert, dass keine vertraulichen Informationen wie etwa private Schlüssel durch das nicht sichere schlichtende Netzwerk übertragen werden müssen. Wie vorstehend in der vorliegenden Anmeldung beschrieben ist, können die öffentlichen Schlüssel ohne Risiko offenbart werden.

[0045] Nachstehend sind Beispiele von erfindungsgemäßen Authentisierungs- und Verschlüsselungsabläufen beschrieben. Der Authentisierungsablauf ist in [Fig. 9](#) gezeigt. Der Ablauf wird durch eine Anfrage für einen eingehenden Datenanruf ausgelöst. Die MSISDN-Nummer des anrufenden Teilnehmers wird an die IDA weitergeleitet. Durch eine Abbildung der MSISDN-Nummer bestätigt die IDA die Identität des Servers, zu dessen Diensten der Teilnehmer Zugang erfragt, sowie die Identität des Authentisierungsservers AS_C des Unternehmensnetzwerks, in dem sich der Server befindet. Diese Informationen werden sodann an den Authentisierungsserver AS_O bei Stufe I1 weitergeleitet.

[0046] In Reaktion auf den Empfang der MSISDN-Nummer des anrufenden Teilnehmers und der Identität des Authentisierungsservers AS_C führt AS_O die nachstehend wiedergegebenen Schritte durch

1. Er erzeugt eine digitale Signatur auf der Grundlage der MSISDN-Nummer mit seinem eigenen privaten Schlüssel (Schritt O01),
2. er verschlüsselt die MSISDN-Nummer und die digitale Signatur unter Verwendung eines Verfahrens bezüglich eines öffentlichen Schlüssels und des in der Schlüsseldatenbank gespeicherten öffentlichen Schlüssels von AS_C (Schritt O02), und
3. er sendet die verschlüsselte MSISDN-Nummer und die Signatur an AS_C (Schritt O03).

[0047] Ein Beispiel für ein zur erfindungsgemäßen Verwendung geeignetes Verschlüsselungsverfahren mit einem öffentlichen Schlüssel ist der gut bekannte RSA-Algorithmus.

[0048] Es sei angemerkt, dass falls die digitale Signatur lediglich auf der Grundlage der MSISDN-Nummer berechnet wird, alle dieselbe MSISDN-Nummer aufweisende Nachrichten identisch sind. Dies ermöglicht eine Nachverfolgung des Verkehrs eines Teilnehmers. Zur Überwindung dieses Problems wird vorgezogen, dass die digitale Signatur nicht nur auf der Grundlage der MSISDN-Nummer berechnet wird, sondern dass die MSISDN-Nummer zusammen mit einer Zufallsnummer signiert wird. Somit sind die denselben Teilnehmer identifizierenden Nachrichten nicht identisch, was eine Nachverfolgung des Teilnehmers unmöglich oder zumindest sehr viel schwieriger macht.

[0049] Der AS_C empfängt die signierte und verschlüsselte Nachricht bei Schritt C01. Bei Schritt C02 entschlüsselt er die Nachricht unter Verwendung seines in seiner Schlüsseldatenbank gespeicherten eigenen privaten Schlüssels. Nachdem somit die Nachricht und die digitale Signatur in Klartext erhalten wurden, verifiziert AS_C bei Schritt P03 die digitale Signatur unter Verwendung des öffentlichen Schlüssels von AS_O, um die Authentizität der Nachricht zu bestätigen.

[0050] Nunmehr hält AS_C die Identifizierung des den Datendienst anfragenden Teilnehmers und bestätigt, dass die Anfrage von einem zuverlässigen Netzwerk, d.h. dem Betreiber Netzwerk, empfangen wurde. Bei Schritt C04 konsultiert AS_C seine Datenbank und überprüft die diesem Teilnehmer beigefügte Zugangserlaubnis, d.h. diese MSISDN-Nummer.

[0051] Falls der Teilnehmer für den Dienst berechtigt ist, wird bei Schritt C05 ein Einmalschlüssel für diese spezielle Sitzung erzeugt. Der Schlüssel wird an den Server gesendet, der ihn bei Schritt S1 empfängt. Um den Einmalschlüssel mit einer sicheren Übertragung über das schlichtende Netzwerk dem Authentisierungsserver AS_O des Betreiber Netzwerks bereitzustellen, wird der Algorithmus für einen öffentlichen Schlüssel zusammen mit einer digitalen

Signatur verwendet. Die digitale Signatur wird unter Verwendung des privaten Schlüssels von AS_C bei Schritt P04 erzeugt. Um es für einen Eindringling noch schwieriger zu machen, den Einmalschlüssel zu erfahren, wird der Einmalschlüssel vorzugsweise zusammen mit einer Zufallszahl signiert. Die Nachricht und die digitale Signatur werden danach unter Verwendung des öffentlichen Schlüssels von AS_O bei Schritt P01 verschlüsselt. Die signierte und verschlüsselte Nachricht wird daraufhin an AS_O über das schlichtende Netzwerk bei Schritt P08 gesendet.

[0052] AS_O empfängt die den Einmalschlüssel enthaltende signierte und verschlüsselte Nachricht bei Schritt O11. Er entschlüsselt die Nachricht unter Verwendung seines eigenen privaten Schlüssels bei Schritt O12. Nach Erhalt des Einmalschlüssels in Klartext und der digitalen Signatur verifiziert AS_O die Signatur unter Verwendung des öffentlichen Schlüssels von AS_C bei Schritt O13.

[0053] Diese Verifikation beweist die Authentizität der Nachricht. Falls die Verifikation zeigt, dass der Einmalschlüssel durch den behaupteten Absender gesendet wurde, d.h. AS_C, leitet AS_O den Einmalschlüssel an die IDA bei Schritt O13 weiter. Die IDA empfängt den Schlüssel bei Schritt I2.

[0054] Es sei angemerkt, dass die Reihenfolge der digitalen Signierung der Nachricht und der Verschlüsselung der Nachricht variieren kann. Gleichfalls sei angemerkt, dass die Signierungsabläufe durch andere Abläufe wie etwa die Verwendung des Nachrichtenauthentizitätscodes ersetzt werden können.

[0055] Der Einmalschlüssel wird dann sowohl von dem den angefragten Datendienst bereitstellenden Server als auch die IDA gehalten. Die tatsächliche Datenübertragung kann nunmehr stattfinden. Die Daten werden über das schlichtende Netzwerk in verschlüsselter Form übertragen. Der Verschlüsselungsablauf ist in [Fig. 10](#) gezeigt.

[0056] Bei der Datenverbindung werden die Daten zunächst von der Mobilstation des Teilnehmers an ein Mobilvermittlungszentrum MSC unter Verwendung des GSM-Dienstes und seiner Datensicherheitsfunktionen gesendet. Das MSC leitet die durch die Mobilstation gesendeten Daten DATA1 an die IDA weiter. Die IDA empfängt die Daten und verschlüsselt sie unter Verwendung eines symmetrischen Verschlüsselungsverfahrens und des von dem AS_O empfangenen Einmalschlüssels KEY. Ein Beispiel für einen zur Verwendung geeigneten symmetrischen Verschlüsselungsalgorithmus ist der gut bekannte DES-Algorithmus. Die verschlüsselte Nachricht E1 wird an den Server über das schlichtende Netzwerk gesendet.

[0057] Der Server empfängt die verschlüsselte

Nachricht und erhält die gesendeten Daten DATA1 bei Entschlüsseln der verschlüsselten Nachricht E1 unter Verwendung des Einmalschlüssels KEY, den er von AS_C während des Authentisierungsablaufs bei Schritt S1 gemäß [Fig. 9](#) empfangen hat. Die erhaltenen Daten werden an die Serveranwendung weitergeleitet.

[0058] Wenn die Serveranwendung Daten DATA2 an den Teilnehmer sendet, verschlüsselt der auf dem Server laufende Verschlüsselungsalgorithmus die Daten unter Verwendung des Einmalschlüssels KEY. Die verschlüsselte Datennachricht wird sodann an die IDA im Betreiber Netzwerk gesendet.

[0059] Die IDA des Betreiber Netzwerks empfängt die Nachricht und entschlüsselt sie unter Verwendung des Einmalschlüssels. Mit der dann in Klartext vorliegenden Nachricht sendet die IDA sie an den Teilnehmer über das Mobilvermittlungszentrum.

[0060] Der Vorgang der weitergeleiteten Authentisierung ist in [Fig. 11](#) gezeigt. Der Teilstrecke zwischen dem Mobilteilnehmer MS und dem Mobilvermittlungszentrum MSC wird mittels des GSM-Authentisierungsablaufs authentisiert. Mit der Hilfe dieses Ablaufs kann das Mobilvermittlungszentrum bestätigen, dass die durch den Mobilteilnehmer bereitgestellten Identifizierungsinformationen korrekt sind, d.h. eine wahrheitsgemäß eigene MSISDN-Nummer. AS_O ist mit dem MSG über das zuverlässige private Datennetzwerk des Betreibers verbunden. Daher kann AS_O sicherstellen, dass der Teilnehmer tatsächlich sich selbst korrekt identifiziert.

[0061] Zum Aufbau einer Verbindung zum Server sendet AS_O an AS_C die MSISDN-Nummer über das schlichtende Netzwerk in verschlüsselter und signierter Form. Die Verschlüsselung stellt sicher, dass die Nachricht lediglich durch den gewünschten Empfänger gelesen werden kann, d.h. das zuverlässige Netzwerkelement AS_C des Unternehmensnetzwerks. Die Signatur authentisiert AS_O gegenüber AS_C. In Reaktion auf eine erfolgreiche Verifikation der Signatur der Nachricht bestätigt AS_C somit, dass die Nachricht von einem zuverlässigen Netzwerkelement AS_O stammt. Daher kann auch der Identität des den Dienst anfordernden Teilnehmers vertraut werden. Somit wird der Mobilteilnehmer gegenüber AS_C authentisiert. Sowohl AS_C als auch der Server befinden sich in demselben Unternehmensnetzwerk, und die Netzwerkelemente innerhalb des Unternehmensnetzwerks vertrauen einander. Daher kann auch dem Server versichert werden, dass der Teilnehmer seine wahre Identität offenbart.

[0062] Das bevorzugte Ausführungsbeispiel der Erfindung stellt eine Authentisierung von AS_C des Unternehmensnetzwerks gegenüber AS_O des Betreiber Netzwerks bereit. Dies wird unter Verwendung

des Verschlüsselungsverfahrens eines öffentlichen Schlüssels erzielt, wenn die Nachricht mit Informationen über die Teilnehmeridentität von AS_O zu AS_C gesendet werden. Eine zusätzliche oder alternative Authentizität wird mittels der digitalen Signatur der Nachricht mit dem Einmalschlüssel verifiziert und von AS_C zu AS_O gesendet. Falls das Betreiber Netzwerk gegenüber der MS authentisiert ist, wird die Authentizität von AS_C auch an den Teilnehmer weitergeleitet. Dies bedeutet, dass das Unternehmensnetzwerk über die Identität des Teilnehmers sicher sein kann, und der Teilnehmer über die Identität des Unternehmensnetzwerks sicher sein kann.

[0063] Die Basis für die Sicherheit der Datenübertragung kann unter Bezugnahme auf [Fig. 12](#) verstanden werden. Auf der Teilstrecke zwischen der Mobilstation MS und der Basisstation BTS wird ein Verschlüsselungsverfahren gemäß den GSM-Spezifikationen verwendet. Von der BTS zu der IDA ist der Übertragungspfad zuverlässig. Auf der Teilstrecke von der IDA über das schlichtende Netzwerk zum Server wird das symmetrische Verschlüsselungsverfahren verwendet. Die Verschlüsselungskette ist in beide Übertragungsrichtungen ähnlich, d.h. von der MS zum Server und umgekehrt. Somit ist die komplette Verbindung zwischen der Mobilstation und dem Server sicher.

[0064] Die bei den Authentisierungsservern benötigten Funktionalitäten sind in den [Fig. 13](#) und [Fig. 14](#) dargestellt. [Fig. 13](#) zeigt die Funktionalitäten des Authentisierungszentrums AS_O im Betreiber Netzwerk. Der Server umfasst:

- eine Empfangseinrichtung für den Empfang einer Teilnehmeridentität von dem Telekommunikationsnetzwerk,
- eine Bestimmungseinrichtung, die zur Bestimmung der Identität einer zweiten Authentisierungsservereinrichtung auf der Grundlage der Identität des Teilnehmers auf die Empfangseinrichtung anspricht,
- eine Signierungseinrichtung, die zur Erzeugung einer digitalen Signatur auf die Empfangseinrichtung anspricht, und
- eine Sendeeinrichtung, die auf die Empfangseinrichtung, die Bestimmungseinrichtung und die Signierungseinrichtung anspricht, und die die Identität und die Signatur an die Authentisierungsservereinrichtung des Unternehmensnetzwerks sendet.

[0065] Die Abbildungseinrichtung und die Signierungseinrichtung benötigen Informationen über die Dienste des Teilnehmers und den privaten Schlüssel des Servers, die in der Datenbank DB gefunden werden können.

[0066] Gemäß dem bevorzugten Ausführungsbeispiel wird zur Verschlüsselung der Teilnehmeridenti-

tät vor der Versendung über das schlichtende Netzwerk außerdem eine auf die Signierungseinrichtung ansprechende Verschlüsselungseinrichtung benötigt. Es muss angemerkt werden, dass die Reihenfolge von Signierung und Verschlüsselung variieren kann. Die Verschlüsselungseinrichtung erfordert den öffentlichen Schlüssel des Authentisierungsservers des Unternehmensnetzwerks und ist daher mit der Datenbank DB verbunden.

[0067] Damit der Einmalschlüssel von dem anderen Authentisierungsserver empfangen werden kann, weist der Authentisierungsserver außerdem eine zweite Empfangseinrichtung zum Empfang eines verschlüsselten Einmalschlüssels von dem Authentisierungsserver des Unternehmensnetzwerks sowie eine auf die zweite Empfangseinrichtung ansprechende Entschlüsselungseinrichtung zum Entschlüsseln des verschlüsselten Einmalschlüssels auf. Falls der Authentisierungsserver des Unternehmensnetzwerks die Einmalschlüssel gemäß dem bevorzugten Ausführungsbeispiel signiert, muss der Authentisierungsserver des Betreibernetzwerks zusätzlich eine auf die zweite Empfangseinrichtung ansprechende Verifikationseinrichtung zum Verifizieren der aus dem Einmalschlüssel berechneten digitalen Signatur aufweisen.

[0068] Die bei dem Authentisierungsserver des Unternehmensnetzwerks benötigten Einrichtungen sind in [Fig. 14](#) gezeigt. Der Authentisierungsserver umfasst:

- eine Empfangseinrichtung für den Empfang einer Teilnehmeridentität und einer aus der Teilnehmeridentität und der Identifikation eines von dem Teilnehmer angefragten Dienstes berechneten digitalen Signatur von dem Authentisierungsserver des Betreibernetzwerks,
- eine Verifikationseinrichtung, die zum Verifizieren der digitalen Signatur auf die Empfangseinrichtung anspricht,
- eine Prüfeinrichtung, die zum Überprüfen, ob der Teilnehmer zu dem angefragten Dienst berechtigt ist, auf die Empfangseinrichtung anspricht,
- eine Erzeugungseinrichtung, die zum Erzeugen eines Einmalschlüssels auf die Prüfeinrichtung anspricht,
- eine Verschlüsselungseinrichtung, die zum Verschlüsseln des Einmalschlüssels auf die Erzeugungseinrichtung anspricht, und
- eine Sendeeinrichtung, die zum Senden der verschlüsselten Nachricht an einen anderen Authentisierungsserver auf die Verschlüsselungseinrichtung anspricht.

[0069] Falls die Teilnehmeridentität verschlüsselt wird, bevor sie an das Unternehmensnetzwerk gesendet wird, weist der Authentisierungsserver zusätzlich eine auf die Empfangseinrichtung ansprechende Einrichtung zum Entschlüsseln der Teilneh-

meridentität unter Verwendung des privaten Schlüssels des Authentisierungsservers auf. Falls zudem der Authentisierungsserver des Unternehmensnetzwerks den Einmalschlüssel signiert, bevor er diesen an den Authentisierungsserver des Betreibernetzwerks sendet, muss der Authentisierungsserver zudem eine auf die Erzeugungseinrichtung ansprechende Signierungseinrichtung zum Signieren des Einmalschlüssels unter Verwendung des privaten Schlüssels des Authentisierungsservers aufweisen.

[0070] Es sei angemerkt, dass der Bereich der Erfindung nicht auf die vorstehend beschriebenen beispielhaften Ausführungsbeispiele beschränkt ist. Beispielsweise kann eine andere Identifizierung als eine MSISDN-Nummer verwendet werden, wenn das Unternehmensnetzwerk kontaktiert wird. Das Wort „Unternehmensnetzwerk“ wird lediglich zur Klarstellung verwendet, da es ein beliebiges privates Netzwerk sein kann, nicht notwendiger Weise ein geschlossenes Datennetzwerk eines Unternehmens. Es kann ebenso ein durch einen Netzbetreiber betriebenes privates Netzwerk sein, das beispielsweise eine Benutzerauthentisierung erfordert. Dies kann durch Bestimmen der bei dem Unternehmensnetzwerk auf der Basis der MSISDN-Nummer des Teilnehmers verwendeten Identifizierung implementiert sein. Die Abbildung kann beispielsweise im AS_O erfolgen. Die Reihenfolge der Signaturerzeugung und Verschlüsselung kann von der in den Beispielen verwendeten Reihenfolge verschieden sein. Genauer können die Nachrichten zunächst verschlüsselt und dann signiert werden.

[0071] Bei den Beispielen für die vorliegende Anmeldung sind der Authentisierungsserver, die IDA und die LAN-Zugangseinheit als getrennte Netzwerkelemente beschrieben. Dies ist jedoch nicht erfindungswesentlich, und eine Vielzahl dieser Funktionalitäten kann in einem einzelnen Netzwerkelement implementiert sein. Außerdem kann eine Funktionalität über eine Vielzahl von Netzwerkelementen verteilt sein. Gleichfalls kann die Signatur im Klartext gesendet sein. Bei diesem Ausführungsbeispiel wird die Nachricht verschlüsselt und die Signatur der verschlüsselten Nachricht ohne Verschlüsselung angefügt.

[0072] Es ist außerdem ersichtlich, dass eine Verwendung der Erfindung nicht auf ein GSM-System als bei den Beispielen der vorliegenden Anmeldung verwendetes System beschränkt ist, sondern dass die Erfindung mit einem beliebigen Telekommunikationssystem verwendet werden kann, bei dem Teilnehmer sicher authentisiert werden, und das mit einem privaten Netzwerk verbunden ist. Ein Beispiel für ein derartiges Telefonsystem ist das Festnetztelefonsystem. Ein anderes Beispiel eines Mobiltelekommunikationssystems ist das GPRS (General Packet Radio System – Allgemeines Paketfunksystem).

Patentansprüche

1. Verfahren zur Bereitstellung der Sicherheit von Datenverbindungen bei einer Anordnung mit einem Telekommunikationsnetzwerk mit Teilnehmern, einem ersten privaten Datennetzwerk, das mit dem Telekommunikationsnetzwerk verbunden ist, einem zweiten privaten Datennetzwerk mit einer Datendienst bereitstellenden Servereinrichtung, wobei der Teilnehmer bei dem Verfahren für das erste private Datennetzwerk unter Verwendung eines Authentisierungsverfahrens des Telekommunikationsnetzwerks authentisiert ist,

dadurch gekennzeichnet, dass zusätzlich zu der Identifikation des Teilnehmers ein Authentizitätscode in dem ersten privaten Datennetzwerk hinzugefügt wird, und eine Nachricht mit der Teilnehmeridentität und dem Authentizitätscode an das zweite private Datennetzwerk gesendet wird, und in Reaktion auf den Empfang der Nachricht in dem zweiten privaten Datennetzwerk der Authentizitätscode verifiziert wird, die identifizierten Benutzerrechte an dem angefragten Dienst geprüft werden, und falls der Benutzer für den angefragten Dienst berechtigt ist, eine Antwort erzeugt und an das erste private Datennetzwerk gesendet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Telekommunikationsnetzwerk ein Mobiltelekommunikationsnetzwerk ist.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Teilnehmeridentifikation die Telefonnummer wie etwa die MSISDN-Nummer des Teilnehmers ist.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Authentizitätscode ein Nachrichtenauthentizitätscode MAC ist.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Authentizitätscode eine digitale Signatur ist.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass die Identifikation des Teilnehmers bei einer in dem ersten privaten Datennetzwerk installierten Authentisierungsservereinrichtung digital signiert wird.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass die Identifikation unter Verwendung des privaten Schlüssels der Authentisierungsservereinrichtung digital signiert wird.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass der Schlüssel in einer an der Authentisierungsservereinrichtung angebrachten Schlüsseldatenbank gespeichert wird.

9. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass zudem die Teilnehmeridentität unter Verwendung eines Verschlüsselungsverfahrens für einen öffentlichen Schlüssel verschlüsselt wird, bevor sie von dem ersten privaten Datennetzwerk an das zweite private Datennetzwerk gesendet wird.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass die Teilnehmeridentität in einer in dem ersten privaten Datennetzwerk installierten Authentisierungsservereinrichtung verschlüsselt wird.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass eine Authentisierungsservereinrichtung in dem zweiten privaten Datennetzwerk installiert wird, und die Identifikation unter Verwendung des öffentlichen Schlüssels der Authentisierungsservereinrichtung des zweiten privaten Datennetzwerks verschlüsselt wird.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass der Schlüssel in einer an der Authentisierungsservereinrichtung des ersten privaten Netzwerks angebrachten Schlüsseldatenbank gespeichert wird.

13. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eine Authentisierungsservereinrichtung in dem zweiten privaten Datennetzwerk installiert ist, und der Authentizitätscode verifiziert wird, die Benutzerrechte an dem angefragten Dienst geprüft werden, und eine Antwort in der Authentisierungsservereinrichtung erzeugt wird.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass eine Authentisierungsservereinrichtung in dem ersten privaten Datennetzwerk installiert wird, und der Authentizitätscode mittels des öffentlichen Schlüssels der Authentisierungsservereinrichtung des ersten privaten Datennetzwerks verifiziert wird.

15. Verfahren nach Anspruch 14, dadurch gekennzeichnet, dass der öffentliche Schlüssel der Authentisierungsservereinrichtung des ersten privaten Datennetzwerks in einer an die Authentisierungsservereinrichtung des zweiten privaten Datennetzwerks angebrachte Schlüsseldatenbank gespeichert wird.

16. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Antwort einen zur Verschlüsselung des Datenverkehrs auf der Teilstrecke zwischen dem ersten und dem zweiten privaten Datennetzwerk in einer zwischen dem Teilnehmer und der Servereinrichtung aufzubauenden Verbindung zu verwendenden Einmalschlüssel umfasst.

17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass die den Einmalschlüssel umfassende Antwort in dem zweiten privaten Datennetzwerk digital signiert wird.

18. Verfahren nach Anspruch 17, dadurch gekennzeichnet, dass eine Authentisierungsservereinrichtung in dem zweiten privaten Datennetzwerk installiert wird, und die den Einmalschlüssel aufweisende Antwort unter Verwendung des privaten Schlüssels der Authentisierungsservereinrichtung signiert wird.

19. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass eine Authentisierungsservereinrichtung in dem ersten privaten Datennetzwerk installiert wird, und die den Einmalschlüssel aufweisende Antwort unter Verwendung eines öffentlichen Schlüssels der Authentisierungsservereinrichtung des ersten privaten Datennetzwerks verschlüsselt wird.

20. Verfahren nach Anspruch 19, dadurch gekennzeichnet, dass eine Authentisierungsservereinrichtung in dem zweiten privaten Datennetzwerk installiert wird, und die den Einmalschlüssel aufweisende Antwort in der Authentisierungsservereinrichtung des zweiten privaten Datennetzwerks verschlüsselt wird.

21. Authentisierungsservereinrichtung für ein mit einem Telekommunikationsnetzwerk verbundenes Datennetzwerk, dadurch gekennzeichnet, dass die Authentisierungsservereinrichtung versehen ist mit einer Empfangseinrichtung für den Empfang einer Teilnehmeridentität von dem Telekommunikationsnetzwerk, einer Bestimmungseinrichtung, die zur Bestimmung der Identität einer zweiten Authentisierungsservereinrichtung auf der Grundlage der Identität des Teilnehmers auf die Empfangseinrichtung anspricht, einer Signierungseinrichtung, die zur Erzeugung einer digitalen Signatur auf die Empfangseinrichtung anspricht, und einer Sendeeinrichtung, die auf die Empfangseinrichtung, die Bestimmungseinrichtung und die Signierungseinrichtung anspricht, und die die Identität und die Signatur an die zweite Authentisierungsservereinrichtung sendet.

22. Authentisierungsservereinrichtung nach Anspruch 21, dadurch gekennzeichnet, dass die Authentisierungsservereinrichtung zudem eine zum Verschlüsseln der Identität unter Verwendung des öffentlichen Schlüssels der zweiten Authentisierungsservereinrichtung auf die Empfangseinrichtung und eine Abbildungseinrichtung ansprechende Verschlüsselungseinrichtung aufweist.

23. Authentisierungsservereinrichtung nach Anspruch 21, dadurch gekennzeichnet, dass die Au-

thentisierungsservereinrichtung zudem versehen ist mit einer zweiten Empfangseinrichtung für den Empfang eines verschlüsselten Einmalschlüssels von der zweiten Authentisierungsservereinrichtung, und einer Entschlüsselungseinrichtung, die zum Entschlüsseln des verschlüsselten Einmalschlüssels auf die zweite Empfangseinrichtung anspricht.

24. Authentisierungsservereinrichtung nach Anspruch 23, dadurch gekennzeichnet, dass die Authentisierungsservereinrichtung zudem eine zum Verifizieren einer auf der Grundlage des Einmalschlüssels berechneten digitalen Signatur auf die zweite Empfangseinrichtung ansprechende Verifikationseinrichtung aufweist.

25. Authentisierungsservereinrichtung für ein Datennetzwerk, dadurch gekennzeichnet, dass die Authentisierungsservereinrichtung versehen ist mit einer Empfangseinrichtung für den Empfang einer Teilnehmeridentität und einer aus der Teilnehmeridentität und der Identifikation eines von dem Teilnehmer angefragten Dienstes berechneten digitalen Signatur, einer Verifikationseinrichtung, die zum Verifizieren der digitalen Signatur auf die Empfangseinrichtung anspricht, einer Prüfeinrichtung, die zum Überprüfen der Rechte des Teilnehmers an dem angefragten Dienst auf die Empfangseinrichtung anspricht, einer Erzeugungseinrichtung, die zum Erzeugen eines Einmalschlüssels auf die Prüfeinrichtung anspricht, einer Verschlüsselungseinrichtung, die zum Verschlüsseln des Einmalschlüssels auf die Erzeugungseinrichtung anspricht, und einer Sendeeinrichtung, die zum Senden des verschlüsselten Einmalschlüssels an eine andere Authentisierungsservereinrichtung auf die Verschlüsselungseinrichtung anspricht.

26. Authentisierungsservereinrichtung nach Anspruch 25, dadurch gekennzeichnet, dass die Authentisierungsservereinrichtung zudem eine zum Entschlüsseln der Teilnehmeridentität unter Verwendung des privaten Schlüssels der Authentisierungsservereinrichtung auf die Empfangseinrichtung ansprechende Einrichtung aufweist.

27. Authentisierungsservereinrichtung nach Anspruch 25, dadurch gekennzeichnet, dass die Authentisierungsservereinrichtung zudem eine zum Signieren des Einmalschlüssels unter Verwendung des privaten Schlüssels der Authentisierungsservereinrichtung auf die Erzeugungseinrichtung ansprechende Signierungseinrichtung aufweist.

Es folgen 11 Blatt Zeichnungen

Anhängende Zeichnungen

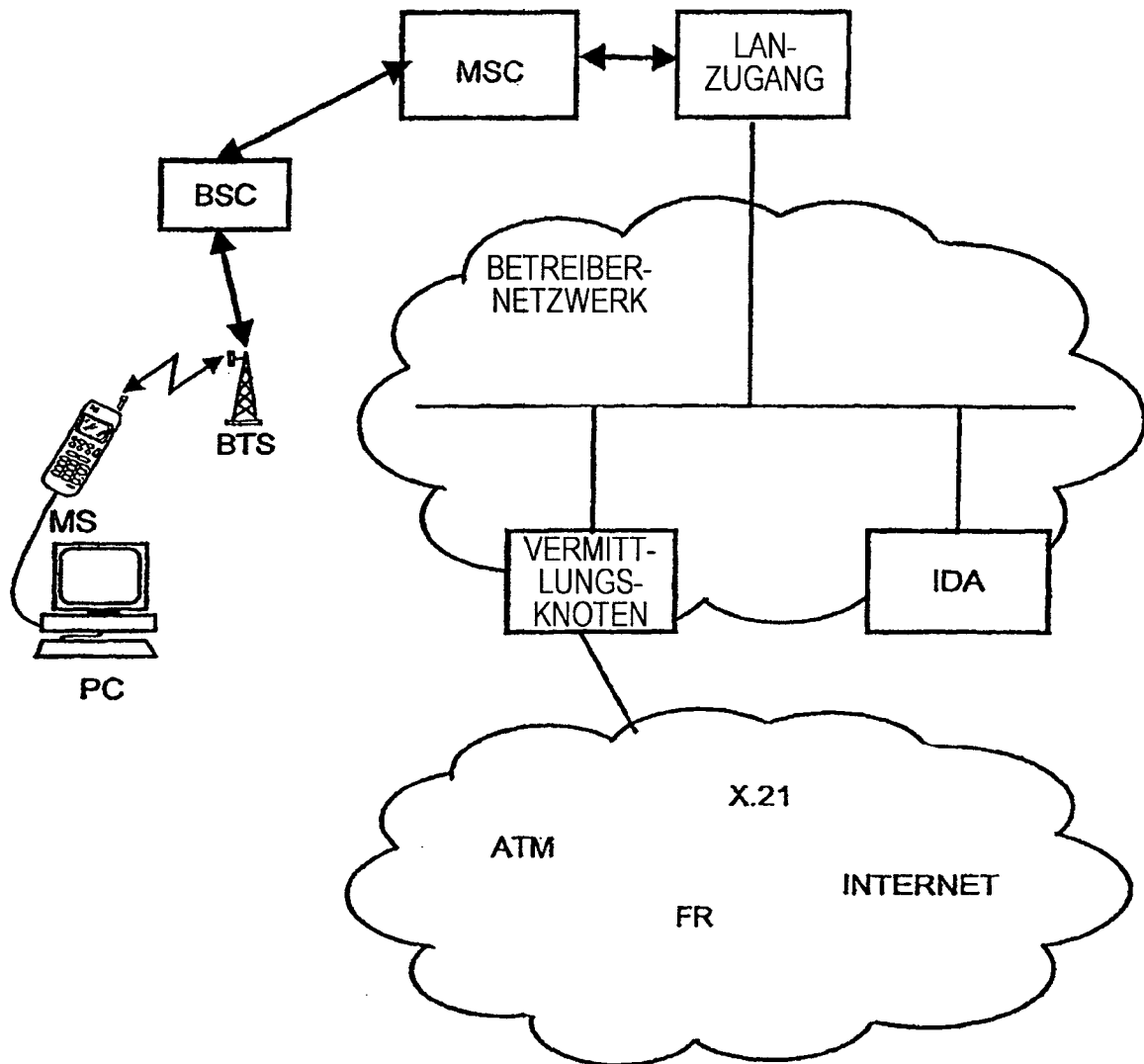


FIG. 1.

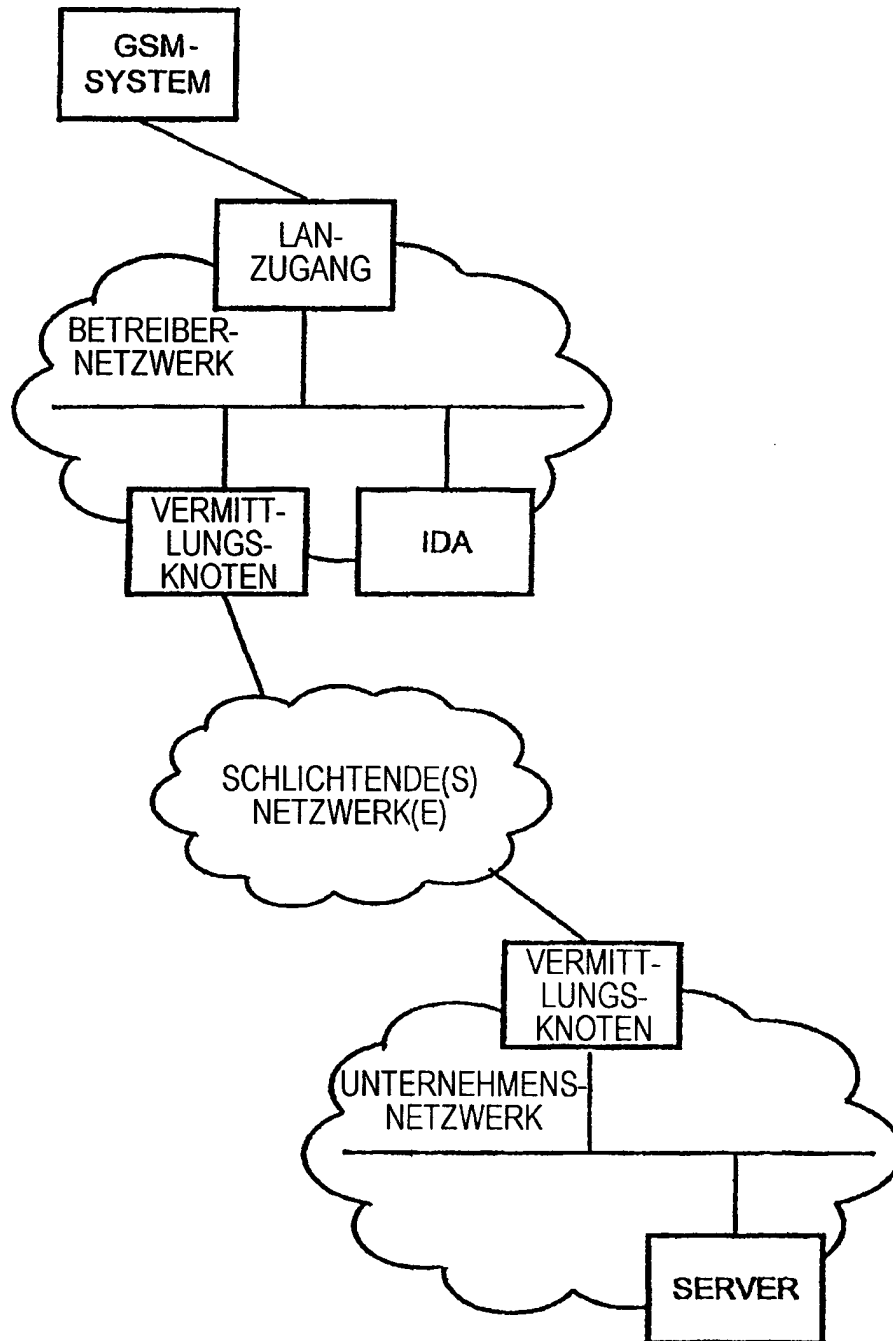


FIG. 2.

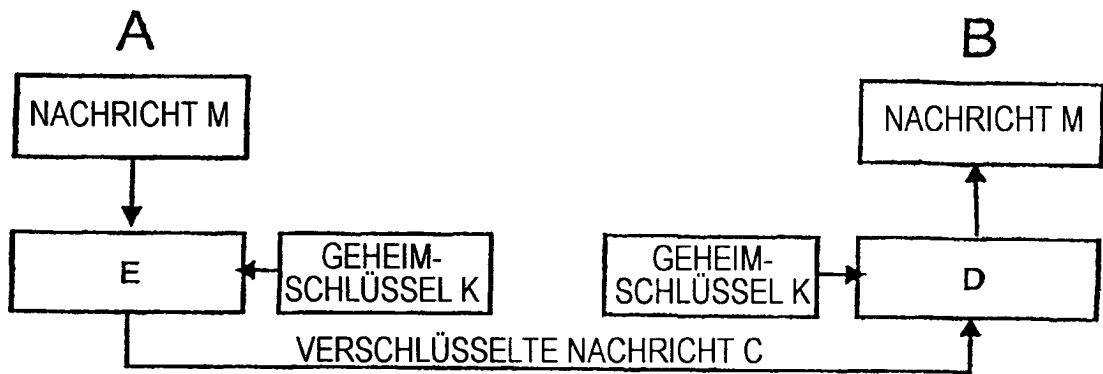


FIG. 3.

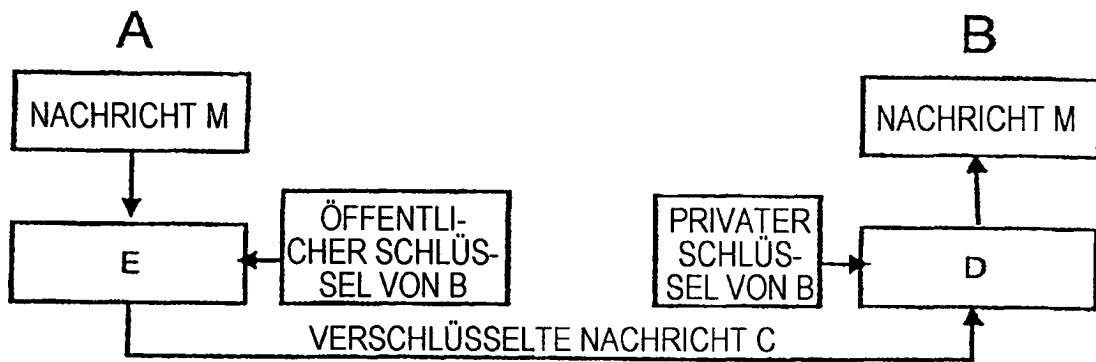


FIG. 4.

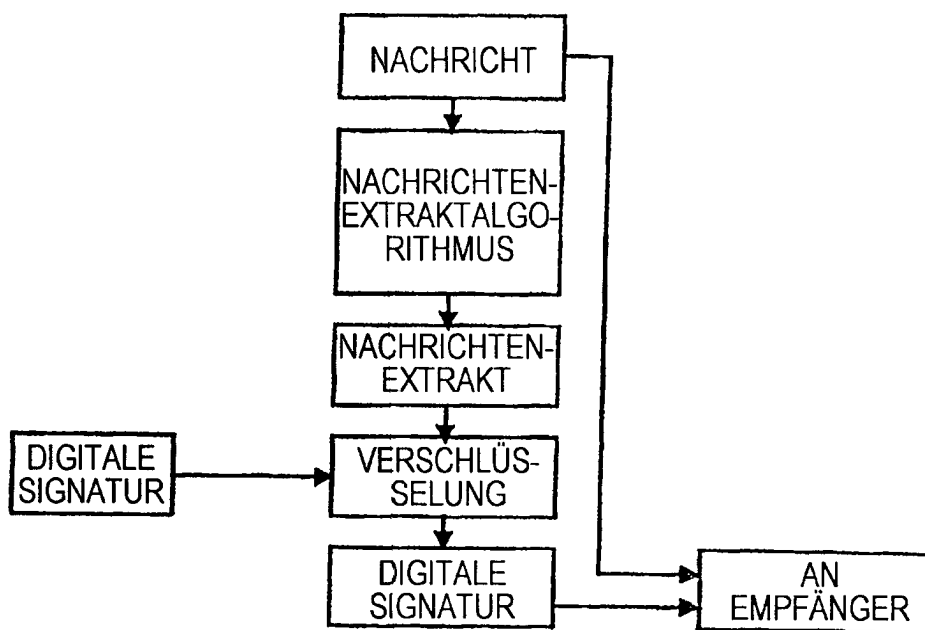


FIG. 5.

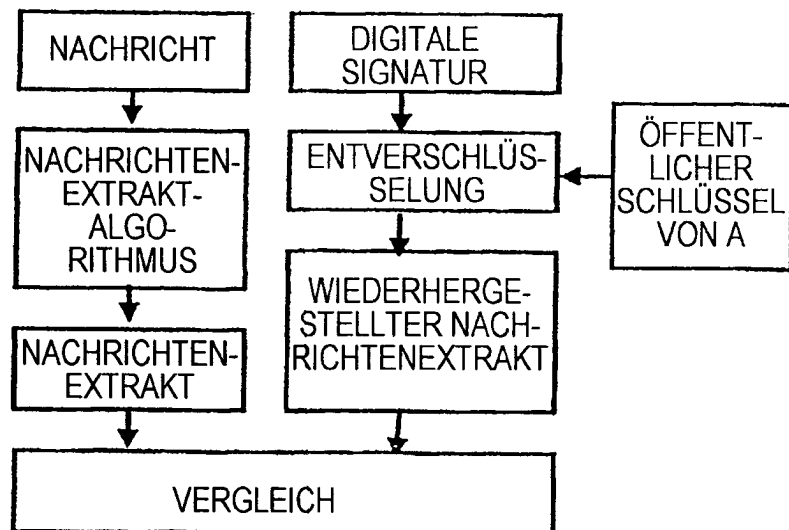


FIG. 6.

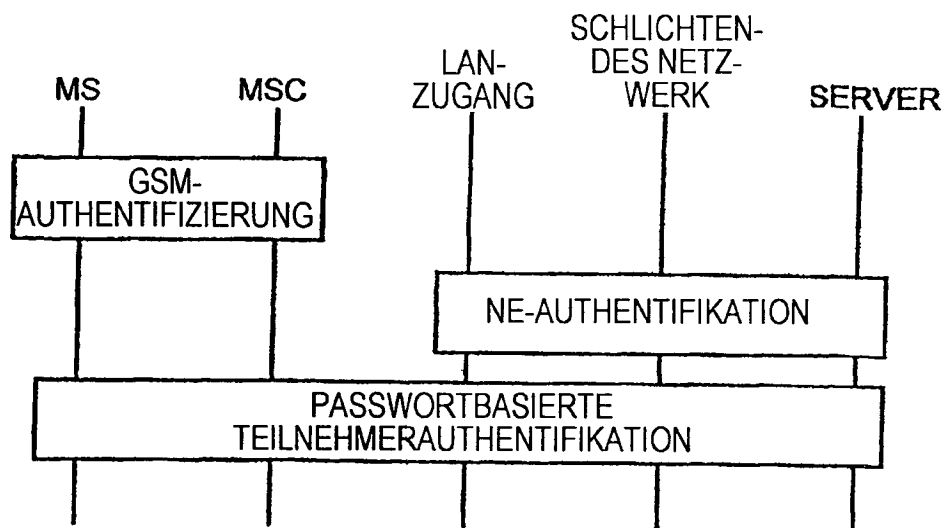


FIG. 7.

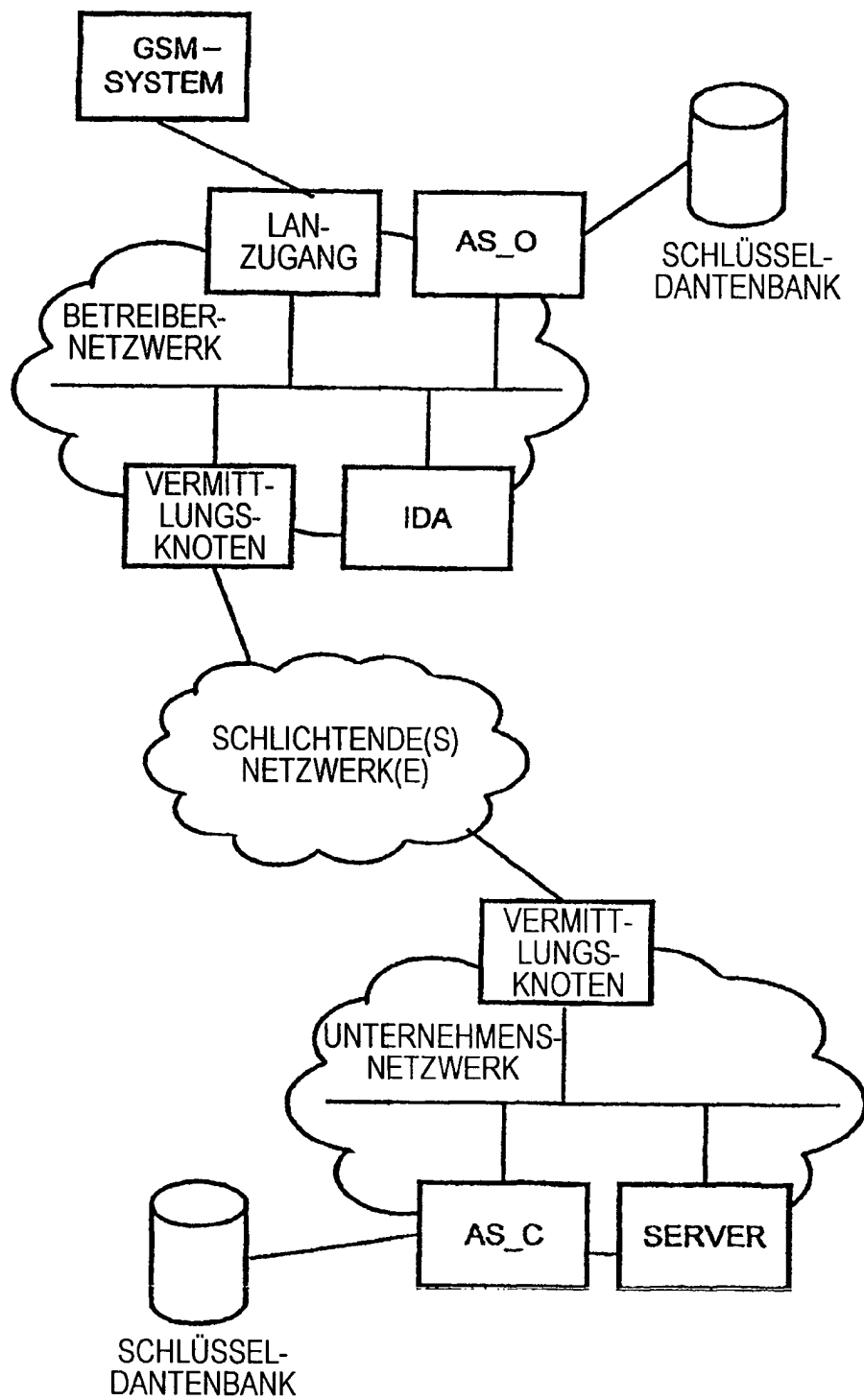


FIG. 8.

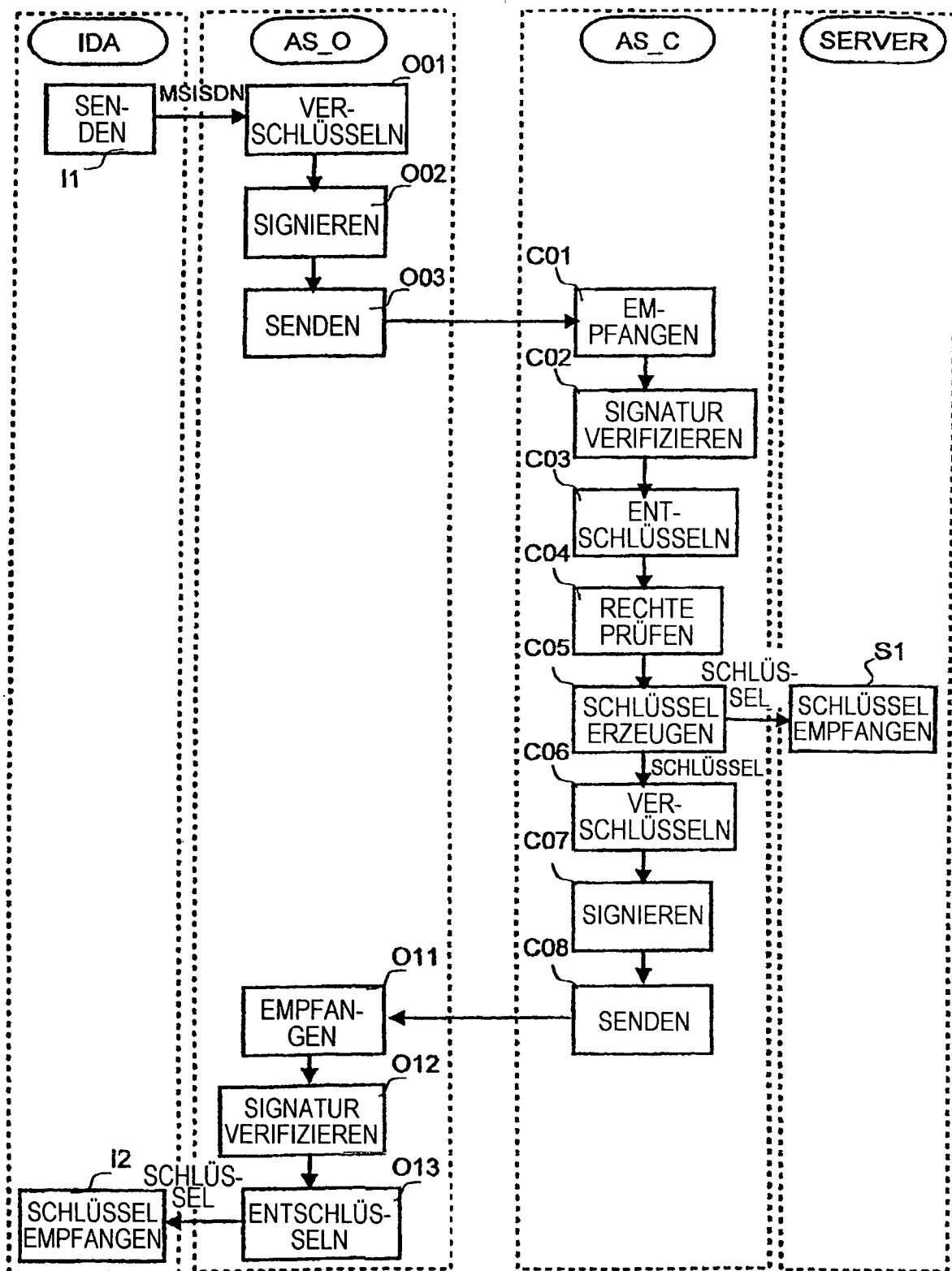


FIG. 9.

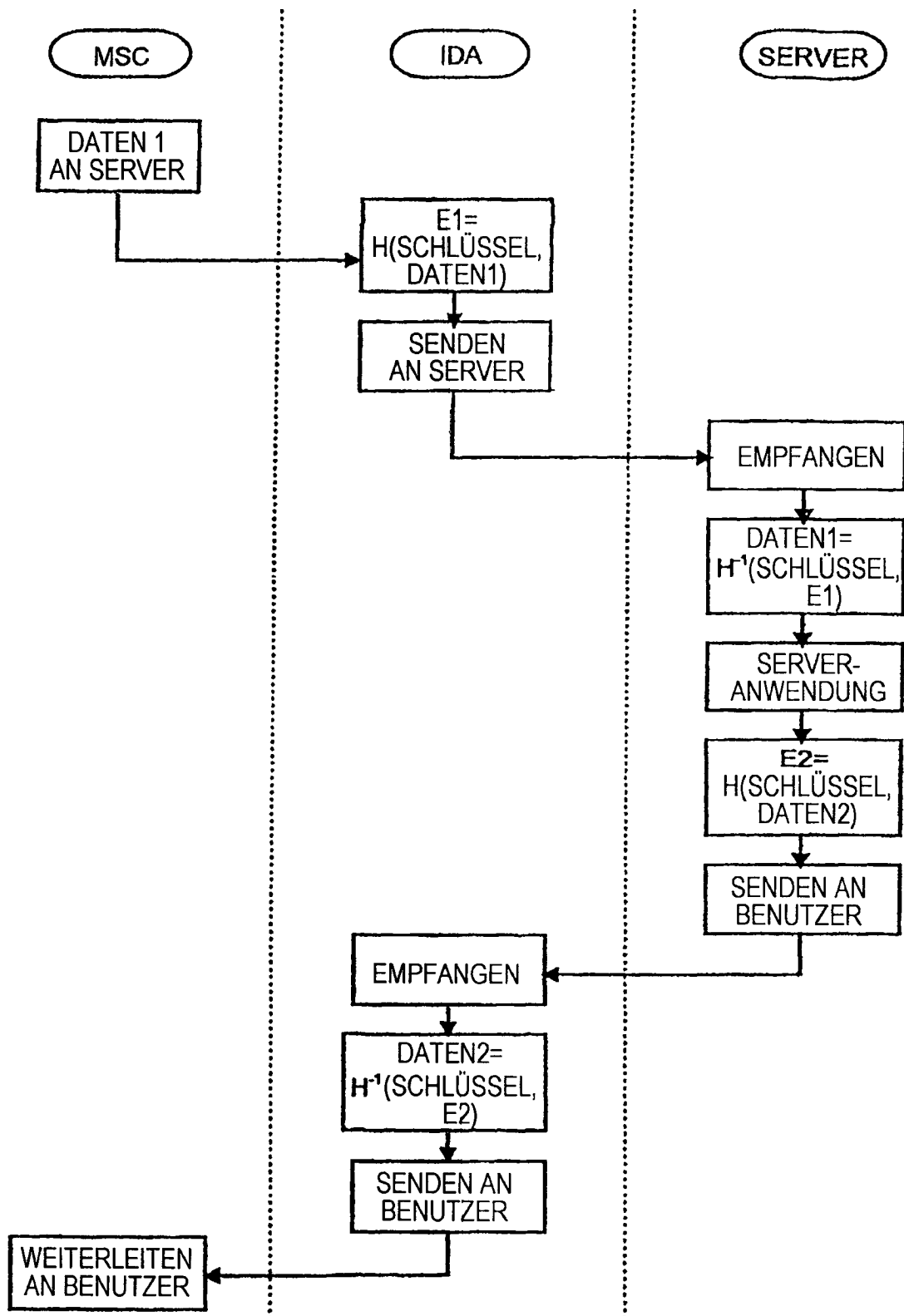


FIG. 10.

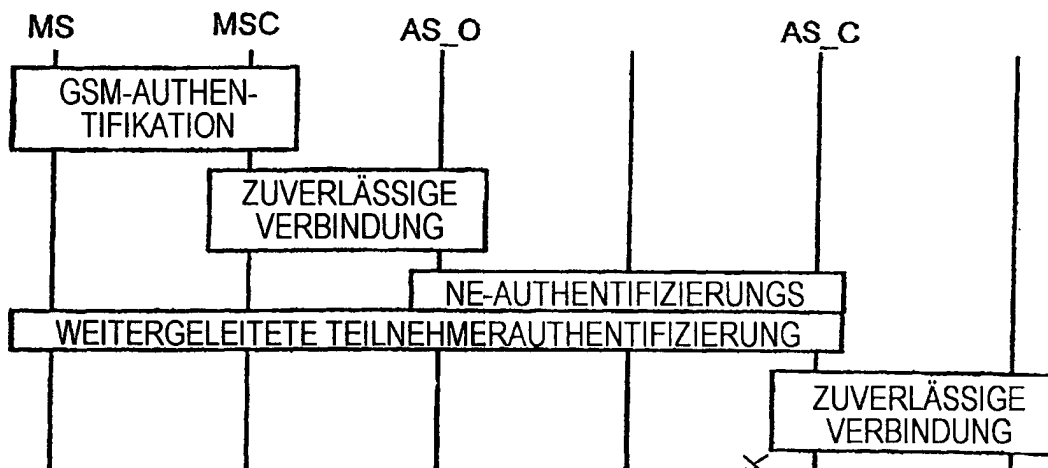


FIG. 11.

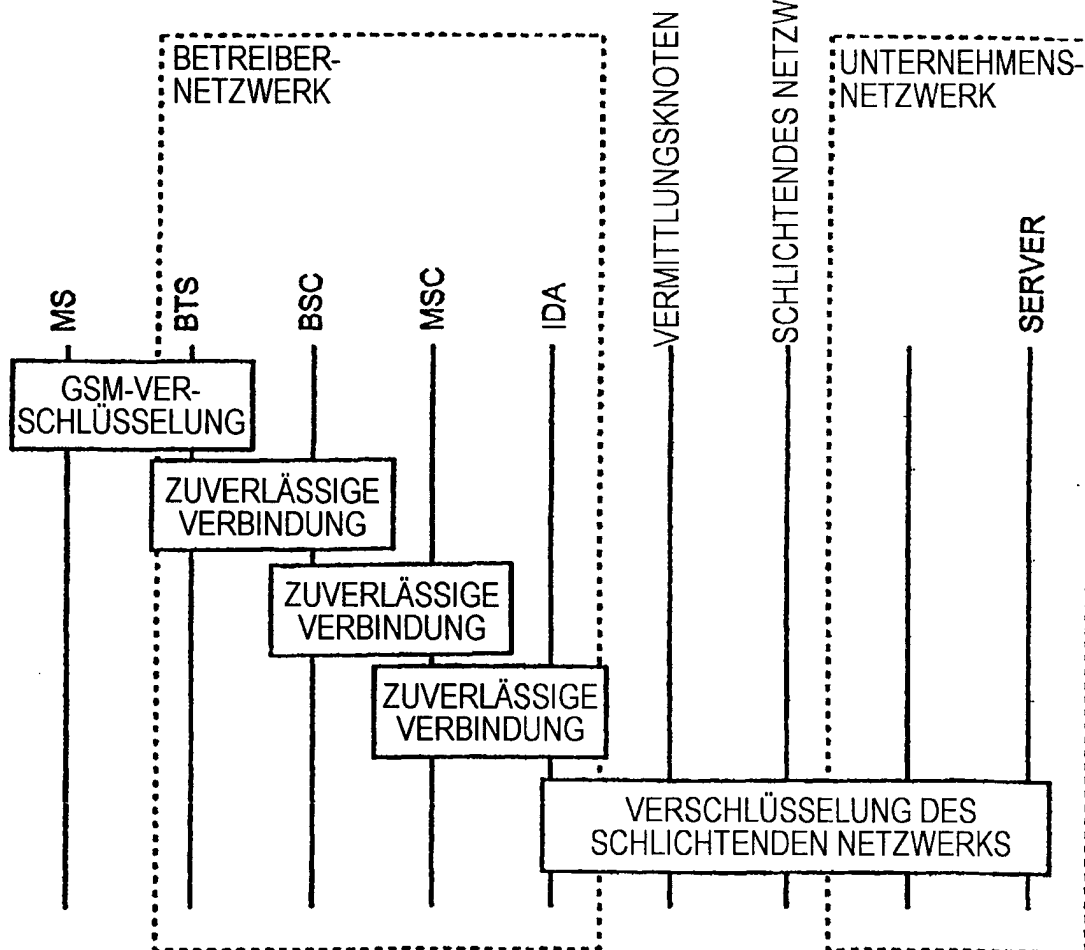


FIG. 12.

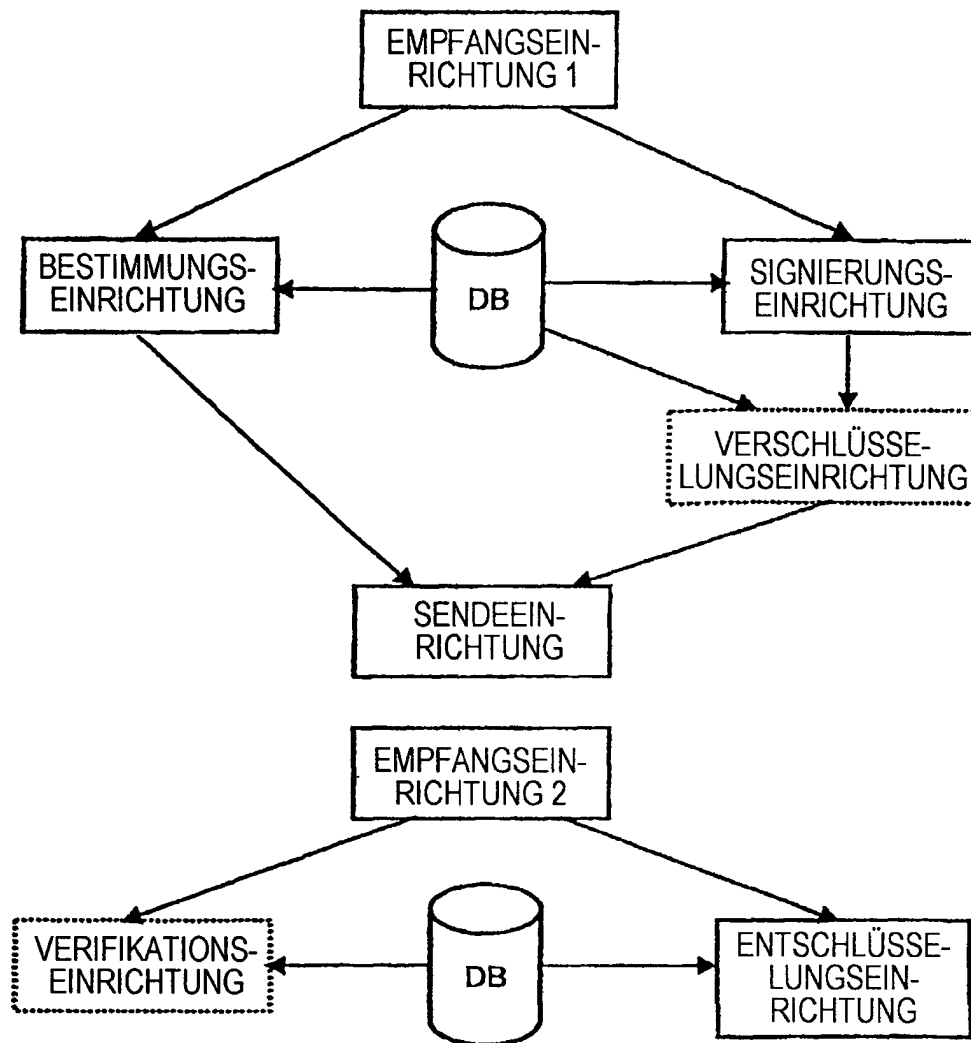


FIG. 13.

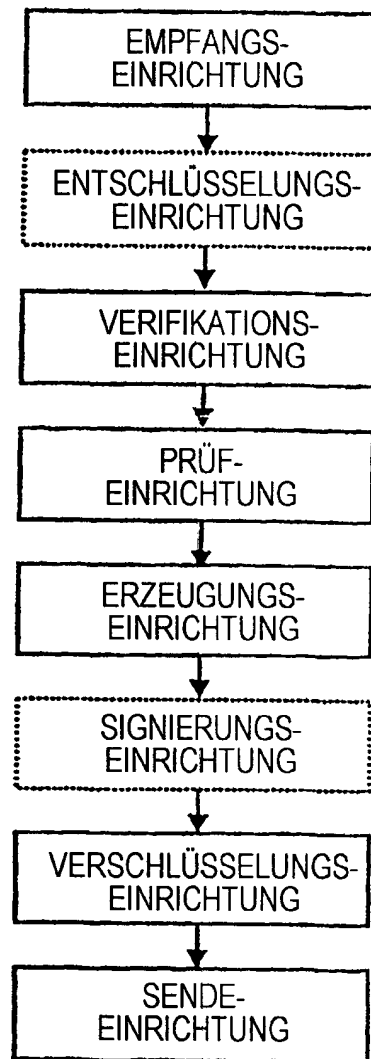


FIG. 14.